**TCVN** **T I Ê U C H U Ẩ N Q U Ố C G I A**

**TCVN xxxx:2024**

**Xuất bản lần 1**

**CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - CÁC YÊU CẦU BẢO ĐẢM AN TOÀN THÔNG TIN TRONG HỆ THỐNG ĐIỀU KHIỂN CÔNG NGHIỆP**

***Information technology - Security techniques –***

***Requirements to ensure information security in industrial control systems***

**HÀ NỘI - 2024**

Mục lục

[Mục lục 2](#_Toc153974467)

[1 Phạm vi áp dụng 7](#_Toc153974468)

[2 Tài liệu viện dẫn 7](#_Toc153974469)

[3 Thuật ngữ và định nghĩa 7](#_Toc153974470)

[4 Ký hiệu và thuật ngữ viết tắt 7](#_Toc153974471)

[5 Các yêu cầu bảo đảm an toàn thông tin trong hệ thống điều khiển công nghiệp 9](#_Toc153974472)

[5.1 Tổng quan về hệ thống điều khiển công nghiệp 9](#_Toc153974473)

[5.1.1 Sự phát triển của các hệ thống điều khiển công nghiệp 10](#_Toc153974474)

[5.1.2 Các lĩnh vực công nghiệp của ISC và sự tương thuộc lẫn nhau 10](#_Toc153974475)

[5.1.2.1 Công nghiệp sản xuất 10](#_Toc153974476)

[5.1.2.2 Công nghiệp phân bố 11](#_Toc153974477)

[5.1.3 Sự hoạt động và các thành phần của ICS 12](#_Toc153974478)

[5.1.3.1 Sự cân nhắc thiết kế hệ thống ICS 13](#_Toc153974479)

[5.1.3.2 Hệ thống SCADA 14](#_Toc153974480)

[5.1.3.3 Hệ thống điều khiển phân tán 20](#_Toc153974481)

[5.1.3.4 Cấu trúc liên kết dựa trên bộ điều khiển logic có thể lập trình 22](#_Toc153974482)

[5.1.4 So sánh ICS và hệ thống bảo mật công nghệ thông tin 23](#_Toc153974483)

[5.1.5 Các loại hệ thống điều khiển khác 28](#_Toc153974484)

[5.2 Đánh giá và quản lý rủi ro cho các hệ thống điều khiển công nghiệp ICS 30](#_Toc153974485)

[5.2.1 Quản lý rủi ro 30](#_Toc153974486)

[5.2.2 Giới thiệu về quy trình quản lý rủi ro 30](#_Toc153974487)

[5.2.3 Cân nhắc đặc biệt khi thực hiện đánh giá rủi ro 32](#_Toc153974488)

[5.2.4 An toàn trong đánh giá rủi ro bảo mật thông tin ICS 32](#_Toc153974489)

[5.2.5 Tác động vật lý tiềm tàng của một sự cố ICS 33](#_Toc153974490)

[5.2.6 Tác động vật lý gián đoạn quy trình ICS 33](#_Toc153974491)

[5.2.7 Kết hợp các khía cạnh phi kỹ thuật số của ICS vào đánh giá tác động 34](#_Toc153974492)

[5.2.8 Kết hợp tác động của các hệ thống an toàn 35](#_Toc153974493)

[5.2.9 Xem xét việc lan truyền tác động đến các hệ thống được kết nối. 36](#_Toc153974494)

[5.3 Quản lý vận hành bảo đảm an toàn thông tin cho các hệ thống điều khiển công nghiệp ICS 36](#_Toc153974495)

[5.3.1 Trường hợp áp dụng cho các tổ chức kinh doanh về bảo mật 36](#_Toc153974496)

[5.3.1.1 Lợi ích 37](#_Toc153974497)

[5.3.1.2 Hậu quả tiềm tàng 37](#_Toc153974498)

[5.3.1.3 Nguồn lực để xây dựng tình huống kinh doanh 38](#_Toc153974499)

[5.3.1.4 Trình bày tình huống kinh doanh với bộ phận lãnh đạo 38](#_Toc153974500)

[5.3.2 Xây dựng và đào tạo nhóm đa chức năng 39](#_Toc153974501)

[5.3.3 Xác định điều lệ và phạm vi 40](#_Toc153974502)

[5.3.4 Xác định các thủ tục và chính sách bảo mật dành riêng cho ICS 40](#_Toc153974503)

[5.3.5 Triển khai khung quản lý rủi ro bảo mật ICS 41](#_Toc153974504)

[5.3.5.1 Phân loại tài sản mạng và hệ thống ICS 41](#_Toc153974505)

[5.3.5.2 Chọn Kiểm soát bảo mật ICS 42](#_Toc153974506)

[5.3.5.3 Thực hiện đánh giá rủi ro 42](#_Toc153974507)

[5.3.5.4 Thực hiện kiểm soát bảo mật 43](#_Toc153974508)

[5.4 Khung kiến trúc bảo đảm an toàn thông tin cho các hệ thống điều khiển công nghiệp ICS 43](#_Toc153974509)

[5.4.1 Phân đoạn và phân tách mạng 44](#_Toc153974510)

[5.4.2 Bảo vệ vùng mạng biên 46](#_Toc153974511)

[5.4.3 Tường lửa 48](#_Toc153974512)

[5.4.4 Mạng điều khiển tách biệt hợp lý 50](#_Toc153974513)

[5.4.5 Phân tách mạng 51](#_Toc153974514)

[5.4.5.1 Máy tính Dual-Homed/Thẻ giao diện mạng kép (NIC) 51](#_Toc153974515)

[5.4.5.2 Tường lửa giữa Mạng công ty và Mạng điều khiển 51](#_Toc153974516)

[5.4.5.3 Tường lửa và Bộ định tuyến giữa Mạng công ty và Mạng điều khiển 53](#_Toc153974517)

[5.4.5.4 Tường lửa với DMZ giữa Mạng công ty và Mạng điều khiển 54](#_Toc153974518)

[5.4.5.5 Tường lửa được phép nối giữa Mạng công ty và Mạng điều khiển 56](#_Toc153974519)

[5.4.5.6 Tóm tắt phân chia mạng 57](#_Toc153974520)

[5.4.6 Kiến trúc chiều sâu phòng ngự được khuyến nghị 58](#_Toc153974521)

[5.4.7 Chính sách tường lửa chung cho ICS 59](#_Toc153974522)

[5.4.8 Quy tắc tường lửa được đề xuất cho các dịch vụ cụ thể 62](#_Toc153974523)

[5.4.8.1 Hệ thống tên miền (DNS) 62](#_Toc153974524)

[5.4.8.2 Giao thức truyền siêu văn bản (HTTP) 62](#_Toc153974525)

[5.4.8.3 FTP và Giao thức truyền tệp tầm thường (TFTP) 62](#_Toc153974526)

[5.4.8.4 Telnet 63](#_Toc153974527)

[5.4.8.5 Giao thức cấu hình máy chủ động (DHCP) 63](#_Toc153974528)

[5.4.8.6 Lớp bảo mật (SSH) 63](#_Toc153974529)

[5.4.8.7 Giao thức truy cập đối tượng đơn giản (SOAP) 63](#_Toc153974530)

[5.4.8.8 Giao thức truyền thư đơn giản (SMTP) 64](#_Toc153974531)

[5.4.8.9 Giao thức quản lý mạng đơn giản (SNMP) 64](#_Toc153974532)

[5.4.8.10 Đối tượng thành phần phân tán Mô hình (DCOM) 64](#_Toc153974533)

[5.4.8.11 SCADA và các giao thức công nghiệp 64](#_Toc153974534)

[5.4.9 Dịch địa chỉ mạng (NAT) 64](#_Toc153974535)

[5.4.10 Các vấn đề về tường lửa ICS cụ thể 65](#_Toc153974536)

[5.4.10.1 Máy chủ lưu trữ dữ liệu 65](#_Toc153974537)

[5.4.10.2 Truy cập hỗ trợ từ xa 66](#_Toc153974538)

[5.4.10.3 Lưu lượng phát đa hướng 66](#_Toc153974539)

[5.4.11 Cổng một chiều 67](#_Toc153974540)

[5.4.12 Điểm lỗi đơn lẻ 67](#_Toc153974541)

[5.4.13 Tình trạng dư thừa và khả năng chịu lỗi 67](#_Toc153974542)

[5.4.14 Ngăn chặn các cuộc tấn công trung gian 68](#_Toc153974543)

[5.4.15 Xác thực và uỷ quyền 70](#_Toc153974544)

[5.4.15.1 Cân nhắc triển khai ICS 71](#_Toc153974545)

[5.4.16 Giám sát, Ghi nhật ký và Kiểm tra 71](#_Toc153974546)

[5.4.17 Phát hiện sự cố, ứng phó và khôi phục hệ thống 71](#_Toc153974547)

[5.5 Biện pháp kiểm soát bảo mật cho các hệ thống điều khiển công nghiệp ICS. 71](#_Toc153974548)

[5.5.1 Khung Quản lý Rủi ro cho các Hệ thống Kiểm soát Công nghiệp 72](#_Toc153974549)

[5.5.1.1 Bước 1: Phân loại hệ thống thông tin 73](#_Toc153974550)

[5.5.1.2 Bước 2: Chọn kiểm soát bảo mật 75](#_Toc153974551)

[5.5.1.3 Bước 3: Thực hiện kiểm soát An toàn 76](#_Toc153974552)

[5.5.1.4 Bước 4: Đánh giá kiểm soát An toàn 76](#_Toc153974553)

[5.5.1.5 Bước 5: Cấp quyền cho hệ thống thông tin 76](#_Toc153974554)

[5.5.1.6 Bước 6: Giám sát các kiểm soát an toàn 76](#_Toc153974555)

[5.5.2 Hướng dẫn về việc áp dụng các biện pháp kiểm soát an toàn cho ICS 76](#_Toc153974556)

[5.5.2.1 Kiểm soát truy cập 78](#_Toc153974557)

[5.5.2.2 Nhận thức và đào tạo 83](#_Toc153974558)

[5.5.2.3 Kiểm toán và trách nhiệm giải trình 83](#_Toc153974559)

[5.5.2.4 Đánh giá bảo mật và ủy quyền 85](#_Toc153974560)

[5.5.2.5 Quản lý cấu hình 85](#_Toc153974561)

[5.5.2.6 Lập kế hoạch dự phòng 86](#_Toc153974562)

[5.5.2.7 Nhận dạng và xác thực 89](#_Toc153974563)

[5.5.2.8 Ứng phó thảm họa 95](#_Toc153974564)

[5.5.2.9 Bảo trì 97](#_Toc153974565)

[5.5.2.10 Bảo vệ phương tiện 97](#_Toc153974566)

[5.5.2.11 Bảo vệ vật lý môi trường 98](#_Toc153974567)

[5.5.2.12 Lập kế hoạch 102](#_Toc153974568)

[5.5.2.13 An toàn nhân sự 103](#_Toc153974569)

[5.5.2.14 Đánh giá rủi ro 103](#_Toc153974570)

[5.5.2.15 Mua lại hệ thống và dịch vụ 104](#_Toc153974571)

[5.2.5.16 Bảo vệ hệ thống và truyền thông 105](#_Toc153974572)

[5.2.5.17 Tính toàn vẹn của hệ thống 108](#_Toc153974573)

[5.2.5.18 Quản lý chương trình 111](#_Toc153974574)

[5.2.5.19 Kiểm soát quyền riêng tư 112](#_Toc153974575)

[Thư mục tài liệu tham khảo 113](#_Toc153974576)

1. **Lời nói đầu**
2. TCVN xxxx:2023 do Cục An toàn thông tin biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

**Công nghệ thông tin - Các kỹ thuật an toàn – Các yêu cầu** **bảo đảm an toàn thông tin trong hệ thống điều khiển công nghiệp**

TIÊU CHUẨN QUỐC GIA TCVN xxxx:2023

*Information Technology - Security techniques - Requirements to ensure information security in industrial control systems*

* 1. Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu cơ bản về an toàn trong hệ thống điều khiển công nghiệp ICS

Yêu cầu an toàn cơ bản quy định trong tiêu chuẩn này tập trung vào các yêu cầu bảo đảm an toàn hệ thống điều khiển công nghiệp ICS. Các yêu cầu khác về an toàn thông tin, không liên quan trực tiếp đến đảm bảo an toàn hệ thống điều khiển công nghiệp ICS (ví dụ: bảo vệ thông tin cá nhân, bảo vệ trẻ em trên mạng,…) không thuộc phạm vi Tiêu chuẩn này.

* 1. Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây là cần thiết để áp dụng đối với tiêu chuẩn này. Đối với tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất (bao gồm cả phiên bản sửa đổi, bổ sung)..

Tiêu chuẩn NIST- SP 800-82 R2, Guide to Industrial Control Systems (ICS) Security

* 1. Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong SP 800-82 R2 và các thuật ngữ, định nghĩa sau:

**Hệ thống Điều khiển Công nghiệp (ICS)**

Hệ thống tự động hóa được sử dụng để kiểm soát và giám sát các quy trình công nghiệp và cơ sở hạ tầng hệ thống. ICS thường được áp dụng trong các môi trường như nhà máy sản xuất, nhà máy điện, xử lý nước, và các hệ thống cơ sở hạ tầng quan trọng khác.

**Hệ thống điều khiển giám sát và thu thập dữ liệu (SCADA)**

Hệ thống giám sát và điều khiển tự động được sử dụng để quản lý và kiểm soát các quy trình công nghiệp, hệ thống cơ sở hạ tầng, và thiết bị trong thời gian thực. SCADA giúp theo dõi, thu thập dữ liệu và thậm chí là điều khiển các thiết bị và quy trình từ xa

**Hệ thống điều khiển phân tán (DCS)**

Hệ thống điều khiển tự động được sử dụng trong các quy trình công nghiệp và nhà máy để quản lý và kiểm soát các hoạt động sản xuất. DCS thường được thiết kế để điều khiển và giám sát các quy trình phức tạp và lớn, như trong ngành công nghiệp hóa chất, dầu và khí đốt, chế biến thực phẩm, và nhiều ngành khác.

**Bộ điều khiển logic lập trình (PLC)**

Thiết bị điện tử được sử dụng trong các ứng dụng tự động hóa công nghiệp để kiểm soát và giám sát các hệ thống và quy trình. PLC thường được sử dụng để thực hiện các nhiệm vụ điều khiển logic và giải quyết các vấn đề kiểm soát trong môi trường công nghiệp.

**Giao diện người và máy (HMI)**

Giao diện người dùng (UI) hoặc màn hình cảm ứng, là phần của hệ thống tự động hóa hoặc điều khiển nơi mà người vận hành có thể tương tác với máy tính hoặc thiết bị để giám sát và kiểm soát các quy trình công nghiệp hoặc hệ thống. HMI chủ yếu thiết kế để làm cho thông tin trở nên trực quan và dễ hiểu, giúp người vận hành có thể thực hiện các nhiệm vụ kiểm soát và giám sát một cách hiệu quả.

**Thiết bị đầu cuối từ xa (RTU)**

Một thiết bị điện tử được sử dụng để thu thập, xử lý, và truyền dữ liệu giữa các cảm biến và thiết bị đo từ xa với hệ thống trung tâm hoặc trạm kiểm soát.

**Thiết bị điện tử thông minh (IED)**

Một loại thiết bị điện tử được sử dụng trong các hệ thống quản lý năng lượng và giám sát của các mạng điện. IED chủ yếu được thiết kế để thực hiện các chức năng thông minh và có khả năng tương tác với các hệ thống tự động hóa và mạng truyền thông.

* 1. Ký hiệu và thuật ngữ viết tắt

|  |  |  |
| --- | --- | --- |
| ARP | Giao thức phân giải địa chỉ | Address Resolution Protocol |
| CVE | Các lỗ hổng và phơi nhiễm phổ biến | Common Vulnerabilities and Exposures |
| DCS | Hệ thống điều khiển phân tán | Certificate Authority |
| DNP3 | Giao thức mạng phân tán DNP3 | Distributed Network Protocol 3 |
| DNS | Hệ Thống Tên Miền | Domain Name System |
| DoS | Từ chối dịch vụ | Denial of Service |
| EAP | Giao thức xác thực mở rộng | Extensible Authentication Protocol |
| FTP | Giao thức truyền tập tin | File Transfer Protocol |
| HTTP | Giao thức truyền siêu văn bản | Hypertext Transfer Protocol |
| HTTPS | Giao thức truyền tải siêu văn bản an toàn | Hypertext Transfer Protocol Secure |
| HMI | Giao diện người và máy | Human-Machine Interface |
| ICCP | Giao thức liên lạc của trung tâm liên điều khiển | Inter-Control Center Communications Protocol |
| ICS | Hệ thống điều khiển công nghiệp | Industrial Control System |
| IDS | Hệ thống phát hiện xâm nhập | Intrusion Detection System |
| IP | Giao thức Internet | Internet Protocol |
| IPS | Hệ thống ngăn chặn xâm nhập | Intrusion Prevention System |
| Ipsec | An toàn giao thức Internet | Internet Protocol Security |
| MAC | Kiểm soát truy cập phương tiện | Media Access Control |
| MES | Hệ thống Thi hành sản xuất | Manufacturing Execution System |
| MIB | Cơ sở thông tin quản lý | Management Information Base |
| MTU | Thiết bị đầu cuối chính (cũng là Thiết bị đo từ xa chính) | Maximum Transmission Unit |
| NAT | Dịch địa chỉ mạng | Network Address Translation |
| OS | Hệ điều hành | Operating System |
| OSI | Kết nối hệ thống mở | Open Systems Interconnection |
| PLC | Bộ điều khiển logic lập trình | Programmable Logic Controller |
| RTU | Thiết bị đầu cuối điều khiển từ xa | Remote Terminal Unit |
| SCADA | Điều khiển giám sát và thu thập dữ liệu | Supervisory Control and Data Acquisition |
| SCP | Sao chép an toàn | Secure Copy Protocol |
| SFTP | Giao thức truyền tệp an toàn | Secure File Transfer Protocol |
| SIS | Hệ thống thiết bị an toàn | Safety Instrumented System |
| SMTP | Giao thức chuyển thư đơn giản | Simple Mail Transfer Protocol |
| SNMP | Giao thức quản lý mạng đơn giản | Simple Network Management Protocol |
| SQL | Ngôn ngữ cấu trúc truy vấn | Structured Query Language |
| SSH | Vỏ an toàn | Secure Shell |
| SSID | Mã định danh bộ dịch vụ | Service Set Identifier |
| SSL | Lớp cổng bảo mật | Secure Sockets Layer |
| TCP | Giao thức điều khiển truyền dẫn | Transmission Control Protocol |
| TCP/IP | Giao thức Kiểm soát Truyền / Giao thức Internet | Transmission Control Protocol/Internet Protocol |
| TFTP | Giao thức truyền tệp tầm thường | Trivial File Transfer Protocol |
| TLS | Bảo mật tầng vận chuyển | Transport Layer Security |
| UDP | Giao thức gói dữ liệu người dùng | User Datagram Protocol |
| UPS | Cung cấp điện liên tục | Uninterruptible Power Supply |
| VLAN | Mạng cục bộ ảo | Virtual Local Area Network |
| VPN | Mạng riêng ảo | Virtual Private Network |
| WAN | Mạng diện rộng | Wide Area Network |

* 1. Các yêu cầu bảo đảm an toàn thông tin trong hệ thống điều khiển công nghiệp

5.1 Tổng quan về hệ thống điều khiển công nghiệp

Hệ thống điều khiển công nghiệp (ICS) là một thuật ngữ chung bao gồm một số loại hệ thống điều khiển, bao gồm hệ thống điều khiển giám sát và thu thập dữ liệu (SCADA), hệ thống điều khiển phân tán (DCS) và các cấu hình hệ thống điều khiển khác như Bộ điều khiển logic lập trình (PLC) thường được tìm thấy trong các lĩnh vực công nghiệp và cơ sở hạ tầng quan trọng. Một ICS bao gồm sự kết hợp của các thành phần điều khiển (ví dụ: điện, cơ khí, thủy lực, khí nén) hoạt động cùng nhau để đạt được mục tiêu công nghiệp (ví dụ: sản xuất, vận chuyển vật chất hoặc năng lượng). Phần của hệ thống chủ yếu liên quan đến việc tạo ra đầu ra được gọi là quy trình. Phần điều khiển của hệ thống bao gồm đặc điểm kỹ thuật của đầu ra hoặc hiệu suất mong muốn. Kiểm soát có thể hoàn toàn tự động hoặc có thể bao gồm một con người trong vòng lặp. Các hệ thống có thể được cấu hình để vận hành chế độ vòng hở, vòng kín và thủ công. Trong các hệ thống điều khiển vòng hở, đầu ra được điều khiển bởi các cài đặt đã thiết lập. Trong các hệ thống điều khiển vòng kín, đầu ra có ảnh hưởng đến đầu vào theo cách để duy trì mục tiêu mong muốn. Ở chế độ thủ công, hệ thống được điều khiển hoàn toàn bởi con người. Phần của hệ thống chủ yếu liên quan đến việc duy trì sự phù hợp với các thông số kỹ thuật được gọi là bộ điều khiển (hoặc bộ điều khiển). Một ICS điển hình có thể chứa nhiều vòng điều khiển, (HMI) và các công cụ bảo trì và chẩn đoán từ xa được xây dựng bằng một loạt các giao thức mạng. Các quy trình công nghiệp kiểm soát ICS thường được sử dụng trong điện, nước và nước thải, dầu mỏ và khí đốt tự nhiên, hóa chất, giao thông vận tải, dược phẩm, bột giấy và giấy, thực phẩm và đồ uống cũng như các ngành sản xuất riêng biệt (ví dụ: tự động hoá, hàng không vũ trụ và hàng hóa lâu bền).

ICS rất quan trọng đối với hoạt động của các cơ sở hạ tầng quan trọng, thường là các hệ thống có mối liên hệ chặt chẽ và phụ thuộc lẫn nhau. Điều quan trọng cần lưu ý là xấp xỉ 85% cơ sở hạ tầng quan trọng của quốc gia thuộc sở hữu và vận hành của tư nhân. Phần này cung cấp tổng quan về các hệ thống SCADA, DCS và PLC, bao gồm các thành phần và cấu trúc liên kết điển hình. Một số sơ đồ được trình bày để mô tả cấu trúc liên kết mạng, kết nối, thành phần và giao thức thường được tìm thấy trên mỗi hệ thống để tạo điều kiện hiểu biết về các hệ thống này. Những ví dụ này chỉ xác định các khái niệm cấu trúc liên kết danh nghĩa. Việc triển khai thực tế của ICS có thể là kết hợp làm mờ ranh giới giữa hệ thống DCS và SCADA.

* + 1. Sự phát triển của các hệ thống điều khiển công nghiệp

Nhiều hệ thống điều khiển công nghiệp (ICS) ngày nay đã phát triển từ việc đưa các khả năng CNTT vào các hệ thống vật lý hiện có, thường thay thế hoặc bổ sung các cơ chế kiểm soát vật lý. Ví dụ, các điều khiển kỹ thuật số nhúng đã thay thế các điều khiển cơ học tương tự trong các máy và động cơ quay. Những cải tiến về chi phí và hiệu suất đã khuyến khích sự phát triển này, dẫn đến nhiều công nghệ “thông minh” ngày nay như lưới điện thông minh, giao thông thông minh, tòa nhà thông minh và sản xuất thông minh. Mặc dù điều này làm tăng khả năng kết nối và mức độ quan trọng của các hệ thống này, nhưng nó cũng tạo ra nhu cầu lớn hơn về khả năng thích ứng, khả năng phục hồi, an toàn và bảo mật của chúng.

Kỹ thuật của ICS tiếp tục phát triển để cung cấp các khả năng mới trong khi vẫn duy trì vòng đời dài điển hình của các hệ thống này. Việc đưa các khả năng CNTT vào các hệ thống vật lý thể hiện hành vi mới nổi có ý nghĩa bảo mật. Các mô hình và phân tích kỹ thuật đang phát triển để giải quyết các thuộc tính mới nổi này bao gồm sự phụ thuộc lẫn nhau về an toàn, bảo mật, quyền riêng tư và tác động môi trường.

* + 1. Các lĩnh vực công nghiệp của ISC và sự phụ thuộc lẫn nhau

Hệ thống điều khiển được sử dụng trong nhiều lĩnh vực công nghiệp khác nhau và cơ sở hạ tầng quan trọng, bao gồm sản xuất, phân phối và vận chuyển.

5.1.2.1 Công nghiệp sản xuất

Sản xuất là một lĩnh vực công nghiệp rộng lớn và đa dạng với nhiều quy trình khác nhau, có thể được phân loại thành sản xuất dựa trên quy trình và sản xuất rời rạc.

Các ngành sản xuất dựa trên quy trình thường sử dụng hai quy trình chính:

- **Quy trình sản xuất liên tục**. Các quy trình này chạy liên tục, thường có sự chuyển đổi để tạo ra các loại sản phẩm khác nhau.Các quy trình sản xuất liên tục điển hình bao gồm dòng nhiên liệu hoặc hơi nước trong nhà máy điện, dầu mỏ trong nhà máy lọc dầu và chưng cất trong nhà máy hóa chất.

- **Quy trình sản xuất hàng loạt.** Các quy trình này có các bước xử lý riêng biệt, được thực hiện trên một lượng vật liệu. Có một bước bắt đầu và kết thúc riêng biệt cho một quy trình hàng loạt với khả năng hoạt động ởtrạng thái ổn định ngắn trong các bước trung gian. Quy trình sản xuất hàng loạt điển hình bao gồm sản xuất thực phẩm.

Các ngành công nghiệp sản xuất rời rạc thường tiến hành một loạt các bước trên một thiết bị duy nhất để tạo ra sản phẩm cuối cùng. Lắp ráp các bộ phận điện tử và cơ khí và gia công các bộ phận là những ví dụ điển hình của loại hình công nghiệp này.

Cả hai ngành công nghiệp dựa trên quy trình và rời rạc đều sử dụng các loại hệ thống điều khiển, cảm biến và mạng giống nhau. Một số cơ sở là sự kết hợp giữa sản xuất rời rạc và dựa trên quy trình.

5.1.2.2 Công nghiệp phân bố

ICS được sử dụng để kiểm soát các tài sản phân tán về mặt địa lý, thường nằm rải rác trên hàng nghìn km2, bao gồm các hệ thống phân phối như hệ thống phân phối nước và thu gom nước thải, hệ thống tưới tiêu nông nghiệp, đường ống dẫn dầu và khí tự nhiên, lưới điện và hệ thống giao thông đường sắt.

**5.1.2.3 Sự khác biệt giữa sản xuất và phân bố ICS**

Mặc dù các hệ thống điều khiển được sử dụng trong các ngành công nghiệp sản xuất và phân bố rất giống nhau về cách vận hành, nhưng chúng lại khác nhau ở một số khía cạnh. Các ngành sản xuất thường được đặt trong một nhà máy hạn chế hoặc khu vực tập trung vào nhà máy, khi so sánh với các ngành phân phối phân tán về mặt địa lý. Truyền thông trong các ngành sản xuất thường được thực hiện bằng cách sử dụng các công nghệ mạng cục bộ (LAN) thường đáng tin cậy hơn và tốc độ cao hơn so với các công nghệ mạng diện rộng (WAN) và không dây/RF (tần số vô tuyến) được sử dụng bởi các ngành công nghiệp phân phối. ICS được sử dụng trong các ngành phân phối được thiết kế để xử lý các thách thức liên lạc đường dài như chậm trễ và mất dữ liệu do các phương tiện truyền thông khác nhau được sử dụng. Các biện pháp kiểm soát bảo mật có thể khác nhau giữa các loại mạng.

**5.1.2.4 ICS và Sự phụ thuộc quan trọng của cơ sở hạ tầng**

Cơ sở hạ tầng quan trọng thường được nhắc đến là “hệ thống của các hệ thống” do sự phụ thuộc lẫn nhau tồn tại giữa các ngành công nghiệp đa dạng cũng như mối liên kết giữa các đối tác kinh doanh. Các cơ sở hạ tầng quan trọng có tính kết nối cao và phụ thuộc lẫn nhau theo những cách phức tạp, cả về mặt vật lý và thông qua một loạt các công nghệ thông tin và truyền thông. Một sự cố trong một cơ sở hạ tầng có thể ảnh hưởng trực tiếp và gián tiếp đến các cơ sở hạ tầng khác thông qua các lỗi theo tầng và leo thang.

Cả ngành truyền tải điện và lưới điện phân phối đều sử dụng công nghệ điều khiển SCADA phân tán theo địa lý để vận hành các hệ thống năng động và có tính kết nối cao bao gồm hàng nghìn tiện ích công cộng và tư nhân cũng như các hợp tác xã nông thôn để cung cấp điện cho người dùng cuối. Một số hệ thống SCADA giám sát và kiểm soát việc phân phối điện bằng cách thu thập dữ liệu và đưa ra lệnh cho các trạm điều khiển trường từ xa về mặt địa lý từ một vị trí tập trung. Các hệ thống SCADA cũng được sử dụng để giám sát và kiểm soát việc phân phối nước, dầu và khí tự nhiên, bao gồm đường ống, tàu, xe tải và hệ thống đường sắt, cũng như hệ thống thu gom nước thải.

Các hệ thống SCADA và DCS thường được kết nối mạng với nhau. Đây là trường hợp của các trung tâm điều khiển năng lượng điện và các cơ sở phát điện. Mặc dù hoạt động của cơ sở phát điện được điều khiển bởi DCS, nhưng DCS phải giao tiếp với hệ thống SCADA để điều phối sản lượng sản xuất với nhu cầu truyền tải và phân phối.

Năng lượng điện thường được cho là một trong những nguồn gây gián đoạn phổ biến nhất đối với các cơ sở hạ tầng quan trọng phụ thuộc lẫn nhau. Ví dụ, sự cố phân tầng có thể bắt đầu do sự gián đoạn của mạng truyền thông vi ba được sử dụng cho hệ thống SCADA truyền tải điện. Việc thiếu khả năng giám sát và kiểm soát có thể khiến một tổ máy phát điện lớn bị ngoại tuyến, một sự kiện có thể dẫn đến mất điện tại một trạm biến áp truyền tải. Sự mất mát này có thể gây ra sự mất cân bằng lớn, gây ra sự cố nối tiếp trên lưới điện. Điều này có thể dẫn đến mất điện trên diện rộng và có khả năng ảnh hưởng đến hoạt động sản xuất dầu và khí đốt tự nhiên, hoạt động của nhà máy lọc dầu, hệ thống xử lý nước, hệ thống thu gom nước thải và hệ thống vận chuyển đường ống dựa vào lưới điện.

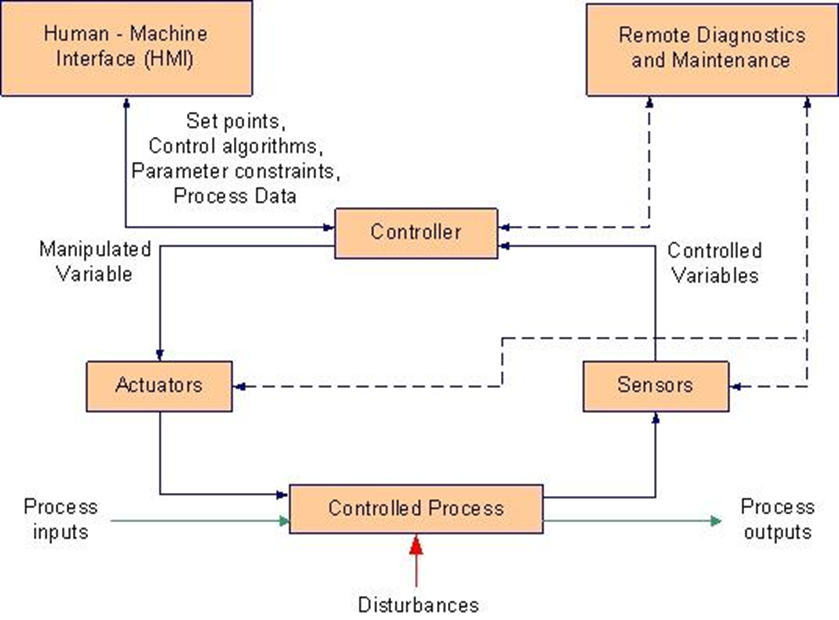
* + 1. Sự hoạt động và các thành phần của ICS

Hoạt động cơ bản của một ICS được thể hiện trong Hình 1. Một số quy trình quan trọng cũng có thể bao gồm các hệ thống an toàn. Các thành phần chính bao gồm:

Một ICS điển hình chứa nhiều vòng điều khiển, giao diện con người và các công cụ bảo trì và chuẩn đoán từ xa được xây dựng bằng cách sử dụng một loạt các giao thức mạng trên kiến trúc mạng phân lớp. Một vòng điều khiển sử dụng các cảm biến, bộ truyền động và bộ điều khiển (VD: PLC) để điều khiển một số quy trình được kiểm soát. Cảm biến là một thiết bị tạo ra phép đo một số thuộc tính vật lý và sau đó gửi thông tin này dưới dạng các biến được kiểm soát tới bộ điều khiển. Bộ điều khiển giải các tín hiệu và tạo ra các biến được thao tác tương ứng, dựa trên thuật toán điều khiển và các điểm đặt mục tiêu, mà nó truyền đến các bộ truyền động. Các thiết bị truyền động như van điều khiển, cầu dao, công tắc và động cơ được sử dụng để điều khiển trực tiếp quá trình được điều khiển dựa trên các lệnh từ bộ điều khiển.

Người vận hành và kỹ sư sử dụng giao diện con người để giám sát và định cấu hình các điểm đặt, thuật toán điều khiển cũng như điều chỉnh và thiết lập các tham số trong bộ điều khiển. Giao diện con người cũng hiển thị thông tin trạng thái quy trình và thông tin lịch sử. Các tiện ích chẩn đoán và bảo trì được sử dụng để ngăn chặn, xác định và phục hồi sau sự cố hoặc hoạt động bất thường.

Đôi khi các vòng điều khiển này được lồng vào nhau và/hoặc xếp tầng – theo đó điểm đặt cho một vòng lặp dựa trên biến quy trình được xác định bởi một vòng lặp khác. Các vòng lặp cấp giám sát và các vòng lặp cấp thấp hơn hoạt động liên tục trong suốt thời gian của một quy trình với thời gian chu kỳ nằm trong khoảng từ một phần nghìn giây đến phút.



**Hình 1. Hoạt động ICS**

5.1.3.1 Sự cân nhắc thiết kế hệ thống ICS

- **Hệ thống cấp bậc**. Kiểm soát giám sát được sử dụng để cung cấp một vị trí trung tâm có thể tổng hợp dữ liệu từ nhiều vị trí để hỗ trợ các quyết định kiểm soát dựa trên trạng thái hiện tại của hệ thống. Một điều khiển phân cấp/tập trung thông thường được sử dụng để cung cấp cho người vận hành cái nhìn toàn diện về toàn bộ hệ thống.

- **Kiểm soát phức tạp.** Thông thường các chức năng điều khiển có thể được thực hiện bằng các bộ điều khiển đơn giản và các thuật toán đặt trước. Tuy nhiên, các hệ thống phức tạp hơn (ví dụ: kiểm soát không lưu) yêu cầu người vận hành phải đảm bảo rằng tất cả các hành động kiểm soát đều phù hợp để đáp ứng các mục tiêu lớn hơn của hệ thống.

- **Khả dụng.** Các yêu cầu về tính khả dụng (nghĩa là độ tin cậy) của hệ thống cũng là một yếu tố quan trọng trong thiết kế. Các hệ thống có yêu cầu cao về tính khả dụng/thời gian hoạt động có thể yêu cầu nhiều dự phòng hơn hoặc triển khai thay thế trên tất cả các giao tiếp và kiểm soát.

- **Ảnh hưởng của sự cố.** Lỗi chức năng kiểm soát có thể gây ra các tác động khác nhau đáng kể giữa các miền. Các hệ thống có tác động lớn hơn thường yêu cầu khả năng tiếp tục hoạt động thông qua các điều khiển dự phòng hoặc khả năng hoạt động ở trạng thái xuống cấp. Thiết kế cần giải quyết các yêu cầu này.

- **Sự an toàn.** Khu vực yêu cầu an toàn của hệ thống cũng là một yếu tố quan trọng trong thiết kế. Các hệ thống phải có khả năng phát hiện các điều kiện không an toàn và kích hoạt các hành động để giảm các điều kiện không an toàn thành các điều kiện an toàn. Trong hầu hết các hoạt động quan trọng về an toàn, sự giám sát và kiểm soát của con người đối với một quy trình nguy hiểm tiềm ẩn là một phần thiết yếu của hệ thống an toàn.

5.1.3.2 Hệ thống SCADA

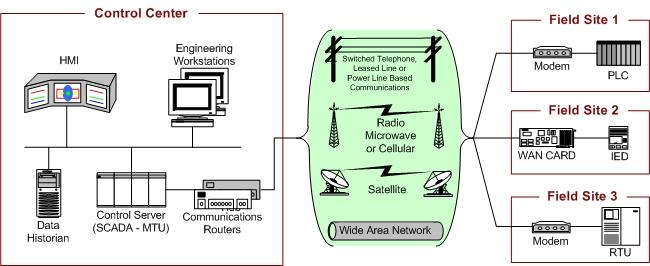
Các hệ thống SCADA được sử dụng để kiểm soát các tài sản phân tán trong đó việc thu thập dữ liệu tập trung cũng quan trọng như kiểm soát. Các hệ thống này được sử dụng trong các hệ thống phân phối như hệ thống phân phối nước và thu gom nước thải, đường ống dẫn dầu và khí đốt tự nhiên, hệ thống truyền tải và phân phối tiện ích điện, đường sắt và các hệ thống giao thông công cộng khác. Hệ thống SCADA tích hợp hệ thống thu thập dữ liệu với hệ thống truyền dữ liệu và phần mềm HMI để cung cấp hệ thống giám sát và hệ thống điều khiển cho nhiềuđầu vào và đầu ra của quy trình. Các hệ thống SCADA được thiết kế để thu thập thông tin trường, chuyển nó đến một cơ sở máy tính trung tâm và hiển thị thông tin cho người vận hành bằng đồ họa hoặc văn bản, do đó cho phép người vận hành giám sát hoặc điều khiển toàn bộ hệ thống từ một vị trí trung tâm trong thời gian thực. Dựa trên sự phức tạp và thiết lập của hệ thống riêng lẻ, việc kiểm soát bất kỳ hệ thống, hoạt động hoặc tác vụ riêng lẻ nào có thể được thực hiện tự động hoặc có thể được thực hiện bằng lệnh của người vận hành.

Phần cứng điển hình bao gồm một máy chủ điều khiển được đặt tại trung tâm điều khiển, thiết bị liên lạc (ví dụ: radio, đường dây điện thoại, cáp hoặc vệ tinh), và một hoặc nhiều địa điểm trường được phân bổ theo địa lý bao gồm Thiết bị đầu cuối từ xa (RTU) và/hoặc PLSs, mà điều khiển bộ truyền động và/ hoặc giám sát các cảm biến. Máy chủ điều khiển lưu trữ và xử lý thông tin từ đầu vào và đầu ra của RTU, trong khi RTU hoặc PLC điều khiển quy trình cục bộ. Phần cứng truyền thông cho phép truyền thông tin và dữ liệu qua lại giữa máy chủ điều khiển và RTU hoặc PLC. Phần mềm được lập trình để báo cho hệ thống biết cái gì và khi nào cần giám sát, phạm vi tham số nào được chấp nhận và phản hồi nào sẽ bắt đầu khi các tham số thay đổi ngoài giá trị chấp nhận được.Thiết bị điện tử thông minh (IED), chẳng hạn như bộ tiếp sóng bảo vệ, có thể kết nối trực tiếp với máy chủ điều khiển, hoặc RTU cục bộ có thể thăm dò IED để thu nhập dữ liệu và chuyển dữ liệu đến máy chủ điều khiển. IED cung cấp giao diện trực tiếp để điều khiển và giám sát thiết bị và cảm biến. IED có thể được thăm dò và kiểm soát trực tiếp bởi máy chủ điều khiển và trong hầu hết các trường hợp đều có lập trình cục bộ cho phép IED hoạt động mà không cần hướng dẫn trực tiếp từ trung tâm điều khiển. Hệ thống SCADA thường được thiết kế để trở thành hệ thống có khả năng chịu lỗi với khả năng dự phòng đáng kể được tích hợp trong hệ thống. Dự phòng có thể không phải là một biện pháp đối phó đầy đủ khi đối mặt với cuộc tấn công độc hại.

Hình 2 cho thấy các thành phần và cấu hình chung của một hệ thống SCADA. Trung tâm điều khiển chứa một máy chủ điều khiển và các bộ định tuyến liên lạc. Các thành phần trung tâm điều khiển khác bao gồm HMI, máy trạm kỹ thuật và lịch sử dữ liệu, tất cả đều được kết nối bằng mạng LAN. Trung tâm điều khiển thu thập và ghi lại thông tin được thu thập bởi các trang trường, hiển thị thông tin cho HMI và có thể tạo các hành động dựa trên các sự kiện được phát hiện. Trung tâm điều khiển cũng chịu trách nhiệm báo động tập trung, phân tích xu hướng và báo cáo. Trang trường thực hiện điều khiển cục bộ các bộ truyền động và giám sát các cảm biến (Lưu ý rằng các cảm biến và bộ truyền động chỉ được thể hiện trong Hình 5). Các địa điểm trường thường được trang bị khả năng truy cập từ xa để cho phép người vận hành thực hiện chẩn đoán và sửa chữa từ xa, thường qua một modem quay số hoặc kết nối WAN riêng biệt. Các giao thức truyền thông tiêu chuẩn và độc quyền chạy qua truyền thông nối tiếp và mạng được sử dụng để truyền thông tin giữa trung tâm điều khiển và các địa điểm thực địa bằng các kỹ thuật đo từ xa như đường dây điện thoại, cáp, cáp quang và tần số vô tuyến như quảng bá, vi ba và vệ tinh.

Các cấu trúc liên kết truyền thông SCADA khác nhau giữa các triển khai. Các cấu trúc liên kết khác nhau được sử dụng, bao gồm điểm đối điểm, chuỗi, chuỗi sao và đa điểm, được hiển thị trong Hình 3.

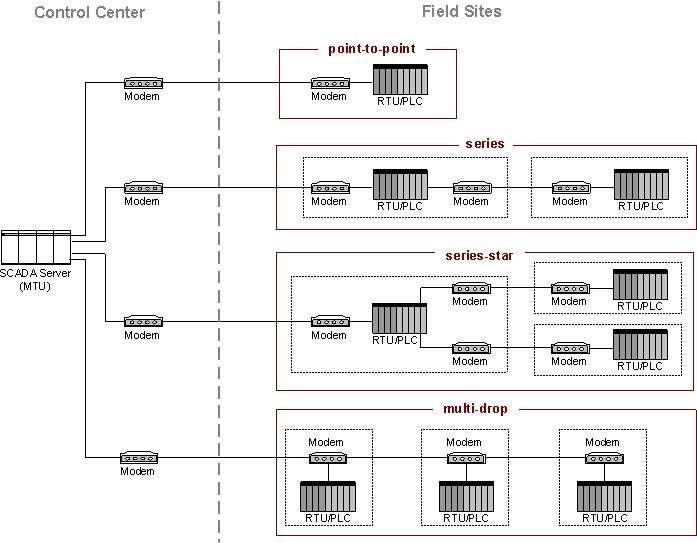
Điểm đối điểm về mặt chức năng là loại đơn giản nhất; tuy nhiên, nó đắt vì cần có các kênh riêng lẻ cho mỗi kết nối. Trong một cấu hình sê-ri, số lượng kênh được sử dụng sẽ giảm đi; tuy nhiên, việc chia sẻ kênh có tác động đến hiệu quả và độ phức tạp của hoạt động SCADA. Tương tự như vậy, việc sử dụng một kênh trên mỗi thiết bị của cấu hình sê-ri sao và đa điểm dẫn đến giảm hiệu quả và tăng độ phức tạp của hệ thống.



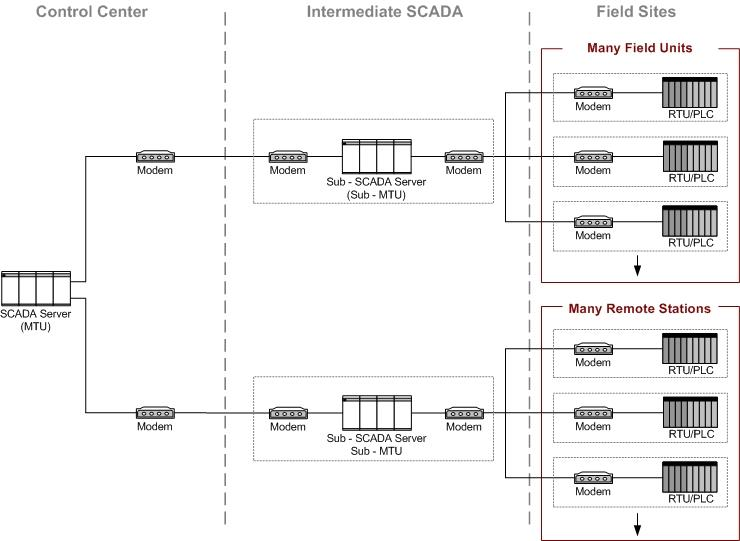
**Hình 2. Bố cục chung của hệ thống SCADA**

Bốn cấu trúc liên kết cơ bản Hình 3 có thể được tăng cường hơn nữa bằng cách sử dụng các thiết bị chuyên dụng để quản lý trao đổi thông tin liên lạc cũng như chuyển đổi và bộ đệm thông báo. Các hệ thống SCADA lớn chứa hàng trăm RTU thường thuê một máy chủ điều khiển phụ để giảm bớt gánh nặng cho máy chủ chính. Loại cấu trúc liên kết này được hiển thị trong Hình 4.

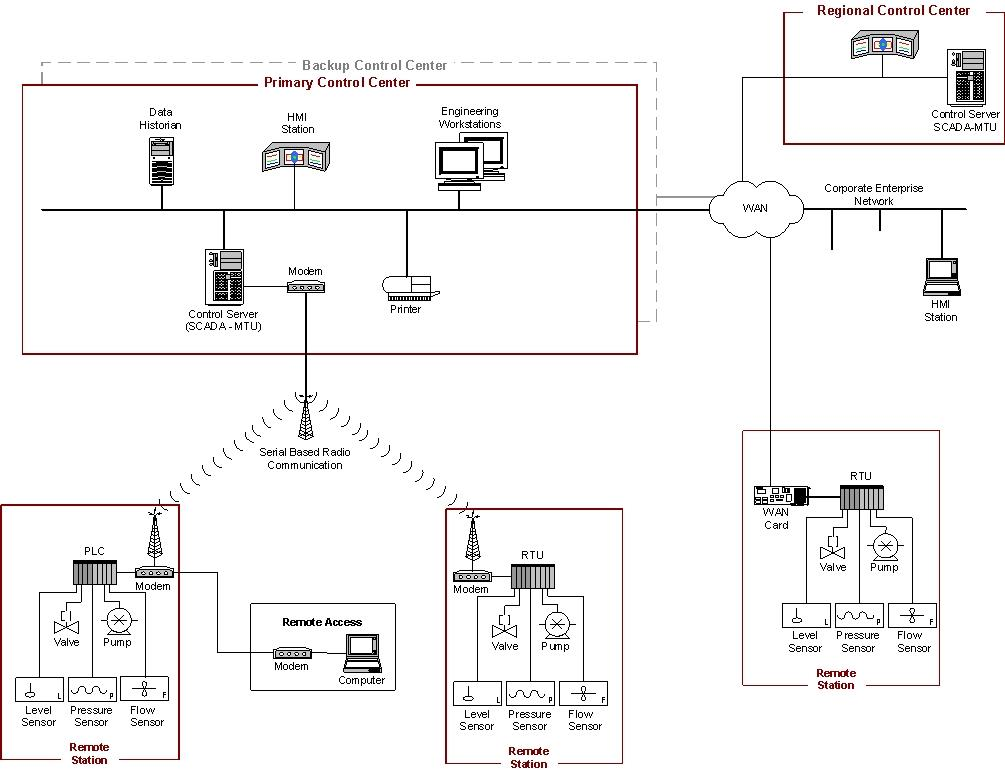
Hình 5 cho thấy một ví dụ về triển khai hệ thống SCADA. Hệ thống SCADA cụ thể này bao gồm một trung tâm điều khiển chính và ba địa điểm trường. Trung tâm điều khiển dự phòng thứ hai cung cấp khả năng dự phòng trong trường hợp trung tâm điều khiển chính gặp trục trặc. Các kết nối điểm đối điểm được sử dụng cho tất cả các liên lạc từ trung tâm điều khiển đến trường, với hai kết nối sử dụng phép đo từ xa vô tuyến. Trang trường thứ ba là cục bộ của trung tâm điều khiển và sử dụng mạng WAN để liên lạc. Một trung tâm điều khiển khu vực nằm phía trên trung tâm điều khiển chính để có mức độ kiểm soát giám sát cao hơn. Mạng công ty có quyền truy cập vào tất cả các trung tâm điều khiển thông qua mạng WAN và các trang trường có thể được truy cập từ xa để xử lý sự cố và vận hành bảo trì. Trung tâm điều khiển chính thăm dò thiết bị trường để lấy dữ liệu theo các khoảng thời gian xác định (ví dụ: 5 giây, 60 giây) và có thể gửi các điểm đặt mới đến thiết bị trường theo yêu cầu. Ngoài việc thăm dò và đưa ra các lệnh cấp cao, máy chủ điều khiển cũng theo dõi các ngắt ưu tiên đến từ các hệ thống báo động tại hiện trường.



**Hình 3. Cấu trúc liên kết truyền thông SCADA cơ bản**

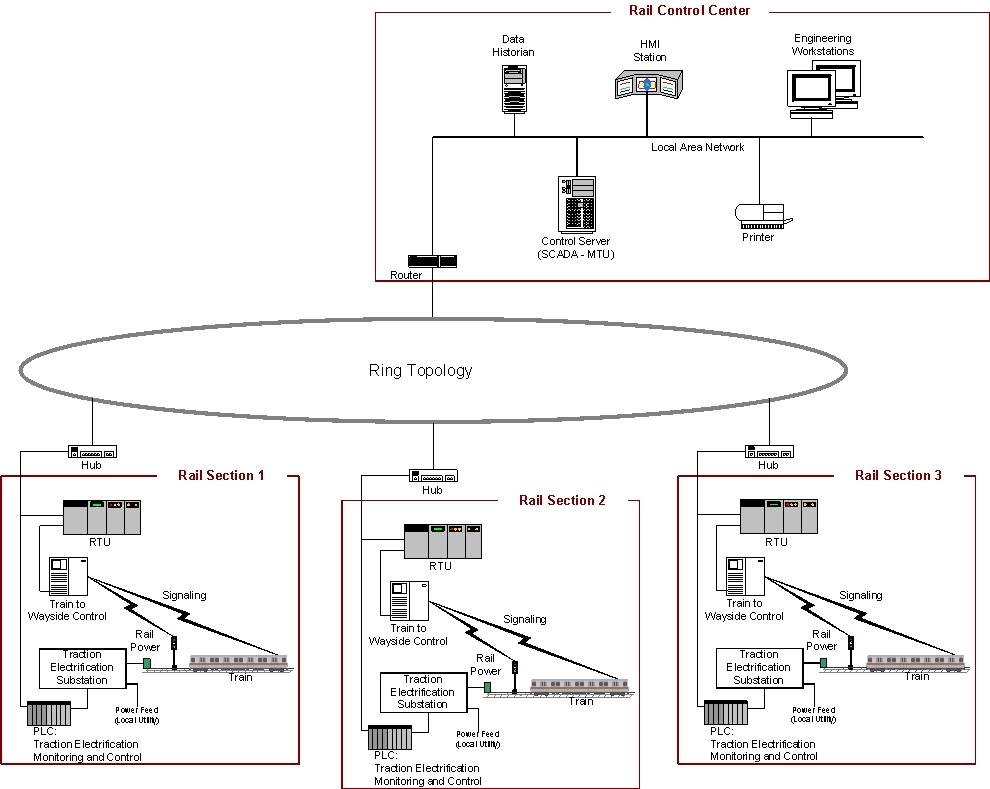


**Hình 4. Cấu trúc liên kết truyền thông SCADA lớn**



**Hình 5. Ví dụ triển khai hệ thống SCADA (Giám sát và kiểm soát phân bố)**

Hình 6 cho thấy một ví dụ triển khai giám sát và kiểm soát đường sắt. Ví dụ này bao gồm một trung tâm điều khiển đường sắt chứa hệ thống SCADA và ba phần của hệ thống đường sắt. Hệ thống SCADA thăm dò các đoạn đường sắt để biết thông tin như trạng thái của đoàn tàu, hệ thống tín hiệu, hệ thống điện khí hóa lực kéo và máy bán vé tự động. Thông tin này cũng được cung cấp cho bảng điều khiển của nhà điều hành tại trạm HMI trong trung tâm điều khiển đường sắt. Hệ thống SCADA cũng giám sát đầu vào của người vận hành tại trung tâm điều khiển đường sắt và phân tán các lệnh của người vận hành cấp cao tới các bộ phận của đoạn đường ray. Ngoài ra, hệ thống SCADA giám sát các điều kiện tại các đoạn đường ray riêng lẻ và đưa ra các lệnh dựa trên các điều kiện này (ví dụ: dừng một đoàn tàu để ngăn đoàn tàu đi vào khu vực đã được xác định là bị ngập lụt hoặc bị chiếm bởi một đoàn tàu khác dựa trên giám sát tình trạng).



**Hình 6. Ví dụ triển khai hệ thống SCADA ( Giám sát và kiểm soát đường đường ray)**

5.1.3.3 Hệ thống điều khiển phân tán

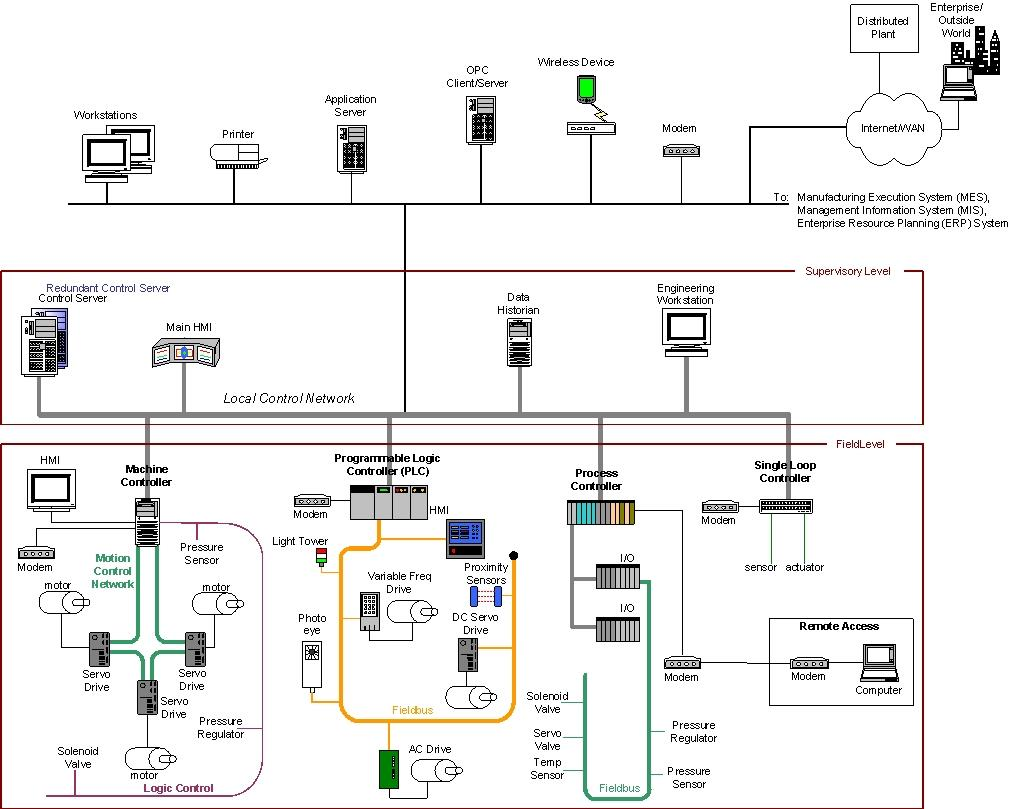
DCS được sử dụng để điều khiển các hệ thống sản xuất trong cùng một vị trí địa lý cho các ngành công nghiệp như nhà máy lọc dầu, xử lý nước và nước thải, nhà máy phát điện, nhà máy sản xuất hóa chất, sản xuất ô tô và cơ sở chế biến dược phẩm. Các hệ thống này thường là hệ thống điều khiển quá trình hoặc điều khiển bộ phận rời rạc.

DCS được tích hợp như một kiến trúc điều khiển chứa cấp độ kiểm soát giám sát giám sát nhiều hệ thống con tích hợp, chịu trách nhiệm kiểm soát các chi tiết của một quy trình cục bộ. Một DCS sử dụng một vòng điều khiển giám sát tập trung để làm trung gian cho một nhóm các bộ điều khiển cục bộ chia sẻ các nhiệm vụ tổng thể để thực hiện toàn bộ quy trình sản xuất. Kiểm soát sản phẩm và kiểm soát quy trình thường đạt được bằng cách phát triển các vòng kiểm soát phản hồi hoặc vòng điều khiển chuyển tiếp các điều kiện chính của sản phẩm và/hoặc quy trình được tự động duy trì xung quanh một điểm đặt mong muốn. Để đạt được sản phẩm mong muốn và/hoặc dung sai xử lý xung quanh một điểm đặt cụ thể, các bộ điều khiển quy trình cụ thể hoặc các PLC có khả năng cao hơn được sử dụng tại hiện trường và được điều chỉnh để cung cấp dung sai mong muốn cũng như tốc độ tự điều chỉnh trong quá trình đảo lộn quy trình. Bằng cách mô đun hóa hệ thống sản xuất, DCS giảm tác động một lỗi đơn lẻ lên toàn bộ hệ thống. Trong nhiều hệ thống hiện đại, DCS được giao tiếp với mạng công ty để cung cấp cho các hoạt động kinh doanh một cái nhìn về sản xuất.

Một ví dụ triển khai hiển thị các thành phần và cấu hình chung của DCS được mô tả trong Hình 7. DCS này bao gồm toàn bộ cơ sở từ các quy trình sản xuất cấp thấp nhất cho đến lớp công ty hoặc doanh nghiệp. Trong ví dụ này, bộ điều khiển giám sát (máy chủ điều khiển) giao tiếp với cấp dưới của nó thông qua mạng điều khiển. Người giám sát gửi các điểm đã đặt đến và yêu cầu dữ liệu từ các bộ điều khiển trường phân tán. Các bộ điều khiển phân tán điều khiển các bộ truyền động quy trình của chúng dựa trên các lệnh của máy chủ điều khiển và phản hồi cảm biến từ các cảm biến quy trình.

Hình 7 đưa ra các ví dụ về bộ điều khiển cấp thấp được tìm thấy trên hệ thống DCS. Các thiết bị điều khiển trường được hiển thị bao gồm PLC, bộ điều khiển quy trình, bộ điều khiển vòng lặp đơn và bộ điều khiển máy. Bộ điều khiển vòng đơn giao tiếp các cảm biến và bộ truyền động bằng cách sử dụng hệ thống dây điểm đối điểm, trong khi ba thiết bị trường khác kết hợp mạng bus trường để giao tiếp với các cảm biến và bộ truyền động xử lý. Mạng bus trường loại bỏ nhu cầu đi dây điểm đối điểm giữa bộ điều khiển và các bộ truyền động và cảm biến trường riêng lẻ. Ngoài ra, bus trường cho phép thực hiện nhiều chức năng hơn ngoài khả năng kiểm soát, bao gồm chẩn đoán thiết bị trường và có thể thực hiện các thuật toán điều khiển trong bus trường, do đó tránh được việc định tuyến tín hiệu trở lại PLC cho mọi hoạt động điều khiển. Các giao thức truyền thông công nghiệp tiêu chuẩn được thiết kế bởi các nhóm công nghiệp như Modbus và Fieldbus thường được sử dụng trên các mạng điều khiển và mạng bus trường.

Ngoài các vòng kiểm soát cấp giám sát và cấp hiện trường, các cấp kiểm soát trung gian cũng có thể tồn tại. Ví dụ, trong trường hợp một DCS kiểm soát một cơ sở sản xuất bộ phận rời rạc, có thể có một giám sát viên cấp trung gian cho mỗi ô trong nhà máy. Người giám sát này sẽ bao gồm một ô sản xuất chứa bộ điều khiển máy xử lý một bộ phận và bộ điều khiển robot xử lý nguyên liệu thô và sản phẩm cuối cùng. Có thể có một vài ô trong số này quản lý các bộ điều khiển cấp trường trong vòng điều khiển giám sát chính của DCS.



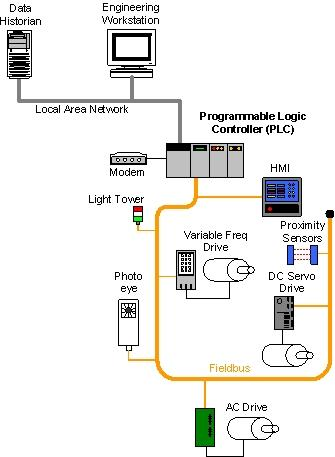
**Hình 7. Ví dụ triển khai hệ thống DCS**

5.1.3.4 Cấu trúc liên kết dựa trên bộ điều khiển logic có thể lập trình

PLC được sử dụng trong cả hệ thống SCADA và DCS làm thành phần điều khiển của hệ thống phân cấp tổng thể để cung cấp khả năng quản lý cục bộ các quy trình thông qua điều khiển phản hồi như được mô tả trong các phần trên. Trong trường hợp hệ thống SCADA, chúng có thể cung cấp chức năng tương tự như RTU. Khi được sử dụng trong DCS, PLC được triển khai dưới dạng bộ điều khiển cục bộ trong sơ đồ điều khiển giám sát.

Ngoài việc sử dụng PLC trong SCADA và DCS, PLC cũng được triển khai làm bộ điều khiển chính trong các cấu hình hệ thống điều khiển nhỏ hơn để cung cấp khả năng điều khiển vận hành các quy trình rời rạc như dây chuyền lắp ráp ô tô và điều khiển máy thổi bồ hóng của nhà máy điện. Các cấu trúc liên kết này khác với SCADA và DCS ở chỗ chúng thường thiếu máy chủ điều khiển trung tâm và HMI, do đó, chủ yếu cung cấp điều khiển vòng kín mà không có sự tham gia trực tiếp của con người. PLC có bộ nhớ do người dùng lập trình để lưu trữ các lệnh nhằm mục đích thực hiện các chức năng cụ thể như điều khiển I/O, logic, định thời gian, đếm, điều khiển ba chế độ đạo hàm tỷ lệ-tích phân (PID), giao tiếp, số học, dữ liệu và xử lý tệp.

Hình 8 cho thấy điều khiển quy trình sản xuất được thực hiện bởi PLC qua mạng bus trường. Có thể truy cập PLC thông qua giao diện lập trình nằm trên máy trạm kỹ thuật và dữ liệu được lưu trữ trong lịch sử dữ liệu, tất cả được kết nối trên mạng LAN.



**Hình 8. Ví dụ triển khai hệ thống điều khiển PLC**

* + 1. So sánh ICS và hệ thống bảo mật công nghệ thông tin

ICS kiểm soát thế giới vật chất và hệ thống CNTT quản lý dữ liệu. ICS có nhiều đặc điểm khác với các hệ thống CNTT truyền thống, bao gồm các rủi ro và mức độ ưu tiên khác nhau. Một số trong số này bao gồm rủi ro đáng kể đối với sức khỏe và sự an toàn của cuộc sống con người, thiệt hại nghiêm trọng đối với môi trường và các vấn đề tài chính như tổn thất sản xuất và tác động tiêu cực đến nền kinh tế của một quốc gia. ICS có các yêu cầu về hiệu suất và độ tin cậy khác nhau, đồng thời sử dụng các hệ điều hành và ứng dụng có thể được coi là khác thường trong môi trường mạng CNTT điển hình. Các biện pháp bảo vệ an toàn phải được triển khai theo cách duy trì tính toàn vẹn của hệ thống trong các hoạt động bình thường cũng như trong thời gian bị tấn công mạng.

Ban đầu, ICS có chút giống với các hệ thống CNTT ở chỗ ICS là các hệ thống biệt lập chạy các giao thức kiểm soát độc quyền sử dụng phần cứng và phần mềm chuyên dụng. Các thiết bị Ethernet và Giao thức Internet (IP) chi phí thấp phổ biến rộng rãi hiện đang thay thế các công nghệ độc quyền cũ hơn, làm tăng khả năng xảy ra các lỗ hổng và sự cố an toàn mạng. Vì ICS đang áp dụng các giải pháp CNTT để thúc đẩy khả năng kết nối và truy cập từ xa của công ty, đồng thời đang được thiết kế và triển khai bằng cách sử dụng các máy tính, hệ điều hành (OS) và giao thức mạng tiêu chuẩn công nghiệp, nên chúng bắt đầu giống với các hệ thống CNTT. Sự tích hợp này hỗ trợ các khả năng CNTT mới, nhưng nó giúp ICS ít bị cô lập hơn so với thế giới bên ngoài so với các hệ thống tiền nhiệm, tạo ra nhu cầu lớn hơn về bảo mật các hệ thống này. Mặc dù các giải pháp bảo mật đã được thiết kế để giải quyết các vấn đề bảo mật này trong các hệ thống CNTT điển hình, nhưng phải thực hiện các biện pháp phòng ngừa đặc biệt khi đưa các giải pháp tương tự này vào môi trường ICS. Trong một số trường hợp, cần có các giải pháp bảo mật mới phù hợp với môi trường ICS.

Môi trường mà các hệ thống ICS và CNTT vận hành luôn thay đổi. Các môi trường hoạt động bao gồm, nhưng không giới hạn ở: không gian đe dọa; lỗ hổng; nhiệm vụ/chức năng kinh doanh; sứ mệnh/quy trình kinh doanh; kiến trúc doanh nghiệp và bảo mật thông tin; công nghệ thông tin; nhân viên; cơ sở; mối quan hệ chuỗi cung ứng; quản trị/văn hóa tổ chức; quy trình mua sắm/mua lại; chính sách/thủ tục của tổ chức; các giả định của tổ chức, các ràng buộc, khả năng chấp nhận rủi ro và các ưu tiên/sự đánh đổi)

Dưới đây liệt kê một số cân nhắc đặc biệt khi xem xét bảo mật cho ICS:

- **Yêu cầu về tính kịp thời và hiệu suất**. ICS nói chung là rất quan trọng về mặt thời gian, với tiêu chí về mức độ trễ và rung hình có thể chấp nhận được do cài đặt riêng lẻ quy định. Một số hệ thống yêu cầu phản ứng xác định, đáng tin cậy. Thông lượng cao thường không cần thiết đối với ICS. Ngược lại, các hệ thống CNTT thường yêu cầu thông lượng cao và chúng thường có thể chịu được một số mức độ trễ và rung. Đối với một số ICS, thời gian phản hồi tự động hoặc phản hồi của hệ thống đối với tương tác của con người là rất quan trọng. Một số ICS được xây dựng trên hệ điều hành thời gian thực (RTOS), trong đó thời gian thực đề cập đến các yêu cầu về tính kịpthời. Các đơn vị thời gian thực phụ thuộc rất nhiều vào ứng dụng và phải được nêu rõ ràng**.**

**- Yêu cầu sẵn có**. Nhiều quy trình ICS có bản chất liên tục. Việc ngừng hoạt động bất ngờ của các hệ thống kiểm soát các quy trình công nghiệp là không thể chấp nhận được. Việc cắt gián đoạn thường phải được lên kế hoạch và lên lịch trước nhiều ngày hoặc nhiều tuần. Thử nghiệm toàn diện trước khi triển khai là điều cần thiết để đảm bảo tính khả dụng cao (nghĩa là độ tin cậy) cho ICS. Các hệ thống điều khiển thường không thể dễ dàng dừng và khởi động mà không ảnh hưởng đến sản xuất. Trong một số trường hợp, các sản phẩm được sản xuất hoặc thiết bị được sử dụng quan trọng hơn thông tin được chuyển tiếp. Do đó, việc sử dụng các chiến lược CNTT điển hình như khởi động lại một thành phần, thường không phải là giải pháp được chấp nhận do tác động bất lợi đến các yêu cầu về tính sẵn sàng cao, độ tin cậy và khả năng bảo trì của ICS. Một số ICS sử dụng các thành phần dự phòng, thường chạy song song, để cung cấp tính liên tục khi các thành phần chính không khả dụng.

- **Yêu cầu quản lý rủi ro.** Trong một hệ thống CNTT điển hình, tính bảo mật và tính toàn vẹn của dữ liệu thường là mối quan tâm chính. Đối với một ICS, sự an toàn của con người và khả năng chịu lỗi để tránh thiệt hại về tính mạng hoặc gây nguy hiểm cho sức khỏe hoặc niềm tin của cộng đồng, tuân thủ quy định, mất thiết bị, mất tài sản trí tuệ hoặc sản phẩm bị mất hoặc hư hỏng là những mối quan tâm chính. Nhân viên chịu trách nhiệm vận hành, bảo mật và duy trì ICS phải hiểu mối liên hệ quan trọng giữa an toàn và bảo mật. Bất kỳ biện pháp an toàn nào làm suy yếu sự an toàn đều không thể chấp nhận được.

**- Hiệu ứng vật lý.** Các thiết bị trường ICS (ví dụ: PLC, trạm vận hành, bộ điều khiển DCS) chịu trách nhiệm trực tiếp cho việc kiểm soát các quy trình vật lý. ICS có thể có những tương tác rất phức tạp với các quá trình vật lý và hậu quả trong miền ICS có thể biểu hiện trong các sự kiện vật lý. Việc hiểu những tác động vật lý tiềm ẩn này thường đòi hỏi phải có sự giao tiếp giữa các chuyên gia trong các hệ thống điều khiển và trong lĩnh vực vật lý cụ thể.

- **Vận hành hệ thống.** Các hệ điều hành ICS (OS) và mạng điều khiển thường khá khác so với các mạng tương ứng CNTT, đòi hỏi các bộ kỹ năng, kinh nghiệm và trình độ chuyên môn khác nhau. Các mạng điều khiển thường được quản lý bởi các kỹ sư điều khiển, không phải nhân viên CNTT. Giả định rằng sự khác biệt không đáng kể có thể gây ra những hậu quả tai hại đối với hoạt động của hệ thống.

- **Ràng buộc tài nguyên.** ICS và hệ điều hành thời gian thực của chúng thường là các hệ thống bị hạn chế về tài nguyên không bao gồm các khả năng bảo mật CNTT hiện đại điển hình. Các hệ thống kế thừa thường thiếu tài nguyên phổ biến trên các hệ thống CNTT hiện đại. Nhiều hệ thống có thể không có các tính năng mong muốn bao gồm khả năng mã hóa, ghi lỗi và bảo vệ bằng mật khẩu. Việc sử dụng bừa bãi các biện pháp bảo mật CNTT trong ICS có thể gây gián đoạn tính khả dụng và thời gian. Có thể không có sẵn tài nguyên máy tính trên các thành phần ICS để trang bị thêm cho các hệ thống này các khả năng bảo mật hiện tại. Việc thêm tài nguyên hoặc tính năng có thể không thực hiện được.

- **Truyền thông.** Các giao thức và phương tiện truyền thông được môi trường ICS sử dụng để điều khiển thiết bị trường và truyền thông trong bộ xử lý thường khác với hầu hết các môi trường CNTT và có thể là tài sản độc quyền.

- **Quản lý thay đổi.** Quản lý thay đổi có tầm quan trọng để duy trì tính toàn vẹn của cả hệ thống CNTT và kiểm soát. Phần mềm chưa được vá đại diện cho một trong những lỗ hổng lớn nhất đối với hệ thống. Các bản cập nhật phần mềm trên hệ thống CNTT, bao gồm các bản vá bảo mật, thường được áp dụng kịp thời dựa trên các thủ tục và chính sách bảo mật phù hợp. Ngoài ra, các quy trình này thường được tự động hóa bằng các công cụ dựa trên máy chủ. Các bản cập nhật phần mềm trên ICS không phải lúc nào cũng được triển khai kịp thời. Các bản cập nhật này cần được kiểm tra kỹ lưỡng bởi cả nhà cung cấp ứng dụng điều khiển công nghiệp và người dùng cuối của ứng dụng trước khi triển khai. Ngoài ra, chủ sở hữu ICS phải lập kế hoạch và lên lịch gián đoạn ICS trước ngày/tuần. ICS cũng có thể yêu cầu xác nhận lại như là một phần của quá trình cập nhật. Một vấn đề khác là nhiều ICS sử dụng các phiên bản cũ hơn của hệ điều hành không còn được nhà cung cấp hỗ trợ. Do đó, các bản vá có sẵn có thể không được áp dụng. Quản lý thay đổi cũng được áp dụng cho phần cứng và phần lõi. Quy trình quản lý thay đổi, khi được áp dụng cho ICS, yêu cầu đánh giá cẩn thận bởi các chuyên gia ICS (ví dụ: kỹ sư kiểm soát) làm việc cùng với nhân viên an toàn và CNTT. Quy trình quản lý thay đổi, khi được áp dụng cho ICS, yêu cầu đánh giá cẩn thận bởi các chuyên gia ICS (ví dụ: kỹ sư kiểm soát) làm việc cùng với nhân viên an toàn và CNTT.

- **Hỗ trợ quản lý.** Các hệ thống CNTT điển hình cho phép các kiểu hỗ trợ đa dạng, có thể hỗ trợ các kiến trúc công nghệ khác nhau nhưng được kết nối với nhau. Đối với ICS, hỗ trợ dịch vụ đôi khi thông qua một nhà cung cấp duy nhất, nhà cung cấp này có thể không có giải pháp hỗ trợ đa dạng và tương tác từ nhà cung cấp khác. Trong một số trường hợp, các giải pháp bảo mật của bên thứ ba không được cấp phép do thỏa thuận dịch vụ và giấy phép của nhà cung cấp ICS và việc mất hỗ trợ dịch vụ có thể xảy ra nếu các ứng dụng của bên thứ ba được cài đặt mà không có xác nhận hoặc phê duyệt của nhà cung cấp.

- **Tuổi thọ thành phần**. Các thành phần CNTT điển hình có tuổi thọ từ 3 đến 5 năm, với thời gian ngắn do sự phát triển nhanh chóng của công nghệ. Đối với ICS nơi công nghệ đã được phát triển trong nhiều trường hợp để sử dụng và triển khai rất cụ thể, vòng đời của công nghệ được triển khai thường theo thứ tự từ 10 đến 15 năm và đôi khi lâu hơn.

- **Vị trí thành phần**. Hầu hết các thành phần CNTT và một số ICS được đặt tại các cơ sở kinh doanh và thương mại có thể tiếp cận được bằng phương tiện giao thông địa phương. Các địa điểm từ xa có thể được sử dụng cho các cơ sở dự phòng. Các thành phần ICS phân tán có thể bị cô lập, từ xa và cần nhiều nỗ lực vận chuyển để tiếp cận. Vị trí thành phần cũng cần xem xét các biện pháp an toàn vật lý và môi trường cần thiết.

|  |  |  |
| --- | --- | --- |
| **Hạng mục** | **Hệ thống công nghệ thông tin** | **Hệ thống điều khiển công nghiệp** |
| **Các yêu cầu thực hiện** | - Phi thời gian thực  - Phản ứng phải nhất quán  - Thông lượng cao được yêu cầu  - Độ trễ và rung cao có thể được chấp nhận  - Tương tác khẩn cấp ít quan trọng hơn  - Kiểm soát truy cập hạn chế chặt chẽ có thể được thực hiện ở mức độ cần thiết để bảo mật | - Thời gian thực  - Phản ứng là thời gian quan trọng  - Thông lượng khiêm tốn có thể chấp nhận được  - Độ trễ cao và/hoặc rung không được chấp nhận  - Ứng phó với con người và tương tác khẩn cấp khác là rất quan trọng  - Quyền truy cập vào ICS phải được kiểm soát chặt chẽ, nhưng không được cản trở hoặc can thiệp vào tương tác giữa người và máy |
| **Yêu cầu về tính khả dụng (độ tin cậy)** | - Các phản hồi như khởi động lại được chấp nhận  - Sự thiếu sót về tính khả dụng thường có thể được chấp nhận, tùy thuộc vào yêu cầu vận hành của hệ thống | - Các phản hồi như khởi động lại có thể không được chấp nhận do các yêu cầu về tính khả dụng của quy trình  - Các yêu cầu về tính khả dụng có thể cần đến các hệ thống dự phòng  - Gián đoạn phải được lên kế hoạch và lên lịch trước ngày/tuần  - Tính sẵn sàng cao yêu cầu thử nghiệm trước khi triển khai đầy đủ |
| **Yêu cầu quản lý rủi ro** | - Quản lý dữ liệu  - Bảo mật và toàn vẹn dữ liệu là có tầm quan trọng  - Khả năng chịu lỗi ít quan trọng hơn – thời gian ngừng hoạt động tạm thời không phải là rủi ro chính  - Tác động rủi ro chính là trì hoãn hoạt động kinh doanh | - Kiểm soát thế giới vật chất  - An toàn con người là trên hết, tiếp theo là bảo vệ quy trình  - Khả năng chịu lỗi là điều cần thiết, thậm chí thời gian ngừng hoạt động tạm thời có thể không được chấp nhận  - Các tác động rủi ro chính là không tuân thủ quy định, tác động môi trường, thiệt hại về người, thiết bị hoặc sản xuất |
| **Vận hành hệ thống** | - Các hệ thống được thiết kế để sử dụng với các hệ điều hành điển hình  - Việc nâng cấp rất đơn giản với sự sẵn có của các công cụ triển khai tự động | - Các hệ điều hành khác nhau và có thể là độc quyền, thường không có khả năng bảo mật được tích hợp sẵn  - Các thay đổi phần mềm phải được thực hiện cẩn thận, thường là bởi các nhà cung cấp phần mềm, do các thuật toán điều khiển chuyên biệt và có thể liên quan đến phần cứng và phần mềm đã được sửa đổi |
| **Hạn chế tài nguyên** | - Các hệ thống được chỉ định với đủ tài nguyên để hỗ trợ bổ sung các ứng dụng của bên thứ ba, chẳng hạn như các giải pháp bảo mật | - Các hệ thống được thiết kế để hỗ trợ quy trình công nghiệp dự kiến và có thể không có đủ bộ nhớ cũng như tài nguyên máy tính để hỗ trợ bổ sung khả năng bảo mật. |
| **Truyền thông** | - Các giao thức truyền thông tiêu chuẩn  - Các mạng có dây chủ yếu với một số khả năng không dây cục bộ  - Thực hành mạng CNTT điển hình | - Nhiều giao thức truyền thông tiêu chuẩn và độc quyền  - Một số loại phương tiện truyền thông được sử dụng bao gồm cả dây và không dây chuyên dụng (radio và vệ tinh)  - Mạng rất phức tạp và đôi khi yêu cầu chuyên môn của các kỹ sư điều khiển |
| **Quản lý thay đổi** | - Các thay đổi phần mềm được áp dụng kịp thời với sự có mặt của các thủ tục và chính sách bảo mật tốt. Các thủ tục thường được tự động hóa | - Các thay đổi phần mềm phải được kiểm tra kỹ lưỡng và triển khai dần dần trong toàn bộ hệ thống để đảm bảo rằng tính toàn vẹn của hệ thống điều khiển được duy trì. Việc gián đoạn ICS thường phải được lên kế hoạch và lên lịch trước nhiều ngày/tuần. ICS có thể sử dụng hệ điều hành không còn được hỗ trợ |
| **Hỗ trợ quản lý** | - Cho phép các kiểu hỗ trợ đa dạng | - Hỗ trợ dịch vụ thường thông qua một nhà cung cấp duy nhất |
| **Tuổi thọ thành phần** | - Tuổi thọ theo thứ tự từ 3 đến 5 năm | - Tuổi thọ theo thứ tự từ 10 đến 15 năm |
| **Vị trí thành phần** | - Các thành phần thường cục bộ và dễ truy cập | - Các thành phần có thể bị cô lập, từ xa và đòi hỏi nhiều nỗ lực vật lý để có quyền truy cập vào chúng |

**Bảng 1. Sự khác biệt về hoạt động và rủi ro giữa các hệ thống ICS và CNTT**

Sự khác biệt về hoạt động và rủi ro giữa các hệ thống ICS và CNTT tạo ra nhu cầu nâng cao mức độ phức tạp trong việc áp dụng các chiến lược vận hành và an toàn mạng. Một nhóm đa chức năng bao gồm các kỹ sư điều khiển, người vận hành hệ thống điều khiển và chuyên gia bảo mật CNTT cần phải hợp tác chặt chẽ để hiểu những tác động có thể có của việc cài đặt, vận hành và bảo trì các giải pháp bảo mật cùng với hoạt động của hệ thống điều khiển. Các chuyên gia CNTT làm việc với ICS cần hiểu tác động về độ tin cậy của các công nghệ bảo mật thông tin trước khi triển khai. Một số OS và ứng dụng chạy trên ICS có thể không hoạt động chính xác với các giải pháp an toàn mạng CNTT có sẵn trên thị trường (COTS) do kiến trúc môi trường ICS chuyên biệt.

* + 1. Các loại hệ thống điều khiển khác

Mặc dù báo cáo này nghiên cứu về bảo đảm an toàn cho hệ thống điều khiển công nghiệp ICS, nhưng các loại hệ thống kiểm soát khác cũng có các đặc điểm tương tự và nhiều khuyến nghị từ hướng dẫn này có thể áp dụng và có thể được sử dụng làm tài liệu tham khảo để bảo vệ các hệ thống đó trước các mối đe dọa an toàn mạng. Ví dụ, mặc dù nhiều hệ thống tòa nhà, giao thông, y tế, an toàn và hậu cần sử dụng các giao thức, cổng và dịch vụ khác nhau, đồng thời được định cấu hình và vận hành ở các chế độ khác với ICS, nhưng chúng có chung các đặc điểm với ICS truyền thống. Ví dụ về một số hệ thống và giao thức này bao gồm:

Các loại hệ thống điều khiển khác

* Hệ thống đo lường tiên tiến
* Hệ thống xây dựng tự động hoá
* Hệ thống điều khiển quản lý xây dựng
* Hệ thống giám sát truyền hình mạch kín
* Giám sát CO2
* Hệ thống biển báo kỹ thuật số
* Hệ thống quản lý video kỹ thuật số
* Hệ thống bảo mật điện tử
* Hệ thống quản lý khẩn cấp
* Hệ thống quản lý năng lượng.
* Hệ thống điều khiển chiếu sáng ngoại thất.
* Hệ thống báo cháy.
* Hệ thống phun nước chữa cháy.
* Hệ thống điều khiển chiếu sáng nội thất.
* Hệ thống phát hiện xâm nhập.
* Hệ thống kiểm soát truy cập vật lý.
* An toàn công cộng/Bộ đàm di động mặt đất.
* Hệ thống địa nhiệt năng lượng tái tạo.
* Hệ thống điện ảnh năng lượng tái tạo.
* Hệ thống kiểm soát vùng tối.
* Hệ thống hút và thanh lọc.
* Hệ thống Giao thông thẳng đứng (Thang máy và Thang cuốn).
* Hệ thống điều khiển dụng cụ phòng thí nghiệm.
* Hệ thống quản lý thông tin phòng thí nghiệm (LIMS).

Giao thức/Cổng và Dịch vụ

* Modbus: Master/Slave - Cổng 502.
* BACnet2: Master/Slave – Cổng 47808.
* LonWorks/LonTalk3: Đồng đẳng - Cổng 1679.
* DNP3: Master/Slave – Cổng 19999 khi sử dụng Bảo mật Tầng Vận tải (TLS), Cổng 20000 khi không sử dụng TLS.
* IEEE 802.x – Đồng đẳng.
* ZigBee – Đồng đẳng.
* Bluetooth – Master/Slave

Không có “một kích thước phù hợp với tất cả” và các rủi ro có thể không giống nhau, ngay cả trong một nhóm cụ thể. Ví dụ, một tòa nhà có nhiều hệ thống phụ khác nhau như tự động hóa tòa nhà, báo cháy, kiểm soát truy cập vật lý, biển báo kỹ thuật số, camera quan sát, v.v. Các hệ thống an toàn tính mạng quan trọng như hệ thống báo cháy và kiểm soát ra vào vật lý có thể khiến mức độ tác động ở mức “Cao”, trong khi các hệ thống khác thường ở mức “Thấp”. Một tổ chức có thể quyết định đánh giá từng hệ thống con riêng lẻ hoặc quyết định sử dụng phương pháp tổng hợp. Việc đánh giá hệ thống kiểm soát phải được kết hợp với Tác động kinh doanh, Kế hoạch dự phòng và Kế hoạch ứng phó sự cố để đảm bảo các chức năng và hoạt động quan trọng của tổ chức có thể được phục hồi và khôi phục như được xác định bởi Mục tiêu thời gian phục hồi của tổ chức.

5.2 Đánh giá và quản lý rủi ro cho các hệ thống điều khiển công nghiệp ICS

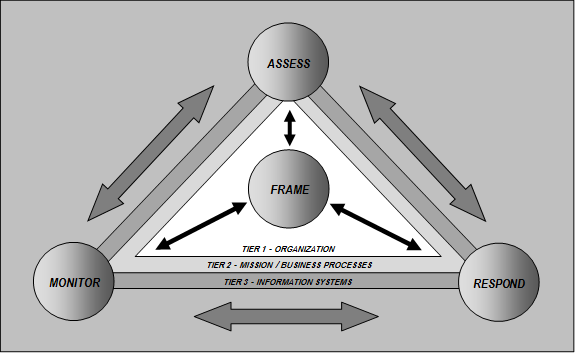
5.2.1 Quản lý rủi ro

Các tổ chức quản lý rủi ro hàng ngày để đáp ứng các mục tiêu kinh doanh của họ. Những rủi ro này có thể bao gồm rủi ro tài chính, rủi ro hỏng hóc thiết bị và rủi ro về an toàn nhân sự, đó chỉ là một số rủi ro. Các tổ chức phải phát triển các quy trình để đánh giá rủi ro liên quan đến hoạt động kinh doanh của họ và quyết định cách giải quyết những rủi ro đó dựa trên các ưu tiên của tổ chức cũng như các ràng buộc bên trong và bên ngoài. Việc quản lý rủi ro này được tiến hành như một quá trình tương tác, liên tục như một phần của vận hành bình thường. Các tổ chức sử dụng ICS có lịch sử quản lý rủi ro thông qua các thông lệ tốt về an toàn và kỹ thuật. Đánh giá an toàn được thiết lập tốt trong hầu hết các lĩnh vực và thường được đưa vào các yêu cầu quy định. Quản lý rủi ro an toàn thông tin là một khía cạnh bổ sung có thể bổ sung. Quy trình và khuôn khổ quản lý rủi ro được nêu trong phần này có thể được áp dụng cho mọi đánh giá rủi ro bao gồm cả an toàn và bảo mật thông tin. Quy trình quản lý rủi ro nên được triển khai trong toàn bộ tổ chức, sử dụng cách tiếp cận ba tầng để giải quyết rủi ro ở (i) cấp độ tổ chức; (ii) nhiệm vụ/cấp độ quy trình nghiệp vụ; và (iii) cấp độ hệ thống thông tin (CNTT và ICS). Quy trình quản lý rủi ro được thực hiện liền mạch trên ba cấp độ với mục tiêu tổng thể là cải tiến liên tục các hoạt động liên quan đến rủi ro của tổ chức và giao tiếp giữa các cấp độ và nội bộ hiểu quả giữa tất cả các chủ sở hữu tầng có chung mối quan tâm đến sứ mệnh/ thành công kinh doanh của tổ chức.

Phần này tập trung chủ yếu vào các yêu cầu cho ICS ở cấp hệ thống thông tin, tuy nhiên, điều quan trọng cần lưu ý là các hoạt động, thông tin và hiện vật quản lý rủi ro ở mỗi cấp tác động và thông báo cho các cấp khác. Phần 6 mở rộng các khái niệm được trình bày ở đây đến cấp độ hệ thồn kiểm soát và cung cấp các khuyến nghị dành riêng cho ICS để tăng cường các hệ thống kiểm soát an toàn.

5.2.2 Giới thiệu về quy trình quản lý rủi ro

Như trong Hình 9, quy trình quản lý rủi ro có bốn thành phần: định khung, đánh giá, phản hồi và giám sát. Các hoạt động này phụ thuộc lẫn nhau và thường xảy ra đồng thời trong một tổ chức. Ví dụ: kết quả của thành phần giám sát sẽ được đưa vào thành phần tạo khung. Vì môi trường mà các tổ chức hoạt động luôn thay đổi, nên quản lý rủi ro phải là một quá trình liên tục trong đó tất cả các thành phần đều phải hoạt động liên tục. Điều quan trọng cần nhớ là các thành phần này áp dụng cho việc quản lý mọi rủi ro dù là bảo mật thông tin, bảo mật vật lý, an toàn hay tài chính.



**Hình 9. Quy trình quản lý rủi ro áp dụng xuyên suốt các tầng**

Thành phần khung trong quy trình quản lý rủi ro bao gồm phát triển một khuôn khổ cho các quyết định quản lý rủi ro được đưa ra. Mức độ rủi ro mà tổ chức sẵn sàng chấp nhận chính là khả năng chịu rủi ro của tổ chức.

Thành phần khung nên bao gồm việc xem xét các tài liệu hiện có, chẳng hạn như các đánh giá rủi ro trước đó. Có thể có các hoạt động liên quan; chẳng hạn như lập kế hoạch quản lý thảm họa trên toàn cộng đồng cũng cần được xem xét vì chúng tác động đến các yêu cầu mà đánh giá rủi ro phải xem xét.

***Khuyến nghị và hướng dẫn dành riêng cho ICS:***

Đối với những người vận hành ICS, an toàn là sự cân nhắc chính ảnh hưởng trực tiếp đến các quyết định về cách thiết kế và vận hành hệ thống. An toàn có thể được định nghĩa là “không bị ảnh hưởng bởi các điều kiện có thể gây tử vong, thương tích, bệnh nghề nghiệp, hư hỏng hoặc mất mát thiết bị hoặc tài sản hoặc thiệt hại cho môi trường.” Một phần của thành phần khung cho một tổ chức ICS đang xác định cách các yêu cầu này tương tác với bảo mật thông tin.Ví dụ, nếu những yêu cầu an toàn mâu thuẫn với thực hành bảo mật tốt, tổ chức sẽ quyết định như thế nào giữa hai sự ưu tiên? Hầu hết các nhà khai thác ICS sẽ trả lời rằng an toàn là mối quan tâm chính – thành phần định khung đưa ra các giả định như vậy một cách rõ ràng để có sự thống nhất trong suốt quá trình và tổ chức.

Một mối quan tâm lớn khác đối với các nhà khai thác ICS là sự sẵn có của các dịch vụ do ICS cung cấp. ICS có thể là một phần của cơ sở hạ tầng quan trọng (ví dụ: hệ thống nước hoặc điện), nơi có nhu cầu đáng kể về hoạt động liên tục và đáng tin cậy. Do đó, ICS có thể có các yêu cầu nghiêm ngặt về tính khả dụng hoặc khả năng phục hồi. Những giả định như vậy nên được phát triển và nêu trong thành phần khung. Nếu không, tổ chức có thể đưa ra các quyết định rủi ro dẫn đến hậu quả không lường trước được đối với những người phụ thuộc vào các dịch vụ được cung cấp.

Môi trường hoạt động vật lý là một khía cạnh khác của khung rủi ro mà các tổ chức nên xem xét khi làm việc với ICS. ICS thường có các yêu cầu cụ thể về môi trường (ví dụ: quy trình sản xuất có thể yêu cầu nhiệt độ chính xác) hoặc chúng có thể bị ràng buộc với môi trường vật lý để vận hành. Các yêu cầu và ràng buộc như vậy cần được nêu rõ ràng trong thành phần khung để các rủi ro phát sinh từ các ràng buộc này có thể được xác định và xem xét.

*Đánh giá rủi ro* yêu cầu các tổ chức xác định các mối đe dọa và lỗ hổng của họ, tác hại mà các mối đe dọa và lỗ hổng đó có thể gây ra cho tổ chức và khả năng các sự kiện bất lợi phát sinh từ các mối đe dọa và lỗ hổng đó có thể thực sự xảy ra.

*Thành phần ứng phó* dựa trên khái niệm về phản ứng nhất quán trên toàn tổ chức đối với việc xác định rủi ro. Ứng phó với việc xác định rủi ro (trái ngược với ứng phó với sự cố) yêu cầu tổ chức trước tiên xác định các chuỗi hành động khả thi để giải quyết rủi ro, đánh giá các khả năng đó dựa trên khả năng chấp nhận rủi ro của tổ chức và các cân nhắc khác được xác định trong bước định khung và chọn phương án tốt nhất cho tổ chức. Thành phần phản hồi bao gồm việc triển khai quá trình hành động đã chọn để giải quyết rủi ro đã xác định: chấp nhận, tránh, giảm thiểu, đóng góp, chuyển giao hoặc bất kỳ sự kết hợp nào của các tùy chọn đó.

*Giám sát* là thành phần thứ tư của các hoạt động quản lý rủi ro. Các tổ chức phải giám sát rủi ro trên cơ sở liên tục bao gồm: việc thực hiện các chiến lược quản lý rủi ro đã chọn; những thay đổi trong môi trường có thể ảnh hưởng đến việc tính toán rủi ro; và, hiệu lực và hiệu quả của các hoạt động giảm thiểu rủi ro. Các hoạt động trong thành phần giám sát tác động đến tất cả các thành phần khác

5.2.3 Cân nhắc đặc biệt khi thực hiện đánh giá rủi ro

Bản chất của ICS có nghĩa là khi một tổ chức thực hiện đánh giá rủi ro, có thể có các cân nhắc bổ sung không tồn tại khi thực hiện đánh giá rủi ro của hệ thống CNTT truyền thống. Vì tác động của sự cố mạng trong ICS có thể bao gồm cả tác động vật lý và kỹ thuật số, nên các đánh giá rủi ro cần kết hợp các tác động tiềm ẩn đó. Phần này sẽ cung cấp một kiểm tra sâu hơn về những điều sau đây:

* Tác động đến an toàn và sử dụng các đánh giá an toàn
* Tác động vật lý của sự cố mạng đối với ICS, bao gồm cả môi trường vật lý lớn hơn; tác động lên quá trình được kiểm soát và tác động vật lý lên chính ICS.
* Hậu quả đối với việc đánh giá rủi ro của các thành phần kiểm soát phi kỹ thuật số trong một ICS.

5.2.4 An toàn trong đánh giá rủi ro bảo mật thông tin ICS

Các đánh giá rủi ro an toàn thông tin nên được coi là bổ sung cho các đánh giá đó mặc dù các đánh giá có thể sử dụng các cách tiếp cận khác nhau và bao gồm các lĩnh vực khác nhau. Đánh giá an toàn chủ yếu liên quan đến thế giới vật lý. Đánh giá rủi ro bảo mật thông tin chủ yếu nhìn vào thế giới kỹ thuật số. Tuy nhiên, trong môi trường ICS, vật lý và kỹ thuật số được kết hợp với nhau và có thể xảy ra sự chồng chéo đáng kể.

Điều quan trọng là các tổ chức phải xem xét tất cả các khía cạnh của quản lý rủi ro để đảm bảo an toàn (ví dụ: khung rủi ro, khả năng chấp nhận rủi ro), cũng như kết quả đánh giá an toàn, khi thực hiện đánh giá rủi ro đối với bảo mật thông tin. Nhân viên chịu trách nhiệm đánh giá rủi ro an toàn thông tin phải có khả năng xác định và truyền đạt các rủi ro đã xác định có thể ảnh hưởng đến an toàn. Ngược lại, nhân viên chịu trách nhiệm đánh giá an toàn phải quen thuộc với các tác động vật lý tiềm ẩn và khả năng xảy ra của chúng bởi quy trình đánh giá rủi ro an toàn thông tin.

5.2.5 Tác động vật lý tiềm tàng của một sự cố ICS

Đánh giá thiệt hại vật chất tiềm ẩn từ sự cố mạng nên kết hợp: i) cách thức một sự cố có thể thao túng hoạt động của các cảm biến và cơ cấu chấp hành để tác động đến môi trường vật lý; ii) những biện pháp kiểm soát dự phòng nào tồn tại trong ICS để ngăn chặn tác động; và iii) làm thế nào một sự cố vật lý có thể xuất hiện dựa trên những điều kiện này.Một tác động vật lý có thể tác động tiêu cực đến thế giới xung quanh thông qua nhiều phương tiện, bao gồm giải phóng các vật liệu nguy hiểm (ví dụ: ô nhiễm, dầu thô), gây tổn hại cho các lực động học (ví dụ: vụ nổ) và tiếp xúc với các nguồn năng lượng (ví dụ: điện, hơi nước). Sự cố vật lý có thể tác động tiêu cực đến ICS và cơ sở hạ tầng hỗ trợ, các quy trình khác nhau do ICS thực hiện hoặc môi trường vật lý rộng lớn hơn. Việc đánh giá các tác động vật lý tiềm ẩn phải bao gồm tất cả các bộ phận của ICS, bắt đầu bằng việc đánh giá các tác động tiềm ẩn đối với bộ cảm biến và cơ cấu chấp hành. Mỗi lĩnh vực này sẽ được mở rộng thêm dưới đây.

Đánh giá tác động của sự cố mạng đối với môi trường vật lý nên tập trung vào thiệt hại tiềm ẩn đối với sự an toàn của con người, môi trường tự nhiên và các cơ sở hạ tầng quan trọng khác. Các tác động an toàn của con người nên được đánh giá dựa trên việc liệu có thể xảy ra thương tích, bệnh tật hoặc tử vong do sự cố của ICS hay không. Điều này nên kết hợp mọi đánh giá tác động an toàn đã thực hiện trước đó do tổ chức thực hiện liên quan đến cả nhân viên và công chúng. Tác động môi trường cũng có thể cần phải được giải quyết. Phân tích này nên kết hợp mọi đánh giá tác động môi trường sẵn có do tổ chức thực hiện để xác định xem một sự cố có thể tác động như thế nào đến tài nguyên thiên nhiên và động vật hoang dã trong ngắn hạn hoặc dài hạn. Ngoài ra, cần lưu ý rằng ICS có thể không được đặt trong một địa điểm được kiểm soát, duy nhất và có thể được phân phối trên một khu vực vật lý rộng và tiếp xúc với môi trường không được kiểm soát. Cuối cùng, tác động đối với môi trường vật lý sẽ mở rộng mức độ mà một sự cố có thể làm hỏng cơ sở hạ tầng bên ngoài ICS (ví dụ: sản xuất/phân phối điện, cơ sở hạ tầng giao thông và dịch vụ nước)

5.2.6 Tác động vật lý gián đoạn quy trình ICS

Ngoài tác động đối với môi trường vật lý, đánh giá rủi ro cũng nên ước lượng các tác động tiềm ẩn đối với quy trình vật lý do ICS thực hiện đang được xem xét, cũng như các hệ thống khác. Một sự cố tác động đến ICS và làm gián đoạn quy trình phụ thuộc có thể gây ra tác động theo tầng đến các quy trình ICS liên quan khác và sự phụ thuộc của công chúng vào các sản phẩm và dịch vụ tạo ra. Tác động đến các quy trình ICS liên quan có thể bao gồm cả hệ thống và quy trình trong tổ chức (ví dụ: một quy trình sản xuất phụ thuộc vào quy trình được kiểm soát bởi hệ thống đang được xem xét) hoặc các hệ thống và quy trình bên ngoài tổ chức (ví dụ: một tiện ích bán năng lượng được tạo ra cho một nhà máy gần đó)

Một sự cố mạng cũng có thể tác động tiêu cực đến ICS vật lý được xem xét. Loại tác động này chủ yếu bao gồm cơ sở hạ tầng vật chất của nhà máy (ví dụ: bể chứa, van, động cơ), cùng với cả cơ chế điều khiển kỹ thuật số và phi kỹ thuật số (ví dụ: dây cáp, PLC, đồng hồ đo áp suất). Thiệt hại đối với ICS hoặc nhà máy vật lý có thể gây ra mất điện ngắn hạn hoặc dài hạn tùy thuộc vào mức độ của sự cố. Một ví dụ về sự cố mạng ảnh hưởng đến ICS là phần mềm độc hại Stuxnet, phần mềm độc hại này đã gây ra thiệt hại vật chất cho máy ly tâm cũng như làm gián đoạn các quy trình phụ thuộc.

5.2.7 Kết hợp các khía cạnh phi kỹ thuật số của ICS vào đánh giá tác động

Không thể xác định đầy đủ các tác động đối với ICS bằng cách chỉ tập trung vào các khía cạnh kỹ thuật số của hệ thống, vì thường có sẵn các cơ chế phi kỹ thuật số cung cấp khả năng chịu lỗi và ngăn ICS hoạt động ngoài các thông số có thể chấp nhận được. Do đó, các cơ chế này có thể giúp giảm bất kỳ tác động tiêu cực nào mà sự cố kỹ thuật số trên ICS có thể gây ra và phải được đưa vào quy trình đánh giá rủi ro. Ví dụ: ICS thường có các cơ chế kiểm soát phi kỹ thuật số có thể ngăn ICS hoạt động bên ngoài ranh giới an toàn và do đó hạn chế tác động của một cuộc tấn công (ví dụ: van giảm áp cơ học). Ngoài ra, các cơ chế tương tự (ví dụ: đồng hồ đo, báo động) có thể được sử dụng để quan sát trạng thái hệ thống vật lý nhằm cung cấp cho người vận hành dữ liệu đáng tin cậy nếu các chỉ số kỹ thuật số không khả dụng hoặc bị hỏng. Bảng 2 cung cấp phân loại các cơ chế kiểm soát phi kỹ thuật số có thể có sẵn để giảm tác động của sự cố ICS**.**

|  |  |
| --- | --- |
| **Loại hệ thống** | **Mô tả** |
| Hiển thị tương tự hoặc báo động | Các cơ chế phi kỹ thuật số đo lường và hiển thị trạng thái của hệ thống vật lý (ví dụ: nhiệt độ, áp suất, điện áp, dòng điện) và có thể cung cấp cho người vận hành thông tin chính xác trong các tình huống khi màn hình kỹ thuật số không khả dụng hoặc bị hỏng. Thông tin có thể được cung cấp cho người vận hành trên một số màn hình phi kỹ thuật số (ví dụ: nhiệt kế, đồng hồ đo áp suất) và thông qua báo động âm thanh. |
| Cơ chế điều khiển thủ công | Các cơ chế điều khiển thủ công (ví dụ: điều khiển van thủ công, công tắc cầu dao vật lý) cung cấp cho người vận hành khả năng điều khiển thủ công bộ truyền động mà không cần dựa vào hệ thống điều khiển kỹ thuật số. Điều này đảm bảo rằng bộ truyền động có thể được điều khiển ngay cả khi hệ thống điều khiển không khả dụng hoặc bị xâm phạm. |
| Hệ thống điều khiển tương tự | Các hệ thống điều khiển tương tự sử dụng các cảm biến và bộ truyền động phi kỹ thuật số để theo dõi và kiểm soát một quá trình vật lý. Những thứ này có thể ngăn quá trình vật lý đi vào trạng thái không mong muốn trong các tình huống khi hệ thống điều khiển kỹ thuật số không khả dụng hoặc bị hỏng. Điều khiển tương tự bao gồm các thiết bị như bộ điều chỉnh, bộ điều tốc và rơle điện cơ. |

**Bảng 2. Cung cấp phân loại các cơ chế kiểm soát phi kỹ thuật số có thể có sẵn để giảm tác động của sự cố ICS**

Việc xác định tác động tiềm tàng mà một sự cố mạng có thể gây ra đối với ICS nên kết hợp phân tích tất cả các cơ chế kiểm soát phi kỹ thuật số và mức độ mà chúng có thể giảm thiểu tác động tiêu cực tiềm ẩn đối với ICS. Có nhiều cân nhắc khi xem xét các tác động giảm thiểu có thể có của các cơ chế kiểm soát phi kỹ thuật số, chẳng hạn như:

- Các cơ chế kiểm soát phi kỹ thuật số có thể cần thêm thời gian và sự tham gia của con người để thực hiện các chức năng giám sát hoặc kiểm soát cần thiết và những nỗ lực này có thể là đáng kể. Ví dụ, các cơ chế như vậy có thể yêu cầu người vận hành di chuyển đến một địa điểm từ xa để thực hiện các chức năng điều khiển nhất định. Các cơ chế như vậy cũng có thể phụ thuộc vào thời gian phản hồi của con người, có thể chậm hơn so với các biện pháp kiểm soát tự động.

- Các hệ thống thủ công và tương tự có thể không cung cấp khả năng giám sát hoặc điều khiển với cùng mức độ chính xác và độ tin cậy như hệ thống điều khiển kỹ thuật số. Điều này có thể gây rủi ro nếu hệ thống điều khiển chính không khả dụng hoặc bị hỏng do giảm chất lượng, an toàn hoặc hiệu quả của hệ thống. Ví dụ: rơle bảo vệ kỹ thuật số/kỹ thuật số cung cấp khả năng phát hiện lỗi chính xác và đáng tin cậy hơn so với rơle tương tự/tĩnh, do đó, hệ thống có nhiều khả năng bị ngắt rơle giả nếu không có rơle kỹ thuật số.

5.2.8 Kết hợp tác động của các hệ thống an toàn

Các hệ thống an toàn cũng có thể làm giảm tác động của sự cố mạng đối với ICS. Các hệ thống an toàn thường được triển khai để thực hiện các chức năng giám sát và kiểm soát cụ thể nhằm đảm bảo an toàn cho con người, môi trường, quy trình và ICS. Mặc dù các hệ thống này được triển khai theo truyền thống để dự phòng hoàn toàn đối với ICS chính, nhưng chúng có thể không cung cấp dự phòng hoàn toàn trước các sự cố mạng, đặc biệt là từ một kẻ tấn công tinh vi. Tác động của các biện pháp kiểm soát an toàn được triển khai đối với hệ thống an toàn cần được đánh giá để xác định rằng chúng không tác động tiêu cực đến hệ thống.

5.2.9 Xem xét việc lan truyền tác động đến các hệ thống được kết nối.

Việc đánh giá tác động của một sự cố cũng phải kết hợp tác động từ việc làm thế nào tác động từ ICS có thể lan truyền đến một ICS được kết nối hoặc hệ thống vật lý. Một ICS có thể được kết nối với các hệ thống khác, do đó các lỗi trong một hệ thống hoặc quy trình có thể dễ dàng chuyển sang các hệ thống khác bên trong hoặc bên ngoài tổ chức. Sự lan truyền tác động có thể xảy ra do cả sự phụ thuộc về mặt vật lý và logic. Giao tiếp riêng về kết quả đánh giá rủi ro cho người vận hành các hệ thống và quy trình được kết nối hoặc phụ thuộc lẫn nhau là một cách để giảm thiểu các tác động đó.

Thiệt hại logic đối với ICS được kết nối với nhau có thể xảy ra nếu sự cố mạng lan đến các hệ thống điều khiển được kết nối. Một ví dụ có thể là nếu vi-rút hoặc sâu lan truyền đến ICS được kết nối và sau đó tác động đến hệ thống đó. Thiệt hại vật chất cũng có thể lan sang các ICS khác được kết nối với nhau. Nếu một sự cố tác động đến môi trường vật lý của ICS, thì nó cũng có thể tác động đến các miền vật lý liên quan khác. Ví dụ, tác động có thể dẫn đến nguy cơ vật chất làm suy giảm môi trường vật chất lân cận. Ngoài ra, sự tác động cũng có thể làm suy giảm các phụ thuộc được chia sẻ phổ biến (ví dụ: nguồn điện) hoặc dẫn đến tình trạng thiếu nguyên liệu cần thiết cho giai đoạn sau trong quy trình công nghiệp.

5.3 Quản lý vận hành bảo đảm an toàn thông tin cho các hệ thống điều khiển công nghiệp ICS

5.3.1 Trường hợp áp dụng cho các tổ chức kinh doanh về bảo mật

Bước đầu tiên trong việc triển khai chương trình bảo mật thông tin cho ICS là phát triển một trường hợp kinh doanh hấp dẫn cho các nhu cầu riêng của tổ chức. Trường hợp kinh doanh nên nắm bắt được mối quan tâm kinh doanh của quản lý cấp cao trong khi được thành lập dựa trên kinh nghiệm của những người đã đối phó với nhiều rủi ro tương tự. Trường hợp kinh doanh cung cấp ảnh hưởng kinh doanh và biện minh tài chính để tạo ra một chương trình bảo mật thông tin tích hợp. Nó nên bao gồm thông tin chi tiết về những điều sau đây:

- Các lợi ích, bao gồm độ tin cậy và tính khả dụng của hệ thống kiểm soát được cải thiện, khi tạo một chương trình bảo mật tích hợp.

- Chi phí tiềm năng được ưu tiên và các tình huống thiệt hại nếu chương trình bảo mật thông tin cho ICS không được triển khai.

- Tổng quan cấp cao về quy trình cần thiết để thực hiện, vận hành, giám sát, xem xét, duy trì và cải thiện chương trình bảo mật thông tin.

- Chi phí và nguồn lực cần thiết để phát triển, triển khai và duy trì chương trình bảo mật.

Trước khi trình bày trường hợp kinh doanh cho ban quản lý, cần có một kế hoạch chi phí và triển khai bảo mật được cân nhắc kỹ lưỡng và phát triển. Ví dụ: chỉ yêu cầu tường lửa là không đủ.

5.3.1.1 Lợi ích

Chính sách quản lý rủi ro có trách nhiệm quy định rằng mối đe dọa đối với ICS phải được đo lường và giám sát để bảo vệ lợi ích của nhân viên, công chúng, cổ đông, khách hàng, nhà cung cấp, xã hội và quốc gia. Phân tích rủi ro cho phép cân nhắc chi phí và lợi ích để có thể đưa ra các quyết định sáng suốt về các hành động bảo vệ. Ngoài việc giảm thiểu rủi ro, việc thực hiện thẩm định và thể hiện trách nhiệm cũng giúp các tổ chức bằng cách:

- Cải thiện độ an toàn, độ tin cậy và tính sẵn sàng của hệ thống điều khiển.

- Cải thiện tinh thần, lòng trung thành và giữ chân nhân viên.

- Giảm mối quan tâm của cộng đồng.

- Gia tăng niềm tin của nhà đầu tư.

- Giảm trách nhiệm pháp lý.

- Đáp ứng yêu cầu quy định.

- Nâng cao hình ảnh và uy tín của công ty.

- Hỗ trợ bảo hiểm và chi phí

- Cải thiện quan hệ nhà đầu tư và ngân hàng.

Một chương trình quản lý an toàn và bảo mật thông tin mạnh mẽ là nền tảng cho một mô hình kinh doanh bền vững.

Các chính sách cải thiện hệ thống bảo mật kiểm soát và bảo mật hệ thống kiểm soát an toàn cụ thể có khả năng nâng cao độ tin cậy và tính khả dụng của hệ thống điều khiển. Điều này cũng bao gồm việc giảm thiểu các tác động bảo mật thông tin hệ thống kiểm soát không chủ ý do thử nghiệm, chính sách và hệ thống bị định cấu hình sai không phù hợp.

5.3.1.2 Hậu quả tiềm tàng

Tầm quan trọng của các hệ thống an toàn cần được nhấn mạnh hơn nữa khi sự phụ thuộc của doanh nghiệp vào khả năng kết nối ngày càng tăng. Các cuộc tấn công từ chối dịch vụ (DoS) và phần mềm độc hại (ví dụ: sâu, vi rút) đã trở nên quá phổ biến và đã ảnh hưởng đến ICS. Các cuộc tấn công mạng có thể có tác động vật lý và hậu quả đáng kể. Quản lý rủi ro được đề cập trong Phần 3. Các loại tác động chính như sau:

- **Tác động vật lý**. Các tác động vật lý bao gồm tập hợp các hậu quả trực tiếp của sự cố ICS. Các tác động tiềm ẩn hết sức quan trọng bao gồm thương tích cá nhân và mất mạng. Các tác động khác bao gồm mất tài sản (bao gồm cả dữ liệu) và thiệt hại tiềm ẩn đối với môi trường.

- **Tác động kinh tế**. Tác động kinh tế là tác động bậc hai từ các tác động vật lý phát sinh từ sự cố ICS. Các tác động vật lý có thể dẫn đến hậu quả đối với hoạt động của hệ thống, từ đó gây ra tổn thất kinh tế lớn hơn cho cơ sở, tổ chức hoặc những người khác phụ thuộc vào ICS. Không có sẵn cơ sở hạ tầng quan trọng (ví dụ: điện, giao thông vận tải) có thể có tác động kinh tế vượt xa các hệ thống chịu thiệt hại trực tiếp và vật chất. Những tác động này có thể tác động tiêu cực đến nền kinh tế địa phương, khu vực, quốc gia hoặc có thể là toàn cầu.

- **Tác động xã hội**. Một tác động cấp hai khác, hậu quả của việc mất niềm tin của quốc gia hoặc công chúng vào một tổ chức, thường bị bỏ qua. Tuy nhiên, đó là một hậu quả rất thực tế có thể xảy ra do sự cố ICS.

5.3.1.3 Nguồn lực để xây dựng tình huống kinh doanh

Các nguồn thông tin quan trọng để giúp hình thành một trường hợp kinh doanh có thể được tìm thấy trong các nguồn bên ngoài trong các tổ chức khác trong các ngành kinh doanh tương tự–cá nhân hoặc trong các trao đổi chia sẻ thông tin, các tổ chức thương mại và tiêu chuẩn, các công ty tư vấn–và các nguồn nội bộ trong các chương trình hoặc chương trình quản lý rủi ro có liên quan kỹ thuật và vận hành. Các tổ chức bên ngoài thường có thể cung cấp những lời khuyên hữu ích về những yếu tố nào ảnh hưởng mạnh mẽ nhất đến ban quản lý để hỗ trợ những nỗ lực của họ và những nguồn lực nào trong tổ chức của họ chứng tỏ ra hữu ích nhất. Đối với các ngành khác nhau, các yếu tố này có thể khác nhau, nhưng có thể có những điểm tương đồng về vai trò mà các chuyên gia quản lý rủi ro khác có thể đảm nhận.

Các nguồn lực nội bộ trong các nỗ lực quản lý rủi ro liên quan (ví dụ: bảo mật thông tin, rủi ro về sức khỏe, an toàn và môi trường, bảo mật vật lý, tính liên tục của doanh nghiệp) có thể cung cấp hỗ trợ to lớn dựa trên kinh nghiệm của họ với các sự cố liên quan trong tổ chức. Thông tin này hữu ích từ quan điểm ưu tiên các mối đe dọa và ước tính tác động kinh doanh. Những tài nguyên này cũng có thể cung cấp thông tin chi tiết về việc người quản lý nào đang tập trung vào việc giải quyết những rủi ro nào và do đó, người quản lý nào có thể phù hợp nhất hoặc dễ tiếp nhận vai trò người hỗ trợ nhất. Tài nguyên nội bộ trong kỹ thuật và vận hành hệ thống kiểm soát có thể cung cấp thông tin chi tiết về cách hệ thống kiểm soát được triển khai trong tổ chức, chẳng hạn như sau:

- Cách các mạng thường được phân vùng và tách biệt.

- Những kết nối truy cập từ xa nào thường được sử dụng.

- Hệ thống kiểm soát rủi ro cao hoặc hệ thống thiết bị an toàn thường được thiết kế như thế nào.

- Những biện pháp đối phó an toàn thường được sử dụng.

5.3.1.4 Trình bày tình huống kinh doanh với bộ phận lãnh đạo

Phần 3 mô tả cách tiếp cận ba tầng giải quyết rủi ro ở: (i) cấp độ tổ chức; (ii) cấp độ nhiệm vụ/quy trình kinh doanh; và (iii) cấp độ hệ thống thông tin. Quá trình quản lý rủi ro được thực hiện liền mạch trên ba cấp độ với mục tiêu tổng thể là cải tiến liên tục các hoạt động liên quan đến rủi ro của tổ chức và trao đổi thông tin hiệu quả giữa các cấp độ và nội bộ giữa tất cả các bên liên quan có lợi ích chung đối với sứ mệnh/sự thành công trong kinh doanh của tổ chức.

Điều quan trọng đối với sự thành công của chương trình bảo mật ICS là ban quản lý cấp tổ chức đồng ý và tham gia vào chương trình bảo mật ICS. Cấp quản lý cấp tổ chức bậc 1 bao gồm cả hoạt động CNTT và ICS có quan điểm và thẩm quyền để hiểu và chịu trách nhiệm về các rủi ro.

Lãnh đạo bậc 1 của doanh nghiệp sẽ chịu trách nhiệm phê duyệt và thúc đẩy các chính sách bảo mật thông tin, phân công vai trò và trách nhiệm bảo mật cũng như triển khai chương trình bảo mật thông tin trong toàn tổ chức. Tài trợ cho toàn bộ chương trình thường có thể được thực hiện theo từng giai đoạn. Mặc dù có thể cần một số kinh phí để bắt đầu hoạt động bảo mật thông tin, nhưng có thể nhận thêm kinh phí sau này vì các lỗ hổng bảo mật và nhu cầu của chương trình được hiểu rõ hơn và các chiến lược bổ sung được phát triển. Ngoài ra, các chi phí (cả trực tiếp và gián tiếp) nên được xem xét để trang bị thêm ICS để bảo mật so với bắt đầu với giải quyết bảo mật.

Thông thường, một cách tiếp cận tốt để có được sự ủng hộ của ban quản lý nhằm giải quyết vấn đề là đặt trường hợp kinh doanh vào một ví dụ thực tế thành công của bên thứ ba. Trường hợp kinh doanh nên trình bày với ban quản lý rằng tổ chức khác cũng gặp vấn đề tương tự và sau đó trình bày rằng họ đã tìm ra giải pháp và cách họ giải quyết vấn đề đó. Điều này thường sẽ nhắc ban quản lý hỏi giải pháp là gì và nó có thể áp dụng như thế nào đối với tổ chức của họ.

5.3.2 Xây dựng và đào tạo nhóm đa chức năng

Điều cần thiết đối với nhóm bảo mật thông tin đa chức năng là chia sẻ kiến thức và kinh nghiệm về lĩnh vực đa dạng của họ để đánh giá và giảm thiểu rủi ro trong ICS. Ở mức tối thiểu, nhóm bảo mật thông tin phải bao gồm một thành viên trong đội ngũ CNTT của tổ chức, kỹ sư điều khiển, người vận hành hệ thống điều khiển, chuyên gia về chủ đề bảo mật và thành viên của ban quản lý rủi ro doanh nghiệp. Kiến thức và kỹ năng bảo mật phải bao gồm kiến trúc mạng và thiết kế, quy trình và thực hành bảo mật, cũng như thiết kế và vận hành cơ sở hạ tầng an toàn. Suy nghĩ đương thời rằng cả an toàn và bảo mật đều là những đặc tính nổi bật của các hệ thống được kết nối với điều khiển kỹ thuật số gợi ý bao gồm một chuyên gia về an toàn. Để đảm bảo tính liên tục và đầy đủ, nhóm bảo mật thông tin cũng nên bao gồm nhà cung cấp hệ thống kiểm soát và/hoặc nhà tích hợp hệ thống.

Nhóm bảo mật thông tin phải báo cáo trực tiếp với người quản lý bảo mật thông tin ở cấp tổ chức/quy trình kinh doanh hoặc nhiệm vụ, người này sẽ báo cáo lại cho người quản lý quy trình kinh doanh/nhiệm vụ (ví dụ: giám đốc cơ sở) hoặc người quản lý bảo mật thông tin doanh nghiệp (ví dụ: CIO của công ty/CSO), tương ứng. Quyền hạn và trách nhiệm cuối cùng thuộc về chức năng điều hành rủi ro Bậc 1, chức năng này cung cấp cách tiếp cận toàn diện, toàn tổ chức để quản lý rủi ro. Chức năng điều hành rủi ro làm việc với ban quản lý cấp cao để chấp nhận mức độ rủi ro còn lại và trách nhiệm giải trình đối với bảo mật thông tin của ICS. Trách nhiệm giải trình ở cấp quản lý sẽ giúp đảm bảo cam kết liên tục đối với các nỗ lực bảo mật thông tin.

Mặc dù các kỹ sư điều khiển sẽ đóng một vai trò lớn trong việc bảo mật ICS, nhưng họ sẽ không thể làm như vậy nếu không có sự cộng tác và hỗ trợ từ cả bộ phận CNTT và ban quản lý. CNTT thường có nhiều năm kinh nghiệm về bảo mật, phần lớn trong số đó có thể áp dụng cho ICS. Do văn hóa của kỹ thuật điều khiển và CNTT thường khác biệt đáng kể nên việc tích hợp chúng sẽ rất cần thiết cho sự phát triển của sự hợp tác giữa thiết kế bảo mật và vận hành.

5.3.3 Xác định điều lệ và phạm vi

Người quản lý bảo mật thông tin nên thiết lập chính sách xác định điều lệ hướng dẫn của tổ chức bảo mật thông tin và vai trò, trách nhiệm và trách nhiệm giải trình của chủ sở hữu hệ thống, người quản lý quy trình kinh doanh/nhiệm vụ và người dùng. Người quản lý bảo mật thông tin nên quyết định và ghi lại mục tiêu của chương trình bảo mật, các tổ chức kinh doanh bị ảnh hưởng, tất cả các hệ thống máy tính và mạng liên quan, ngân sách và tài nguyên cần thiết cũng như sự phân chia trách nhiệm. Phạm vi cũng có thể đề cập đến các yêu cầu kinh doanh, đào tạo, kiểm toán, pháp lý và quy định, cũng như thời gian biểu và trách nhiệm. Điều lệ hướng dẫn của tổ chức bảo mật thông tin là một phần cấu thành của kiến trúc bảo mật thông tin, là một phần của kiến trúc doanh nghiệp.

Có thể đã có sẵn một chương trình bảo mật thông tin hoặc đang được phát triển cho các hệ thống kinh doanh CNTT của tổ chức. Người quản lý bảo mật thông tin ICS nên xác định những phương pháp hiện có nào cần tận dụng và phương pháp nào dành riêng cho hệ thống kiểm soát. Về lâu dài, sẽ dễ dàng đạt được kết quả tích cực hơn nếu nhóm có thể chia sẻ tài nguyên với những người khác trong tổ chức có cùng mục tiêu.

5.3.4 Xác định các thủ tục và chính sách bảo mật dành riêng cho ICS

Các chính sách và thủ tục là cơ sở của để bảo đảm an toàn thông tin. Bất cứ khi nào có thể, các thủ tục và chính sách bảo mật cụ thể của ICS nên được tích hợp với các thủ tục và chính sách vận hành/quản lý hiện có. Các chính sách và thủ tục giúp đảm bảo rằng việc bảo vệ an toàn là nhất quán và hiện hành để bảo vệ chống lại các mối đe dọa đang phát triển. Sau khi phân tích rủi ro bảo mật thông tin đã được thực hiện, người quản lý bảo mật thông tin nên kiểm tra các chính sách bảo mật hiện có để xem liệu chúng có giải quyết thỏa đáng các rủi ro đối với ICS hay không. Nếu cần, các chính sách hiện tại nên được sửa đổi hoặc tạo ra các chính sách mới.

Quản lý Bậc 1 chịu trách nhiệm phát triển và truyền đạt mức độ chấp nhận rủi ro của tổ chức–mức độ rủi ro mà tổ chức sẵn sàng chấp nhận–điều này cho phép người quản lý bảo mật thông tin xác định mức độ giảm thiểu rủi ro cần thực hiện để giảm rủi ro còn lại xuống mức chấp nhận được. Việc phát triển các chính sách bảo mật phải dựa trên đánh giá rủi ro việc đó sẽ đặt ra các ưu tiên và mục tiêu bảo mật cho tổ chức để các rủi ro do các mối đe dọa gây ra được giảm thiểu đầy đủ. Các thủ tục hỗ trợ các chính sách cần được phát triển để các chính sách được thực hiện đầy đủ và đúng cách cho ICS. Các quy trình bảo mật phải được ghi lại, kiểm tra và cập nhật định kỳ để đáp ứng với các thay đổi về chính sách, công nghệ và mối đe dọa.

5.3.5 Triển khai khung quản lý rủi ro bảo mật ICS

Từ một quan điểm trừu tượng, việc quản lý rủi ro ICS là một rủi ro khác được thêm vào danh sách các rủi ro mà một tổ chức phải đối mặt (ví dụ: tài chính, an toàn, CNTT, môi trường). Trong mỗi trường hợp, các nhà quản lý chịu trách nhiệm về nhiệm vụ hoặc quy trình kinh doanh sẽ thiết lập và thực hiện chương trình quản lý rủi ro phối hợp với chức năng điều hành rủi ro của ban quản lý cấp cao. Cũng giống như các lĩnh vực nhiệm vụ/quy trình kinh doanh khác, nhân viên liên quan đến ICS áp dụng kiến thức chuyên môn về chủ đề của họ để thiết lập và tiến hành quản lý rủi ro bảo mật ICS và giao tiếp với ban quản lý doanh nghiệp để hỗ trợ quản lý rủi ro hiệu quả trên toàn doanh nghiệp. Các phần sau đây tóm tắt quy trình này và áp dụng RMF cho môi trường ICS.

Quy trình RMF bao gồm một tập hợp các nhiệm vụ liên quan đến rủi ro được xác định rõ ràng sẽ được thực hiện bởi các cá nhân hoặc nhóm được lựa chọn trong các vai trò tổ chức được xác định rõ ràng (ví dụ: [chức năng] điều hành rủi ro, quan chức ủy quyền, đại diện được ủy quyền chính thức, giám đốc thông tin, nhân viên bảo mật thông tin cấp cao, kiến trúc sư doanh nghiệp, kiến trúc sư bảo mật thông tin, chủ sở hữu/người quản lý thông tin, chủ sở hữu hệ thống thông tin, nhà cung cấp kiểm soát chung, nhân viên bảo mật hệ thống thông tin và người đánh giá kiểm soát bảo mật). Nhiều vai trò quản lý rủi ro có các vai trò đối tác được xác định trong các quy trình vòng đời phát triển hệ thống thông thường. Các tác vụ RMF được thực thi đồng thời với hoặc như một phần của quy trình vòng đời phát triển hệ thống, có tính đến các yếu tố phụ thuộc thích hợp.

5.3.5.1 Phân loại tài sản mạng và hệ thống ICS

Nhóm bảo mật thông tin nên xác định, kiểm kê và phân loại các ứng dụng và hệ thống máy tính trong ICS, cũng như các mạng bên trong và giao tiếp với ICS. Nên tập trung vào các hệ thống thay vì các thiết bị và nên bao gồm PLC, DCS, SCADA và các hệ thống dựa trên công cụ sử dụng thiết bị giám sát như HMI. Tài sản sử dụng giao thức có thể định tuyến hoặc có thể truy cập quay số phải được ghi lại. Nhóm nên xem xét và cập nhật danh sách tài sản ICS hàng năm và sau mỗi lần thêm hoặc xóa tài sản.

Có một số công cụ kiểm kê CNTT dành cho doanh nghiệp thương mại có thể xác định và ghi lại tất cả phần cứng và phần mềm nằm trên mạng. Phải thận trọng trước khi sử dụng các công cụ này để xác định tài sản ICS; trước tiên các nhóm nên tiến hành đánh giá cách thức hoạt động của các công cụ này và tác động của chúng đối với thiết bị điều khiển được kết nối. Đánh giá công cụ có thể bao gồm thử nghiệm trong các môi trường hệ thống kiểm soát phi sản xuất tương tự để đảm bảo rằng các công cụ không tác động xấu đến hệ thống sản xuất. Tác động có thể là do bản chất của thông tin hoặc lưu lượng mạng. Mặc dù tác động này có thể được chấp nhận trong các hệ thống CNTT, nhưng nó có thể không được chấp nhận trong ICS.

Hệ thống quản lý tự động cho kiểm kê (ví dụ: Hệ thống quản lý bảo trì máy tính hóa (CMMS), Hệ thống quản lý cơ sở có sự hỗ trợ của máy tính (CAFM), Mô hình thông tin tòa nhà (BIM), Hệ thống thông tin không gian địa lý (GIS), Dữ liệu trao đổi thông tin tòa nhà vận hành xây dựng (COBie, Trao đổi thông tin Quản lý Tự động hóa Tòa nhà (BAMie), Trình tạo Hệ thống Quản lý Bền vững (SMS)) cho phép tổ chức lưu giữ tài khoản chính xác về những gì có trên hệ thống vì lý do bảo mật cũng như lý do ngân sách.

5.3.5.2 Chọn Kiểm soát bảo mật ICS

Các biện pháp kiểm soát bảo mật được chọn dựa trên phân loại bảo mậtcủa ICS được ghi lại trong kế hoạch bảo mật để cung cấp tổng quan về các yêu cầu bảo mật cho chương trình bảo mật thông tin ICS và mô tả các biện pháp kiểm soát bảo mật tại chỗ hoặc được lên kế hoạch để đáp ứng các yêu cầu đó. Kế hoạch bảo mật có thể là một tài liệu hoặc nó có thể là tập hợp tất cả các tài liệu giải quyết các mối lo ngại về bảo mật cho một hệ thống và các kế hoạch đối phó với những mối lo ngại này Việc triển khai thành công các biện pháp kiểm soát bảo mật cho hệ thống thông tin của tổ chức phụ thuộc vào việc triển khai thành công các biện pháp kiểm soát quản lý chương trình trên toàn tổ chức. Cách thức mà các tổ chức triển khai các biện pháp kiểm soát quản lý chương trình phụ thuộc vào các đặc điểm cụ thể của tổ chức, chẳng hạn như quy mô, độ phức tạp và các yêu cầu về sứ mệnh/kinh doanh của các tổ chức tương ứng. Các biện pháp kiểm soát quản lý chương trình bổ sung cho các biện pháp kiểm soát bảo mật và tập trung vào các yêu cầu bảo mật thông tin toàn tổ chức, có lập trình, độc lập với bất kỳ hệ thống thông tin cụ thể nào và rất cần thiết để quản lý các chương trình bảo mật thông tin.

Các tổ chức lập tài liệu kiểm soát quản lý chương trình trong kế hoạch chương trình bảo mật thông tin. Kế hoạch chương trình bảo mật thông tin toàn tổ chức bổ sung cho các kế hoạch bảo mật riêng lẻ được phát triển cho từng hệ thống thông tin của tổ chức. Kết hợp lại, các kế hoạch bảo mật cho các hệ thống thông tin riêng lẻ và chương trình bảo mật thông tin bao trùm toàn bộ các biện pháp kiểm soát bảo mật được tổ chức sử dụng.

5.3.5.3 Thực hiện đánh giá rủi ro

Bởi vì mọi tổ chức đều có một tập hợp nguồn lực hạn chế, nên các tổ chức nên đánh giá các tác động đối với hoạt động của tổ chức (nghĩa là sứ mệnh, chức năng, hình ảnh và danh tiếng), tài sản của tổ chức, cá nhân, các tổ chức khác và Quốc gia. các tổ chức có thể gặp hậu quả/tác động của các sự kiện bất lợi ở cấp độ hệ thống ICS riêng lẻ (ví dụ: không thực hiện theo yêu cầu), ở cấp độ nhiệm vụ/quy trình kinh doanh (ví dụ: không đáp ứng đầy đủ các mục tiêu nhiệm vụ/kinh doanh ) và ở cấp độ tổ chức (ví dụ: không tuân thủ các yêu cầu pháp lý hoặc quy định, làm tổn hại danh tiếng hoặc các mối quan hệ hoặc làm suy yếu khả năng tồn tại lâu dài). Một sự kiện bất lợi có thể gây ra nhiều hậu quả và các loại tác động khác nhau, ở các cấp độ khác nhau và trong các khung thời gian khác nhau.

Tổ chức có thể thực hiện đánh giá rủi ro chi tiết đối với các hệ thống có tác động cao nhất và đánh giá đối với các hệ thống có tác động thấp hơn nếu được coi là khôn ngoan và khi các nguồn lực cho phép. Đánh giá rủi ro sẽ giúp xác định bất kỳ điểm yếu nào góp phần tạo ra rủi ro bảo mật thông tin và các phương pháp giảm thiểu rủi ro. Đánh giá rủi ro được tiến hành nhiều lần trong vòng đời của hệ thống. Trọng tâm và mức độ chi tiết thay đổi tùy theo mức độ trưởng thành của hệ thống.

5.3.5.4 Thực hiện kiểm soát bảo mật

Các tổ chức nên phân tích đánh giá rủi ro chi tiết và các tác động đối với hoạt động của tổ chức (nghĩa là sứ mệnh, chức năng, hình ảnh và danh tiếng), tài sản của tổ chức, cá nhân, các tổ chức khác và Quốc gia, đồng thời ưu tiên lựa chọn các biện pháp kiểm soát giảm thiểu. Các tổ chức nên tập trung vào việc giảm thiểu rủi ro với tác động tiềm năng lớn nhất. Sự triển khai kiểm soát bảo mật phải nhất quán với kiến trúc doanh nghiệp và kiến trúc bảo mật thông tin của tổ chức.

Các biện pháp kiểm soát để giảm thiểu rủi ro cụ thể có thể khác nhau giữa các loại hệ thống. Ví dụ: kiểm soát xác thực người dùng có thể khác đối với ICS so với hệ thống trả lương của công ty và hệ thống thương mại điện tử. Người quản lý bảo mật thông tin ICS nên ghi lại và truyền đạt các biện pháp kiểm soát đã chọn, cùng với quy trình sử dụng các biện pháp kiểm soát. Một số rủi ro có thể được xác định và có thể được giảm thiểu bằng các giải pháp “khắc phục nhanh”—các biện pháp thực hành có giá trị cao, chi phí thấp có thể giảm rủi ro đáng kể. Ví dụ về các giải pháp này là hạn chế truy cập Internet và loại bỏ quyền truy cập email trên các trạm hoặc bảng điều khiển của nhà điều hành. Các tổ chức nên xác định, đánh giá và triển khai các giải pháp khắc phục nhanh phù hợp càng sớm càng tốt để giảm rủi ro bảo mật và đạt được lợi ích nhanh chóng

5.4 Khung kiến trúc bảo đảm an toàn thông tin cho các hệ thống điều khiển công nghiệp ICS

Khi thiết kế kiến trúc mạng để triển khai ICS, thông thường nên tách mạng ICS khỏi mạng công ty. Bản chất của lưu lượng mạng trên hai mạng này là khác nhau: truy cập Internet, FTP, email và truy cập từ xa thường sẽ được phép trên mạng công ty nhưng không được phép trên mạng ICS. Các quy trình kiểm soát thay đổi nghiêm ngặt đối với các thay đổi về thiết bị mạng, cấu hình và phần mềm có thể không được áp dụng trên mạng công ty. Nếu lưu lượng mạng ICS được thực hiện trên mạng công ty, nó có thể bị chặn hoặc bị tấn công DoS hoặc Người Trung Gian. Bằng với cách có các mạng riêng biệt, các vấn đề về bảo mật và hiệu suất trên mạng công ty sẽ không thể ảnh hưởng đến mạng ICS.

Những cân nhắc thực tế, chẳng hạn như chi phí cài đặt ICS hoặc duy trì cơ sở hạ tầng mạng đồng nhất, thường có nghĩa là cần có kết nối giữa ICS và mạng công ty. Kết nối này là một rủi ro bảo mật đáng kể và cần được bảo vệ bằng các thiết bị bảo vệ ranh giới. Nếu các mạng phải được kết nối, thì chỉ nên cho phép kết nối tối thiểu (đơn lẻ nếu có thể) và kết nối đó phải thông qua tường lửa và DMZ. DMZ là một phân đoạn mạng riêng biệt kết nối trực tiếp với tường lửa. Các máy chủ chứa dữ liệu từ ICS cần được truy cập từ mạng công ty sẽ được đặt trên phân đoạn mạng này. Chỉ những hệ thống này mới có thể truy cập được từ mạng công ty. Với bất kỳ kết nối bên ngoài nào, quyền truy cập tối thiểu phải được phép thông qua tường lửa, bao gồm chỉ mở các cổng cần thiết cho giao tiếp cụ thể**.**

5.4.1 Phân đoạn và phân tách mạng

Phần này đề cập đến việc phân vùng ICS thành các miền bảo mật và tách ICS khỏi các mạng khác, chẳng hạn như mạng công ty và trình bày kiến trúc bảo mật minh họa. Cần thực hiện phân tích rủi ro hoạt động để xác định các phần quan trọng của từng mạng và hoạt động của ICS, đồng thời giúp xác định những phần nào của ICS cần được phân đoạn. Phân đoạn mạng liên quan đến việc phân vùng mạng thành các mạng nhỏ hơn. Ví dụ: một mạng ICS lớn được phân vùng thành nhiều mạng ICS, trong đó việc phân vùng dựa trên các yếu tố như quyền quản lý, chính sách thống nhất và mức độ tin cậy, mức độ quan trọng của chức năng và lượng lưu lượng truyền thông đi qua ranh giới miền. Phân đoạn và tách biệt mạng là một trong những khái niệm kiến trúc hiệu quả nhất mà một tổ chức có thể triển khai để bảo vệ ICS của mình. Phân đoạn thiết lập các miền bảo mật hoặc vùng bao quanh, thường được xác định là được quản lý bởi cùng một cơ quan, thực thi cùng một chính sách và có mức độ tin cậy thống nhất. Phân đoạn có thể giảm thiểu phương pháp và mức độ truy cập vào thông tin nhạy cảm, cấu hình thiết bị và giao tiếp ICS, đồng thời có thể gây khó khăn hơn đáng kể cho hacker mạng độc hại và có thể chứa các tác động của lỗi và sự cố không ác ý. Một cân nhắc thực tế trong việc xác định miền bảo mật là lượng lưu lượng truyền thông vượt qua ranh giới miền, bởi vì bảo vệ miền thường liên quan đến việc kiểm tra lưu lượng ranh giới và xác định xem nó có được phép hay không.

Mục đích của việc phân đoạn và tách biệt mạng là giảm thiểu quyền truy cập vào thông tin nhạy cảm đối với những hệ thống đó và những người không cần thông tin đó, đồng thời đảm bảo rằng tổ chức có thể tiếp tục hoạt động hiệu quả. Điều này có thể đạt được bằng cách sử dụng một số kỹ thuật và công nghệ tùy thuộc vào kiến trúc và cấu hình của mạng.

Theo truyền thống, phân đoạn và tách biệt mạng được triển khai tại cổng giữa các miền. Môi trường ICS thường có nhiều miền được xác định rõ ràng, chẳng hạn như mạng LAN hoạt động, mạng LAN kiểm soát và DMZ hoạt động, cũng như cổng vào các miền không phải ICS và ít tin cậy hơn như Internet và mạng LAN công ty.

Sự phân tách mạng liên quan đến việc phát triển và thực thi một bộ quy tắc kiểm soát những thông tin liên lạc nào được phép đi qua ranh giới. Các quy tắc thường dựa trên danh tính nguồn và đích cũng như loại hoặc nội dung của dữ liệu được truyền.

Khi triển khai phân đoạn và tách biệt mạng một cách chính xác, bạn đang giảm thiểu phương pháp và mức độ truy cập vào thông tin nhạy cảm. Điều này có thể đạt được bằng cách sử dụng nhiều công nghệ và phương pháp khác nhau. Tùy thuộc vào kiến trúc và cấu hình mạng của bạn, một số công nghệ và phương pháp phổ biến được sử dụng bao gồm:

- Phân tách mạng hợp lý được thực thi bằng mã hóa hoặc phân vùng được thực thi bởi thiết bị mạng.

+ Mạng cục bộ ảo (VLANS).

+ Mạng riêng ảo được mã hóa (VPN) sử dụng cơ chế mã hóa để phân tách lưu lượng được kết hợp trên một mạng.

+ Cổng một chiều hạn chế giao tiếp giữa các kết nối theo một hướng duy nhất, do đó, phân đoạn mạng.

- Tách mạng vật lý để ngăn chặn hoàn toàn mọi kết nối lưu lượng giữa các miền.

+ Lọc lưu lượng mạng có thể sử dụng nhiều công nghệ khác nhau ở các lớp mạng khác nhau để thực thi các miền và yêu cầu bảo mật.

+ Lọc lớp mạng hạn chế hệ thống nào có thể giao tiếp với những hệ thống khác trên mạng dựa trên IP và thông tin tuyến đường.

+ Lọc dựa trên trạng thái hạn chế hệ thống nào có thể giao tiếp với những hệ thống khác trên mạng dựa trên chức năng dự định hoặc trạng thái hoạt động hiện tại của chúng.

+ Lọc cấp độ cổng và/hoặc giao thức hạn chế số lượng và loại dịch vụ mà mỗi hệ thống có thể sử dụng để liên lạc với các hệ thống khác trên mạng.

+ Lọc ứng dụng thường lọc nội dung truyền thông giữa các hệ thống ở lớp ứng dụng. Điều này bao gồm tường lửa cấp ứng dụng, proxy và bộ lọc dựa trên nội dung.

Một số nhà cung cấp đang tạo ra các sản phẩm để lọc các giao thức ICS ở cấp ứng dụng mà họ tiếp thị dưới dạng tường lửa ICS.

Bất kể công nghệ được chọn để triển khai phân đoạn và tách biệt mạng là gì, có bốn chủ đề phổ biến triển khai khái niệm phòng thủ chuyên sâu bằng cách cung cấp khả năng phân đoạn và tách biệt mạng tốt:

- Áp dụng các công nghệ không chỉ ở lớp mạng. Mỗi hệ thống và mạng nên được phân đoạn và tách biệt, nếu có thể, từ lớp liên kết dữ liệu cho đến và bao gồm cả lớp ứng dụng.

- Sử dụng các nguyên tắc về đặc quyền tối thiểu và điều cần biết. Nếu một hệ thống không cần giao tiếp với một hệ thống khác, thì nó không được phép. Nếu một hệ thống chỉ cần giao tiếp với một hệ thống khác trên một cổng hoặc giao thức cụ thể và không có gì khác–hoặc nó cần truyền một tập hợp giới hạn dữ liệu có nhãn hoặc định dạng cố định, thì nó nên bị hạn chế như vậy.

- Thông tin riêng biệt và cơ sở hạ tầng dựa trên yêu cầu bảo mật. Điều này có thể bao gồm việc sử dụng các phần cứng hoặc nền tảng khác nhau dựa trên các môi trường rủi ro và mối đe dọa khác nhau mà mỗi hệ thống hoặc phân đoạn mạng hoạt động. Các thành phần quan trọng nhất yêu cầu cách ly nghiêm ngặt hơn với các thành phần khác. Ngoài việc tách mạng, việc sử dụng ảo hóa có thể được sử dụng để thực hiện việc cách ly cần thiết.

- Thực hiện danh sách trắng thay vì danh sách đen; nghĩa là cấp quyền truy cập vào cái tốt đã biết, thay vì từ chối quyền truy cập vào cái xấu đã biết. Tập hợp các ứng dụng chạy trong ICS về cơ bản là tĩnh, làm cho danh sách trắng trở nên thiết thực hơn. Điều này cũng sẽ cải thiện khả năng phân tích tệp nhật ký của tổ chức.

5.4.2 Bảo vệ vùng mạng biên

Các thiết bị bảo vệ ranh giới kiểm soát luồng thông tin giữa các miền bảo mật được kết nối với nhau để bảo vệ ICS chống lại các hacker không gian mạng độc hại cũng như các lỗi và tai nạn không độc hại. Việc truyền thông tin giữa các hệ thống đại diện cho các miền bảo mật khác nhau với các chính sách bảo mật khác nhau sẽ gây ra rủi ro khi việc truyền đó vi phạm một hoặc nhiều chính sách bảo mật miền. Các thiết bị bảo vệ ranh giới là các thành phần quan trọng của các giải pháp kiến trúc cụ thể nhằm thực thi các chính sách bảo mật cụ thể. Các tổ chức có thể tách biệt ICS và các thành phần hệ thống kinh doanh thực hiện các nhiệm vụ và/hoặc chức năng kinh doanh khác nhau. Sự cô lập như vậy hạn chế các luồng thông tin trái phép giữa các thành phần hệ thống và cũng tạo cơ hội triển khai các mức bảo vệ cao hơn cho các thành phần được chọn. Việc tách các thành phần hệ thống bằng các cơ chế bảo vệ ranh giới cung cấp khả năng tăng cường bảo vệ các thành phần riêng lẻ và kiểm soát hiệu quả hơn các luồng thông tin giữa các thành phần đó.

Kiểm soát bảo vệ ranh giới bao gồm cổng, bộ định tuyến, tường lửa, bảo vệ, hệ thống ảo hóa và phân tích mã độc hại dựa trên mạng, hệ thống phát hiện xâm nhập (dựa trên mạng và dựa trên máy chủ), đường hầm được mã hóa, giao diện được quản lý, cổng thư và cổng một chiều (ví dụ: điốt dữ liệu). Các thiết bị bảo vệ ranh giới xác định xem có cho phép truyền dữ liệu hay không, thường bằng cách kiểm tra dữ liệu hoặc siêu dữ liệu liên quan.

Các kiến trúc sư bảo mật mạng và ICS phải quyết định miền nào được phép liên lạc trực tiếp, các chính sách quản lý việc liên lạc được phép, các thiết bị được sử dụng để thực thi chính sách và cấu trúc liên kết để cung cấp và triển khai các quyết định này, thường dựa trên mối quan hệ tin cậy giữa các miền. Sự tin cậy liên quan đến mức độ kiểm soát mà tổ chức có đối với miền bên ngoài (ví dụ: miền khác trong cùng một tổ chức, nhà cung cấp dịch vụ theo hợp đồng, Internet)

Các thiết bị bảo vệ ranh giới được bố trí phù hợp với kiến trúc bảo mật của tổ chức. Một cấu trúc kiến trúc phổ biến là các khu phi quân sự (DMZ), một máy chủ hoặc phân đoạn mạng được chèn làm “vùng trung lập” giữa các miền bảo mật. Mục đích của nó là thực thi chính sách bảo mật thông tin của miền ICS để trao đổi thông tin bên ngoài và cung cấp cho miền bên ngoài quyền truy cập hạn chế trong khi bảo vệ miền ICS khỏi các mối đe dọa bên ngoài.

Các cân nhắc bổ sung về kiến trúc và chức năng có thể được thực hiện bởi các thiết bị bảo vệ ranh giới cho liên lạc giữa các miền bao gồm:

- Từ chối lưu lượng liên lạc theo mặc định và cho phép lưu lượng liên lạc theo ngoại lệ (nghĩa là từ chối tất cả, cho phép theo ngoại lệ). Chính sách lưu lượng liên lạc từ chối tất cả, cho phép theo ngoại lệ đảm bảo rằng chỉ những kết nối đã được phê duyệt mới được phép. Đây có thể được biết đến là chính sách danh sách trắng.

- Triển khai các máy chủ proxy hoạt động như một trung gian cho các tài nguyên hệ thống thông tin yêu cầu của miền bên ngoài (ví dụ: tệp, kết nối hoặc dịch vụ) từ miền ICS. Các yêu cầu bên ngoài được thiết lập thông qua kết nối ban đầu với máy chủ proxy được đánh giá để quản lý độ phức tạp và cung cấp khả năng bảo vệ bổ sung bằng cách hạn chế kết nối trực tiếp.

- Ngăn chặn việc rò rỉ thông tin trái phép. Ví dụ, các kỹ thuật bao gồm tường lửa kiểm tra gói sâu và cổng XML. Các thiết bị này xác minh việc tuân thủ các định dạng và đặc tả giao thức ở lớp ứng dụng và dùng để xác định các lỗ hổng mà các thiết bị hoạt động ở lớp mạng hoặc lớp vận chuyển không thể phát hiện được. Số lượng định dạng hạn chế, đặc biệt là việc cấm văn bản dạng tự do trong email, giúp giảm bớt việc sử dụng các kỹ thuật như vậy tại các ranh giới của ICS.

- Chỉ cho phép liên lạc giữa các cặp địa chỉ nguồn và đích được ủy quyền và xác thực bởi một hoặc nhiều tổ chức, hệ thống, ứng dụng và cá nhân.

- Ví dụ, việc mở rộng khái niệm DMZ sang các mạng con riêng biệt khác rất hữu ích trong việc cô lập ICS để ngăn chặn các đối thủ khám phá các kỹ thuật phân tích và pháp y của các tổ chức.

- Thực thi kiểm soát truy cập vật lý để hạn chế quyền truy cập được phép vào các thành phần ICS.

- Che giấu địa chỉ mạng của các thành phần ICS khỏi bị phát hiện (ví dụ: địa chỉ mạng không được công bố hoặc nhập vào hệ thống tên miền), yêu cầu kiến thức trước để truy cập.

- Vô hiệu hóa các dịch vụ và giao thức kiểm soát và khắc phục sự cố, đặc biệt là những giao thức sử dụng tin nhắn quảng bá, có thể tạo điều kiện cho việc khám phá mạng.

- Định cấu hình các thiết bị bảo vệ ranh giới không thành công ở trạng thái được xác định trước. Các trạng thái lỗi ưu tiên đối với ICS liên quan đến việc cân bằng nhiều yếu tố bao gồm an toàn và bảo mật.

- Định cấu hình miền bảo mật với các địa chỉ mạng riêng biệt (tức là dưới dạng các mạng con rời rạc).

- Vô hiệu hóa phản hồi (ví dụ: chế độ không dài dòng) cho người gửi khi có lỗi ở định dạng xác thực giao thức để ngăn hacker lấy thông tin.

- Thực hiện luồng dữ liệu một chiều, đặc biệt là giữa các miền bảo mật khác nhau.

- Thiết lập giám sát thụ động các mạng ICS để chủ động phát hiện các thông tin liên lạc bất thường và đưa ra cảnh báo.

5.4.3 Tường lửa

Tường lửa mạng là thiết bị hoặc hệ thống kiểm soát luồng lưu lượng mạng giữa các mạng sử dụng các tư thế bảo mật khác nhau. Trong hầu hết các ứng dụng hiện đại, tường lửa và môi trường tường lửa được thảo luận trong bối cảnh kết nối Internet và bộ giao thức UDP/IP. Tuy nhiên, tường lửa có khả năng ứng dụng trong môi trường mạng không bao gồm hoặc không yêu cầu kết nối Internet. Ví dụ: nhiều mạng công ty sử dụng tường lửa để hạn chế kết nối đến và từ các mạng nội bộ phục vụ các chức năng nhạy cảm hơn, chẳng hạn như phòng kế toán hoặc phòng nhân sự. Tường lửa có thể hạn chế hơn nữa giao tiếp liên mạng con ICS giữa các thiết bị và mạng con bảo mật chức năng. Bằng cách sử dụng tường lửa để kiểm soát kết nối đến các khu vực này, một tổ chức có thể ngăn chặn truy cập trái phép vào các hệ thống và tài nguyên tương ứng trong các khu vực nhạy cảm hơn. Có ba loại tường lửa chung:

- Tường lửa lọc gói. Loại tường lửa cơ bản nhất được gọi là bộ lọc gói tin. Tường lửa lọc gói về cơ bản là các thiết bị định tuyến bao gồm chức năng kiểm soát truy cập cho các địa chỉ hệ thống và các phiên liên lạc. Kiểm soát truy cập được điều chỉnh bởi một tập hợp các chỉ thị được gọi chung là một bộ quy tắc. Ở dạng cơ bản nhất, bộ lọc gói hoạt động ở lớp 3 (mạng) của Kết nối hệ thống mở (OSI), mô hình ISO/IEC 7498. Loại tường lửa này kiểm tra thông tin cơ bản trong mỗi gói, chẳng hạn như địa chỉ IP, dựa trên một bộ tiêu chí trước khi chuyển tiếp gói. Tùy thuộc vào gói và tiêu chí, tường lửa có thể bỏ gói, chuyển tiếp hoặc gửi tin nhắn đến người khởi tạo. Loại tường lửa này có thể cung cấp mức độ bảo mật cao, nhưng có thể dẫn đến các tác động về chi phí và độ trễ đối với hiệu suất mạng.

- Tường lửa kiểm tra trạng thái. Tường lửa kiểm tra trạng thái là các bộ lọc gói kết hợp nhận thức bổ sung về dữ liệu mô hình OSI ở lớp 4 (vận chuyển). Tường lửa kiểm tra trạng thái lọc các gói ở lớp mạng, xác định xem các gói phiên có hợp lệ hay không và cũng đánh giá nội dung của các gói ở lớp vận chuyển (ví dụ: TCP, UDP). Kiểm tra trạng thái theo dõi các phiên hoạt động và sử dụng thông tin đó để xác định xem các gói có nên được chuyển tiếp hoặc chặn hay không. Nó cung cấp mức độ bảo mật cao và hiệu suất tốt, nhưng nó có thể đắt hơn và phức tạp hơn để quản lý. Bộ quy tắc bổ sung cho các ứng dụng ICS có thể được yêu cầu.

- Tường lửa cổng ứng dụng-Proxy. Lớp tường lửa này kiểm tra các gói ở lớp ứng dụng và lọc lưu lượng dựa trên các quy tắc ứng dụng cụ thể, chẳng hạn như các ứng dụng được chỉ định (ví dụ: trình duyệt) hoặc giao thức (ví dụ: FTP). Tường lửa loại này có thể rất hiệu quả trong việc ngăn chặn các cuộc tấn công vào các dịch vụ cấu hình và truy cập từ xa được cung cấp bởi các thành phần ICS. Chúng cung cấp mức độ bảo mật cao, nhưng có thể có tác động về chi phí và độ trễ đối với hiệu suất mạng, điều này có thể không được chấp nhận trong môi trường ICS. Chúng cung cấp mức độ bảo mật cao, nhưng có thể có tác động về chi phí và độ trễ đối với hiệu suất mạng, điều này có thể không được chấp nhận trong môi trường ICS.

Trong môi trường ICS, tường lửa thường được triển khai giữa mạng ICS và mạng công ty. Được cấu hình phù hợp, chúng có thể hạn chế đáng kể quyền truy cập không mong muốn vào và từ các máy chủ và bộ điều khiển của hệ thống điều khiển, do đó cải thiện tính bảo mật. Được cấu hình phù hợp, chúng có thể hạn chế đáng kể quyền truy cập không mong muốn vào và từ các máy chủ và bộ điều khiển của hệ thống điều khiển, do đó cải thiện tính bảo mật. Chúng cũng có khả năng cải thiện khả năng đáp ứng của mạng điều khiển bằng cách loại bỏ lưu lượng không cần thiết khỏi mạng. Khi được thiết kế, định cấu hình và bảo trì phù hợp, tường lửa phần cứng chuyên dụng có thể đóng góp đáng kể vào việc tăng cường bảo mật cho môi trường ICS ngày nay.

Tường lửa cung cấp một số công cụ để thực thi chính sách bảo mật không thể thực hiện cục bộ trên bộ thiết bị kiểm soát quy trình hiện có trên thị trường, bao gồm khả năng:

- Chặn tất cả các giao tiếp ngoại trừ giao tiếp được bật cụ thể giữa các thiết bị trên mạng LAN không được bảo vệ và mạng ICS được bảo vệ. Ví dụ, việc chặn có thể dựa trên các cặp địa chỉ IP nguồn và đích, dịch vụ, cổng, trạng thái kết nối và các ứng dụng hoặc giao thức cụ thể được tường lửa hỗ trợ. Chặn có thể xảy ra trên cả gói gửi đến và gửi đi, điều này hữu ích trong việc hạn chế các giao tiếp có rủi ro cao như email.

- Thực thi xác thực an toàn cho tất cả người dùng đang tìm cách truy cập vào mạng ICS. Có thể linh hoạt sử dụng các mức độ bảo vệ khác nhau của các phương thức xác thực bao gồm mật khẩu đơn giản, mật khẩu phức tạp, công nghệ xác thực đa yếu tố, mã thông báo, sinh trắc học và thẻ thông minh. Chọn phương pháp cụ thể dựa trên lỗ hổng của mạng ICS được bảo vệ, thay vì sử dụng phương pháp khả dụng ở cấp độ thiết bị.

- Thực thi ủy quyền đích. Người dùng có thể bị hạn chế và chỉ được phép tiếp cận các nút trên mạng điều khiển cần thiết cho chức năng công việc của họ. Điều này làm giảm khả năng người dùng cố ý hoặc vô tình có được quyền truy cập và kiểm soát các thiết bị mà họ không được phép sử dụng, nhưng lại làm tăng thêm sự phức tạp cho nhân viên đào tạo tại chỗ hoặc đào tạo chéo.

- Ghi lại luồng thông tin để theo dõi lưu lượng, phân tích và phát hiện xâm nhập.

- Cho phép ICS thực hiện các chính sách hoạt động phù hợp với ICS nhưng điều đó có thể không phù hợp trong mạng CNTT, chẳng hạn như cấm các liên lạc kém an toàn hơn như email và cho phép sử dụng tên người dùng và mật khẩu nhóm dễ nhớ.

- Được thiết kế với các kết nối được ghi lại và tối thiểu (đơn lẻ nếu có thể) cho phép tách mạng ICS khỏi mạng công ty, nếu quyết định đó được đưa ra, trong thời gian xảy ra sự cố mạng nghiêm trọng.

Các triển khai khả thi khác bao gồm sử dụng tường lửa dựa trên máy chủ hoặc tường lửa phần cứng độc lập nhỏ ở phía trước hoặc chạy trên các thiết bị điều khiển riêng lẻ. Sử dụng tường lửa trên cơ sở thiết bị riêng lẻ có thể tạo ra chi phí quản lý đáng kể, đặc biệt là trong việc quản lý thay đổi cấu hình tường lửa, tuy nhiên, cách làm này cũng sẽ đơn giản hóa các bộ quy tắc cấu hình riêng lẻ.

Có một số vấn đề phải được giải quyết khi triển khai tường lửa trong môi trường ICS, đặc biệt là những vấn đề sau:

- Khả năng bổ sung độ trễ để kiểm soát thông tin liên lạc của hệ thống.

- Thiếu kinh nghiệm trong việc thiết kế các bộ quy tắc phù hợp cho các ứng dụng công nghiệp. Tường lửa được sử dụng để bảo vệ các hệ thống điều khiển phải được cấu hình sao cho chúng không cho phép lưu lượng truy cập vào hoặc ra theo mặc định. Cấu hình mặc định chỉ nên được sửa đổi khi cần để cho phép các kết nối đến hoặc từ các hệ thống đáng tin cậy để thực hiện các chức năng ICS được ủy quyền

Tường lửa yêu cầu hỗ trợ, bảo trì và sao lưu liên tục. Các bộ quy tắc cần được xem xét để đảm bảo rằng chúng đang cung cấp sự bảo vệ đầy đủ trước các mối đe dọa an toàn luôn thay đổi. Các khả năng của hệ thống (ví dụ: không gian lưu trữ cho nhật ký tường lửa) phải được giám sát để đảm bảo rằng tường lửa đang thực hiện các tác vụ thu thập dữ liệu của nó và có thể phụ thuộc vào trong trường hợp vi phạm bảo mật. Giám sát thời gian thực của tường lửa và các cảm biến bảo mật khác là cần thiết để nhanh chóng phát hiện và bắt đầu ứng phó với các sự cố mạng.

5.4.4 Mạng điều khiển tách biệt hợp lý

Ở mức tối thiểu, mạng ICS phải được tách biệt hợp lý khỏi mạng công ty trên các thiết bị mạng riêng biệt về mặt vật lý. Dựa trên cấu hình mạng ICS, cần xem xét tách biệt bổ sung cho Hệ thống thiết bị an toàn và Hệ thống bảo mật (ví dụ: giám sát vật lý và kiểm soát truy cập, cửa ra vào, cổng, camera, VoIP, đầu đọc thẻ truy cập) thường là một phần của mạng ICS hoặc sử dụng cùng một cơ sở hạ tầng truyền thông cho các trang web từ xa. Khi kết nối doanh nghiệp yêu cầu:

- Cần có các điểm truy cập tối thiểu (đơn lẻ nếu có thể) được lập thành văn bản và ghi lại giữa mạng ICS và mạng công ty. Các điểm truy cập dự phòng (nghĩa là dự phòng), nếu có, phải được ghi lại.

- Tường lửa trạng thái giữa mạng ICS và mạng công ty phải được định cấu hình để từ chối tất cả lưu lượng truy cập ngoại trừ lưu lượng được ủy quyền rõ ràng.

- Các quy tắc tường lửa ở mức tối thiểu phải cung cấp khả năng lọc nguồn và đích (nghĩa là lọc trên địa chỉ [MAC] kiểm soát truy cập phương tiện), ngoài việc lọc cổng TCP và Giao thức gói dữ liệu người dùng (UDP) cũng như loại và mã Giao thức thông báo điều khiển Internet (ICMP) và lọc mã.

Một cách tiếp cận có thể chấp nhận được để cho phép giao tiếp giữa mạng ICS và mạng công ty là triển khai mạng DMZ trung gian. DMZ phải được kết nối với tường lửa sao cho giao tiếp cụ thể (bị hạn chế) chỉ có thể xảy ra giữa mạng công ty và DMZ, mạng ICS và DMZ. Mạng công ty và mạng ICS không được giao tiếp trực tiếp với nhau. Có thể đạt được bảo mật bổ sung bằng cách triển khai Mạng riêng ảo (VPN) giữa ICS và các mạng bên ngoài.

5.4.5 Phân tách mạng

Mạng ICS và mạng công ty có thể được tách biệt để tăng cường an toàn mạng bằng cách sử dụng các kiến trúc khác nhau. Phần này mô tả một số kiến trúc khả thi và giải thích những ưu điểm và nhược điểm của từng loại.

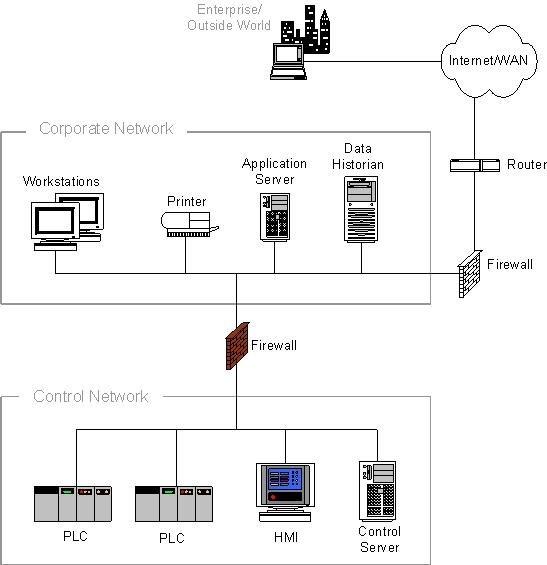
5.4.5.1 Máy tính Dual-Homed/Thẻ giao diện mạng kép (NIC)

Máy tính dual-homed có thể truyền lưu lượng mạng từ mạng này sang mạng khác. Một máy tính không có các biện pháp kiểm soát bảo mật phù hợp có thể gây ra các mối đe dọa bổ sung. Để ngăn chặn điều này, không có hệ thống nào khác ngoài tường lửa được cấu hình là Dual-Homed để mở rộng cả mạng điều khiển và mạng công ty. Tất cả các kết nối giữa mạng điều khiển và mạng công ty phải thông qua tường lửa. Cấu hình này không cung cấp cải tiến bảo mật và không được sử dụng để kết nối các mạng (ví dụ: ICS và mạng công ty).

5.4.5.2 Tường lửa giữa Mạng công ty và Mạng điều khiển

Bằng cách giới thiệu một tường lửa hai cổng đơn giản giữa mạng công ty và mạng điều khiển, như trong Hình 10, có thể đạt được một cải tiến bảo mật đáng kể. Được cấu hình đúng cách, tường lửa sẽ giảm đáng kể khả năng tấn công thành công từ bên ngoài vào mạng điều khiển.

Thật không may, vẫn còn hai vấn đề với thiết kế này. Đầu tiên, nếu lịch sử dữ liệu cư trú trên mạng công ty, tường lửa phải cho phép lịch sử dữ liệu giao tiếp với các thiết bị điều khiển trên mạng điều khiển. Một gói bắt nguồn từ một máy chủ độc hại hoặc được định cấu hình không chính xác trên mạng công ty (có vẻ là lịch sử dữ liệu) sẽ được chuyển tiếp đến các PLC/DCS riêng lẻ.



**Hình 10. Tường lửa giữa Mạng công ty và Mạng điều khiển**

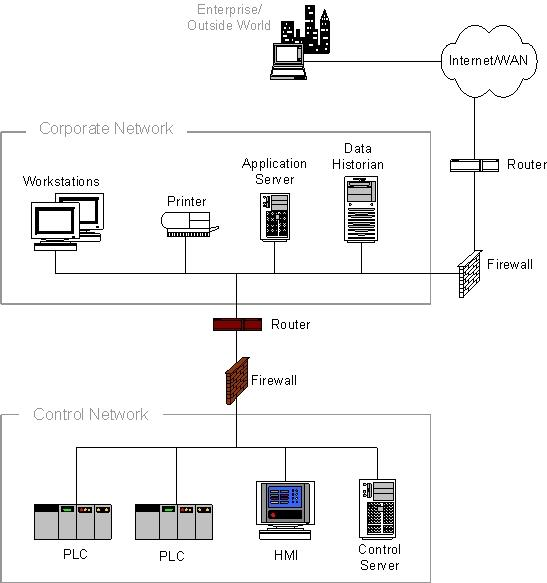
Nếu lịch sử dữ liệu nằm trên mạng điều khiển, phải tồn tại quy tắc tường lửa cho phép tất cả các máy chủ từ doanh nghiệp liên lạc với lịch sử. Thông thường, giao tiếp này xảy ra ở lớp ứng dụng dưới dạng các yêu cầu Ngôn ngữ truy vấn có cấu trúc (SQL) hoặc Giao thức truyền siêu văn bản (HTTP). Các lỗi trong mã lớp ứng dụng của nhà sử học có thể dẫn đến một nhà sử học bị xâm nhập. Khi lịch sử bị xâm phạm, các nút còn lại trên mạng điều khiển dễ bị sâu lan truyền hoặc tấn công tương tác.

Một vấn đề khác với việc có một tường lửa đơn giản giữa các mạng là các gói tin giả mạo có thể được xây dựng có thể ảnh hưởng đến mạng điều khiển, có khả năng cho phép dữ liệu bí mật được tạo đường hầm trong các giao thức được phép. Ví dụ: nếu các gói HTTP được phép đi qua tường lửa, thì phần mềm ngựa thành Troia vô tình được đưa vào HMI hoặc máy tính xách tay mạng điều khiển có thể bị một thực thể từ xa kiểm soát và gửi dữ liệu (chẳng hạn như mật khẩu bị bắt) đến thực thể đó, được ngụy trang dưới dạng lưu lượng truy cập hợp pháp.

Mặc dù kiến trúc này là một cải tiến đáng kể so với mạng không tách biệt, nhưng nó yêu cầu sử dụng các quy tắc tường lửa cho phép liên lạc trực tiếp giữa mạng công ty và các thiết bị mạng điều khiển. Điều này có thể dẫn đến các vi phạm an toàn có thể xảy ra nếu không được thiết kế và giám sát an toàn.

5.4.5.3 Tường lửa và Bộ định tuyến giữa Mạng công ty và Mạng điều khiển

Một thiết kế phức tạp hơn một chút, như trong Hình 11, là việc sử dụng kết hợp bộ định tuyến/tường lửa. Bộ định tuyến nằm phía trước tường lửa và cung cấp các dịch vụ lọc gói cơ bản, trong khi tường lửa xử lý các vấn đề phức tạp hơn bằng cách sử dụng kỹ thuật kiểm tra trạng thái hoặc proxy. Kiểu thiết kế này rất phổ biến trong các tường lửa kết nối Internet vì nó cho phép bộ định tuyến nhanh hơn xử lý phần lớn các gói đến, đặc biệt là trong trường hợp tấn công DoS và giảm tải cho tường lửa. Nó cũng mang lại khả năng phòng thủ chuyên sâu được cải thiện vì có hai thiết bị khác nhau mà hacker phải vượt qua

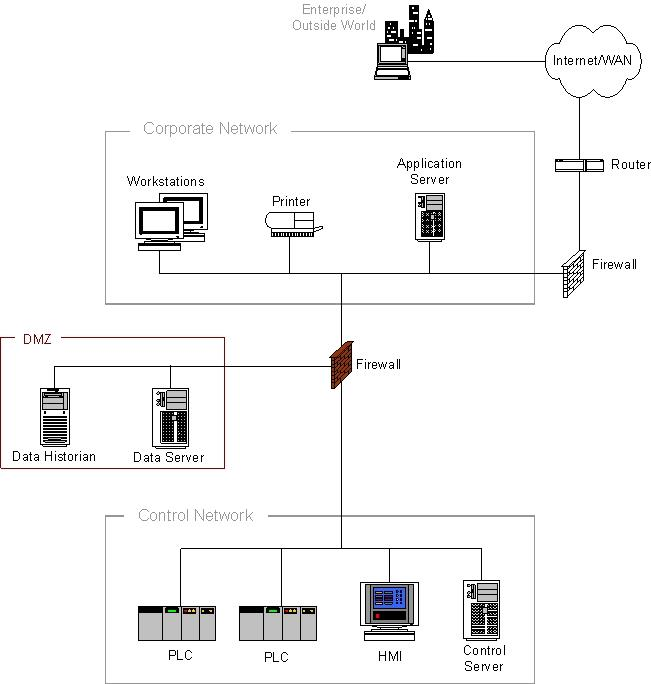


**Hình 11. Tường lửa và Bộ định tuyến giữa Mạng công ty và Mạng điều khiển**

5.4.5.4 Tường lửa với DMZ giữa Mạng công ty và Mạng điều khiển

Một cải tiến đáng kể là việc sử dụng tường lửa với khả năng thiết lập DMZ giữa mạng công ty và mạng điều khiển. Mỗi DMZ chứa một hoặc nhiều thành phần quan trọng, chẳng hạn như lịch sử dữ liệu, điểm truy cập không dây hoặc hệ thống truy cập từ xa và bên thứ ba. Trên thực tế, việc sử dụng tường lửa có khả năng DMZ cho phép tạo một mạng trung gian.

Việc tạo DMZ yêu cầu tường lửa cung cấp ba giao diện trở lên, thay vì các giao diện chung và riêng thông thường. Một trong các giao diện được kết nối với mạng công ty, giao diện thứ hai với mạng điều khiển và các giao diện còn lại với các thiết bị dùng chung hoặc không an toàn, chẳng hạn như máy chủ lịch sử dữ liệu hoặc các điểm truy cập không dây trên mạng DMZ. Việc thực hiện giám sát lưu lượng truy cập vào và ra liên tục trên DMZ được khuyến nghị. Ngoài ra, các bộ quy tắc tường lửa chỉ cho phép các kết nối giữa mạng điều khiển và DMZ được khởi tạo bởi các thiết bị mạng điều khiển được khuyến nghị. Hình 12 cung cấp một ví dụ về kiến trúc này.



**Hình 12. Tường lửa với DMZ giữa Mạng công ty và Mạng điều khiển**

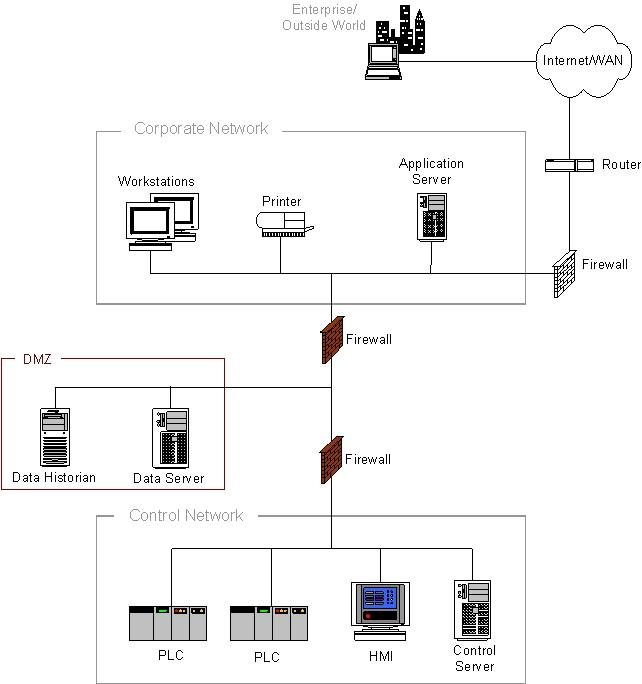
Bằng cách đặt các thành phần có thể truy cập của công ty trong DMZ, sẽ không yêu cầu đường truyền thông trực tiếp từ mạng công ty đến mạng điều khiển; mỗi đường kết thúc hiệu quả trong DMZ. Hầu hết các tường lửa có thể cho phép nhiều DMZ và có thể chỉ định loại lưu lượng nào có thể được chuyển tiếp giữa các vùng. Như Hình 12 cho thấy, tường lửa có thể chặn các gói tùy ý từ mạng công ty xâm nhập vào mạng điều khiển và cũng có thể điều chỉnh lưu lượng từ các vùng mạng khác bao gồm cả mạng điều khiển. Với các bộ quy tắc được lập kế hoạch tốt, có thể duy trì sự tách biệt rõ ràng giữa mạng điều khiển và các mạng khác, với rất ít hoặc không có lưu lượng truy cập trực tiếp giữa mạng công ty và mạng điều khiển.

Nếu máy chủ quản lý bản vá, máy chủ chống vi-rút hoặc máy chủ bảo mật khác được sử dụng cho mạng điều khiển, thì máy chủ đó phải được đặt trực tiếp trên DMZ. Cả hai chức năng có thể nằm trên một máy chủ. Có quản lý bản vá và quản lý chống vi-rút dành riêng cho mạng điều khiển cho phép cập nhật được kiểm soát và an toàn có thể được điều chỉnh cho phù hợp với nhu cầu riêng của môi trường ICS. Nó cũng có thể hữu ích nếu sản phẩm chống vi-rút được chọn để bảo vệ ICS không giống với sản phẩm chống vi-rút được sử dụng cho mạng công ty. Ví dụ: nếu xảy ra sự cố phần mềm độc hại và một sản phẩm chống vi-rút không thể phát hiện hoặc ngăn chặn phần mềm độc hại, thì có khả năng một sản phẩm khác có thể có khả năng đó.

Rủi ro bảo mật chính trong kiểu kiến trúc này là nếu một máy tính trong DMZ bị xâm phạm, thì nó có thể được sử dụng để khởi động một cuộc tấn công vào mạng điều khiển thông qua lưu lượng ứng dụng được phép từ DMZ đến mạng điều khiển. Rủi ro này có thể giảm đáng kể nếu một nỗ lực phối hợp được thực hiện để tăng cường và tích cực vá các máy chủ trong DMZ và nếu bộ quy tắc tường lửa chỉ cho phép các kết nối giữa mạng điều khiển và DMZ được khởi tạo bởi các thiết bị mạng điều khiển. Các mối quan tâm khác với kiến trúc này là sự phức tạp được thêm vào và chi phí tường lửa có thể tăng lên với một số cổng. Tuy nhiên, đối với các hệ thống quan trọng hơn, sự cải thiện an toàn sẽ bù đắp nhiều hơn những nhược điểm này.

5.4.5.5 Tường lửa được phép nối giữa Mạng công ty và Mạng điều khiển

Một biến thể của tường lửa với giải pháp DMZ là sử dụng một cặp tường lửa được đặt giữa mạng công ty và mạng ICS, như trong Hình 13. Các máy chủ phổ biến, chẳng hạn như lịch sử dữ liệu, được đặt giữa các tường lửa trong vùng mạng giống như DMZ, đôi khi được gọi là lớp Hệ thống Thực thi Sản xuất (MES). Như trong các kiến trúc được mô tả trước đây, tường lửa đầu tiên chặn các gói tùy ý tiến tới mạng điều khiển hoặc các lịch sử được chia sẻ. Tường lửa thứ hai có thể ngăn lưu lượng truy cập không mong muốn từ máy chủ bị xâm nhập vào mạng điều khiển và ngăn lưu lượng mạng điều khiển ảnh hưởng đến máy chủ dùng chung.



**Hình 13. Tường lửa được phép nối giữa Mạng công ty và Mạng điều khiển**

Nếu tường lửa từ hai nhà sản xuất khác nhau được sử dụng, thì giải pháp này có thể mang lại lợi thế. Nó cũng cho phép nhóm kiểm soát và nhóm CNTT có trách nhiệm thiết bị được phân tách rõ ràng vì mỗi nhóm có thể tự quản lý tường lửa, nếu quyết định được đưa ra trong tổ chức để làm như vậy. Nhược điểm chính của kiến trúc hai tường lửa là chi phí gia tăng và độ phức tạp trong quản lý. Đối với các môi trường có yêu cầu bảo mật nghiêm ngặt hoặc cần phân tách quản lý rõ ràng,thì kiến trúc này có một số ưu điểm mạnh.

5.4.5.6 Tóm tắt phân chia mạng

Tóm lại, máy tính dual-homed thường không cung cấp sự cách ly phù hợp giữa mạng điều khiển và mạng công ty. Các giải pháp hai vùng (không có DMZ) không được khuyến nghị vì chúng chỉ cung cấp khả năng bảo vệ yếu. Nếu được sử dụng, chúng chỉ nên được triển khai hết sức cẩn thận. Kiến trúc phân tách mạng công ty và mạng điều khiển an toàn, dễ quản lý và có thể mở rộng nhất thường dựa trên một hệ thống có ít nhất ba vùng, kết hợp một hoặc nhiều DMZ.

5.4.6 Kiến trúc chiều sâu phòng ngự được khuyến nghị

Một sản phẩm, công nghệ hoặc giải pháp bảo mật riêng lẻ không thể tự bảo vệ đầy đủ một ICS. Một chiến lược nhiều lớp liên quan đến hai (hoặc nhiều) cơ chế bảo mật chồng chéo khác nhau, một kỹ thuật còn được gọi là chiều sâu phòng ngự, được mong muốn để giảm thiểu tác động của lỗi trong bất kỳ cơ chế nào. Chiến lược kiến trúc chiều sâu phòng ngự bao gồm việc sử dụng tường lửa, tạo các khu phi quân sự, khả năng phát hiện xâm nhập cùng với các chính sách bảo mật hiệu quả, các chương trình đào tạo, cơ chế ứng phó sự cố và bảo mật vật lý. Ngoài ra, một chiến lược chiều sâu phòng ngự hiệu quả đòi hỏi sự hiểu biết thấu đáo về các vectơ tấn công có thể có trên ICS. Bao gồm các:

* Backdoor và lỗ hổng trong chu vi mạng.
* Lỗ hổng trong các giao thức phổ biến.
* Tấn công vào các thiết bị trường.
* Các cuộc tấn công cơ sở dữ liệu.
* Chiếm đoạt thông tin liên lạc và các cuộc tấn công 'người trung gian’.
* Các cuộc tấn công giả mạo.
* Tấn công vào các tài khoản đặc quyền và/hoặc chia sẻ.

Hình 14 cho thấy một chiến lược kiến trúc chiều sâu phòng ngự ICS đã được phát triển bởi Ủy ban Thực hành Đề xuất của Chương trình An toàn Hệ thống Kiểm soát DHS (CSSP) NCCIC/ICS-CERT13 được mô tả trong tài liệu Tài liệu Chiến lược Phòng thủ Chuyên sâu của Hệ thống Kiểm soát [36]. Các tài liệu hỗ trợ bổ sung đề cập đến các vấn đề cụ thể và các biện pháp giảm thiểu liên quan cũng được đưa vào trang web.

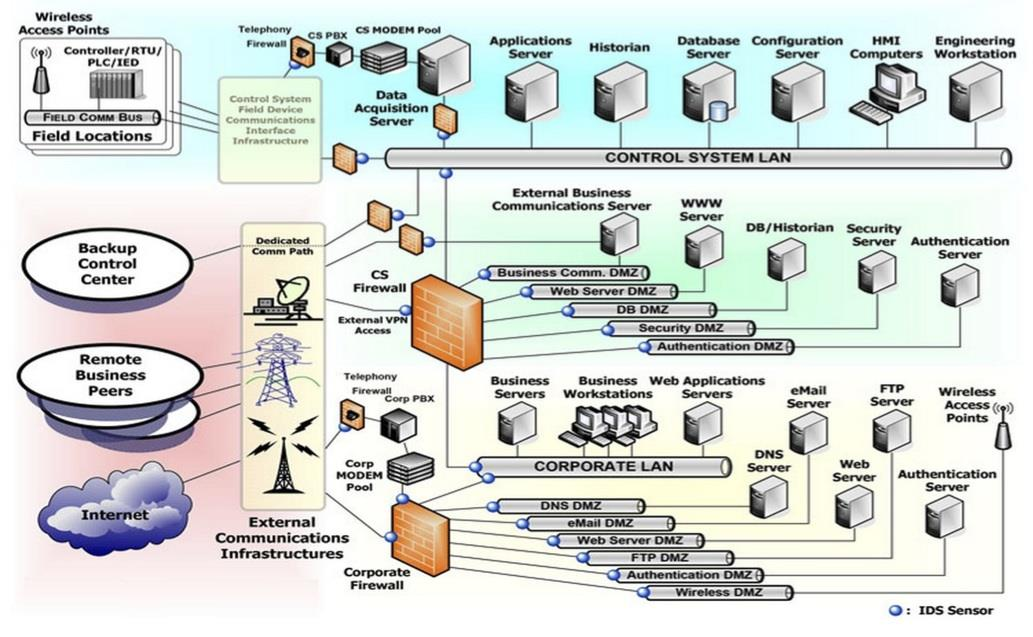
Tài liệu Hệ thống kiểm soát An toàn mạng: Chiến lược phòng thủ chuyên sâu cung cấp hướng dẫn và định hướng để phát triển các chiến lược kiến trúc chiều sâu phòng ngự cho các tổ chức sử dụng mạng hệ thống kiểm soát trong khi duy trì kiến trúc thông tin nhiều tầng yêu cầu:

- Bảo trì các thiết bị trường khác nhau, thu thập phép đo từ xa và/hoặc các hệ thống quy trình cấp công nghiệp.

- Truy cập vào các cơ sở thông qua liên kết dữ liệu từ xa hoặc modem.

- Các dịch vụ công cộng cho các hoạt động của khách hàng hoặc công ty.

Chiến lược này bao gồm tường lửa, việc sử dụng các khu phi quân sự và khả năng phát hiện xâm nhập qua toàn bộ kiến trúc ICS. Việc sử dụng một số vùng phi quân sự trong Hình 14 cung cấp khả năng bổ sung để phân tách các chức năng và đặc quyền truy cập và đã chứng tỏ rằng rất hiệu quả trong việc bảo vệ các kiến trúc lớn bao gồm các mạng với các nhiệm vụ hoạt động khác nhau. Triển khai phát hiện xâm nhập áp dụng các bộ quy tắc khác và chữ ký duy nhất cho từng miền được giám sát.



**Hình 14. Kiến trúc chiều sâu phòng ngự được CSSP đề xuất**

5.4.7 Chính sách tường lửa chung cho ICS

Khi đã có kiến trúc chiều sâu phòng ngự, công việc xác định chính xác lưu lượng nào sẽ được phép đi qua tường lửa sẽ bắt đầu. Định cấu hình tường lửa để từ chối tất cả ngoại trừ lưu lượng hoàn toàn cần thiết cho nhu cầu kinh doanh là tiền đề cơ bản của mọi tổ chức, nhưng thực tế khó khăn hơn nhiều. Chính xác thì “hoàn toàn cần thiết cho doanh nghiệp” nghĩa là gì và tác động bảo mật của việc cho phép lưu lượng truy cập đó là gì? Ví dụ: nhiều tổ chức đã cân nhắc việc cho phép lưu lượng truy cập SQL qua tường lửa theo yêu cầu đối với hoạt động kinh doanh đối với nhiều máy chủ lịch sử dữ liệu.

Lỗ hổng SQL cũng là mục tiêu của sâu Slammer, Nhiều giao thức quan trọng được sử dụng trong lĩnh vực công nghiệp, chẳng hạn như HTTP, FTP, OPC/DCOM, EtherNet/IP và Modbus/TCP, có các lỗ hổng bảo mật nghiêm trọng

Khi cài đặt một tường lửa hai cổng không có DMZ cho các máy chủ dùng chung, cần phải đặc biệt cẩn thận với thiết kế quy tắc. Ở mức tối thiểu, tất cả các quy tắc phải là quy tắc trạng thái có cả địa chỉ IP và cổng (ứng dụng) cụ thể. Phần địa chỉ của các quy tắc sẽ hạn chế lưu lượng truy cập đến đối với một tập hợp rất nhỏ các thiết bị dùng chung (ví dụ: bộ lưu trữ dữ liệu) trên mạng điều khiển từ một tập hợp địa chỉ được kiểm soát trên mạng công ty. Không nên cho phép bất kỳ địa chỉ IP nào trên mạng công ty truy cập vào các máy chủ bên trong mạng điều khiển. Ngoài ra, các cổng được phép nên được hạn chế cẩn thận đối với các giao thức tương đối an toàn, chẳng hạn như Bảo mật Giao thức Truyền Siêu văn bản (HTTPS). Việc cho phép HTTP, FTP hoặc các giao thức không bảo mật khác vượt qua tường lửa là một rủi ro bảo mật do khả năng bị đánh cắp và sửa đổi lưu lượng truy cập. Các quy tắc nên được thêm vào để từ chối các máy chủ bên ngoài mạng điều khiển bắt đầu kết nối với các máy chủ trên mạng điều khiển. Các quy tắc chỉ nên cho phép các thiết bị bên trong mạng điều khiển có khả năng thiết lập kết nối bên ngoài mạng điều khiển.

Mặt khác, nếu kiến trúc DMZ đang được sử dụng, thì có thể định cấu hình hệ thống để không có lưu lượng nào đi trực tiếp giữa mạng công ty và mạng điều khiển. Với một số ngoại lệ đặc biệt (được lưu ý bên dưới), tất cả lưu lượng từ một trong hai bên có thể chấm dứt tại các máy chủ trong DMZ. Điều này cho phép linh hoạt hơn trong các giao thức được phép thông qua tường lửa. Ví dụ: Modbus/TCP có thể được sử dụng để liên lạc từ PLC đến lịch sử dữ liệu, trong khi HTTP có thể được sử dụng để liên lạc giữa lịch sử và khách hàng doanh nghiệp. Cả hai giao thức đều không an toàn, nhưng trong trường hợp này, chúng có thể được sử dụng một cách an toàn vì không giao thức nào thực sự giao nhau giữa hai mạng. Một phần mở rộng cho khái niệm này là ý tưởng sử dụng các giao thức “rời rạc” trong tất cả các mạng điều khiển truyền thông mạng công ty. Nghĩa là, nếu một giao thức được cho phép giữa mạng điều khiển và DMZ, thì giao thức đó rõ ràng là không được phép giữa DMZ và mạng công ty. Thiết kế này làm giảm đáng kể khả năng sâu máy tính như Slammer xâm nhập vào mạng điều khiển, bởi vì sâu máy tính sẽ phải sử dụng hai cách khai thác khác nhau trên hai giao thức khác nhau.

Một lĩnh vực khác biệt đáng kể trong thực tiễn là kiểm soát lưu lượng ra khỏi mạng kiểm soát, điều này có thể gây ra rủi ro đáng kể nếu không được quản lý. Một ví dụ là phần mềm ngựa thành Troa sử dụng đường hầm HTTP để khai thác các quy tắc gửi đi được xác định kém. Vì vậy, điều quan trọng là các quy tắc bên ngoài phải nghiêm ngặt như các quy tắc bên trong.

Ví dụ quy tắc gửi đi bao gồm:

- Lưu lượng gửi đi thông qua tường lửa mạng điều khiển chỉ nên được giới hạn đối với các liên lạc thiết yếu và chỉ nên giới hạn đối với lưu lượng được ủy quyền bắt nguồn từ các máy chủ DMZ.

- Tất cả lưu lượng gửi đi từ mạng điều khiển đến mạng công ty phải được giới hạn nguồn và đích theo dịch vụ và cổng.

Ngoài các quy tắc này, tường lửa phải được cấu hình với bộ lọc gửi đi để ngăn chặn các gói IP giả mạo rời khỏi mạng điều khiển hoặc DMZ. Trong thực tế, điều này đạt được bằng cách kiểm tra địa chỉ IP nguồn của các gói gửi đi so với địa chỉ giao diện mạng tương ứng của tường lửa. Mục đích là để ngăn không cho mạng điều khiển trở thành nguồn liên lạc giả mạo (nghĩa là giả mạo), thường được sử dụng trong các cuộc tấn công DoS. Do đó, tường lửa chỉ nên được cấu hình để chuyển tiếp các gói IP nếu các gói đó có địa chỉ IP nguồn chính xác cho mạng điều khiển hoặc mạng DMZ. Cuối cùng, việc truy cập Internet bằng các thiết bị trên mạng điều khiển nên được khuyến khích mạnh mẽ.

Tóm lại, những điều sau đây nên được coi là thông lệ được đề xuất cho các bộ quy tắc tường lửa chung:

- Bộ quy tắc cơ sở nên từ chối tất cả, không cho phép.

- Các cổng và dịch vụ giữa môi trường mạng điều khiển và mạng công ty phải được bật và cấp quyền theo từng trường hợp cụ thể.

- Cần có lý do kinh doanh được lập thành văn bản cùng với phân tích rủi ro và người chịu trách nhiệm cho từng luồng dữ liệu vào hoặc ra được phép.

- Tất cả các quy tắc “cho phép” phải là cả địa chỉ IP và cổng TCP/UDP cụ thể, và có trạng thái nếu thích hợp.

- Tất cả các quy tắc nên hạn chế lưu lượng truy cập vào một địa chỉ IP hoặc dải địa chỉ cụ thể.

- Lưu lượng nên được ngăn chặn chuyển trực tiếp từ mạng điều khiển sang mạng công ty. Tất cả lưu lượng nên kết thúc trong DMZ.

- Mọi giao thức cho phép giữa mạng điều khiển và DMZ nên dứt khoát KHÔNG cho phép giữa DMZ và mạng công ty (và ngược lại).

- Tất cả lưu lượng gửi đi từ mạng điều khiển đến mạng công ty phải được giới hạn nguồn và đích theo dịch vụ và cổng.

- Các gói gửi đi từ mạng điều khiển hoặc DMZ được phép chỉ khi nếu các gói đó có địa chỉ IP nguồn chính xác được gán cho mạng điều khiển hoặc thiết bị DMZ.

- Các thiết bị mạng điều khiển không được phép truy cập Internet.

- Các mạng điều khiển không được kết nối trực tiếp với Internet, ngay cả khi được bảo vệ thông qua tường lửa.

- Tất cả lưu lượng quản lý tường lửa phải được thực hiện trên mạng quản lý bảo mật, riêng biệt (ví dụ: ngoài băng tần) hoặc qua mạng được mã hóa với xác thực đa yếu tố. Lưu lượng truy cập cũng nên được hạn chế bởi địa chỉ IP đối với các trạm quản lý cụ thể.

- Tất cả các chính sách tường lửa nên được kiểm tra định kỳ.

- Tất cả tường lửa phải được sao lưu ngay lập tức trước khi chạy thử.

Đây chỉ nên được coi là hướng dẫn. Cần phải đánh giá cẩn thận từng môi trường kiểm soát trước khi triển khai bất kỳ bộ quy tắc tường lửa nào.

5.4.8 Quy tắc tường lửa được đề xuất cho các dịch vụ cụ thể

5.4.8.1 Hệ thống tên miền (DNS)

Hệ thống tên miền (DNS) chủ yếu được sử dụng để dịch giữa tên miền và địa chỉ IP. Ví dụ: DNS có thể ánh xạ tên miền chẳng hạn như control.com thành địa chỉ IP chẳng hạn như 192.168.1.1. Hầu hết các dịch vụ Internet chủ yếu dựa vào DNS, nhưng việc sử dụng nó trên mạng điều khiển là tương đối hiếm vào thời điểm này. Trong hầu hết các trường hợp, có rất ít lý do để cho phép các yêu cầu DNS từ mạng điều khiển đến mạng công ty và không có lý do gì để cho phép các yêu cầu DNS vào mạng điều khiển. Các yêu cầu DNS từ mạng điều khiển đến DMZ phải được xử lý cơ bản theo từng trường hợp. DNS cục bộ hoặc sử dụng tệp máy chủ được khuyến nghị

5.4.8.2 Giao thức truyền siêu văn bản (HTTP)

HTTP là giao thức nằm bên dưới các dịch vụ duyệt Web trên Internet. Giống như DNS, nó rất quan trọng đối với hầu hết các dịch vụ Internet. Nó đang được sử dụng ngày càng nhiều trên sàn nhà máy cũng như một công cụ truy vấn đa năng. Thật không may, nó có rất ít bảo mật vốn có và nhiều ứng dụng HTTP có lỗ hổng có thể bị khai thác. HTTP có thể là một cơ chế vận chuyển cho nhiều cuộc tấn công được thực hiện thủ công và sâu máy tính tự động.

HTTP không được phép chuyển từ mạng công cộng/công ty sang mạng điều khiển. Nếu các công nghệ dựa trên web là hoàn toàn bắt buộc, thì nên áp dụng các phương pháp hay nhất sau đây:

- Kiểm soát quyền truy cập vào các dịch vụ dựa trên web trên lớp vật lý hoặc lớp mạng bằng cách sử dụng danh sách trắng;

- Áp dụng kiểm soát truy cập cho cả nguồn và đích;

- Thực hiện ủy quyền để truy cập dịch vụ trên lớp ứng dụng (thay vì kiểm tra vật lý hoặc lớp mạng);

- Triển khai dịch vụ chỉ sử dụng các công nghệ cần thiết (ví dụ: các tập lệnh chỉ được sử dụng nếu chúng được yêu cầu);

- Kiểm tra dịch vụ theo các thông lệ bảo mật ứng dụng đã biết;

- Ghi lại tất cả các nỗ lực sử dụng dịch vụ;

- Sử dụng HTTPS thay vì HTTP và chỉ dành cho các thiết bị được ủy quyền cụ thể.

5.4.8.3 FTP và Giao thức truyền tệp tầm thường (TFTP)

FTP và Giao thức truyền tệp tầm thường (TFTP) được sử dụng để truyền tệp giữa các thiết bị. Chúng được triển khai trên hầu hết mọi nền tảng bao gồm nhiều hệ thống SCADA, DCS, PLC và RTU, vì chúng rất nổi tiếng và sử dụng sức mạnh xử lý tối thiểu. Thật không may, không có giao thức nào được tạo ra với mục đích bảo mật; đối với FTP, mật khẩu đăng nhập không được mã hóa và đối với TFTP, không yêu cầu đăng nhập. Hơn nữa, một số triển khai FTP có lịch sử lỗ hổng tràn bộ đệm. Do đó, tất cả các giao tiếp TFTP sẽ bị chặn, trong khi giao tiếp FTP chỉ được phép cho các phiên gửi đi hoặc nếu được bảo mật bằng xác thực đa yếu tố dựa trên mã thông báo bổ sung và một đường hầm được mã hóa. Các giao thức an toàn hơn, chẳng hạn như FTP an toàn (SFTP) hoặc Sao chép an toàn (SCP), nên được sử dụng bất cứ khi nào có thể.

5.4.8.4 Telnet

Giao thức telnet xác định một phiên giao tiếp dựa trên văn bản tương tác giữa máy khách và máy chủ. Nó được sử dụng chủ yếu cho các dịch vụ đăng nhập từ xa và điều khiển đơn giản cho các hệ thống có tài nguyên hạn chế hoặc các hệ thống có nhu cầu bảo mật hạn chế. Đây là một rủi ro bảo mật nghiêm trọng vì tất cả lưu lượng telnet, bao gồm cả mật khẩu, đều không được mã hóa và nó có thể cho phép một cá nhân từ xa kiểm soát đáng kể thiết bị. Nên sử dụng giao thức Secure Shell (SSH) để quản trị từ xa. Các phiên telnet gửi từ công ty đến mạng điều khiển nên bị cấm trừ khi được bảo mật bằng xác thực đa yếu tố dựa trên mã thông báo và đường hầm được mã hóa. Các phiên telnet gửi đi chỉ được phép qua các đường hầm được mã hóa (ví dụ: VPN) tới các thiết bị được ủy quyền cụ thể.

5.4.8.5 Giao thức cấu hình máy chủ động (DHCP)

DHCP được sử dụng trên các mạng IP để phân phối động các tham số cấu hình mạng, chẳng hạn như địa chỉ IP cho các giao diện và dịch vụ. DHCP cơ sở không bao gồm cơ chế xác thực máy chủ và máy khách. Máy chủ DHCP giả mạo có thể cung cấp thông tin không chính xác cho khách hàng. Máy khách trái phép có thể có quyền truy cập vào máy chủ và gây cạn kiệt tài nguyên có sẵn (ví dụ: địa chỉ IP). Để ngăn chặn điều này, nên sử dụng cấu hình tĩnh thay vì phân bổ địa chỉ động, đây phải là cấu hình điển hình cho các thiết bị ICS. Nếu cần phân bổ động, bạn nên bật mò DHCP để bảo vệ chống lại các máy chủ DHCP giả mạo, Giao thức phân giải địa chỉ (ARP) và giả mạo IP. Các máy chủ DHCP phải được đặt trong cùng một phân đoạn mạng với thiết bị được định cấu hình (ví dụ: trên bộ định tuyến). Chuyển tiếp DHCP không được khuyến khích.

5.4.8.6 Lớp bảo mật (SSH)

SSH cho phép truy cập từ xa vào một thiết bị. Nó cung cấp xác thực và ủy quyền an toàn dựa trên mật mã. Nếu cần truy cập từ xa vào mạng điều khiển, SSH được khuyến nghị là giải pháp thay thế cho telnet, rlogin, rsh, rcp và các công cụ truy cập từ xa không an toàn khác

5.4.8.7 Giao thức truy cập đối tượng đơn giản (SOAP)

SOAP là một cú pháp định dạng dựa trên XML để trao đổi thông điệp. Các luồng lưu lượng liên quan đến các dịch vụ dựa trên SOAP nên được kiểm soát tại tường lửa giữa các phân đoạn mạng công ty và ICS. Nếu các dịch vụ này là cần thiết, nên sử dụng tường lửa kiểm tra gói sâu và/hoặc lớp ứng dụng để hạn chế nội dung của thư.

5.4.8.8 Giao thức truyền thư đơn giản (SMTP)

SMTP là giao thức chuyển email chính trên Internet. Thư email thường chứa phần mềm độc hại, vì vậy không được phép gửi email đến bất kỳ thiết bị mạng điều khiển nào. Thư SMTP gửi đi từ mạng điều khiển đến mạng công ty được chấp nhận để gửi thông báo cảnh báo.

5.4.8.9 Giao thức quản lý mạng đơn giản (SNMP)

SNMP được sử dụng để cung cấp các dịch vụ quản lý mạng giữa bảng điều khiển quản lý trung tâm và các thiết bị mạng như bộ định tuyến, máy in và PLC. Mặc dù SNMP là một dịch vụ cực kỳ hữu ích để duy trì mạng, nhưng nó lại rất yếu về bảo mật. Phiên bản 1 và 2 của SNMP sử dụng mật khẩu không được mã hóa để đọc và định cấu hình thiết bị (bao gồm cả thiết bị như PLC) và trong nhiều trường hợp, mật khẩu đã được biết rõ và không thể thay đổi. Phiên bản 3 an toàn hơn đáng kể nhưng vẫn còn hạn chế sử dụng. Các lệnh SNMP V1 & V2 đến và từ mạng điều khiển đều bị cấm trừ khi chúng ở trên một mạng quản lý bảo mật, riêng biệt, trong khi các lệnh SNMP V3 có thể được gửi đến ICS bằng các tính năng bảo mật vốn có của V3.

5.4.8.10 Đối tượng thành phần phân tán Mô hình (DCOM)

DCOM là giao thức cơ bản cho OLE cho Kiểm soát quy trình (OPC). Nó sử dụng dịch vụ Cuộc gọi thủ tục từ xa (RPC) của Microsoft, khi chưa được vá, có nhiều lỗ hổng. Những lỗ hổng này là cơ sở cho việc khai thác Blaster worm14. Ngoài ra, OPC, sử dụng DCOM, tự động mở nhiều loại cổng (1024 đến 65535) có thể cực kỳ khó lọc tại tường lửa. Giao thức này chỉ nên được cho phép giữa mạng điều khiển và mạng DMZ và bị chặn rõ ràng giữa DMZ và mạng công ty. Ngoài ra, người dùng nên hạn chế phạm vi cổng được sử dụng bằng cách thực hiện sửa đổi sổ đăng ký trên thiết bị sử dụng DCOM.

5.4.8.11 SCADA và các giao thức công nghiệp

SCADA và các giao thức công nghiệp, chẳng hạn như Modbus/TCP, EtherNet/IP, IEC 61850, ICCP và DNP315, rất quan trọng để liên lạc với hầu hết các thiết bị điều khiển. Thật không may, nhiều giao thức trong số này được thiết kế mà không có bảo mật tích hợp sẵn và thường không yêu cầu bất kỳ xác thực nào để thực thi các lệnh từ xa trên thiết bị điều khiển. Các giao thức này chỉ được phép trong mạng điều khiển và không được phép đi vào mạng công ty.

5.4.9 Dịch địa chỉ mạng (NAT)

Dịch địa chỉ mạng (NAT) là dịch vụ trong đó các địa chỉ IP được sử dụng trên một mặt của thiết bị mạng có thể được ánh xạ sang một bộ khác ở mặt kia trên cơ sở khi cần. Ban đầu nó được thiết kế cho mục đích giảm địa chỉ IP để một tổ chức có số lượng lớn thiết bị thỉnh thoảng cần truy cập Internet có thể sử dụng một nhóm địa chỉ Internet được chỉ định nhỏ hơn.

Để làm điều này, hầu hết các triển khai NAT đều dựa trên tiền đề rằng không phải mọi thiết bị bên trong đều đang giao tiếp tích cực với các máy chủ bên ngoài tại một thời điểm nhất định. Tường lửa được cấu hình để có một số địa chỉ IP hiển thị bên ngoài giới hạn. Khi một máy chủ nội bộ tìm cách liên lạc với một máy chủ bên ngoài,để hạn chế hơn tường lửa sẽ ánh xạ lại địa chỉ IP nội bộ và cổng tới một trong những địa chỉ IP công cộng, tập trung hiệu quả lưu lượng truy cập đi vào ít địa chỉ IP hơn. Tường lửa phải theo dõi trạng thái của từng kết nối và cách mà mỗi địa chỉ IP nội bộ riêng và cổng nguồn được ánh xạ lại vào một cặp địa chỉ/cổng IP có thể nhìn thấy bên ngoài. Khi lưu lượng truy cập trở lại tường lửa, ánh xạ bị đảo ngược và các gói được chuyển tiếp đến máy chủ nội bộ thích hợp.

Ví dụ: thiết bị mạng điều khiển có thể cần thiết lập kết nối với máy chủ mạng bên ngoài, không điều khiển (ví dụ: để gửi email cảnh báo quan trọng). NAT cho phép thay thế địa chỉ IP nội bộ của máy chủ mạng điều khiển khởi tạo bằng tường lửa; các gói lưu lượng truy cập trở lại tiếp theo được ánh xạ trở lại địa chỉ IP nội bộ và được gửi đến thiết bị mạng điều khiển thích hợp. Cụ thể hơn, nếu mạng điều khiển được chỉ định mạng con riêng 192.168.1.xxx và mạng Internet mong muốn thiết bị sử dụng địa chỉ được chỉ định của công ty trong dải 192.6.yyy.zzz, thì tường lửa NAT sẽ thay thế (và theo dõi) một địa chỉ nguồn 192.6.yyy.zzz vào mọi gói IP gửi đi do thiết bị mạng điều khiển tạo ra.

Các giao thức nhà sản xuất-người tiêu dùng, chẳng hạn như EtherNet/IP và nền tảng Fieldbus, đặc biệt rắc rối vì NAT không hỗ trợ lưu lượng dựa trên phát đa hướng mà các giao thức này cần để cung cấp các dịch vụ đầy đủ của chúng.

Nói chung, mặc dù NAT mang lại một số lợi thế khác biệt nhưng tác động của nó đối với các giao thức và cấu hình công nghiệp thực tế cần được đánh giá cẩn thận trước khi triển khai. Hơn nữa, một số giao thức nhất định bị phá vỡcụ thể bởi NAT do thiếu địa chỉ trực tiếp. Ví dụ: OPC yêu cầu phần mềm đường hầm đặc biệt của bên thứ ba hoạt động với NAT.

5.4.10 Các vấn đề về tường lửa ICS cụ thể

Ngoài các vấn đề về tường lửa và ICS đã được thảo luận, còn có một số vấn đề khác cần được xem xét chi tiết hơn. Phần còn lại của phần này thảo luận về ba lĩnh vực quan tâm cụ thể: vị trí của lịch sử dữ liệu, truy cập từ xa để hỗ trợ ICS và lưu lượng phát đa hướng.

5.4.10.1 Máy chủ lưu trữ dữ liệu

Sự tồn tại của các máy chủ mạng điều khiển/mạng công ty dùng chung như máy chủ lưu trữ dữ liệuvà máy chủ quản lý tài sản có thể có tác động đáng kể đến thiết kế và cấu hình tường lửa. Trong hệ thống ba vùng, việc đặt các máy chủ này trong DMZ tương đối đơn giản, nhưng trong thiết kế hai vùng, các vấn đề trở nên phức tạp. Đặt lịch sử ở phía công ty của tường lửa có nghĩa là một số giao thức không an toàn, chẳng hạn như Modbus/TCP hoặc DCOM, phải được phép đi qua tường lửa và mọi thiết bị điều khiển báo cáo cho lịch sử đều được hiển thị ở phía công ty của mạng. Mặt khác, đặt lịch sử ở phía mạng điều khiển có nghĩa là các giao thức có vấn đề không kém khác, chẳng hạn như HTTP hoặc SQL, phải được phép thông qua tường lửa và hiện tại có một máy chủ có thể truy cập được đối với hầu hết mọi người trong tổ chức trên mạng điều khiển.

Giải pháp tốt nhất là tránh các hệ thống hai vùng (không có DMZ) và sử dụng thiết kế ba vùng, đặt bộ thu thập dữ liệu trong mạng điều khiển và thành phần lịch sử trong DMZ.

5.4.10.2 Truy cập hỗ trợ từ xa

Một vấn đề khác đối với thiết kế tường lửa ICS là quyền truy cập từ xa của người dùng và/hoặc nhà cung cấp vào mạng điều khiển. Bất kỳ người dùng nào truy cập mạng điều khiển từ các mạng từ xa đều phải được yêu cầu xác thực bằng cơ chế mạnh thích hợp, chẳng hạn như xác thực dựa trên mã thông báo. Mặc dù nhóm kiểm soát có thể thiết lập hệ thống truy cập từ xa của riêng họ với xác thực đa yếu tố trên DMZ, nhưng trong hầu hết các tổ chức, việc sử dụng các hệ thống hiện có do bộ phận CNTT thiết lập thường hiệu quả hơn. Trong trường hợp này, cần có kết nối thông qua tường lửa từ máy chủ truy cập từ xa CNTT.

Nhân viên hỗ trợ từ xa kết nối qua Internet hoặc qua modem quay số nên sử dụng giao thức được mã hóa, chẳng hạn như chạy máy khách kết nối VPN công ty, máy chủ ứng dụng hoặc truy cập HTTP an toàn và xác thực bằng cơ chế mạnh, chẳng hạn như xác thực đa yếu tố dựa trên mã thông báo chương trình, để kết nối với mạng công ty chung. Nhân viên hỗ trợ từ xa kết nối qua Internet hoặc qua modem quay số nên sử dụng giao thức được mã hóa. Sau khi kết nối, họ sẽ được yêu cầu xác thực lần thứ hai tại tường lửa mạng điều khiển bằng cơ chế mạnh, chẳng hạn như sơ đồ xác thực đa yếu tố dựa trên mã thông báo, để có được quyền truy cập vào mạng điều khiển. Máy chủ proxy cũng có thể cung cấp các khả năng bổ sung để đảm bảo quyền truy cập hỗ trợ từ xa.

5.4.10.3 Lưu lượng phát đa hướng

Hầu hết các giao thức công nghiệp của nhà sản xuất-người tiêu dùng (hoặc nhà xuất bản thuê bao) hoạt động qua Ethernet, chẳng hạn như EtherNet/IP và Nền tảng Fieldbus HSE, đều dựa trên IP phát đa hướng. Ưu điểm đầu tiên của phát đa hướng IP là hiệu quả của mạng; bằng cách không lặp lại việc truyền dữ liệu đến nhiều đích, có thể giảm tải mạng đáng kể. Ưu điểm thứ hai là máy chủ gửi không cần quan tâm đến việc biết mọi địa chỉ IP của mọi máy chủ đích đang nghe thông tin quảng bá. Thứ ba, và có lẽ là quan trọng nhất đối với các mục đích điều khiển công nghiệp, đó là một thông báo phát đa hướng duy nhất cung cấp khả năng đồng bộ hóa thời gian giữa nhiều thiết bị điều khiển tốt hơn nhiều so với nhiều thông báo đơn hướng.

Nếu nguồn và đích của gói phát đa hướng được kết nối mà không có bộ định tuyến hoặc tường lửa can thiệp giữa chúng, thì việc truyền phát đa hướng tương đối liền mạch. Tuy nhiên, nếu nguồn và đích không nằm trong cùng một mạng LAN, việc chuyển tiếp các thông báo phát đa hướng đến đích sẽ trở nên phức tạp hơn. Để giải quyết vấn đề định tuyến thông báo phát đa hướng, các máy chủ cần tham gia (hoặc rời khỏi) một nhóm bằng cách thông báo cho bộ định tuyến phát đa hướng trên mạng của họ về ID nhóm có liên quan thông qua việc sử dụng Giao thức quản lý nhóm Internet (IGMP). Các bộ định tuyến phát đa hướng sau đó biết các thành viên của nhóm phát đa hướng trên mạng của họ và có thể quyết định có chuyển tiếp một thông báo phát đa hướng đã nhận được vào mạng của họ hay không. Một giao thức định tuyến đa hướng cũng được yêu cầu. Từ góc độ quản trị tường lửa, việc giám sát và lọc lưu lượng IGMP trở thành một loạt các bộ quy tắc khác để quản lý, làm tăng thêm độ phức tạp của tường lửa.

Một vấn đề tường lửa khác liên quan đến phát đa hướng là việc sử dụng NAT. Tường lửa thực hiện NAT nhận gói phát đa hướng từ máy chủ bên ngoài không có ánh xạ ngược cho ID nhóm bên trong sẽ nhận dữ liệu. Nếu nhận biết IGMP, nó có thể phát nó tới mọi ID nhóm mà nó biết, vì một trong số chúng sẽ đúng, nhưng điều này có thể gây ra sự cố nghiêm trọng nếu một gói điều khiển ngoài ý muốn được phát tới một nút quan trọng. Hành động an toàn nhất để tường lửa thực hiện là loại bỏ gói tin. Do đó, việc phát đa hướng thường được coi là không thân thiện với NAT.

5.4.11 Cổng một chiều

Các cổng một chiều được thực thi bằng phần cứng (ví dụ: điốt dữ liệu) ngày càng được triển khai ở ranh giới giữa mạng ICS và mạng CNTT, cũng như giữa mạng Hệ thống thiết bị an toàn và mạng điều khiển. Cổng một chiều là sự kết hợp giữa phần cứng và phần mềm. Phần cứng cho phép dữ liệu truyền từ mạng này sang mạng khác, nhưng về mặt vật lý không thể gửi bất kỳ thông tin nào trở lại mạng nguồn. Phần mềm sao chép cơ sở dữ liệu và mô phỏng các máy chủ và thiết bị giao thức.

5.4.12 Điểm lỗi đơn lẻ

Các điểm lỗi đơn lẻ có thể tồn tại ở bất kỳ cấp độ nào của ngăn xếp ANSI/ISO. Một ví dụ là điều khiển PLC của khóa liên động an toàn. Vì bảo mật thường được thêm vào môi trường ICS, nên việc đánh giá phải được thực hiện để xác định các điểm lỗi tiềm ẩn và đánh giá rủi ro được thực hiện để đánh giá mức độ tiếp xúc của từng điểm. Các phương pháp khắc phục sau đó có thể được đưa ra và đánh giá, đồng thời xác định “rủi ro so với phần thưởng” cũng như thiết kế và triển khai được hoàn thành.

5.4.13 Tình trạng dư thừa và khả năng chịu lỗi

Các thành phần hoặc mạng ICS được phân loại là quan trọng đối với tổ chức có yêu cầu về tính sẵn sàng cao. Một phương pháp để đạt được tính sẵn sàng cao là thông qua việc sử dụng dự phòng. Ngoài ra, nếu một thành phần bị lỗi, thì nó nên bị lỗi theo cách không tạo ra lưu lượng không cần thiết trên ICS hoặc không gây ra sự cố khác ở nơi khác, chẳng hạn như sự kiện xếp tầng.

Hệ thống điều khiển phải có khả năng thực hiện quy trình dự phòng an toàn phù hợp khi mất liên lạc với ICS hoặc mất chính ICS. Tổ chức nên xác định "mất liên lạc" nghĩa là gì (ví dụ: 500 mili giây, 5 giây, 5 phút, v.v. không có liên lạc). Sau đó, tổ chức nên, dựa trên các hậu quả tiềm ẩn, xác định quy trình an toàn khi xảy ra sự cố thích hợp cho ngành của họ.

Các bản sao lưu nên được thực hiện bằng cách sử dụng phương pháp "sao lưu chuyên sâu", với các lớp sao lưu (ví dụ: cục bộ, cơ sở, thảm họa) được sắp xếp theo thời gian sao cho các bản sao lưu cục bộ gần đây nhanh chóng có sẵn để sử dụng ngay và các bản sao lưu an toàn có sẵn để khôi phục từ một sự cố an toàn lớn. Nên sử dụng kết hợp các phương pháp sao lưu/khôi phục và phương pháp lưu trữ để đảm bảo rằng các bản sao lưu được tạo ra một cách chặt chẽ, lưu trữ an toàn và có thể truy cập phù hợp để khôi phục.

5.4.14 Ngăn chặn các cuộc tấn công trung gian

Một cuộc tấn công trung gian đòi hỏi kiến thức về giao thức đang bị thao túng. Cuộc tấn công trung gian của Giao thức phân giải địa chỉ (ARP) là một phương pháp phổ biến để hacker có quyền truy cập vào luồng thông tin mạng trên hệ thống đích. Điều này được thực hiện bằng cách tấn công các bảng bộ đệm ARP mạng của bộ điều khiển và máy trạm. Sử dụng máy tính bị xâm nhập trên mạng điều khiển, hacker đầu độc các bảng ARP trên mỗi máy chủ và thông báo cho họ rằng họ phải định tuyến tất cả lưu lượng truy cập của mình thông qua một địa chỉ phần cứng và IP cụ thể (tức là máy của hacker). Bằng cách thao túng các bảng ARP, hacker có thể chèn máy của chúng vào giữa hai máy và/hoặc thiết bị mục tiêu.

Cuộc tấn công trung gian ARP hoạt động bằng cách bắt đầu các lệnh ARP vô cớ để gây nhầm lẫn cho từng máy chủ (tức là đầu độc ARP). Các lệnh ARP này khiến mỗi một trong hai máy chủ mục tiêu sử dụng địa chỉ MAC của đối thủ làm địa chỉ cho máy chủ mục tiêu khác. Khi một cuộc tấn công trung gian thành công được thực hiện, các máy chủ ở mỗi bên của cuộc tấn công không biết rằng dữ liệu mạng của họ đang đi theo một con đường khác thông qua máy tính của hacker.

Sau khi hacker đã đưa thành công máy của họ vào luồng thông tin, giờ đây họ có toàn quyền kiểm soát việc truyền dữ liệu và có thể thực hiện một số kiểu tấn công. Một phương pháp tấn công có thể là tấn công lặp lại. Ở dạng đơn giản nhất, dữ liệu đã chụp từ điều khiển/HMI được sửa đổi để khởi tạo hoạt động khi bộ điều khiển thiết bị nhận được. Dữ liệu đã chụp phản ánh các hoạt động bình thường trong ICS có thể được phát lại cho người vận hành theo yêu cầu. Điều này sẽ khiến HMI của người vận hành có vẻ bình thường và cuộc tấn công sẽ không bị quan sát. Trong cuộc tấn công lặp lại này, hacker có thể tiếp tục gửi lệnh đến bộ điều khiển và/hoặc thiết bị hiện trường để gây ra sự kiện không mong muốn trong khi người vận hành không biết về trạng thái thực sự của hệ thống.

Một cuộc tấn công khác có thể được thực hiện với cuộc tấn công trung gian là gửi thông báo sai cho người điều hành và có thể ở dạng âm tính giả hoặc dương tính giả. Điều này có thể khiến người vận hành thực hiện một hành động, chẳng hạn như lật cầu dao, khi không cần thiết, hoặc có thể khiến người vận hành nghĩ rằng mọi thứ đều ổn và không thực hiện hành động khi hành động đó được yêu cầu. Hacker có thể gửi lệnh đến bảng điều khiển của người vận hành để chỉ ra sự thay đổi hệ thống và khi người vận hành tuân theo các quy trình thông thường và cố gắng khắc phục sự cố, hành động của người vận hành có thể gây ra sự kiện không mong muốn. Có các biến thể của việc sửa đổi và phát lại dữ liệu điều khiển mà điều đó có thể ảnh hưởng đến hoạt động của hệ thống.

Thao tác giao thức và tấn công trung gian là một trong những cách phổ biến nhất để thao tác các giao thức không an toàn, chẳng hạn như các giao thức được tìm thấy trong các hệ thống điều khiển. Tuy nhiên, có những kỹ thuật giảm thiểu có thể được áp dụng để bảo mật hệ thống thông qua khóa địa chỉ MAC, bảng tĩnh, mã hóa, xác thực và giám sát.

- Khóa địa chỉ MAC - Cuộc tấn công trung gian ARP yêu cầu đối thủ phải được kết nối với mạng cục bộ hoặc có quyền kiểm soát máy tính cục bộ trên mạng. Bảo mật cổng, còn được gọi là khóa địa chỉ MAC, là một phương pháp để bảo mật kết nối vật lý ở cuối mỗi cổng trên bộ chuyển đổi mạng. Thiết bị chuyển mạch mạng cấp doanh nghiệp cao cấp thường có một số loại tùy chọn để khóa địa chỉ MAC. Khóa địa chỉ MAC rất hiệu quả đối với một cá nhân lừa đảo đang tìm cách kết nối vật lý vào mạng nội bộ. Nếu không có bảo mật cổng, bất kỳ giắc cắm mạng mở nào trên tường đều có thể được sử dụng làm đường dẫn vào mạng doanh nghiệp. Bảo mật cổng khóa một địa chỉ MAC cụ thể vào một cổng cụ thể trên một công tắc được quản lý. Nếu địa chỉ MAC không khớp, liên kết giao tiếp sẽ bị vô hiệu hóa và kẻ xâm nhập sẽ không thể đạt được mục tiêu của chúng. Một số công tắc nâng cao hơn có tùy chọn đặt lại tự động, tùy chọn này sẽ đặt lại biện pháp bảo mật nếu MAC ban đầu được đưa trở lại cổng.

- Mặc dù bảo mật cổng không phải là bằng chứng của kẻ tấn công, nhưng nó bổ sung thêm một lớp bảo mật bổ sung cho mạng vật lý. Nó cũng bảo vệ mạng cục bộ khỏi việc nhân viên cắm các hệ thống chưa được vá lỗi và lỗi thời vào mạng được bảo vệ. Điều này làm giảm số lượng mục tiêu máy tính mà hacker từ xa có thể truy cập. Các biện pháp bảo mật này không chỉ bảo vệ chống lại các cuộc tấn công từ các mạng bên ngoài mà còn cung cấp thêm khả năng bảo vệ vật lý.

- Bảng tĩnh – Một mạng ICS tương đối tĩnh có thể cố triển khai các bảng ARP được mã hóa tĩnh. Hầu hết các hệ điều hành đều có khả năng mã hóa tĩnh tất cả các địa chỉ MAC vào bảng ARP trên mỗi máy tính. Mã hóa tĩnh các bảng ARP trên mỗi máy tính ngăn không cho hacker thay đổi chúng bằng cách gửi các gói trả lời ARP đến máy tính nạn nhân. Mặc dù kỹ thuật này không khả thi trên mạng công ty lớn và/hoặc năng động, nhưng số lượng máy chủ hạn chế trên mạng ICS có thể được bảo vệ hiệu quả theo cách này.

- Mã hóa - Là một giải pháp dài hạn, các hệ thống nên được thiết kế để bao gồm mã hóa giữa các thiết bị nhằm gây khó khăn cho việc đảo ngược các giao thức và giả mạo các gói trên mạng của hệ thống điều khiển. Việc mã hóa thông tin liên lạc giữa các thiết bị sẽ khiến cho cuộc tấn công này gần như không thể thực hiện được. Các giao thức cung cấp xác thực mạnh cũng cung cấp khả năng phục hồi trước các cuộc tấn công trung gian. Tác động của mã hóa đối với hiệu suất hoạt động và mạng cần được xem xét.

- Xác thực - Các giao thức có xác thực mạnh cung cấp khả năng phục hồi trước các cuộc tấn công trung gian.

- Giám sát - Giám sát nhiễm độc ARP cung cấp thêm một lớp phòng thủ. Có một số chương trình có sẵn (ví dụ: ARPwatch) có thể giám sát việc thay đổi địa chỉ MAC thông qua các gói ARP.

5.4.15 Xác thực và uỷ quyền

Một ICS có thể chứa một số lượng lớn các hệ thống, mỗi hệ thống phải được truy cập bởi nhiều người dùng khác nhau. Việc thực hiện xác thực và ủy quyền cho những người dùng này là một thách thức đối với ICS. Việc quản lý tài khoản của những người dùng này có thể gặp vấn đề khi nhân viên được thêm, xóa và khi vai trò của họ thay đổi. Khi số lượng hệ thống và người dùng tăng lên, quá trình quản lý các tài khoản này trở nên phức tạp hơn.

Việc xác thực người dùng hoặc hệ thống là quá trình xác minh danh tính được yêu cầu. Ủy quyền, quá trình phân loại các đặc quyền truy cập của người dùng, được xác định bằng cách áp dụng các quy tắc chính sách cho danh tính được xác thực và các thông tin liên quan khác16. Ủy quyền được thực thi bởi một số cơ chế kiểm soát truy cập. Quá trình xác thực có thể được sử dụng để kiểm soát quyền truy cập vào cả hệ thống (ví dụ: HMI, thiết bị hiện trường, máy chủ SCADA) và mạng (ví dụ: mạng LAN của trạm biến áp từ xa).

Xác thực và ủy quyền có thể được thực hiện theo cách tiếp cận phân tán hoặc tập trung. Với xác thực và ủy quyền phân tán, mọi hệ thống sẽ tự thực hiện các bước này. Mỗi hệ thống chịu trách nhiệm lưu trữ bộ tài khoản người dùng, thông tin đăng nhập và vai trò của riêng mình và thực hiện nhận dạng và xác thực người dùng. Cách tiếp cận này thường không yêu cầu bất kỳ cơ sở hạ tầng bổ sung nào. Tuy nhiên, cách tiếp cận này có vấn đề ở chỗ nó không mở rộng tốt khi kích thước của hệ thống tăng lên. Ví dụ: nếu người dùng rời khỏi tổ chức, tài khoản người dùng tương ứng phải được xóa khỏi từng hệ thống riêng lẻ.

Trái ngược với cách tiếp cận phân tán, các hệ thống xác thực và ủy quyền tập trung thường được sử dụng để quản lý số lượng người dùng và tài khoản lớn hơn. Cách tiếp cận tập trung sử dụng một số hệ thống xác thực trung tâm (ví dụ: Microsoft Active Directory, Giao thức truy cập thư mục nhẹ (LDAP) để lưu trữ tất cả tài khoản và quản lý xác thực cũng như ủy quyền của tất cả các cá nhân và hệ thống. Giao thức xác thực (ví dụ: Kerberos, RADIUS, TACACS+) sau đó được sử dụng để liên lạc dữ liệu giữa máy chủ xác thực và hệ thống thực hiện xác thực.

Mặc dù cách tiếp cận tập trung cung cấp cải thiện đáng kể khả năng mở rộng, nhưng nó cũng đưa ra nhiều mối lo ngại bổ sung có thể ảnh hưởng đến việc sử dụng nó trong môi trường ICS. Những cân nhắc sau đây được áp dụng:

- Các máy chủ xác thực tạo ra một hệ thống duy nhất chịu trách nhiệm quản lý tất cả các tài khoản của hệ thống và phải được bảo mật cao.

- Hệ thống máy chủ xác thực yêu cầu tính sẵn sàng cao vì lỗi của nó có thể ngăn chặn người dùng xác thực với hệ thống trong trường hợp khẩn cấp. Dự phòng có thể được yêu cầu.

- Một số máy khách có thể lưu trữ cục bộ thông tin đăng nhập của người dùng để đảm bảo rằng người dùng vẫn có thể được xác thực khi không có máy chủ. Bộ nhớ đệm chỉ có thể khả dụng cho những người dùng đã được xác thực gần đây. Bộ nhớ đệm cũng giới thiệu các biến chứng để thu hồi.

- Các mạng được sử dụng để hỗ trợ giao thức xác thực phải đáng tin cậy và an toàn để đảm bảo các nỗ lực xác thực không bị cản trở.

5.4.15.1 Cân nhắc triển khai ICS

Mặc dù các máy chủ xác thực và ủy quyền tập trung thường được sử dụng trong môi trường CNTT, nhưng chúng có nhiều thách thức khi tích hợp chúng vào ICS. Mặc dù các giao thức và máy chủ xác thực tích hợp với nhiều sản phẩm CNTT hàng hóa (ví dụ: Microsoft Windows, Linux, Oracle), nhưng ICS thường có thể sử dụng các tài khoản và cơ chế xác thực dành riêng cho ứng dụng của riêng chúng không được thiết kế để giao tiếp với các giao thức và máy chủ của bên thứ ba. Điều này hạn chế việc áp dụng cơ chế như vậy trong môi trường ICS. Các thiết bị mạng cũ hơn và hầu hết các thiết bị trường không hỗ trợ bất kỳ cơ chế nào để tích hợp với hệ thống xác thực tập trung.

5.4.16 Giám sát, Ghi nhật ký và Kiểm tra

Kiến trúc bảo mật của ICS cũng phải kết hợp các cơ chế để giám sát, ghi nhật ký và kiểm tra các hoạt động xảy ra trên các hệ thống và mạng khác nhau. Các hoạt động giám sát, ghi nhật ký và kiểm tra là bắt buộc để hiểu được trạng thái hiện tại của ICS, xác thực rằng hệ thống đang hoạt động như dự định và không có vi phạm chính sách hoặc sự cố mạng nào cản trở hoạt động của hệ thống. Giám sát an toàn mạng rất có giá trị để mô tả trạng thái bình thường của ICS và có thể cung cấp dấu hiệu cho thấy các hệ thống bị xâm nhập khi các công nghệ dựa trên chữ ký gặp sự cố. Ngoài ra, cần phải giám sát, ghi nhật ký và kiểm tra hệ thống mạnh mẽ để khắc phục sự cố và thực hiện bất kỳ phân tích pháp y cần thiết nào đối với hệ thống.

5.4.17 Phát hiện sự cố, ứng phó và khôi phục hệ thống

Sự cố là không thể tránh khỏi và các kế hoạch phát hiện, ứng phó và khôi phục hệ thống là rất cần thiết. Các đặc điểm chính của một chương trình bảo mật tốt là thời gian phát hiện sự cố ngay sau khi sự cố xảy ra và hệ thống có thể được khôi phục nhanh như thế nào sau khi sự cố được phát hiện. Ứng phó sự cố trong ICS được liên kết chặt chẽ với khắc phục thảm họa, đặc biệt là để giải quyết các yêu cầu nghiêm ngặt về thời gian hoạt động của ICS. Người ứng phó sự cố phải được đào tạo cho các tình huống dành riêng cho ICS, vì các phương pháp khôi phục hệ thống CNTT thông thường có thể không áp dụng cho ICS.

5.5 Biện pháp kiểm soát bảo mật cho các hệ thống điều khiển công nghiệp ICS.

Một sản phẩm hoặc công nghệ bảo mật đơn lẻ không đủ để bảo vệ một hệ thống Điều khiển Công nghiệp (ICS) một cách đầy đủ. Việc bảo mật một ICS dựa trên sự kết hợp giữa các chính sách bảo mật hiệu quả và một bộ các biện pháp kiểm soát bảo mật được cấu hình đúng. Việc lựa chọn và triển khai các biện pháp kiểm soát bảo mật để áp dụng cho một ICS có thể có những tác động lớn đến hoạt động, do đó, việc cân nhắc các yếu tố sau là rất quan trọng:

- Các biện pháp kiểm soát bảo mật nào cần thiết để giảm thiểu rủi ro một cách đủ độ, đồng thời hỗ trợ các nhiệm vụ và chức năng kinh doanh của tổ chức?

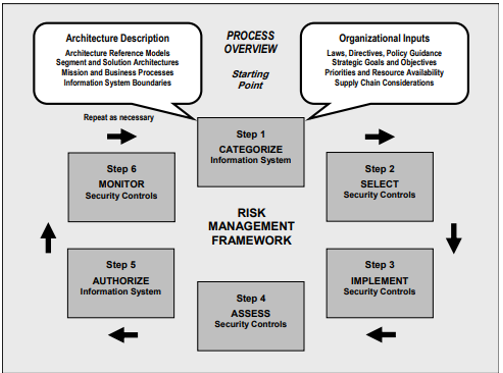
- Các biện pháp kiểm soát bảo mật đã được triển khai hay có kế hoạch triển khai thực tế?

- Mức độ đảm bảo cần thiết cho việc triển khai chính xác các biện pháp kiểm soát bảo mật đã chọn, hoạt động theo ý định và đạt được kết quả mong muốn là gì?

Các câu hỏi này nên được trả lời trong ngữ cảnh của một quy trình quản lý rủi ro toàn diện và chiến lược an toàn mạng tổ chức, xác định, giảm thiểu (nếu cần) và liên tục giám sát các rủi ro đối với hệ thống ICS. Một chiến lược an toàn mạng hiệu quả cho một ICS nên áp dụng nguyên tắc "defense-in-depth" (bảo vệ đa lớp), một kỹ thuật xây dựng các cơ chế bảo mật theo tầng lớp sao cho tác động của một thảm họa trong bất kỳ cơ chế nào cũng được giảm thiểu. Sử dụng chiến lược như vậy được khám phá trong các cuộc thảo luận về các biện pháp kiểm soát bảo mật và áp dụng chúng cho hệ thống ICS.

5.5.1 Khung Quản lý Rủi ro cho các Hệ thống Kiểm soát Công nghiệp

Dưới đây là mô tả quy trình áp dụng Khung Quản lý Rủi ro (RMF) cho hệ thống Điều khiển Công nghiệp (ICS). Quy trình bao gồm một mô tả ngắn gọn về mỗi hoạt động và xác định các tài liệu hỗ trợ (tham chiếu theo TCVN thực tế) Các bước sau đây, mặc dù được thể hiện theo trình tự, có thể được triển khai theo một thứ tự khác để phù hợp với quy trình quản lý và quy trình vòng đời phát triển hệ thống đã được thiết lập.



**Hình 15. Các nhiệm vụ của khung quản lý rủi ro**

5.5.1.1 Bước 1: Phân loại hệ thống thông tin

Hoạt động đầu tiên trong RMF là phân loại thông tin và hệ thống thông tin dựa trên khả năng tác động của tổn thất. Đối với mỗi loại thông tin và hệ thống thông tin được xem xét, ba mục tiêu bảo mật được định nghĩa - bảo mật thông tin, toàn vẹn và khả dụng - được liên kết với ba mức tiềm năng ảnh hưởng trong trường hợp có vi phạm bảo mật. Quan trọng là cần nhớ rằng đối với một ICS, khả dụng thường là mối quan tâm lớn nhất.

Ví dụ ICS sau đây tham chiếu theo TCVN thực tế:

Khuyến nghị và hướng dẫn cụ thể của ICS

Một nhà máy điện có hệ thống SCADA kiểm soát việc phân phối điện cho một cơ sở quân sự lớn. Hệ thống SCADA chứa dữ liệu cảm biến thời gian thực và thông tin quản trị thông thường. Ban quản lý tại nhà máy điện xác định rằng: (i) dữ liệu cảm biến được hệ thống SCADA thu thập, không có tác động tiềm ẩn nào do mất tính bảo mật, tác động tiềm ẩn cao do mất tính toàn vẹn và tác động tiềm tàng cao từ việc mất tính sẵn có; và (ii) đối với thông tin hành chính đang được hệ thống xử lý, có ít tác động tiềm ẩn do mất tính bảo mật, tác động tiềm ẩn thấp do mất tính toàn vẹn và tác động tiềm ẩn do mất tính toàn vẹn khả dụng. Các phân loại kết quả bảo mật, SC, của các loại thông tin này được thể hiện dưới dạng:

***Dữ liệu cảm biến SC = {(Tính bí mật, NA), (Tính toàn vẹn, Cao), (Tính khả dụng, Cao)}.***

***Và***

***Thông tin quản trị SC = {(Tính bí mật, Thấp), (Tính toàn vẹn, Thấp), (Tính sẵn sàng, Thấp)}.***

Các loại kết quả bảo mật của hệ thống thông tin ban đầu được thể hiện dưới dạng:

***Hệ thống SCADA SC = {(Tính bí mật, Thấp), (Tính toàn vẹn, Cao), (Tính sẵn sàng, Cao)***

Đại diện cho mức nước cao hoặc giá trị tác động tiềm ẩn tối da cho từng mục tiêu bảo mật từ các loại thông tin có trên hệ thống SCADA. Ban quản lý tại nhà máy điện lựa chọn tăng tác động tiềm tàng từ việc mất tính bảo mật từ mức thấp đến trung bình, phản ánh cái nhìn thực tế hơn về tác động tiềm tàng đối với hệ thống thông tin nếu có lỗ hổng do bị tiết lộ trái phép cấp độ hệ thống, thông tin hoặc chức năng xử lý. Loại bảo mật cuối cùng của hệ thống thông tin được thể hiện như sau:

***Hệ thống SCADA SC = {(Tính bí mật, Trung bình), (Tính toàn vẹn, Cao), (Tính sẵn sàng, Cao)}***

Tham chiếu theo TCVN thực tế quy định hệ thống thông tin sẽ được phân loại là hệ thống tác động thấp, tác động vừa, hoặc tác động cao đối với các mục tiêu bảo mật gồm bảo mật thông tin, toàn vẹn và khả dụng. Các định nghĩa có thể cho các mức độ bảo mật thấp, vừa và cao dựa trên tác động đối với ICS dựa trên tham chiếu TCVN thực tế được cung cấp trong Bảng 3. Các định nghĩa có thể cho các mức độ tác động của ICS dựa trên sản phẩm sản xuất, ngành công nghiệp và quan ngại về bảo mật được cung cấp trong Bảng 4.

|  |  |  |  |
| --- | --- | --- | --- |
| **Danh mục tác động** | **Tác động thấp** | **Tác động vừa phải** | **Tác động cao** |
| **Chấn thương** | Vết cắt, vết thâm gây ra những tổn thương cần sơ cứu. | Yêu cầu nhập viện | Mất mạng hoặc chân tay |
| **Tổn thất tài chính** | $1,000 | $100,000 | Millions |
| **Phát hành môi trường** | Thiệt hại tạm thời | Thiệt hại lâu dài | Thiệt hại vĩnh viễn, thiệt hại bên ngoài |
| **Gián đoạn sản xuất** | Biên bản | Ngày | Tuần |
| **Hình ảnh công cộng** | Thiệt hại tạm thời | Thiệt hại lâu dài | Thiệt hại vĩnh viễn |

**Bảng 3. Các định nghĩa khả thi cho các mức độ tác động của ICS tham chiếu theo TCVN thực tế**

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Low-Impact** | **Moderate-Impact** | **High-Impact** |
| **Loại** | **Tác động tháp** | **Tác động vừa phải** | **Tác động cao** |
| **Sản phẩm sản xuất** | • Vật liệu sản phẩm không nguy hiểm  • Sản phẩm tiêu dùng không ăn vào | • Một số sản phẩm hoặc bước nguy hiểm trong quá trình sản xuất  • Thông tin độc quyền cao | • Cơ sở hạ tầng quan trọng  (ví dụ: điện)  • Vật liệu nguy hiểm  • Sản phẩm ăn vào |
| **Ví dụ trong ngành** | • Ép phun nhựa  • Ứng dụng kho | • Ngành công nghiệp kim loại ô tô  • Bột giấy và giấy  • Chất bán dẫn | • Tiện ích  • Hóa dầu  • Thực phẩm và đồ uống  • Dược phẩm |
| **Quan ngại về bảo mật** | • Bảo vệ chống lại thương tích nhẹ  • Đảm bảo thời gian hoạt động | • Bảo vệ chống lại chấn thương vừa phải  • Ensuring uptime  • Đầu tư vốn | • Bảo vệ chống lại chính  thương tích / mất mạng  • Đảm bảo thời gian hoạt động  • Đầu tư vốn  • Bí mật kinh doanh  • Đảm bảo các dịch vụ xã hội cơ bản  • Tuân thủ quy định |

**Bảng 4. Các định nghĩa có thể có đối với các mức độ tác động của ICS dựa trên sản phẩm được sản xuất, các mối quan tâm về ngành và an toàn**

5.5.1.2 Bước 2: Chọn kiểm soát bảo mật

Hoạt động trong khung này bao gồm việc lựa chọn ban đầu các kiểm soát an toàn tối thiểu được lên kế hoạch hoặc đã được triển khai để bảo vệ hệ thống thông tin dựa trên một tập hợp yêu cầu. Tham chiếu theo TCVN thực tế, mô tả một tập hợp các yêu cầu bảo mật tối thiểu liên quan đến 18 lĩnh vực liên quan đến bảo vệ tính bảo mật thông tin, tính toàn vẹn và tính khả dụng của hệ thống thông tin liên bang và thông tin được xử lý, lưu trữ và truyền qua các hệ thống đó.

Các điều khiển cơ bản là điểm khởi đầu cho quá trình lựa chọn các kiểm soát an toàn và được chọn dựa trên danh mục bảo mật và mức độ tác động liên quan đến hệ thống thông tin được xác định ở Bước 1.

Để đáp ứng nhu cầu phát triển các tập hợp kiểm soát an toàn cộng đồng và chuyên ngành cho hệ thống thông tin và tổ chức, khái niệm về "lớp phủ" được giới thiệu. Một "lớp phủ" là một tập hợp đầy đủ các kiểm soát an toàn, cải tiến kiểm soát và hướng dẫn bổ sung được tạo ra từ việc áp dụng hướng dẫn tùy chỉnh cho các kiểm soát an toàn cơ bản được mô tả tham chiếu theo TCVN thực tế

Nói chung, lớp phủ được thiết kế nhằm giảm nhu cầu tùy chỉnh cơ bản tùy ý bằng cách lựa chọn một tập hợp các điều khiển và cải tiến kiểm soát mà tương ứng gần hơn với các tình huống, trường hợp và/hoặc điều kiện phổ biến. Tuy nhiên, việc sử dụng lớp phủ không loại trừ khả năng tùy chỉnh tiếp theo của các tổ chức (tức là lớp phủ cũng có thể được tùy chỉnh) để phản ánh các yêu cầu, giả định hoặc ràng buộc cụ thể của tổ chức.

5.5.1.3 Bước 3: Thực hiện kiểm soát An toàn

Hoạt động này liên quan đến việc triển khai các kiểm soát an toàn trong các hệ thống thông tin mới hoặc cũ. Quá trình lựa chọn kiểm soát an toàn được mô tả trong phần này có thể áp dụng cho ICS từ hai góc độ khác nhau: (i) hệ thống phát triển mới; và (ii) hệ thống cũ.

Đối với các hệ thống phát triển mới, quá trình lựa chọn kiểm soát an toàn được áp dụng từ góc định nghĩa yêu cầu vì các hệ thống này chưa tồn tại và tổ chức đang tiến hành phân loại bảo mật ban đầu. Các kiểm soát an toàn được bao gồm trong kế hoạch bảo mật cho hệ thống thông tin đóng vai trò là một đặc tả bảo mật và được dự kiến sẽ được tích hợp vào các hệ thống trong quá trình phát triển và triển khai của vòng đời phát triển hệ thống.

Trái lại, đối với các hệ thống thông tin cũ, quá trình lựa chọn kiểm soát an toàn được áp dụng từ góc độ phân tích khoảng cách khi tổ chức dự đoán các thay đổi đáng kể đối với hệ thống (ví dụ: trong quá trình nâng cấp lớn, sửa đổi hoặc giao phó). Vì các hệ thống thông tin đã tồn tại, tổ chức có thể đã hoàn thành quá trình phân loại bảo mật và lựa chọn kiểm soát an toàn dẫn đến việc thiết lập các kiểm soát an toàn đã được thống nhất trước đó trong các kế hoạch bảo mật tương ứng và triển khai các điều khiển đó trong các hệ thống thông tin.

5.5.1.4 Bước 4: Đánh giá kiểm soát An toàn

Hoạt động này xác định mức độ hiệu quả của các kiểm soát an toàn trong hệ thống thông tin. Tham chiếu theo TCVN thực tế, cung cấp hướng dẫn để đánh giá các kiểm soát an toàn được lựa chọn ban đầu tham chiếu theo TCVN thực tế để đảm bảo rằng chúng được triển khai đúng cách, hoạt động như dự định và đạt được kết quả mong muốn liên quan đến đáp ứng yêu cầu bảo mật của hệ thống. Để thực hiện điều này, tham chiếu theo TCVN thực tế cung cấp các kỳ vọng dựa trên yêu cầu đảm bảo được định nghĩa tham chiếu theo TCVN thực tế để mô tả các kỳ vọng của các đánh giá bảo mật theo mức độ tác động tham chiếu theo TCVN thực tế

5.5.1.5 Bước 5: Cấp quyền cho hệ thống thông tin

Hoạt động này dẫn đến một quyết định quản lý để ủy quyền hoạt động của một hệ thống thông tin và chấp nhận rõ ràng rủi ro đối với hoạt động của cơ quan, tài sản của cơ quan hoặc cá nhân dựa trên việc triển khai một tập hợp các kiểm soát an toàn đã được thống nhất.

5.5.1.6 Bước 6: Giám sát các kiểm soát an toàn

Hoạt động này liên tục theo dõi những thay đổi trong hệ thống thông tin có thể ảnh hưởng đến các kiểm soát an toàn và đánh giá hiệu quả của các điều khiển đó. Tham chiếu theo TCVN thực tế cung cấp hướng dẫn về việc theo dõi liên tục an toàn thông tin

5.5.2 Hướng dẫn về việc áp dụng các biện pháp kiểm soát an toàn cho ICS

Bởi vì các hệ thống ICS hiện nay thường là sự kết hợp của các hệ thống kế thừa, thường có tuổi thọ dự kiến trong khoảng hai mươi đến ba mươi năm, hoặc là sự kết hợp của các hệ thống kế thừa được bổ sung với phần cứng và phần mềm mới hơn và được kết nối với các hệ thống khác, thường khó khăn hoặc không khả thi để áp dụng một số kiểm soát an toàn tham chiếu theo TCVN thực tế

Tham chiếu theo TCVN thực tế, các biện pháp kiểm soát được tổ chức thành 18 nhóm; mỗi nhóm chứa các kiểm soát an toàn liên quan đến chủ đề bảo mật tổng quát của nhóm. Các kiểm soát an toàn có thể liên quan đến các khía cạnh về chính sách, giám sát, giám sát, quy trình thủ công, hành động của cá nhân hoặc các cơ chế tự động được triển khai bởi hệ thống thông tin/thiết bị. Các lĩnh vực liên quan đến bảo mật trong 18 nhóm được thảo luận trong các phần tiếp theo là:

- **Kiểm soát Truy cập (AC):** quá trình cho phép hoặc từ chối các yêu cầu cụ thể để có được và sử dụng thông tin và dịch vụ xử lý thông tin liên quan cho truy cập vật lý vào các khu vực trong môi trường hệ thống thông tin.

- **Nhận thức và Đào tạo (AT):** chính sách và quy trình để đảm bảo rằng tất cả người dùng hệ thống thông tin được đào tạo bảo mật phù hợp liên quan đến việc sử dụng hệ thống và rằng hồ sơ đào tạo chính xác được duy trì.

- **Kiểm toán và Chịu trách nhiệm (AU):** xem xét độc lập và kiểm tra các hồ sơ và hoạt động để đánh giá tính phù hợp của các điều khiển hệ thống, đảm bảo tuân thủ các chính sách và quy trình hoạt động, và đề xuất các thay đổi cần thiết trong các điều khiển, chính sách hoặc quy trình.

- **Đánh giá và Ủy quyền Bảo mật (CA):** đảm bảo rằng các điều khiển được chỉ định được triển khai đúng cách, hoạt động như dự kiến và đạt được kết quả mong muốn.

- **Lập kế hoạch Khẩn cấp (CP):** chính sách và quy trình được thiết kế để duy trì hoặc khôi phục hoạt động kinh doanh, bao gồm hoạt động máy tính, có thể tại một vị trí thay thế, trong trường hợp khẩn cấp, hỏng hóc hệ thống hoặc thảm họa.

- **Quản lý Cấu hình (CM):** chính sách và quy trình để kiểm soát các sửa đổi đối với phần cứng, firmware, phần mềm và tài liệu để đảm bảo hệ thống thông tin được bảo vệ khỏi các sửa đổi không đúng trước, trong và sau giai đoạn triển khai hệ thống.

- **Xác định và Xác thực (IA):** quá trình xác minh danh tính của người dùng, quy trình hoặc thiết bị, thông qua việc sử dụng các thông tin xác thực cụ thể (ví dụ: mật khẩu, token, sinh trắc học), là điều kiện tiên quyết để cấp quyền truy cập vào tài nguyên trong hệ thống IT.

- **Phản ứng thảm họa (IR):** chính sách và quy trình liên quan đến việc đào tạo, kiểm tra, xử lý, giám sát, báo cáo và hỗ trợ phản ứng thảm họa.

- **Bảo trì (MA):** chính sách và quy trình để quản lý tất cả các khía cạnh bảo trì của hệ thống thông tin.

- **Bảo vệ Phương tiện (MP):** chính sách và thủ tục nhằm đảm bảo việc xử lý an toàn cho các phương tiện. Các biện pháp bao gồm kiểm soát truy cập, nhãn dán, lưu trữ, vận chuyển, làm sạch, phá hủy và xử lý.

- **Bảo vệ Vật lý và Môi trường (PE):** chính sách và thủ tục đảm bảo kiểm soát truy cập vật lý, truyền thông và hiển thị, cũng như kiểm soát môi trường bao gồm điều chỉnh (ví dụ: nhiệt độ, độ ẩm) và các biện pháp khẩn cấp (ví dụ: tắt, nguồn điện, chiếu sáng, bảo vệ chống cháy).

- **Lập kế hoạch (PL):** phát triển và duy trì một kế hoạch nhằm đảm bảo an toàn hệ thống thông tin bằng cách tiến hành đánh giá, chỉ định và triển khai các biện pháp kiểm soát an toàn, gán cấp độ an toàn và ứng phó với thảm họa.

- **An toàn Nhân sự (PS):** chính sách và thủ tục liên quan đến phân loại vị trí, sàng lọc, chuyển đổi, xử phạt và chấm dứt nhân viên; cũng bao gồm an toàn nhân viên của bên thứ ba.

- **Đánh giá Rủi ro (RA):** quá trình xác định các rủi ro đối với hoạt động, tài sản hoặc cá nhân bằng cách xác định xác suất xảy ra, tác động kết quả và các biện pháp kiểm soát an toàn bổ sung để giảm thiểu tác động này.

- **Mua sắm Hệ thống và Dịch vụ (SA):** phân bổ tài nguyên cho an toàn hệ thống thông tin suốt vòng đời hệ thống và phát triển chính sách mua sắm dựa trên kết quả đánh giá rủi ro, bao gồm yêu cầu, tiêu chí thiết kế, thủ tục kiểm tra và tài liệu liên quan.

- **Bảo vệ Hệ thống và Truyền thông (SC):** cơ chế bảo vệ cả thành phần hệ thống và truyền thông dữ liệu.

**- An toàn và Trung thực Thông tin Hệ thống (SI):** chính sách và thủ tục nhằm bảo vệ hệ thống thông tin và dữ liệu khỏi các lỗi thiết kế và sửa đổi dữ liệu bằng cách xác minh chức năng, kiểm tra tính toàn vẹn dữ liệu, phát hiện xâm nhập, phát hiện mã độc và kiểm soát cảnh báo và tư vấn an toàn.

- **Quản lý Chương trình (PM):** cung cấp các biện pháp kiểm soát an toàn ở mức tổ chức chứ không chỉ ở mức hệ thống thông tin.

5.5.2.1 Kiểm soát truy cập

Các biện pháp kiểm soát an toàn Access Control (AC) tham chiếu theo TCVN thực tế, cung cấp chính sách và thủ tục để xác định việc sử dụng tài nguyên hệ thống chỉ được thực hiện bởi người dùng, chương trình, quy trình hoặc hệ thống khác được ủy quyền. Nhóm này chỉ định các biện pháp kiểm soát quản lý tài khoản hệ thống thông tin, bao gồm thiết lập, kích hoạt, sửa đổi, xem xét, vô hiệu hóa và xóa tài khoản. Các biện pháp kiểm soát bao gồm vấn đề kiểm soát truy cập và luồng thông tin như phân tách trách nhiệm, nguyên tắc cấp đặc quyền thấp nhất, các lần đăng nhập không thành công, thông báo sử dụng hệ thống, thông báo lần đăng nhập trước đó, kiểm soát phiên đồng thời, khóa phiên và chấm dứt phiên. Còn có các biện pháp kiểm soát để giải quyết việc sử dụng các thiết bị di động và từ xa và các hệ thống thông tin thuộc sở hữu cá nhân để truy cập vào hệ thống thông tin cũng như việc sử dụng khả năng truy cập từ xa và triển khai công nghệ không dây. Truy cập có thể có nhiều hình thức khác nhau, bao gồm xem, sử dụng và thay đổi dữ liệu cụ thể hoặc chức năng thiết bị.

Nếu sử dụng Xác minh danh tính cá nhân PIV của chính phủ mới như một mã thông báo xác thực, hệ thống kiểm soát truy cập phải tuân thủ các yêu cầu tham chiếu theo TCVN thực tế và sử dụng xác thực mật mã học hoặc xác thực sinh trắc học. Khi hệ thống kiểm soát truy cập dựa trên token sử dụng xác thực mật mã học, hệ thống kiểm soát truy cập phải tuân thủ các yêu cầu tham chiếu theo TCVN thực tế. Khi hệ thống kiểm soát truy cập dựa trên mã xác thực sinh trắc học, hệ thống kiểm soát truy cập phải tuân thủ các yêu cầu tham chiếu theo TCVN thực tế

Các công nghệ kiểm soát truy cập là các công nghệ lọc và chặn được thiết kế để điều hướng và quy định luồng thông tin giữa các thiết bị hoặc hệ thống sau khi đã xác định được sự ủy quyền. Các phần sau trình bày một số công nghệ kiểm soát truy cập và cách sử dụng chúng trong ICS.

**4.5.2.1.1 Kiểm soát truy cập dựa trên vai trò (RBAC)**

RBAC là một công nghệ có tiềm năng giúp giảm độ phức tạp và chi phí quản lý an toàn trong các mạng với số lượng thiết bị thông minh lớn. Dưới RBAC, việc quản lý an toàn được đơn giản hóa thông qua việc sử dụng vai trò, hệ thống phân cấp và ràng buộc để tổ chức cấp độ truy cập của người dùng. RBAC giúp giảm chi phí trong tổ chức vì nó chấp nhận việc nhân viên thay đổi vai trò và trách nhiệm thường xuyên hơn là trách nhiệm trong vai trò và trách nhiệm.

***Khuyến nghị và hướng dẫn cụ thể cho ICS:***

RBAC có thể được sử dụng để cung cấp một phương tiện thống nhất để quản lý quyền truy cập vào các thiết bị ICS, đồng thời giảm chi phí duy trì các cấp độ truy cập riêng lẻ cho từng thiết bị và giảm thiểu lỗi. RBAC nên được sử dụng để hạn chế đặc quyền người dùng ICS chỉ vào những đặc quyền cần thiết để thực hiện công việc của từng người (tức là cấu hình mỗi vai trò dựa trên nguyên tắc cấp đặc quyền thấp nhất). Cấp độ truy cập có thể có nhiều hình thức khác nhau, bao gồm xem, sử dụng và thay đổi dữ liệu cụ thể hoặc chức năng thiết bị ICS.

Các công cụ RBAC có thể đặt, sửa đổi hoặc xóa các quyền ủy quyền trong các ứng dụng, nhưng chúng không thay thế cơ chế ủy quyền; chúng không kiểm tra và xác thực người dùng mỗi khi người dùng muốn truy cập vào một ứng dụng. Các công cụ RBAC cung cấp giao diện cho cơ chế ủy quyền trên hầu hết các nền tảng hiện tại trong lĩnh vực CNTT. Tuy nhiên, các hệ thống ICS cổ điển hoặc các thiết bị ICS chuyên dụng có thể yêu cầu phát triển phần mềm giao diện đặc biệt. Vấn đề này là một vấn đề lớn đối với ICS sử dụng nhiều hệ điều hành độc quyền hoặc các thiết bị và giao diện hệ điều hành tùy chỉnh.

**4.5.2.1.2 Máy chủ Web**

Các công nghệ Web và Internet đang được thêm vào nhiều sản phẩm ICS khác nhau vì chúng làm cho thông tin dễ tiếp cận hơn và sản phẩm dễ sử dụng hơn và dễ cấu hình từ xa. Tuy nhiên, chúng cũng có thể tạo ra các rủi ro về mạng và tạo ra các lỗ hổng bảo mật mới cần được giải quyết.

***Khuyến nghị và hướng dẫn cụ thể cho ICS:***

Các nhà cung cấp phần mềm SCADA và lịch sử thông tin thường cung cấp các máy chủ Web như một tùy chọn sản phẩm để người dùng ngoài phòng điều khiển có thể truy cập thông tin ICS. Trong nhiều trường hợp, các thành phần phần mềm như điều khiển ActiveX hoặc ứng dụng Java phải được cài đặt hoặc tải xuống trên mỗi máy khách truy cập máy chủ Web. Một số sản phẩm, như PLC và các thiết bị điều khiển khác, có sẵn với các máy chủ Web, FTP và email được nhúng để làm cho việc cấu hình từ xa dễ dàng hơn và cho phép chúng tạo ra thông báo qua email và báo cáo khi xảy ra một số điều kiện nhất định. Khi khả thi, hãy sử dụng HTTPS thay vì HTTP, sử dụng SFTP hoặc SCP thay vì FTP, chặn lưu lượng truy cập FTP và email từ bên ngoài, vv. Các thiết bị bảo mật (hoặc cổng) đang xuất hiện với các ứng dụng proxy có khả năng kiểm tra lưu lượng Web, FTP và email để chặn các cuộc tấn công và ngăn chặn việc tải xuống các điều khiển ActiveX® hoặc ứng dụng Java®.

Trừ khi có lợi ích đáng kể từ việc kết nối ICS với Internet, hệ thống nên được giữ không kết nối.

**4.5.2.1.3 Mạng cục bộ ảo (VLAN)**

VLAN (Mạng cục bộ ảo) chia mạng vật lý thành các mạng logic nhỏ hơn để tăng hiệu suất, cải thiện khả năng quản lý và đơn giản hóa thiết kế mạng. VLAN được thực hiện thông qua cấu hình các thiết bị chuyển mạch Ethernet. Mỗi VLAN bao gồm một miền phát sóng đơn lẻ cô lập lưu lượng khỏi các VLAN khác. Tương tự như việc thay thế các hub bằng các thiết bị chuyển mạch giúp giảm va chạm, sử dụng VLAN giới hạn lưu lượng phát sóng, đồng thời cho phép các mạng con logic trải dài trên nhiều vị trí vật lý. Có hai loại VLAN:

- VLAN tĩnh, thường được gọi là dựa trên cổng, trong đó các cổng thiết bị chuyển mạch được gán vào một VLAN sao cho người dùng cuối không nhìn thấy sự khác biệt.

- VLAN động, trong đó một thiết bị cuối đàm phán các đặc điểm VLAN với thiết bị chuyển mạch hoặc xác định VLAN dựa trên địa chỉ IP hoặc địa chỉ phần cứng.

quan hệ một-một giữa các mạng con và VLAN. Thực hành này đòi hỏi sử dụng một bộ định tuyến hoặc thiết bị chuyển mạch đa tầng để kết nối nhiều VLAN. Nhiều bộ định tuyến và tường lửa hỗ trợ các khung được gắn thẻ để một giao diện vật lý duy nhất có thể được sử dụng để định tuyến giữa nhiều mạng logic.

VLAN thường không được triển khai để giải quyết các lỗ hổng của máy chủ hoặc mạng như tường lửa hoặc hệ thống IDS. Tuy nhiên, khi được cấu hình đúng, VLAN cho phép các thiết bị chuyển mạch thi hành các chính sách bảo mật và phân tách lưu lượng ở tầng Ethernet. Mạng được phân đoạn đúng cách cũng có thể giảm thiểu các rủi ro từ cơn bão phát sóng có thể xảy ra do quét cổng hoặc hoạt động của sâu.

Các thiết bị chuyển mạch có thể bị tấn công như giả mạo MAC, tràn bảng địa chỉ và tấn công chống các giao thức cây bao phủ, tùy thuộc vào thiết bị và cấu hình của nó. VLAN hopping, khả năng cho một cuộc tấn công tiêm vào các cổng không được ủy quyền, đã được chứng minh bằng cách sử dụng giả mạo thiết bị chuyển mạch hoặc khung được bao đôi. Những cuộc tấn công này không thể được tiến hành từ xa và yêu cầu truy cập vật lý cục bộ vào thiết bị chuyển mạch. Các tính năng khác nhau như lọc địa chỉ MAC, xác thực dựa trên cổng sử dụng IEEE 802.1x và các thực hành được khuyến nghị bởi nhà cung cấp cụ thể có thể được sử dụng để giảm thiểu những cuộc tấn công này, tùy thuộc vào thiết bị và cài đặt.

***Khuyến nghị và Hướng dẫn cụ thể cho ICS:***

VLAN đã được triển khai hiệu quả trong các mạng ICS, với mỗi ổ điều khiển tự động được gán cho một VLAN duy nhất để giới hạn lưu lượng tràn ngập không cần thiết và cho phép các thiết bị mạng trên cùng một VLAN trải dài qua nhiều thiết bị chuyển mạch.

**4.5.2.1.4 Modem quay số**

Hệ thống ICS có yêu cầu về độ tin cậy và sẵn có rất cao. Khi cần phải khắc phục thảm họa và sửa chữa, các nguồn tài nguyên kỹ thuật có thể không được đặt vật lý tại phòng điều khiển hoặc cơ sở. Do đó, ICS thường sử dụng modem để cho phép nhà cung cấp, nhà tích hợp hệ thống hoặc kỹ sư điều khiển bảo trì hệ thống kết nối và chẩn đoán, sửa chữa, cấu hình và bảo trì mạng hoặc thành phần. Mặc dù điều này cho phép nhân viên có quyền truy cập dễ dàng, nếu modem kết nối bằng số điện thoại không được bảo mật đúng cách, chúng cũng có thể tạo điểm vào không được ủy quyền.

Giao tiếp qua điện thoại thường sử dụng phần mềm điều khiển từ xa cho phép người dùng từ xa có quyền truy cập quyền quản trị hoặc quyền root vào hệ thống mục tiêu. Phần mềm như vậy thường có các tùy chọn bảo mật mà nên được xem xét và cấu hình cẩn thận.

***Khuyến nghị và hướng dẫn cụ thể cho ICS:***

- Xem xét sử dụng hệ thống gọi lại (callback systems) khi cài đặt modem kết nối qua số điện thoại trong ICS. Điều này đảm bảo rằng người gọi là người dùng được ủy quyền bằng cách cho modem thiết lập kết nối dựa trên thông tin của người gọi và một số điện thoại gọi lại được lưu trữ trong danh sách người dùng được ủy quyền đã được phê duyệt của ICS.

- Đảm bảo rằng các mật khẩu mặc định đã được thay đổi và mật khẩu mạnh đã được áp dụng cho mỗi modem.

- Xác định vật lý các modem đang được sử dụng cho các nhà điều khiển phòng điều khiển.

- Cấu hình phần mềm điều khiển từ xa để sử dụng tên người dùng và mật khẩu duy nhất, xác thực mạnh, mã hóa nếu được xác định là thích hợp và ghi nhật ký kiểm tra. Việc sử dụng phần mềm này bởi người dùng từ xa nên được giám sát với tần suất gần như thời gian thực.

- Nếu khả thi, ngắt kết nối modem khi không sử dụng hoặc xem xét tự động quá trình ngắt kết nối này bằng cách cho phép modem ngắt kết nối sau một khoảng thời gian nhất định. Cần lưu ý rằng đôi khi việc kết nối modem là một phần của hợp đồng dịch vụ hỗ trợ pháp lý với nhà cung cấp (ví dụ: hỗ trợ 24/7 với thời gian phản hồi 15 phút). Nhân viên cần nhận thức rằng việc ngắt kết nối/xóa bỏ modem có thể đòi hỏi phải đàm phán lại hợp đồng.

**4.5.2.1.4 Mạng không dây**

Việc sử dụng công nghệ mạng không dây trong hệ thống ICS là một quyết định dựa trên mức độ rủi ro phải được tổ chức xác định. Nhìn chung, mạng LAN không dây chỉ nên được triển khai khi các yếu tố liên quan đến sức khỏe, an toàn, môi trường và tài chính là thấp.

***Khuyến nghị và hướng dẫn cụ thể cho ICS:***

Mạng LAN không dây

- Trước khi cài đặt, nên thực hiện một khảo sát mạng không dây để xác định vị trí và cường độ của ăng-ten nhằm giảm thiểu sự phơi bày của mạng không dây. Khảo sát nên xem xét việc tấn công viên có thể sử dụng các ăng-ten hướng mạnh, làm tăng phạm vi hiệu lực của mạng không dây vượt quá phạm vi tiêu chuẩn dự kiến. Có sẵn cách thức như lồng Faraday và các phương pháp khác để giảm thiểu sự phơi bày của mạng không dây ngoài các khu vực được chỉ định.

- Việc truy cập của người dùng không dây nên sử dụng xác thực IEEE 802.1x bằng cách sử dụng giao thức xác thực an toàn (ví dụ: Extensible Authentication Protocol [EAP] với TLS [EAP-TLS]) để xác thực người dùng qua chứng chỉ người dùng hoặc máy chủ Remote Authentication Dial In User Service (RADIUS).

- Các điểm truy cập không dây và máy chủ dữ liệu cho thiết bị làm việc không dây nên được đặt trên một mạng cô lập với kết nối tài liệu và tối thiểu (nếu có thể chỉ một kết nối) với mạng ICS.

- Các điểm truy cập không dây nên được cấu hình có một định danh dịch vụ mạng (SSID) duy nhất, tắt phát sóng SSID và bật bộ lọc MAC ít nhất.

- Thiết bị không dây, nếu được sử dụng trong mạng ICS Windows, nên được cấu hình vào một đơn vị tổ chức riêng biệt của miền Windows.

- Giao tiếp của thiết bị không dây nên được mã hóa và bảo vệ tính toàn vẹn. Quá trình mã hóa không được làm giảm hiệu suất hoạt động của thiết bị cuối. Nên xem xét việc sử dụng mã hóa tại lớp OSI Layer 2, thay vì tại Layer 3 để giảm độ trễ mã hóa. Cũng nên xem xét việc sử dụng bộ gia tốc phần cứng để thực hiện các chức năng mật mã hóa.

Đối với mạng lưới (mesh networks), xem xét việc sử dụng khóa phát sóng so với quản lý khóa công khai thực hiện tại OSI Layer 2 để tối đa hóa hiệu suất. Cần sử dụng mã hóa không đối xứng để thực hiện các chức năng quản trị, và sử dụng mã hóa đối xứng để bảo mật từng luồng dữ liệu cũng như lưu lượng điều khiển mạng. Nên xem xét sử dụng giao thức định tuyến linh hoạt nếu các thiết bị được sử dụng cho tính di động không dây. Thời gian hội tụ của mạng nên nhanh nhất có thể để hỗ trợ khôi phục mạng nhanh chóng trong trường hợp xảy ra thảm họa hoặc mất điện. Việc sử dụng mạng lưới lưới cũng có thể cung cấp khả năng chống lỗi thông qua việc lựa chọn tuyến đường thay thế và khôi phục mạng trước khi xảy ra thảm họa.

5.5.2.2 Nhận thức và đào tạo

Đối với môi trường ICS, điều này phải bao gồm thông tin cụ thể về nhận thức và đào tạo bảo mật hệ thống điều khiển cho các ứng dụng ICS cụ thể. Ngoài ra, tổ chức phải xác định, ghi nhận và đào tạo tất cả nhân viên có vai trò và trách nhiệm quan trọng đối với hệ thống ICS. Nhận thức và đào tạo phải bao gồm quy trình vật lý được kiểm soát cũng như hệ thống ICS.

Nhận thức bảo mật là một phần quan trọng trong việc ngăn chặn thảm họa ICS, đặc biệt là đối với các mối đe dọa về kỹ thuật xã hội. Kỹ thuật xã hội là một kỹ thuật được sử dụng để thao túng cá nhân để lấy thông tin riêng tư, như mật khẩu. Thông tin này sau đó có thể được sử dụng để xâm nhập vào các hệ thống ban đầu được bảo mật.

Triển khai một chương trình bảo mật ICS có thể mang lại các thay đổi về cách nhân viên truy cập chương trình máy tính, ứng dụng và desktop máy tính. Tổ chức nên thiết kế các chương trình đào tạo hiệu quả và phương tiện truyền thông để giúp nhân viên hiểu tại sao phương pháp truy cập và kiểm soát mới được yêu cầu, ý tưởng mà họ có thể sử dụng để giảm rủi ro, và tác động lên tổ chức nếu các phương pháp kiểm soát không được tích hợp. Các chương trình đào tạo cũng thể hiện sự cam kết và giá trị của quản lý đối với chương trình an toàn mạng. Phản hồi từ nhân viên tiếp xúc với loại đào tạo này có thể là một nguồn thông tin quý giá để hoàn thiện điều lệ và phạm vi của chương trình bảo mật.

5.5.2.3 Kiểm toán và trách nhiệm giải trình

Kiểm toán là một cuộc xem xét và kiểm tra độc lập các hồ sơ và hoạt động để đánh giá tính đầy đủ của các biện pháp kiểm soát hệ thống, đảm bảo tuân thủ các chính sách và quy trình hoạt động đã thiết lập, và đề xuất các thay đổi cần thiết trong các biện pháp kiểm soát, chính sách hoặc quy trình.

Các biện pháp kiểm soát cũng cung cấp các biện pháp bảo vệ để xử lý các vấn đề như lỗi kiểm toán hoặc đạt giới hạn dung lượng hồ sơ kiểm toán. Dữ liệu kiểm toán phải được bảo vệ khỏi sửa đổi và được thiết kế với khả năng không thể chối bỏ.

***Khuyến nghị và hướng dẫn cụ thể cho môi trường ICS:***

Cần xác định rằng hệ thống hoạt động theo ý định ban đầu. Cần thực hiện kiểm toán định kỳ của hệ thống ICS để xác nhận các yếu tố sau:

- Các biện pháp kiểm soát bảo mật có mặt trong quá trình kiểm tra xác nhận hệ thống (ví dụ: kiểm tra chấp nhận nhà máy và kiểm tra chấp nhận trang web) vẫn được cài đặt và hoạt động đúng trong hệ thống sản xuất.

- Hệ thống sản xuất không bị chiếm đoạt bảo mật và cung cấp thông tin về tự nhiên và mức độ tác động của các cuộc chiếm đoạt nếu có khả năng xảy ra.

- Chương trình quản lý thay đổi được tuân thủ chặt chẽ với một loạt các xem xét và phê duyệt cho tất cả các thay đổi.

Kết quả từ mỗi kiểm toán định kỳ nên được biểu diễn dưới dạng hiệu suất so với một tập hợp các chỉ số đã được định nghĩa trước và phù hợp để hiển thị hiệu suất bảo mật và xu hướng bảo mật. Các chỉ số hiệu suất bảo mật nên được gửi cho các bên liên quan thích hợp, cùng với một cái nhìn về xu hướng hiệu suất bảo mật.

Truyền thống, cơ sở chính cho kiểm toán trong các hệ thống CNTT đã là việc lưu giữ hồ sơ. Việc sử dụng các công cụ phù hợp trong môi trường ICS đòi hỏi kiến thức sâu rộng từ các chuyên gia CNTT quen thuộc với ICS, các ảnh hưởng quan trọng đến sản xuất và an toàn cho cơ sở. Nhiều thiết bị điều khiển quy trình được tích hợp vào ICS đã được lắp đặt từ nhiều năm và không có khả năng cung cấp các hồ sơ kiểm toán được mô tả trong phần này. Do đó, tính ứng dụng của các công cụ hiện đại hơn cho việc kiểm toán hoạt động và mạng phụ thuộc vào khả năng của các thành phần trong ICS.

Các nhiệm vụ quan trọng trong quản lý mạng trong môi trường ICS là đảm bảo tính tin cậy và khả dụng để hỗ trợ hoạt động an toàn và hiệu quả. Trong các ngành công nghiệp được quy định, tuân thủ quy định có thể làm tăng sự phức tạp trong việc quản lý bảo mật và xác thực, quản lý registry và tính toàn vẹn cài đặt, và tất cả các chức năng có thể tăng cường việc lắp đặt và thực hiện một bài tập xác nhận và bài tập hoạt động. Việc sử dụng đúng đắn các công cụ kiểm toán và quản lý nhật ký có thể cung cấp sự hỗ trợ quý giá trong việc duy trì và chứng minh tính toàn vẹn của ICS từ quá trình lắp đặt đến vòng đời của hệ thống. Giá trị của các công cụ này trong môi trường này có thể được tính toán thông qua nỗ lực yêu cầu để tái xác nhận hoặc kiểm tra lại ICS khi tính toàn vẹn do tấn công, tai nạn hoặc lỗi bị đặt vào câu hỏi. Hệ thống nên cung cấp các dấu thời gian đáng tin cậy, đồng bộ để hỗ trợ các công cụ kiểm toán.

Việc giám sát cảm biến, nhật ký, Hệ thống phát hiện xâm nhập (IDS), phần mềm chống vi-rút, quản lý bản vá, phần mềm quản lý chính sách và các cơ chế bảo mật khác nên được thực hiện theo thời gian thực nếu khả thi. Một dịch vụ giám sát hàng đầu sẽ nhận được cảnh báo, xác định vấn đề ban đầu nhanh chóng và thực hiện các biện pháp để cảnh báo cho nhân viên phù hợp trong cơ sở can thiệp.

Các tiện ích kiểm toán hệ thống nên được tích hợp vào các dự án ICS mới và hiện có. Các tiện ích kiểm toán này nên được kiểm tra (ví dụ: ngoại tuyến trên một hệ thống ICS tương đồng) trước khi triển khai trên một ICS hoạt động. Các công cụ này có thể cung cấp các hồ sơ cụ thể và tính toàn vẹn của hệ thống. Ngoài ra, các tiện ích quản lý nhật ký hoạt động thực tế thực tế có thể nhận diện một cuộc tấn công hoặc sự kiện đang diễn ra và cung cấp thông tin về vị trí và theo dõi để giúp phản ứng với thảm họa.

Nên có một phương pháp để theo dõi tất cả các hoạt động của bảng điều khiển đến một người dùng, bằng cách thủ công (ví dụ: đăng nhập phòng điều khiển) hoặc tự động (ví dụ: đăng nhập vào ứng dụng và / hoặc lớp hệ điều hành). Nên phát triển các chính sách và quy trình cho việc đăng nhập, cách lưu trữ nhật ký (hoặc in ấn), cách bảo vệ nhật ký, ai có quyền truy cập vào nhật ký và cách / khi nào chúng được xem.Hãy đảm bảo rằng quản lý cơ sở hạ tầng (thiết bị và mạng) trong ICS đáp ứng được các yêu cầu hiệu suất và bảo mật. Việc sử dụng các công cụ kiểm tra và quản lý đáng tin cậy có thể giúp đảm bảo rằng hệ thống đáp ứng được các tiêu chuẩn hiệu suất và bảo mật.

5.5.2.4 Đánh giá bảo mật và ủy quyền

Các biện pháp kiểm soát bảo mật thuộc Đánh giá và ủy quyền (CA) tham chiếu theo TCVN thực tế, cung cấp cơ sở để thực hiện các đánh giá định kỳ và cấp chứng chỉ cho các biện pháp kiểm soát bảo mật được triển khai trong hệ thống thông tin, nhằm xác định xem các biện pháp kiểm soát này có được triển khai đúng cách, hoạt động như ý định và tạo ra kết quả mong muốn để đáp ứng yêu cầu bảo mật của hệ thống. Một quan chức cấp cao trong tổ chức chịu trách nhiệm chấp nhận rủi ro còn lại và ủy quyền hoạt động hệ thống. Các bước này cấu thành quy trình cấp phép. Ngoài ra, tất cả các biện pháp kiểm soát bảo mật cần được theo dõi theo dõi liên tục.

Các hoạt động theo dõi bao gồm quản lý cấu hình và kiểm soát các thành phần hệ thống thông tin, phân tích tác động bảo mật của các thay đổi đối với hệ thống, đánh giá liên tục các biện pháp kiểm soát bảo mật và báo cáo tình trạng.

5.5.2.5 Quản lý cấu hình

Chính sách và quy trình quản lý cấu hình được sử dụng để kiểm soát các sửa đổi đối với phần cứng, phần lõi, phần mềm và tài liệu nhằm đảm bảo rằng hệ thống thông tin được bảo vệ khỏi các sửa đổi không đúng trước, trong và sau quá trình triển khai hệ thống.

Các biện pháp kiểm soát cũng được chỉ định để duy trì, theo dõi và ghi nhận các thay đổi kiểm soát cấu hình. Việc truy cập vào cài đặt cấu hình nên bị hạn chế, và các cài đặt bảo mật của sản phẩm IT nên được thiết lập ở chế độ hạn chế nhất phù hợp với yêu cầu vận hành của ICS.

**Đề xuất và hướng dẫn cụ thể cho môi trường ICS:**

Một chương trình quản lý thay đổi chính thức nên được thiết lập và sử dụng các quy trình để đảm bảo rằng tất cả các sửa đổi trên mạng ICS đáp ứng các yêu cầu bảo mật tương tự như các thành phần ban đầu được xác định trong đánh giá tài sản và các kế hoạch đánh giá và giảm thiểu rủi ro đi kèm. Đánh giá rủi ro nên được thực hiện cho tất cả các thay đổi trên mạng ICS có thể ảnh hưởng đến bảo mật, bao gồm các thay đổi cấu hình, việc thêm các thành phần mạng và cài đặt phần mềm. Có thể yêu cầu thay đổi các chính sách và quy trình. Cấu hình mạng ICS hiện tại và các cấu hình thiết bị luôn phải được biết đến và được ghi nhận.

5.5.2.6 Lập kế hoạch dự phòng

Kế hoạch khẩn cấp được thiết kế để duy trì hoặc khôi phục hoạt động kinh doanh, bao gồm hoạt động máy tính, có thể tại một địa điểm thay thế, trong trường hợp khẩn cấp, hỏng hóc hệ thống hoặc thiên tai. Các biện pháp kiểm soát bảo mật thuộc nhóm Contingency Planning (CP) tham chiếu theo TCVN thực tế cung cấp chính sách và quy trình để triển khai kế hoạch khẩn cấp bằng cách chỉ định vai trò và trách nhiệm, và phân công nhân viên và hoạt động liên quan đến khôi phục hệ thống thông tin sau khi xảy ra thảm họa hoặc hỏng hóc.

Ngoài việc lập kế hoạch, các biện pháp kiểm soát cũng tồn tại để đào tạo, kiểm tra và cập nhật kế hoạch khẩn cấp, cũng như các trang web xử lý thông tin sao lưu và lưu trữ.

**Đề xuất và hướng dẫn cụ thể cho môi trường ICS:**

Kế hoạch khẩn cấp nên bao gồm toàn bộ loạt thảm họa hoặc vấn đề có thể do các thảm họa mạng xảy ra. Kế hoạch khẩn cấp nên bao gồm các thủ tục để khôi phục hệ thống từ các bản sao lưu hợp lệ đã biết, tách hệ thống khỏi mọi sự can thiệp và kết nối không cần thiết có thể cho phép xâm nhập an toàn mạng, và các phương án thay thế để đạt được các giao diện và phối hợp cần thiết. Nhân viên nên được đào tạo và làm quen với nội dung của kế hoạch khẩn cấp. Kế hoạch khẩn cấp nên được xem xét định kỳ với nhân viên chịu trách nhiệm khôi phục ICS, và được kiểm tra để đảm bảo rằng chúng tiếp tục đáp ứng các mục tiêu của mình. Tổ chức cũng có kế hoạch duy trì hoạt động kinh doanh và kế hoạch phục hồi sau thảm họa liên quan chặt chẽ với kế hoạch khẩn cấp. Vì kế hoạch duy trì hoạt động kinh doanh và kế hoạch phục hồi sau thảm họa đặc biệt quan trọng đối với ICS, chúng được mô tả chi tiết hơn trong các phần tiếp theo.

**5.5.2.6.1 Lập kế hoạch kinh doanh liên tục**

Kế hoạch duy trì hoạt động kinh doanh (Business Continuity Planning - BCP) giải quyết vấn đề chung về duy trì hoặc khôi phục lại sản xuất trong trường hợp xảy ra gián đoạn. Những gián đoạn này có thể là các thảm họa tự nhiên (ví dụ: cơn bão, vụ lốc xoáy, động đất, lũ lụt), thảm họa không cố ý do con người gây ra (ví dụ: hỏng hóc thiết bị không may, hỏa hoạn hoặc vụ nổ, lỗi của nhân viên), thảm họa có cố ý do con người gây ra (ví dụ: tấn công bằng bom, vũ khí hoặc phá hoại, tin tặc hoặc virus), hoặc hỏng hóc thiết bị. Từ quan điểm nguy cơ gián đoạn, điều này có thể liên quan đến khoảng thời gian bình thường từ vài ngày, vài tuần, hoặc vài tháng để phục hồi sau một thảm họa tự nhiên, hoặc vài phút hoặc vài giờ để phục hồi sau một lây nhiễm phần mềm độc hại hoặc một hỏng hóc cơ/máy điện. Vì thường có một lĩnh vực riêng biệt xử lý vấn đề đáng tin cậy và bảo trì cơ/máy điện, một số tổ chức chọn định nghĩa sự tiếp tục hoạt động kinh doanh một cách loại trừ những nguồn gốc gây ra thảm họa này. Vì kế hoạch duy trì hoạt động kinh doanh cũng chủ yếu xem xét các tác động dài hạn của gián đoạn sản xuất, một số tổ chức cũng chọn đặt một giới hạn tối thiểu về thời gian gián đoạn cho các rủi ro cần xem xét. Đối với mục đích bảo mật ICS, khuyến nghị không nên áp đặt bất kỳ hạn chế nào này. Cả gián đoạn dài hạn (phục hồi sau thảm họa) và gián đoạn ngắn hạn (phục hồi hoạt động) đều nên được xem xét. Vì một số gián đoạn tiềm năng này liên quan đến thảm họa do con người gây ra, cũng quan trọng để làm việc phối hợp với tổ chức an toàn vật lý để hiểu rõ các rủi ro tương đối của các thảm họa này và các biện pháp phòng ngừa an toàn vật lý đã được triển khai. Đối với tổ chức an toàn vật lý, cũng quan trọng để hiểu rõ những khu vực của một cơ sở sản xuất chứa hệ thống thu thập dữ liệu và kiểm soát dữ liệu có thể có mức rủi ro cao hơn.

Trước khi tạo một kế hoạch duy trì hoạt động kinh doanh (BCP) để xử lý các gián đoạn tiềm năng, quan trọng là xác định các mục tiêu phục hồi cho các hệ thống và phụ hệ thống khác nhau dựa trên nhu cầu kinh doanh thông thường. Có hai loại mục tiêu khác nhau: phục hồi hệ thống và phục hồi dữ liệu. Phục hồi hệ thống liên quan đến việc khôi phục kết nối truyền thông và khả năng xử lý, và thường được xác định dưới dạng Mục tiêu Thời gian Phục hồi (Recovery Time Objective - RTO). Điều này được xác định là thời gian cần thiết để khôi phục kết nối truyền thông và khả năng xử lý cần thiết. Phục hồi dữ liệu liên quan đến việc khôi phục dữ liệu mô tả điều kiện sản xuất hoặc sản phẩm trong quá khứ và thường được xác định dưới dạng Mục tiêu Điểm Phục hồi (Recovery Point Objective - RPO). Điều này được xác định là khoảng thời gian dài nhất mà sự vắng mặt dữ liệu có thể chấp nhận được.

Sau khi xác định các mục tiêu phục hồi, cần tạo danh sách các gián đoạn tiềm năng và phát triển và mô tả các thủ tục phục hồi. Đối với hầu hết các gián đoạn nhỏ hơn, các hoạt động sửa chữa và thay thế dựa trên một kho dự trữ phần cứng quan trọng sẽ đủ để đáp ứng các mục tiêu phục hồi. Khi điều này không đúng, cần phát triển các kế hoạch khẩn cấp. Do chi phí tiềm năng và quan trọng của các kế hoạch khẩn cấp này, nên xem xét xem chúng có được chứng minh là đáng đầu tư hay không, và nên được xem xét với các quản lý có trách nhiệm về kế hoạch duy trì hoạt động kinh doanh để đảm bảo tính chính xác.

Sau khi tài liệu các thủ tục phục hồi được ghi lại, cần phát triển lịch trình để kiểm tra một phần hoặc toàn bộ các thủ tục phục hồi. Phải chú ý đặc biệt đến việc xác minh các bản sao lưu dữ liệu cấu hình hệ thống và dữ liệu sản phẩm hoặc sản xuất. Các ví dụ về dữ liệu cấu hình hệ thống bao gồm các bản sao lưu cấu hình máy tính, các bản sao lưu cấu hình ứng dụng, giới hạn điều khiển hoạt động, các nhóm điều khiển và điểm thiết lập cho hoạt động trước thảm họa cho tất cả các thiết bị có thể được lập trình của ICS. Chúng không chỉ nên được kiểm tra khi được tạo ra, mà cần xem xét định kỳ các thủ tục được tuân thủ cho việc lưu trữ chúng để đảm bảo rằng các bản sao lưu không bị vô dụng do điều kiện môi trường và được lưu trữ ở một vị trí an toàn, để có thể nhanh chóng được lấy ra bởi những người được ủy quyền khi cần thiết.

**5.5.2.6.2 Lập kế hoạch khắc phục thảm họa**

Một kế hoạch phục hồi sau thảm họa (DRP) là một quy trình hoặc tập hợp các thủ tục được ghi lại để khôi phục và bảo vệ cơ sở hạ tầng công nghệ thông tin trong trường hợp xảy ra thảm họa. DRP, thường được ghi lại dưới dạng văn bản, xác định các thủ tục mà một tổ chức sẽ tuân thủ trong trường hợp xảy ra thảm họa. Đây là một tuyên bố toàn diện về các hành động nhất quán cần được thực hiện trước, trong và sau một thảm họa. Thảm họa có thể là tự nhiên, môi trường hoặc do con người gây ra. Thảm họa do con người có thể có tính cố ý hoặc không cố ý.

**Đề xuất và hướng dẫn cụ thể cho môi trường ICS**

Một DRP là rất quan trọng để đảm bảo khả dụng liên tục của ICS. DRP nên bao gồm các mục sau:

- Các phản ứng cần thiết đối với các sự kiện hoặc tình trạng có thời gian và mức độ nghiêm trọng khác nhau mà sẽ kích hoạt kế hoạch phục hồi.

- Thủ tục để vận hành ICS ở chế độ thủ công với tất cả các kết nối điện tử bên ngoài bị cắt đứt cho đến khi điều kiện an toàn có thể được khôi phục.

- Vai trò và trách nhiệm của các nhân viên phản ứng.

- Quy trình và thủ tục để sao lưu và lưu trữ thông tin một cách an toàn.

- Sơ đồ mạng logic đầy đủ và cập nhật.

- Danh sách nhân viên được ủy quyền truy cập vật lý và truy cập mạng vào ICS.

- Quy trình giao tiếp và danh sách nhân viên cần liên hệ trong trường hợp khẩn cấp bao gồm các nhà cung cấp ICS, quản trị mạng, nhân viên hỗ trợ ICS, v.v.

- Thông tin cấu hình hiện tại cho tất cả các thành phần.

- Lịch trình thực hiện DRP.

- Kế hoạch cũng nên chỉ ra yêu cầu về việc thay thế kịp thời các thành phần trong trường hợp khẩn cấp. Nếu có thể, nên giữ các thành phần quan trọng khó có được trong kho lưu trữ.

Kế hoạch bảo mật nên xác định một chính sách sao lưu và khôi phục toàn diện. Khi xây dựng chính sách này, cần xem xét các yếu tố sau:

Tốc độ cần khôi phục dữ liệu hoặc hệ thống. Yêu cầu này có thể đòi hỏi sự cần thiết của một hệ thống dự phòng, máy tính dự phòng ngoại tuyến hoặc các bản sao lưu hệ thống tệp tin hợp lệ.

- Tần suất thay đổi dữ liệu và cấu hình quan trọng. Điều này sẽ quy định tần suất và đầy đủ của các bản sao lưu.

- Lưu trữ an toàn trên cơ sở và ngoài cơ sở của bản sao lưu đầy đủ và bổ sung.

- Lưu trữ an toàn của phương tiện cài đặt, khóa cấp phép và thông tin cấu hình.

- Xác định những người chịu trách nhiệm thực hiện, kiểm tra, lưu trữ và khôi phục lại bản sao lưu.

5.5.2.7 Nhận dạng và xác thực

Xác thực (Authentication) mô tả quá trình xác định danh tính của người dùng, máy chủ, ứng dụng, dịch vụ và tài nguyên mạng bằng việc sử dụng một số yếu tố nhận dạng hoặc thông tin xác thực. Kết quả của quá trình xác thực này sau đó trở thành cơ sở để cho phép hoặc từ chối các hành động tiếp theo (ví dụ: khi một máy rút tiền tự động yêu cầu mã PIN). Dựa trên quyết định xác thực, hệ thống có thể cho hoặc không cho phép người dùng tiềm năng truy cập vào tài nguyên của nó. Ủy quyền (Authorization) là quá trình xác định ai và cái gì được phép truy cập vào một tài nguyên cụ thể; kiểm soát truy cập (Access control) là cơ chế để thi hành ủy quyền.

Có một số yếu tố khả thi để xác định tính xác thực của một người, thiết bị hoặc hệ thống, bao gồm thông tin bạn biết, vật phẩm bạn sở hữu hoặc điều bạn là. Ví dụ, xác thực có thể dựa trên một thông tin đã biết (ví dụ: mã PIN hoặc mật khẩu), một vật phẩm mà bạn sở hữu (ví dụ: chìa khóa, thiết bị kết nối, thẻ thông minh), hoặc một đặc điểm sinh học như vân tay, kính ngắm mắt), vị trí (ví dụ: vị trí của Hệ thống định vị toàn cầu [GPS]), thời gian yêu cầu được thực hiện hoặc sự kết hợp của các thuộc tính này. Nói chung, càng sử dụng nhiều yếu tố trong quá trình xác thực, quá trình sẽ càng mạnh mẽ. Khi sử dụng hai hoặc nhiều yếu tố, quá trình được gọi chung là xác thực đa yếu tố (multi-factor authentication).

**Đề xuất và hướng dẫn cụ thể cho môi trường ICS:**

Hệ thống máy tính trong môi trường ICS thường phụ thuộc vào mật khẩu truyền thống để xác thực. Các nhà cung cấp hệ thống điều khiển thường cung cấp hệ thống với mật khẩu mặc định. Những mật khẩu này được thiết lập từ nhà máy và thường dễ đoán hoặc thay đổi không thường xuyên, tạo ra những rủi ro bảo mật bổ sung. Ngoài ra, các giao thức hiện được sử dụng trong môi trường ICS thường không có hoặc không đủ xác thực dịch vụ mạng. Hiện có một số hình thức xác thực khả dụng ngoài kỹ thuật mật khẩu truyền thống được sử dụng với ICS. Một số hình thức này, bao gồm xác thực mật khẩu, được trình bày trong các phần sau với những cuộc thảo luận liên quan đến việc sử dụng chúng với ICS.

**5.5.2.7.1 Xác thực mật khẩu**

Công nghệ xác thực mật khẩu xác định tính xác thực dựa trên việc kiểm tra thông tin mà thiết bị hoặc người yêu cầu truy cập nên biết, chẳng hạn như mã PIN hoặc mật khẩu. Các hệ thống xác thực mật khẩu được coi là hình thức đơn giản và phổ biến nhất.

Nhược điểm của mật khẩu có thể được giảm bớt bằng cách sử dụng công cụ kiểm tra mật khẩu hoạt động để ngăn chặn mật khẩu yếu, gần đây sử dụng hoặc phổ biến. Một điểm yếu khác là việc nghe trộm bên thứ ba dễ dàng. Mật khẩu được gõ trên bàn phím dễ dàng quan sát hoặc ghi lại, đặc biệt là trong các khu vực mà hacker có thể đặt các máy ảnh không dây nhỏ gọn hoặc thiết bị ghi nhớ phím. Xác thực dịch vụ mạng thường truyền mật khẩu dưới dạng văn bản thuần (không được mã hóa), cho phép bất kỳ công cụ chụp mạng nào cũng có thể tiết lộ mật khẩu.

**Đề xuất và hướng dẫn cụ thể cho môi trường ICS:**

Một vấn đề với mật khẩu duy nhất cho môi trường ICS là khả năng của người dùng để ghi nhớ và nhập mật khẩu có thể bị ảnh hưởng bởi căng thẳng trong thời điểm cần thiết. Trong một tình huống khẩn cấp lớn khi sự can thiệp của con người là cần thiết để kiểm soát quy trình, một nhân viên có thể hoảng loạn và gặp khó khăn trong việc nhớ hoặc nhập mật khẩu và có thể bị khóa hoàn toàn hoặc bị trì hoãn trong việc phản ứng với sự kiện. Nếu mật khẩu đã được nhập sai và hệ thống có giới hạn về số lần nhập sai mật khẩu được cho phép, nhân viên có thể bị khóa vĩnh viễn cho đến khi một nhân viên có quyền được phép có thể thiết lập lại tài khoản. Các yếu tố nhận dạng sinh trắc học có thể có những nhược điểm tương tự. Tổ chức nên cân nhắc kỹ càng các yêu cầu về bảo mật và hậu quả tiềm tàng của việc sử dụng các cơ chế xác thực trên các hệ thống quan trọng này.

Trong những tình huống mà hệ thống ICS không thể hỗ trợ hoặc tổ chức xác định là không khuyến nghị (ví dụ: hiệu suất, an toàn hoặc độ tin cậy bị ảnh hưởng), để triển khai các cơ chế xác thực trong một ICS, tổ chức sử dụng các biện pháp kiểm soát bù, chẳng hạn như kiểm soát bảo mật vật lý chặt chẽ (ví dụ: truy cập bằng thẻ từ vào trung tâm điều khiển cho người dùng được ủy quyền) để cung cấp mức độ bảo mật hoặc mức độ bảo vệ tương đương cho ICS. Hướng dẫn này cũng áp dụng cho việc sử dụng khóa phiên và chấm dứt phiên trong một ICS.

Cần xem xét đặc biệt khi áp dụng chính sách dựa trên xác thực mật khẩu đăng nhập trong môi trường ICS. Nếu không có danh sách loại trừ dựa trên xác định máy (ID), việc đăng nhập không phải là nhân viên điều hành có thể dẫn đến việc áp dụng các chính sách như thời gian tự động đăng xuất và thay thế mật khẩu quản trị viên có thể gây hại cho hoạt động của hệ thống. Một số hệ điều hành ICS làm cho việc thiết lập mật khẩu an toàn khó khăn, vì kích thước mật khẩu rất nhỏ và hệ thống chỉ cho phép mật khẩu nhóm ở mỗi cấp độ truy cập, không phải mật khẩu riêng lẻ. Một số giao thức công nghiệp (và Internet) truyền mật khẩu dưới dạng văn bản thô, khiến chúng dễ bị chặn giữa chừng. Trong trường hợp không thể tránh được việc này, quan trọng là người dùng có các mật khẩu khác nhau (và không liên quan) để sử dụng với các giao thức được mã hóa và không được mã hóa.

Một số hệ điều hành ICS làm cho việc thiết lập mật khẩu an toàn khó khăn, vì kích thước mật khẩu rất nhỏ và hệ thống chỉ cho phép mật khẩu nhóm ở mỗi cấp độ truy cập, không phải mật khẩu riêng lẻ. Một số giao thức công nghiệp (và Internet) truyền mật khẩu dưới dạng văn bản thô, khiến chúng dễ bị chặn giữa chừng. Trong trường hợp không thể tránh được việc này, quan trọng là người dùng có các mật khẩu khác nhau (và không liên quan) để sử dụng với các giao thức được mã hóa và không được mã hóa.

Dưới đây là các khuyến nghị và yếu tố cần xem xét chung liên quan đến việc sử dụng mật khẩu

- Độ dài, sức mạnh và độ phức tạp của mật khẩu nên cân nhắc để cân bằng giữa bảo mật và tiện lợi trong truy cập hoạt động dựa trên khả năng của phần mềm và hệ điều hành cơ bản.

- Mật khẩu nên có độ dài và độ phức tạp phù hợp với yêu cầu bảo mật. Đặc biệt, chúng không nên có thể được tìm thấy trong từ điển hoặc chứa các chuỗi dự đoán có thể nhận biết được bằng số hoặc chữ cái.

- Mật khẩu nên được sử dụng cẩn thận trên các thiết bị giao diện của người điều khiển như bảng điều khiển kiểm soát trong các quy trình quan trọng. Việc sử dụng mật khẩu trên các bảng điều khiển này có thể gây ra các vấn đề an toàn tiềm tàng nếu nhân viên điều hành bị khóa hoặc bị trì hoãn trong việc truy cập trong các sự kiện quan trọng. Bảo mật vật lý nên bổ sung cho bảng điều khiển người điều khiển khi bảo vệ mật khẩu không khả thi.

- Người giữ mật khẩu chính phải là một nhân viên đáng tin cậy, sẵn có trong các tình huống khẩn cấp. Bất kỳ bản sao của mật khẩu chính nên được lưu trữ ở một vị trí rất an toàn với quyền truy cập hạn chế.

- Mật khẩu của người dùng có đặc quyền (như kỹ thuật viên mạng, kỹ thuật viên điện hoặc điện tử và quản lý, nhà thiết kế/điều hành mạng) nên được bảo mật nhất và thay đổi thường xuyên. Quyền thay đổi mật khẩu chính nên được hạn chế cho nhân viên đáng tin cậy. Một bản ghi kiểm tra mật khẩu, đặc biệt là mật khẩu chính, nên được duy trì riêng biệt so với hệ thống điều khiển.

- Trong môi trường có nguy cơ cao về chặn hoặc xâm nhập (như giao diện điều khiển từ xa trong một cơ sở thiếu các điều khiển an toàn vật lý địa phương), tổ chức nên xem xét bổ sung xác thực mật khẩu bằng các hình thức xác thực khác như xác thực đa yếu tố sử dụng sinh trắc học hoặc token vật lý.

- Đối với mục đích xác thực người dùng, việc sử dụng mật khẩu là phổ biến và chấp nhận được cho người dùng đăng nhập trực tiếp vào thiết bị hoặc máy tính cục bộ. Mật khẩu không nên được gửi qua mạng nếu không được bảo vệ bằng một hình thức mã hóa được chấp nhận tham chiếu theo TCVN thực tế hoặc băm mã hóa được thiết kế để ngăn chặn các cuộc tấn công phát lại. Điều được giả định là thiết bị được sử dụng để nhập mật khẩu đã kết nối với mạng một cách an toàn.

- Đối với mục đích xác thực dịch vụ mạng, mật khẩu không nên được truyền dưới dạng văn bản thô. Có các phương pháp an toàn hơn, như thay đổi/đáp ứng hoặc xác thực khóa công khai.

**5.5.2.7.2 Thay đổi/ phản hồi xác thực**

Xác thực thay đổi/đáp ứng yêu cầu cả người yêu cầu dịch vụ và nhà cung cấp dịch vụ biết trước một "mã" bí mật. Khi có yêu cầu dịch vụ, nhà cung cấp dịch vụ gửi một số ngẫu nhiên hoặc chuỗi làm thay đổi cho người yêu cầu dịch vụ. Người yêu cầu dịch vụ sử dụng mã bí mật để tạo ra một phản hồi duy nhất cho nhà cung cấp dịch vụ. Nếu phản hồi như dự kiến, điều đó chứng tỏ người yêu cầu dịch vụ có quyền truy cập vào "mã" bí mật mà không bao giờ tiết lộ mã đó trên mạng.

Xác thực thay đổi/đáp ứng giải quyết các lỗ hổng bảo mật của xác thực mật khẩu truyền thống. Khi mật khẩu (đã được băm hoặc văn bản thô) được gửi qua mạng, một phần của "mã" thực tế đang được gửi đi, cho phép thiết bị từ xa thực hiện xác thực. Do đó, việc trao đổi mật khẩu truyền thống luôn mang theo nguy cơ phát hiện hoặc phát lại. Bởi vì mã bí mật đã biết trước và không bao giờ được gửi trong các hệ thống thay đổi/đáp ứng, nguy cơ phát hiện được loại bỏ. Nếu nhà cung cấp dịch vụ không bao giờ gửi lại thay đổi giống nhau và người nhận có thể phát hiện được tất cả các trùng lặp, nguy cơ chụp mạng và cuộc tấn công phát lại được loại bỏ.

**Khuyến nghị và hướng dẫn cụ thể cho ICS:**

Đối với Xác thực Người dùng, việc sử dụng trực tiếp xác thực thay đổi/đáp ứng có thể không khả thi đối với hệ thống kiểm soát do sự trễ có thể xảy ra trong quá trình truy cập nhanh cần thiết cho hệ thống kiểm soát hoặc mạng công nghiệp. Đối với Xác thực Dịch vụ Mạng, việc sử dụng xác thực thay đổi/đáp ứng được ưu tiên hơn so với các hệ thống xác thực mật khẩu truyền thống hoặc xác thực nguồn gốc.

Xác thực thay đổi/đáp ứng cung cấp sự bảo mật hơn so với mật khẩu được mã hóa để xác thực người dùng qua mạng. Quản lý thuật toán mã hóa chính và mật khẩu chính trở nên phức tạp hơn khi có nhiều bên tham gia vào quy trình bảo mật và đó là một yếu tố quan trọng trong tính mạnh mẽ của hệ thống bảo mật.

**5.5.2.7.3 Xác thực mã hóa vật lý**

Xác thực vật lý hoặc bằng token tương tự như xác thực mật khẩu, ngoại trừ rằng các công nghệ này xác định tính xác thực bằng cách kiểm tra mã bí mật hoặc khóa được tạo ra bởi thiết bị hoặc token mà người yêu cầu truy cập sở hữu, chẳng hạn như token bảo mật hoặc thẻ thông minh. Ngày càng nhiều khóa riêng được nhúng trong các thiết bị vật lý như USB dongle. Một số token chỉ hỗ trợ xác thực một yếu tố, tức là chỉ cần sở hữu token là đủ để được xác thực. Nhưng cũng có những token hỗ trợ xác thực đa yếu tố yêu cầu biết một mã PIN hoặc mật khẩu cùng với việc sở hữu token.

Vulnerability chính mà xác thực bằng token giải quyết là việc nhân bản mã bí mật một cách dễ dàng hoặc chia sẻ nó với người khác. Nó loại bỏ tình huống phổ biến khi mật khẩu cho hệ thống "an toàn" được để lại trên tường bên cạnh máy tính hoặc trạm điều khiển. Token bảo mật không thể nhân bản mà không cần truy cập đặc biệt vào thiết bị và vật tư.

Lợi ích thứ hai là mã bí mật trong token vật lý có thể rất lớn, được bảo vệ vật lý và được tạo ngẫu nhiên. Vì nó được nhúng trong kim loại hoặc silic, nó không có các rủi ro tương tự như mật khẩu được nhập vào thủ công. Nếu một token bảo mật bị mất hoặc bị đánh cắp, người dùng đã được ủy quyền sẽ mất quyền truy cập, không giống như mật khẩu truyền thống có thể bị mất hoặc bị đánh cắp mà không có thông báo.

Các hình thức phổ biến của xác thực vật lý/token bao gồm:

- Khóa vật lý truyền thống.- Thẻ an toàn (ví dụ: từ có nam châm, chip thông minh, mã quang).

- Thiết bị tần số vô tuyến dưới dạng thẻ, chìa khóa hoặc tag gắn trên.

- Dongle với các khóa mã hóa an toàn gắn vào cổng USB, cổng serial hoặc cổng song song của máy tính.

- Thiết bị tạo mã xác thực một lần (ví dụ: key fob).

Đối với xác thực một yếu tố, điểm yếu lớn nhất là việc chỉ cần sở hữu token vật lý là có quyền truy cập (ví dụ: bất kỳ ai tìm thấy một bộ chìa khóa bị mất bây giờ có quyền truy cập vào bất cứ thứ gì mà chìa khóa đó mở). Xác thực vật lý/token an toàn hơn khi kết hợp với một hình thức xác thực thứ hai, chẳng hạn như mã PIN được ghi nhớ sử dụng cùng với token

**Khuyến nghị và hướng dẫn cụ thể cho ICS**

Xác thực đa yếu tố là một thực hành tốt được chấp nhận để truy cập vào ứng dụng hệ thống kiểm soát công nghiệp từ bên ngoài tường lửa của hệ thống.

Xác thực vật lý/token có tiềm năng đóng một vai trò mạnh trong môi trường kiểm soát công nghiệp. Một thẻ truy cập hoặc token khác có thể là một hình thức xác thực hiệu quả cho truy cập máy tính, miễn là máy tính đó ở trong khu vực an toàn (ví dụ: sau khi nhân viên đã có quyền truy cập vào phòng với xác thực phụ hợp lệ, chỉ cần sử dụng thẻ để thực hiện các hành động điều khiển).

**5.5.2.7.4 Xác thực thẻ thông minh**

Thẻ thông minh tương tự xác thực thông qua token, nhưng có thể cung cấp các chức năng bổ sung. Thẻ thông minh có thể được cấu hình để chạy nhiều ứng dụng trên thẻ để hỗ trợ quyền truy cập vào tòa nhà, xác thực hai yếu tố hoặc ba yếu tố cho máy tính và hỗ trợ thanh toán không dùng tiền mặt trên một thẻ duy nhất, đồng thời cũng đóng vai trò như thẻ nhận dạng hình ảnh của công ty cho cá nhân.

Thông thường, thẻ thông minh có kích thước tương tự thẻ tín dụng, có thể được in, ép chìm và được cá nhân hóa. Thẻ thông minh có thể được tùy chỉnh, cá nhân hóa và được phát hành trong nội bộ hoặc được giao cho nhà cung cấp dịch vụ, thường phát hành hàng trăm ngàn thẻ mỗi ngày.Thẻ thông minh cải thiện các giải pháp chỉ dựa trên phần mềm như xác thực bằng mật khẩu bằng cách cung cấp một yếu tố xác thực bổ sung và loại bỏ yếu tố con người trong việc nhớ các bí mật phức tạp. Thẻ thông minh cũng có các lợi ích sau:

- Cô lập các tính toán quan trọng về bảo mật, bao gồm xác thực, chữ ký số và trao đổi khóa, khỏi các phần khác của hệ thống không cần biết thông tin đó.

- Cho phép di động các thông tin nhận dạng và thông tin cá nhân khác giữa nhiều hệ thống máy tính.

- Cung cấp bộ nhớ chống xâm phạm để bảo vệ khóa cá nhân và các thông tin cá nhân khác.

Hầu hết các vấn đề liên quan đến thẻ thông minh là vấn đề về hậu cần, đặc biệt là việc phát hành lại thẻ bị mất hoặc bị đánh cắp.

**Khuyến nghị và Hướng dẫn cụ thể cho ICS:**

Mặc dù thẻ thông minh có giá rẻ và cung cấp các chức năng hữu ích trong ngữ cảnh của hệ thống điều khiển công nghiệp, triển khai chúng phải được thực hiện trong bối cảnh bảo mật tổng thể của nhà máy. Việc xác định cá nhân, phát hành thẻ, thu hồi khi có nghi ngờ về sự vi phạm và phân công quyền cho các nhận dạng đã được xác thực đại diện cho một thách thức quan trọng ban đầu và liên tục. Trong một số trường hợp, công nghệ thông tin doanh nghiệp hoặc các nguồn lực khác có thể sẵn sàng hỗ trợ trong việc triển khai cơ sở hạ tầng dựa trên thẻ thông minh và khóa công khai.

Nếu triển khai thẻ thông minh trong một môi trường điều khiển công nghiệp, cần xem xét các biện pháp quản lý thẻ bị mất hoặc hỏng, cũng như chi phí để tích hợp hệ thống kiểm soát truy cập tương ứng và cung cấp quy trình quản lý cho việc phân phối và thu hồi thẻ.

**5.5.2.7.5 Xác thực sinh trắc học**

Công nghệ xác thực sinh trắc học xác định tính xác thực bằng cách xác định các đặc điểm sinh học có khả năng duy nhất của con người yêu cầu truy cập. Các đặc điểm sinh trắc học có thể sử dụng bao gồm các điểm nhỏ trên ngón tay, hình học khuôn mặt, chữ ký võng mạc và giác mạc, mẫu giọng nói, mẫu gõ phím và hình học bàn tay.

Tương tự như các token vật lý và thẻ thông minh, xác thực sinh trắc học tăng cường các giải pháp chỉ dựa trên phần mềm như xác thực mật khẩu bằng cách cung cấp một yếu tố xác thực bổ sung và loại bỏ yếu tố con người trong việc nhớ các bí mật phức tạp. Hơn nữa, vì các đặc điểm sinh trắc học là duy nhất đối với mỗi cá nhân cụ thể, xác thực sinh trắc học giải quyết vấn đề về việc mất hoặc mất cắp các token vật lý và thẻ thông minh.

Một số vấn đề đáng chú ý với xác thực sinh trắc học bao gồm:

- Phân biệt đối tượng thật và đối tượng giả (ví dụ: làm thế nào để phân biệt một ngón tay người thật và một bản sao từ cao su silicon hoặc làm thế nào để phân biệt giọng nói của con người thật và một bản ghi âm).

- Phát sinh lỗi loại I và lỗi loại II (xác suất từ chối một hình ảnh sinh trắc học hợp lệ và xác suất chấp nhận một hình ảnh sinh trắc học không hợp lệ, tương ứng). Thiết bị xác thực sinh trắc học nên được cấu hình sao cho xác suất chéo thấp nhất giữa hai xác suất này, còn được gọi là tỷ lệ lỗi chéo.

- Xử lý các yếu tố môi trường như nhiệt độ và độ ẩm mà một số thiết bị sinh trắc học nhạy cảm.

- Đối mặt với các ứng dụng trong ngành công nghiệp trong đó nhân viên có thể đeo kính bảo hộ và/hoặc găng tay và hóa chất công nghiệp có thể ảnh hưởng đến máy quét sinh trắc học.

- Huấn luyện lại máy quét sinh trắc học khi chúng có thể "thay đổi" theo thời gian. Đặc điểm sinh trắc học của con người cũng có thể thay đổi theo thời gian, đòi hỏi việc huấn luyện lại máy quét định kỳ.

- Yêu cầu hỗ trợ kỹ thuật và xác minh trực tiếp để đào tạo thiết bị, khác với mật khẩu có thể được truyền qua điện thoại hoặc thẻ truy cập có thể được giao cho lễ tân.

- Từ chối quyền truy cập cần thiết vào hệ thống điều khiển vì khả năng tạm thời của thiết bị cảm biến không thể xác nhận người dùng hợp lệ.

- Sự chấp nhận xã hội. Người dùng xem xét một số thiết bị xác thực sinh trắc học dễ chấp nhận hơn các thiết bị khác. Ví dụ, quét võng mạc có thể được coi là rất thấp trên thang đánh giá sự chấp nhận, trong khi máy quét vân tay có thể được coi là cao trên thang đánh giá sự chấp nhận. Người dùng các thiết bị xác thực sinh trắc học sẽ cần xem xét tính chấp nhận xã hội cho nhóm mục tiêu của họ khi lựa chọn giữa các công nghệ xác thực sinh trắc học khác nhau.

**Khuyến nghị và hướng dẫn cụ thể cho ICS:**

Các thiết bị sinh trắc học tạo ra một kiểm tra phụ hữu ích so với các hình thức xác thực khác có thể bị mất hoặc được mượn. Sử dụng xác thực sinh trắc học kết hợp với kiểm soát truy cập dựa trên token hoặc đồng hồ chấm công nhân viên hoạt động bằng thẻ tăng cường mức độ bảo mật. Một ứng dụng có thể là trong một phòng điều khiển được kiểm soát môi trường và được bảo mật vật lý.

Công nghệ sinh trắc học có thể cung cấp một cơ chế xác thực giá trị, nhưng cần được đánh giá cẩn thận đối với các ứng dụng công nghiệp, vì vấn đề về mặt vật lý và môi trường trong môi trường lắp đặt có thể cần được cấu trúc lại để đảm bảo xác thực ủy quyền đáng tin cậy. Các thuộc tính vật lý và môi trường chính xác của một cài đặt cụ thể nên được phối hợp với nhà cung cấp hệ thống hoặc nhà sản xuất.

5.5.2.8 Ứng phó thảm họa

Một kế hoạch phản ứng sự cố là tài liệu ghi lại một bộ hướng dẫn hoặc thủ tục được xác định trước để phát hiện, phản ứng và giới hạn hậu quả của các sự cố đối với hệ thống thông tin của một tổ chức. Phản ứng nên được đo đạc dựa trên "dịch vụ được cung cấp" trước hết, không chỉ là hệ thống bị xâm phạm. Nếu phát hiện một sự cố, cần tiến hành một đánh giá rủi ro nhanh để đánh giá tác động của cả cuộc tấn công và các lựa chọn để phản ứng. Ví dụ, một lựa chọn phản ứng có thể là cô lập vật lý hệ thống đang bị tấn công. Tuy nhiên, điều này có thể ảnh hưởng nghiêm trọng đến dịch vụ đến mức không khả thi.

Các khuyến nghị và hướng dẫn cụ thể cho ICS:

Bất kể các biện pháp được thực hiện để bảo vệ một hệ thống ICS, luôn có khả năng nó có thể bị tấn công bởi một sự cố cố ý hoặc vô ý. Có thể có những triệu chứng sau đây xuất hiện do các vấn đề mạng thông thường, nhưng khi một số triệu chứng bắt đầu xuất hiện, một mô hình có thể chỉ ra rằng hệ thống ICS đang bị tấn công và có thể xứng đáng được điều tra sâu hơn. Nếu hacker là người có kỹ năng, có thể không rõ ràng rằng một cuộc tấn công đang diễn ra.

Các triệu chứng của một sự cố có thể bao gồm các điểm sau:

- Luồng dữ liệu mạng không bình thường.

- Không gian đĩa đầy hoặc không gian đĩa trống giảm đáng kể.

- Sử dụng CPU quá cao.

- Tạo tài khoản người dùng mới.

- Cố gắng hoặc thực tế sử dụng tài khoản cấp quản trị.

- Tài khoản bị khóa.

- Tài khoản đang được sử dụng khi người dùng không có mặt tại nơi làm việc.

- Xóa các tệp nhật ký.

- Tệp nhật ký đầy với số lượng sự kiện không bình thường.

- Cảnh báo từ phần mềm diệt virus hoặc hệ thống phát hiện xâm nhập (IDS).

- Vô hiệu hóa phần mềm diệt virus và các biện pháp kiểm soát bảo mật khác.

- Thay đổi vá không đáng ngờ.

- Các máy kết nối với địa chỉ IP bên ngoài.

- Yêu cầu thông tin về hệ thống (cố gắng xâm nhập bằng kỹ thuật xã hội).

- Thay đổi cấu hình không đáng ngờ.

- Tắt hệ thống đột ngột.

Để giảm thiểu tác động của các cuộc xâm nhập này, cần lập kế hoạch phản ứng. Kế hoạch phản ứng sự cố định nghĩa các thủ tục cần được thực hiện khi xảy ra một cuộc xâm nhập. Tham chiếu theo TCVN thực tế, Hướng dẫn Xử lý Sự cố Bảo mật Máy tính, cung cấp hướng dẫn về kế hoạch phản ứng sự cố, bao gồm các mục sau đây:

- **Phân loại Sự cố:** Các loại sự cố ICS khác nhau nên được xác định và phân loại theo tiềm năng ảnh hưởng để xác định phản ứng thích hợp cho mỗi sự cố tiềm năng.

- **Hành động Phản ứng:** Có nhiều phản ứng có thể được thực hiện khi có một sự cố. Các phản ứng này có thể từ không làm gì đến tắt hệ thống hoàn toàn (mặc dù việc tắt hệ thống ICS hoàn toàn là phản ứng rất không thường xảy ra). Phản ứng được chọn sẽ phụ thuộc vào loại sự cố và tác động của nó đối với hệ thống ICS và quy trình vật lý đang được điều khiển. Nên chuẩn bị một kế hoạch viết tài liệu ghi lại các loại sự cố và phản ứng với từng loại để cung cấp hướng dẫn trong những lúc có thể có sự nhầm lẫn hoặc áp lực do sự cố. Kế hoạch này nên bao gồm các bước cụ thể mà các tổ chức khác nhau cần thực hiện. Nếu có yêu cầu báo cáo, những yêu cầu này cũng nên được ghi chú cùng với nơi nộp báo cáo và số điện thoại để giảm sự nhầm lẫn trong việc báo cáo.

- **Hành động khôi phục:** Kết quả của cuộc xâm nhập có thể nhẹ nhàng hoặc có thể gây ra nhiều vấn đề trong hệ thống ICS. Phân tích rủi ro nên được tiến hành để xác định mức độ nhạy cảm của hệ thống vật lý đang được điều khiển đối với các chế độ lỗi trong ICS. Trong mọi trường hợp, các hành động khôi phục từng bước nên được ghi lại để hệ thống có thể trở lại hoạt động bình thường một cách nhanh chóng và an toàn. Các hành động khôi phục cho một cuộc xâm nhập ảnh hưởng đến hoạt động của ICS sẽ tương đồng với Kế hoạch Phục hồi Thảm họa của hệ thống và nên tính đến kế hoạch và phối hợp đã được thiết lập trước đó.

Trong quá trình lập kế hoạch phản ứng sự cố, cần thu thập thông tin từ các bên liên quan bao gồm các hoạt động, kỹ thuật, công nghệ thông tin, nhà cung cấp hỗ trợ hệ thống, quản lý, lao động tổ chức, pháp lý và an toàn. Những bên liên quan này cũng nên xem xét và phê duyệt kế hoạch.

5.5.2.9 Bảo trì

Các biện pháp kiểm soát bảo mật tham chiếu theo TCVN thực tế cung cấp chính sách và quy trình để thực hiện bảo trì định kỳ và ngăn ngừa trên các thành phần của một hệ thống thông tin. Điều này bao gồm việc sử dụng các công cụ bảo trì (cả địa phương và từ xa) và quản lý nhân viên bảo trì.

5.5.2.10 Bảo vệ phương tiện

Các biện pháp kiểm soát bảo mật thuộc tham chiếu theo TCVN thực tế cung cấp chính sách và quy trình để hạn chế truy cập vào phương tiện lưu trữ thông tin cho các người dùng được ủy quyền. Các biện pháp kiểm soát cũng áp dụng cho việc gắn nhãn các phương tiện truyền thông để đáp ứng yêu cầu về phân phối và xử lý, cũng như lưu trữ, vận chuyển, vệ sinh (loại bỏ thông tin từ phương tiện kỹ thuật số), phá hủy và tiêu hủy các phương tiện đó.

**Khuyến nghị và hướng dẫn cụ thể cho ICS:**

Tài sản truyền thông bao gồm các phương tiện lưu trữ có thể gỡ ra được như đĩa mềm, đĩa CD, đĩa DVD và USB, cũng như các báo cáo và tài liệu in. Các biện pháp kiểm soát về bảo mật vật lý nên đáp ứng các yêu cầu cụ thể để bảo quản an toàn các tài sản này và cung cấp hướng dẫn cụ thể cho việc vận chuyển, xử lý, xóa hoặc phá hủy các tài sản này. Các yêu cầu về bảo mật có thể bao gồm việc lưu trữ an toàn để tránh mất mát, cháy, mất cắp, phân phối vô tình hoặc tổn hại môi trường.

Nếu hacker có được quyền truy cập vào phương tiện sao lưu liên quan đến một hệ thống ICS, nó có thể cung cấp dữ liệu quý giá để tiến hành một cuộc tấn công. Khôi phục một tệp xác thực từ sao lưu có thể cho phép hacker chạy các công cụ phá mật khẩu và trích xuất mật khẩu có thể sử dụng. Ngoài ra, các sao lưu thường chứa tên máy, địa chỉ IP, số phiên bản phần mềm, tên người dùng và các dữ liệu khác hữu ích trong việc lập kế hoạch tấn công.

Việc sử dụng bất kỳ đĩa CD, đĩa DVD, đĩa mềm, USB hoặc các phương tiện lưu trữ gỡ ra được tương tự không được phép trên bất kỳ nút nào thuộc hệ thống ICS hoặc kết nối với nó để ngăn chặn việc đưa vào phần mềm độc hại hoặc mất mát hoặc mất cắp dữ liệu không cố ý. Khi các thành phần hệ thống sử dụng các giao thức chuẩn ngành không được sửa đổi, phần mềm quản lý chính sách tự động có thể được sử dụng để áp dụng chính sách bảo vệ phương tiện truyền thông.

5.5.2.11 Bảo vệ vật lý môi trường

Các biện pháp kiểm soát bảo mật tham chiếu theo TCVN thực tế cung cấp chính sách và quy trình cho việc kiểm soát truy cập vật lý vào hệ thống thông tin, bao gồm các điểm vào/ra được chỉ định, phương tiện truyền tải và phương tiện hiển thị. Điều này bao gồm các biện pháp kiểm soát việc giám sát truy cập vật lý, duy trì nhật ký và xử lý khách thăm. Nhóm này cũng bao gồm các biện pháp kiểm soát triển khai và quản lý các biện pháp bảo vệ khẩn cấp như tắt khẩn cấp hệ thống IT, dự phòng nguồn điện và chiếu sáng, kiểm soát nhiệt độ và độ ẩm, và bảo vệ chống cháy và hỏng do nước.

Biện pháp bảo mật vật lý được thiết kế để giảm rủi ro mất mát hoặc hỏng tình cờ hoặc cố ý đối với tài sản nhà máy và môi trường xung quanh. Các tài sản đang được bảo vệ có thể là tài sản vật lý như công cụ và thiết bị nhà máy, môi trường, cộng đồng xung quanh và tài sản trí tuệ, bao gồm dữ liệu độc quyền như cài đặt quy trình và thông tin khách hàng. Triển khai các biện pháp kiểm soát bảo mật vật lý thường phụ thuộc vào yêu cầu về môi trường, an toàn, quy định, pháp lý và các yêu cầu khác phải được xác định và giải quyết cụ thể cho từng môi trường cụ thể. Chủ đề triển khai các biện pháp kiểm soát bảo mật vật lý là rất rộng và cần phải cụ thể cho loại bảo vệ cần thiết.

**Khuyến nghị và hướng dẫn cụ thể cho ICS:**

Bảo vệ vật lý của các thành phần công nghệ thông tin và dữ liệu liên quan đến ICS phải được xem xét như một phần của an toàn tổng thể của một nhà máy. An toàn tại nhiều cơ sở ICS có mối liên hệ chặt chẽ với an toàn nhà máy. Mục tiêu chính là ngăn người khỏi tình huống nguy hiểm mà không ngăn cản họ làm việc hoặc thực hiện các thủ tục khẩn cấp. Các biện pháp kiểm soát bảo mật vật lý là các biện pháp vật lý, có tính chất hoạt động hoặc không hoạt động, giới hạn truy cập vật lý vào bất kỳ tài sản thông tin nào trong môi trường ICS. Những biện pháp này được áp dụng để ngăn chặn nhiều loại tác động không mong muốn, bao gồm:

- Truy cập vật lý trái phép vào các vị trí nhạy cảm.

- Sửa đổi vật lý, thao tác, ăn cắp hoặc gỡ bỏ, hoặc phá hủy các hệ thống hiện có, cơ sở hạ tầng, giao diện giao tiếp, nhân viên hoặc vị trí vật lý.

- Quan sát vật lý trái phép các tài sản thông tin nhạy cảm thông qua quan sát hình ảnh, ghi chú, chụp ảnh hoặc các phương pháp khác.

- Ngăn chặn việc giới thiệu trái phép các hệ thống mới, cơ sở hạ tầng, giao diện giao tiếp hoặc phần cứng khác.

- Ngăn chặn việc giới thiệu trái phép các thiết bị được thiết kế có chức năng gây sự can thiệp vào phần cứng, nghe trộm thông tin giao tiếp hoặc tác động có hại khác.

Có được quyền truy cập vật lý vào một phòng điều khiển hoặc các thành phần hệ thống điều khiển thường ngụ ý có được quyền truy cập logic vào hệ thống điều khiển quy trình. Tương tự, việc có quyền truy cập logic vào các hệ thống như máy chủ chính và máy tính trong phòng điều khiển cho phép kẻ tấn công tiếp quản quyền kiểm soát về quá trình vật lý.

Nếu các máy tính dễ dàng truy cập và chúng có ổ đĩa removable media (ví dụ: đĩa mềm, đĩa CD, ổ cứng ngoài) hoặc cổng USB, ổ đĩa có thể được trang bị khóa hoặc loại bỏ khỏi máy tính và cổng USB bị vô hiệu hóa. Tùy thuộc vào nhu cầu bảo mật và rủi ro, cũng có thể khôn ngoan tắt hoặc bảo vệ vật lý các nút nguồn để ngăn chặn việc sử dụng trái phép. Đối với độ bảo mật tối đa, máy chủ nên được đặt trong các khu vực khóa và các cơ chế xác thực (như chìa khóa) được bảo vệ. Ngoài ra, các thiết bị mạng trên mạng ICS, bao gồm switch, router, cổng mạng, máy chủ, máy trạm và bộ điều khiển, nên được đặt trong một khu vực an toàn chỉ có nhân viên được ủy quyền truy cập. Khu vực an toàn cũng nên tương thích với các yêu cầu môi trường của các thiết bị

Một giải pháp phòng thủ sâu về an toàn vật lý nên bao gồm các yếu tố sau:

- **Bảo vệ Vị trí Vật lý**. Các yếu tố bảo mật vật lý cổ điển thường liên quan đến kiến trúc vòng tròn của các biện pháp bảo mật lớp. Tạo ra một số rào cản vật lý, cả hoạt động và không hoạt động, xung quanh các tòa nhà, cơ sở, phòng, thiết bị hoặc tài sản thông tin khác, thiết lập các ranh giới bảo mật vật lý này. Các biện pháp kiểm soát an toàn vật lý nhằm bảo vệ các vị trí vật lý bao gồm hàng rào, mương chứa xe cộ, đồi đất, tường, chướng ngại chắn củng cố, cổng hoặc các biện pháp khác. Hầu hết các tổ chức áp dụng mô hình lớp này bằng cách ngăn chặn việc tiếp cận vào nhà máy trước tiên bằng cách sử dụng hàng rào, căn cứ bảo vệ, cổng và cửa khóa.

- **Kiểm soát Truy cập.** Hệ thống kiểm soát truy cập nên đảm bảo chỉ có những người được ủy quyền mới có quyền truy cập vào các không gian kiểm soát. Hệ thống kiểm soát truy cập nên linh hoạt. Nhu cầu truy cập có thể dựa trên thời gian (ca ban ngày và ban đêm), cấp độ đào tạo, tình trạng việc làm, nhiệm vụ công việc, tình trạng nhà máy và một loạt các yếu tố khác. Hệ thống phải có khả năng xác minh rằng những người được cấp quyền truy cập là người họ nói mình là (thường bằng cách sử dụng một thứ gì đó mà người đó có, như một thẻ truy cập hoặc chìa khóa; một điều gì đó họ biết, như một số nhận dạng cá nhân (PIN); hoặc một thứ gì đó về họ, bằng cách sử dụng thiết bị sinh trắc học). Kiểm soát truy cập nên đáng tin cậy, nhưng không làm cản trở công việc hàng ngày hoặc khẩn cấp của nhân viên nhà máy. Tích hợp kiểm soát truy cập vào hệ thống quy trình cho phép xem không chỉ truy cập an toàn, mà còn theo dõi tài sản vật lý và nhân viên, tăng tốc độ đáp ứng trong tình huống khẩn cấp, giúp chuyển hướng cá nhân đến các vị trí an toàn và nâng cao năng suất tổng thể. Trong một khu vực, việc truy cập vào tủ mạng và tủ máy tính nên được hạn chế chỉ cho những người có nhu cầu, như kỹ thuật viên mạng và kỹ sư, hoặc nhân viên bảo trì máy tính. Tủ thiết bị nên được khóa và dây cáp nên gọn gàng và nằm trong tủ. Cân nhắc giữ tất cả các máy tính trong các khung gắn kín và sử dụng công nghệ mở rộng bộ giao diện người-máy để kết nối các giao diện người-máy với các máy tính được gắn kín.

- **Hệ thống Giám sát Truy cập.** Hệ thống giám sát truy cập bao gồm camera tĩnh và camera video, các cảm biến và các loại hệ thống nhận dạng khác nhau. Ví dụ về các hệ thống này bao gồm camera giám sát các bãi đỗ xe, cửa hàng tiện lợi hoặc an toàn sân bay. Các thiết bị này không ngăn chặn cụ thể việc truy cập vào một vị trí cụ thể; thay vào đó, chúng lưu trữ và ghi lại sự hiện diện hoặc không có sự hiện diện vật lý của cá nhân, phương tiện, động vật hoặc các thực thể vật lý khác. Ánh sáng đầy đủ phải được cung cấp dựa trên loại thiết bị giám sát truy cập được triển khai.

- **Hệ thống Hạn chế Truy cập**. Hệ thống hạn chế truy cập có thể sử dụng một số thiết bị kết hợp để kiểm soát hoặc ngăn chặn việc truy cập vào các tài nguyên được bảo vệ. Hệ thống hạn chế truy cập bao gồm các thiết bị an toàn hoạt động và không hoạt động như hàng rào, cửa, két sắt, cổng và người bảo vệ. Chúng thường được kết hợp với các hệ thống nhận dạng và giám sát để cung cấp truy cập dựa trên vai trò cho các cá nhân cụ thể hoặc nhóm cá nhân.

- **Theo dõi Nhân viên và Tài sản**. Xác định vị trí của nhân viên và phương tiện trong một cơ sở lớn là quan trọng vì lý do an toàn, và nó càng ngày càng quan trọng vì lý do bảo mật. Công nghệ vị trí tài sản có thể được sử dụng để theo dõi di chuyển của nhân viên và phương tiện trong nhà máy, đảm bảo rằng họ ở trong các khu vực được ủy quyền, xác định nhân viên cần hỗ trợ và hỗ trợ phản ứng khẩn cấp.

- **Yếu tố môi trường**. Trong việc đáp ứng nhu cầu bảo mật của hệ thống và dữ liệu, việc xem xét các yếu tố môi trường là quan trọng. Ví dụ, nếu một công trường có nhiều bụi, hệ thống nên được đặt trong một môi trường có bộ lọc. Điều này đặc biệt quan trọng nếu bụi có khả năng dẫn điện hoặc từ, như trong trường hợp các công trường chế biến than hoặc sắt. Nếu rung động có thể gây vấn đề, hệ thống nên được gắn trên các ống đệm cao su để ngăn ngừa sự sụp đổ đĩa và vấn đề kết nối dây. Ngoài ra, các môi trường chứa hệ thống và phương tiện (ví dụ: băng sao lưu, đĩa mềm) nên có nhiệt độ và độ ẩm ổn định. Một cảnh báo đến hệ thống kiểm soát quy trình nên được tạo ra khi các thông số môi trường như nhiệt độ và độ ẩm vượt quá giới hạn quy định.

- **Hệ thống Điều khiển Môi trường**. Hệ thống điều hòa không khí, thông gió và điều hòa (HVAC) cho phòng điều khiển phải hỗ trợ nhân viên nhà máy trong quá trình hoạt động bình thường và tình huống khẩn cấp, có thể bao gồm việc phát hành các chất độc hại. Hệ thống chữa cháy phải được thiết kế cẩn thận để tránh gây thêm hại (ví dụ: tránh trộn nước với các sản phẩm không tương thích). HVAC và hệ thống chữa cháy có vai trò quan trọng tăng lên trong bảo mật do sự tương phụ thuộc giữa điều khiển quy trình và bảo mật. Ví dụ, phòng ngừa cháy và hệ thống HVAC hỗ trợ máy tính điều khiển công nghiệp cần được bảo vệ chống lại các sự cố mạng.

- **Nguồn điện.** Nguồn điện đáng tin cậy cho Hệ thống Điều khiển Công nghiệp (ICS) là điều cần thiết, vì vậy nên cung cấp một nguồn dự phòng không bị gián đoạn (UPS). Nếu trang web có máy phát điện khẩn cấp, tuổi thọ pin UPS có thể chỉ cần vài giây; tuy nhiên, nếu trang web phụ thuộc vào nguồn điện bên ngoài, tuổi thọ pin UPS có thể cần kéo dài đến vài giờ. Nó nên được thiết kế với kích thước tối thiểu sao cho hệ thống có thể được tắt an toàn.

**5.5.2.11.1 Trung tâm điều khiển / Phòng điều khiển**

***Khuyến nghị và Hướng dẫn cụ thể cho ICS***

Đảm bảo an toàn vật lý cho trung tâm điều khiển/phòng điều khiển là điều cần thiết để giảm thiểu nguy cơ từ nhiều mối đe dọa. Trung tâm điều khiển/phòng điều khiển thường có các bàn điều khiển luôn được đăng nhập vào máy chủ điều khiển chính, nơi tốc độ phản hồi và việc theo dõi liên tục của nhà máy là rất quan trọng. Những khu vực này thường chứa chính các máy chủ, các nút máy tính quan trọng khác và đôi khi là các bộ điều khiển nhà máy. Việc giới hạn quyền truy cập vào những khu vực này chỉ được phép cho người dùng có quyền, sử dụng các phương pháp xác thực như thẻ thông minh hoặc từ tính hoặc các thiết bị sinh trắc học. Trong trường hợp cực đoan, có thể xem xét cần thiết để tạo ra một trung tâm điều khiển/phòng điều khiển chống nổ, hoặc cung cấp một trung tâm điều khiển/phòng điều khiển khẩn cấp ngoại trú để duy trì quyền điều khiển nếu trung tâm điều khiển/phòng điều khiển chính trở nên không thể sống được.

**5.5.2.11.2 Thiết bị di động**

***Khuyến nghị và Hướng dẫn cụ thể cho ICS***

Các máy tính và thiết bị được sử dụng cho các chức năng ICS (như lập trình PLC) không được phép rời khỏi khu vực ICS. Các máy tính xách tay, máy trạm kỹ thuật cầm tay và các thiết bị cầm tay (ví dụ như 375 HART communicator) nên được bảo mật chặt chẽ và không được phép sử dụng bên ngoài mạng ICS. Cần duy trì cập nhật các phần mềm diệt virus và quản lý bản vá.

**5.5.2.11.3 Cáp**

***Khuyến nghị và Hướng dẫn cụ thể cho ICS***

Thiết kế và triển khai hệ thống cáp cho mạng điều khiển nên được xem xét trong kế hoạch an toàn mạng. Cáp truyền thông xoắn không mạch được sử dụng trong môi trường văn phòng có thể chấp nhận được, nhưng thường không phù hợp với môi trường nhà máy do dễ bị nhiễu từ các trường từ, sóng radio, nhiệt độ cực đoan, độ ẩm, bụi và rung động. Nên sử dụng các đầu nối RJ-45 công nghiệp thay vì các loại đầu nối xoắn không mạch khác để đảm bảo bảo vệ chống lại độ ẩm, bụi và rung động. Cáp quang và cáp đồng trục thường là lựa chọn tốt hơn cho mạng điều khiển vì chúng không bị ảnh hưởng bởi nhiều điều kiện môi trường thông thường, bao gồm nhiễu điện và nhiễu tần số radio thường gặp trong môi trường điều khiển công nghiệp. Cáp và đầu nối nên được mã màu và gắn nhãn để mạng ICS và mạng IT được phân biệt rõ ràng và giảm khả năng kết nối chéo vô ý. Cáp nên được lắp đặt sao cho việc truy cập được giảm thiểu (tức chỉ giới hạn cho nhân viên có quyền) và thiết bị nên được lắp đặt trong tủ khóa với thông gió và lọc không khí đủ.

5.5.2.12 Lập kế hoạch

Một kế hoạch bảo mật là một tài liệu chính thức cung cấp tổng quan về các yêu cầu bảo mật cho một hệ thống thông tin và mô tả các kiểm soát an toàn hiện có hoặc được kế hoạch để đáp ứng các yêu cầu đó. Các kiểm soát an toàn lập kế hoạch (PL) tham chiếu theo TCVN thực tế cung cấp cơ sở cho việc phát triển một kế hoạch bảo mật. Các điều khiển này cũng đề cập đến vấn đề bảo trì để định kỳ cập nhật một kế hoạch bảo mật. Một tập hợp các quy tắc mô tả trách nhiệm của người dùng và hành vi dự kiến liên quan đến việc sử dụng hệ thống thông tin với việc cho phép người dùng ký tín nhận cho thấy họ đã đọc, hiểu và đồng ý tuân thủ các quy tắc hành vi trước khi cho phép truy cập vào hệ thống thông tin.

***Khuyến nghị và hướng dẫn cụ thể cho ICS***

Một kế hoạch bảo mật cho một hệ thống điều khiển công nghiệp (ICS) nên được xây dựng dựa trên những kinh nghiệm, chương trình và thực tiễn bảo mật IT phù hợp đã tồn tại. Tuy nhiên, những khác biệt quan trọng giữa IT và ICS được đề cập sẽ ảnh hưởng đến cách thức áp dụng bảo mật cho ICS. Một kế hoạch hướng tới tương lai cần được xác định để cung cấp phương pháp để liên tục cải tiến bảo mật. Khi một hệ thống mới đang được thiết kế và cài đặt, điều cần thiết là dành thời gian để xem xét bảo mật trong suốt quá trình vòng đời, từ kiến trúc đến mua sắm, cài đặt, bảo trì và đình chỉ. Bảo mật ICS là một lĩnh vực đang phát triển nhanh chóng, yêu cầu quá trình lập kế hoạch bảo mật liên tục khám phá khả năng bảo mật ICS mới nổi cùng với các mối đe dọa mới được xác định bởi các tổ chức như ICS-CERT.

5.5.2.13 An toàn nhân sự

Các biện pháp bảo mật Personnel Security (PS) tham chiếu theo TCVN thực tế cung cấp chính sách và thủ tục nhằm giảm rủi ro về lỗi của con người, trộm cắp, gian lận hoặc việc sử dụng sai ý định tình ý hoặc vô tình đối với hệ thống thông tin.

Các biện pháp bảo mật nhân sự được thiết kế nhằm giảm khả năng và rủi ro của lỗi con người, trộm cắp, gian lận hoặc việc sử dụng sai ý định tình ý hoặc vô tình đối với tài sản thông tin. Có ba khía cạnh chính của bảo mật nhân sự:

- Chính sách tuyển dụng: Bao gồm quá trình kiểm tra tiền sử như kiểm tra lý lịch, quá trình phỏng vấn, các điều khoản và điều kiện việc làm, mô tả công việc đầy đủ và chi tiết, các điều khoản và điều kiện việc làm, và quyền và trách nhiệm pháp lý của nhân viên hoặc nhà thầu.

- Chính sách và thực tiễn tổ chức: Bao gồm các chính sách bảo mật, phân loại thông tin, chính sách vận hành và xử lý tài liệu và phương tiện truyền thông, đào tạo người dùng, chính sách sử dụng chấp nhận được cho tài sản tổ chức, xem xét hiệu suất định kỳ của nhân viên, kiểm tra tiền sử phù hợp và bất kỳ chính sách và biện pháp nào khác mô tả hành vi kỳ vọng và yêu cầu của nhân viên, nhà thầu và khách thăm. Các chính sách tổ chức cần được áp dụng nên được viết xuống và dễ dàng tiếp cận cho tất cả nhân viên thông qua một sổ tay nhân viên, được phân phát dưới dạng thông báo qua email, được đặt trong một khu vực tài nguyên tập trung hoặc được đăng trực tiếp tại khu vực trách nhiệm của một nhân viên.

- Điều khoản và Điều kiện việc làm: Loại này bao gồm trách nhiệm công việc và vị trí, thông báo cho nhân viên về các hành vi có thể chấm dứt, biện pháp kỷ luật và hình phạt, và xem xét hiệu suất định kỳ của nhân viên.

***Khuyến nghị và Hướng dẫn cụ thể cho ICS***

Các vị trí nên được phân loại với một mức đánh giá rủi ro và tiêu chí đánh giá, và những cá nhân đảm nhiệm một vị trí nên được kiểm tra dựa trên tiêu chí này cũng như ký một thỏa thuận truy cập trước khi được cấp quyền truy cập vào hệ thống thông tin. Nhân viên nên được kiểm tra đối với các vị trí quan trọng điều khiển và duy trì hệ thống điều khiển công nghiệp (ICS).

Ngoài ra, chương trình đào tạo nên được phát triển một cách cẩn thận để đảm bảo rằng mỗi nhân viên đã nhận được đào tạo liên quan và cần thiết cho công việc của mình. Hơn nữa, đảm bảo rằng nhân viên đã chứng minh được năng lực trong các chức năng công việc của mình.

5.5.2.14 Đánh giá rủi ro

Các biện pháp bảo mật thuộc Đánh giá rủi ro (RA) tham chiếu theo TCVN thực tế cung cấp chính sách và thủ tục để phát triển, phân phối và duy trì một chính sách đánh giá rủi ro được tài liệu hóa, mô tả mục đích, phạm vi, vai trò, trách nhiệm và tuân thủ cũng như các thủ tục triển khai chính sách. Hệ thống thông tin và dữ liệu liên quan được phân loại dựa trên các mục tiêu bảo mật và một loạt các mức rủi ro. Một đánh giá rủi ro được thực hiện để xác định các rủi ro và mức độ thiệt hại có thể xảy ra do truy cập, sử dụng, tiết lộ, làm gián đoạn, thay đổi hoặc phá hủy trái phép hệ thống thông tin và dữ liệu. Các biện pháp bảo mật này bao gồm cơ chế để cập nhật đánh giá rủi ro và thực hiện kiểm tra định kỳ và đánh giá lỗ hổng.

***Khuyến nghị và Hướng dẫn cụ thể cho ICS***

Tổ chức phải xem xét các hậu quả tiềm tàng sau một sự cố trên hệ thống điều khiển công nghiệp (ICS). Chính sách và thủ tục rõ ràng dẫn đến các kỹ thuật giảm thiểu được thiết kế nhằm ngăn chặn các sự cố và quản lý rủi ro để loại bỏ hoặc giảm thiểu các hậu quả. Sự suy giảm tiềm năng của cơ sở vật chất, tình hình kinh tế hoặc sự tin tưởng của các bên liên quan/quốc gia có thể xác định việc giảm thiểu.

Đối với một hệ thống điều khiển công nghiệp (ICS), một khía cạnh rất quan trọng của đánh giá rủi ro là xác định giá trị của dữ liệu đang chuyển từ mạng điều khiển đến mạng doanh nghiệp. Trong những trường hợp quyết định về giá cả được xác định từ dữ liệu này, dữ liệu có thể có giá trị rất cao. Cơ sở lý do tài chính cho việc giảm thiểu phải được xác định bằng cách so sánh chi phí giảm thiểu với hiệu quả của hậu quả. Tuy nhiên, không thể xác định một tập hợp yêu cầu bảo mật phù hợp cho tất cả các trường hợp. Một mức độ bảo mật rất cao có thể được đạt được nhưng không mong muốn trong nhiều tình huống do mất mát chức năng và các chi phí liên quan khác. Việc triển khai bảo mật cần được suy nghĩ kỹ càng là sự cân đối giữa rủi ro và chi phí. Trong một số tình huống, rủi ro có thể liên quan đến an toàn, sức khỏe hoặc môi trường thay vì chỉ là vấn đề kinh tế tạm thời.

5.5.2.15 Mua lại hệ thống và dịch vụ

Các biện pháp bảo mật thuộc Mua lại hệ thống và dịch vụ (SA) tham chiếu theo TCVN thực tế cung cấp cơ sở để phát triển chính sách và thủ tục cho việc mua sắm các nguồn lực cần thiết để bảo vệ một hệ thống thông tin một cách đủ đảm bảo. Các giao dịch mua sắm này dựa trên yêu cầu bảo mật và thông số kỹ thuật bảo mật. Là một phần của các thủ tục mua sắm, hệ thống thông tin được quản lý bằng cách sử dụng phương pháp vòng đời phát triển hệ thống mà bao gồm các yếu tố liên quan đến bảo mật thông tin. Như một phần của quá trình mua sắm, tài liệu đầy đủ phải được duy trì về hệ thống thông tin và các thành phần thành phần của nó.

Mua lại hệ thống và dịch vụ cũng đề cập đến các hệ thống được giao cho bên thứ ba và việc bao gồm các biện pháp bảo mật đủ đáp ứng từ các nhà cung cấp theo yêu cầu của tổ chức được hỗ trợ. Các nhà cung cấp cũng có trách nhiệm về quản lý cấu hình và kiểm tra bảo mật cho các hệ thống thông tin được giao cho bên thứ ba này.

***Khuyến nghị và Hướng dẫn cụ thể cho ICS***

Các yêu cầu bảo mật của một tổ chức giao việc quản lý và điều khiển một phần hoặc toàn bộ các hệ thống thông tin, mạng và môi trường máy tính để bàn nên được đề cập trong một hợp đồng được thỏa thuận giữa các bên. Các nhà cung cấp bên ngoài có tác động đến bảo mật của tổ chức phải tuân thủ các chính sách và thủ tục bảo mật tương tự để duy trì mức độ bảo mật chung của ICS. Chính sách và thủ tục bảo mật của các nhà cung cấp cấp hai và cấp ba cũng phải tuân thủ các chính sách và thủ tục bảo mật của doanh nghiệp theo trường hợp chúng ảnh hưởng đến bảo mật ICS.

5.2.5.16 Bảo vệ hệ thống và truyền thông

**5.2.5.16.1 Mã hóa**

Mã hóa là quá trình chuyển đổi dữ liệu (gọi là văn bản gốc) thành một dạng (gọi là văn bản mã hóa) che giấu ý nghĩa ban đầu của dữ liệu để ngăn người khác biết hoặc sử dụng nó. Nếu quá trình chuyển đổi có thể đảo ngược, quá trình đảo ngược tương ứng được gọi là giải mã, là quá trình khôi phục dữ liệu đã được mã hóa về trạng thái ban đầu.

***Khuyến nghị và hướng dẫn cụ thể cho ICS***

Trước khi triển khai mã hóa, trước tiên hãy xác định xem mã hóa có phải là giải pháp phù hợp cho ứng dụng ICS cụ thể hay không, vì xác thực và tính toàn vẹn thường là những vấn đề bảo mật chính đối với các ứng dụng ICS. Cần xem xét cũng các giải pháp mật mã khác như băm mật mã.

Việc sử dụng mã hóa trong một môi trường ICS có thể gây ra độ trễ trong giao tiếp do thời gian và tài nguyên tính toán bổ sung cần thiết để mã hóa, giải mã và xác thực từng tin nhắn. Đối với ICS, bất kỳ độ trễ nào do việc sử dụng mã hóa hoặc bất kỳ kỹ thuật bảo mật nào khác cũng không được phép làm giảm hiệu suất hoạt động của thiết bị hoặc hệ thống cuối cùng. Trước khi triển khai mã hóa trong một môi trường ICS, các giải pháp nên trải qua kiểm tra hiệu suất kỹ lưỡng. Mã hóa tại tầng OSI lớp 2 nên được xem xét, thay vì tại lớp 3 để giảm độ trễ của mã hóa.

Ngoài ra, tin nhắn đã được mã hóa thường lớn hơn so với tin nhắn chưa được mã hóa do một hoặc nhiều yếu tố sau:

* Kiểm tra bổ sung để giảm lỗi.
* Giao thức để kiểm soát mật mã.
* Đệm (cho các mã khối).
* Quy trình xác thực.
* Các quy trình mật mã yêu cầu khác.

Mật mã cũng đưa ra các vấn đề quản lý khóa. Các chính sách bảo mật đáng tin cậy yêu cầu thay đổi khóa định kỳ. Quá trình này trở nên khó khăn hơn khi quy mô địa lý của ICS tăng lên, với các hệ thống SCADA quy mô lớn là ví dụ cực kỳ nghiêm trọng. Vì việc thay đổi khóa bằng cách thực hiện viếng thăm địa điểm có thể tốn kém và chậm chạp, việc có thể thay đổi khóa từ xa là hữu ích.

Nếu mã hóa được chọn, biện pháp bảo vệ hiệu quả nhất là sử dụng một hệ thống mật mã hoàn chỉnh được phê duyệt bởi Chương trình Chứng nhận Mô-đun Mật mã tham chiếu theo TCVN thực tế. Trong chương trình này, các tiêu chuẩn được duy trì để đảm bảo rằng các hệ thống mật mã đã được nghiên cứu kỹ lưỡng về các điểm yếu bởi một loạt các chuyên gia, thay vì được phát triển bởi một số kỹ sư trong một tổ chức duy nhất. Tối thiểu, việc chứng nhận làm cho việc sử dụng mật mã trở nên có thể:

- Một phương pháp (như chế độ bộ đếm) sẽ được sử dụng để đảm bảo rằng cùng một thông điệp không tạo ra cùng một giá trị mỗi lần.

- Các tin nhắn ICS được bảo vệ chống lại việc chơi lại và giả mạo.

- Quản lý khóa an toàn trong suốt vòng đời của khóa.

- Hệ thống đang sử dụng một bộ tạo số ngẫu nhiên hiệu quả.

- Toàn bộ hệ thống đã được triển khai một cách an toàn.

Tuy nhiên, công nghệ chỉ có hiệu quả nếu nó là một phần không thể thiếu của một chính sách bảo mật thông tin được áp dụng hiệu quả. Mặc dù nó được định hướng cho một hệ thống SCADA khí đốt tự nhiên, nhưng nhiều khuyến nghị về chính sách của nó có thể áp dụng cho bất kỳ ICS nào.

Đối với ICS, mã hóa có thể triển khai như một phần của một chính sách bảo mật toàn diện và được tuân thủ. Tổ chức nên chọn bảo vệ mật mã dựa trên một đánh giá rủi ro và giá trị xác định của thông tin được bảo vệ và các ràng buộc hoạt động của ICS. Cụ thể, một khóa mật mã nên đủ dài để đoán đúng nó hoặc xác định nó qua phân tích mất nhiều nỗ lực, thời gian và chi phí hơn giá trị của tài sản được bảo vệ.

Phần cứng mã hóa cần được bảo vệ khỏi làm hỏng vật lý và kết nối điện tử không kiểm soát. Giả sử mã hóa là giải pháp phù hợp, tổ chức nên chọn bảo vệ mật mã với quản lý khóa từ xa nếu các đơn vị đang được bảo vệ là quá nhiều hoặc phân tán địa lý đến mức việc thay đổi khóa là khó khăn hoặc tốn kém.

Sử dụng các cổng văn bản gốc và văn bản mã hóa riêng biệt trừ khi mạng yêu cầu hạn chế để thông qua cả văn bản gốc và văn bản mã hóa qua mỗi cổng.

**5.2.5.16.2 Mạng riêng ảo (VPN)**

Một phương pháp để mã hóa dữ liệu truyền thông là thông qua VPN (Mạng riêng ảo), một mạng riêng hoạt động như một lớp phủ trên cơ sở hạ tầng công cộng, để mạng riêng có thể hoạt động trên mạng công cộng. Các công nghệ VPN phổ biến nhất được triển khai hiện nay bao gồm:

**- Bảo mật giao thức Internet (IPsec):** IPsec là một tập hợp các tiêu chuẩn được định nghĩa bởi IETF (Tổ chức Tiêu chuẩn và Công nghệ Internet) để điều chỉnh việc truyền thông an toàn của dữ liệu qua các mạng công cộng ở tầng IP. IPsec được bao gồm trong nhiều hệ điều hành hiện tại. Mục đích của các tiêu chuẩn này là đảm bảo tính tương thích giữa các nền tảng của các nhà cung cấp khác nhau; tuy nhiên, việc xác định tính tương thích của các triển khai đa nhà cung cấp phụ thuộc vào việc thử nghiệm triển khai cụ thể do tổ chức cuối cùng sử dụng thực hiện. IPsec hỗ trợ hai chế độ mã hóa: chế độ vận chuyển (transport) và chế độ đường hầm (tunnel). Chế độ vận chuyển chỉ mã hóa phần dữ liệu (payload) của từng gói tin, nhưng để lại phần tiêu đề không thay đổi. Chế độ đường hầm an toàn hơn bổ sung một tiêu đề mới cho từng gói tin và mã hóa cả tiêu đề gốc và phần dữ liệu. Ở phía nhận, một thiết bị tương thích IPsec giải mã từng gói tin. Giao thức này đã được liên tục cải tiến để đáp ứng các yêu cầu cụ thể, như mở rộng giao thức để xử lý xác thực người dùng cá nhân và điều qua thiết bị NAT. Các phần mở rộng này thường do từng nhà cung cấp cụ thể và có thể dẫn đến vấn đề tương thích chủ yếu trong môi trường từ máy chủ đến cổng an toàn.

**- Lớp cổng bảo mật (SSL):** SSL cung cấp một kênh an toàn giữa hai máy tính mã hóa nội dung của mỗi gói tin. IETF đã thực hiện một số chỉnh sửa nhỏ vào phiên bản 3 của SSL và tạo ra một giao thức mới được gọi là Transport Layer Security (TLS). Các thuật ngữ "SSL" và "TLS" thường được sử dụng thay thế cho nhau, và tài liệu này sử dụng thuật ngữ SSL một cách chung chung. SSL thường được nhận biết nhiều nhất để bảo mật lưu lượng HTTP; việc triển khai giao thức này được biết đến là HTTP Secure (HTTPS). Tuy nhiên, SSL không chỉ giới hạn trong lưu lượng HTTP; nó có thể được sử dụng để bảo mật nhiều chương trình ứng dụng khác nhau. Các sản phẩm VPN dựa trên SSL đã được chấp nhận vì thị trường các sản phẩm VPN "không cần cài đặt" (clientless). Các sản phẩm này sử dụng trình duyệt web tiêu chuẩn làm khách hàng, có sẵn hỗ trợ SSL tích hợp sẵn. Thuật ngữ "không cần cài đặt" có nghĩa là không cần cài đặt hoặc cấu hình phần mềm VPN bên thứ ba trên hệ thống người dùng

**- Vỏ bảo mật (SSH):** SSH là một giao diện lệnh và giao thức cho phép truy cập an toàn vào một máy tính từ xa. Nó được sử dụng rộng rãi bởi các quản trị viên mạng để từ xa điều khiển các máy chủ Web và các loại máy chủ khác. Phiên bản mới nhất, SSH2, là một tập hợp các tiêu chuẩn đề xuất từ IETF. Thông thường, SSH được triển khai như một phương thức thay thế an toàn cho ứng dụng telnet. SSH được bao gồm trong hầu hết các bản phân phối UNIX và thường được thêm vào các nền tảng khác thông qua gói phần mềm bên thứ ba.

***Các khuyến nghị và hướng dẫn cụ thể cho ICS***

VPN thường được sử dụng trong môi trường ICS để cung cấp truy cập an toàn từ mạng không đáng tin cậy vào mạng điều khiển ICS. Mạng không đáng tin cậy có thể là Internet hoặc LAN của công ty. Nếu được cấu hình đúng, VPN có thể hạn chế mạnh việc truy cập vào và từ các máy tính chủ và bộ điều khiển hệ thống điều khiển, do đó cải thiện bảo mật. Ngoài ra, nó cũng có thể cải thiện khả năng phản hồi của mạng điều khiển bằng cách loại bỏ lưu lượng không cần thiết không được ủy quyền từ mạng trung gian.

Các triển khai khác có thể bao gồm việc sử dụng cổng an toàn dựa trên máy chủ hoặc mini-standalone, được đặt giữa hoặc chạy trên từng thiết bị điều khiển riêng lẻ. Kỹ thuật triển khai VPN trên từng thiết bị riêng lẻ này có thể tạo ra khối lượng công việc quản lý đáng kể.

Các thiết bị VPN được sử dụng để bảo vệ hệ thống điều khiển nên được kiểm tra kỹ để xác minh rằng công nghệ VPN tương thích với ứng dụng và triển khai của các thiết bị VPN không ảnh hưởng không chấp nhận đến các đặc điểm lưu lượng mạng.

5.2.5.17 Tính toàn vẹn của hệ thống

Bảo đảm tính toàn vẹn hệ thống và thông tin đảm bảo rằng dữ liệu nhạy cảm không bị sửa đổi hoặc xóa một cách trái phép và không bị phát hiện. Các biện pháp kiểm soát an toàn tham chiếu theo TCVN thực tế cung cấp chính sách và quy trình để xác định, báo cáo và khắc phục nhược điểm hệ thống thông tin. Các biện pháp kiểm soát tồn tại để phát hiện mã độc, bảo vệ chống thư rác và phần mềm gián điệp, và phát hiện xâm nhập, mặc dù chúng có thể không phù hợp cho tất cả các ứng dụng ICS. Ngoài ra, cung cấp các biện pháp kiểm soát để nhận cảnh báo và lời khuyên về an toàn, và xác minh chức năng an toàn trên hệ thống thông tin. Ngoài ra, trong nhóm này còn có các biện pháp kiểm soát để phát hiện và bảo vệ khỏi các thay đổi trái phép vào phần mềm và dữ liệu, cung cấp hạn chế cho đầu vào và đầu ra dữ liệu, và kiểm tra tính chính xác, đầy đủ và hợp lệ của dữ liệu cũng như xử lý các điều kiện lỗi, mặc dù chúng có thể không phù hợp cho tất cả các ứng dụng ICS**.**

***Khuyến nghị và hướng dẫn cụ thể cho ICS***

Có các biện pháp kiểm soát để phát hiện mã độc, bảo vệ chống thư rác và phần mềm gián điệp, và phát hiện xâm nhập, mặc dù chúng có thể không phù hợp cho tất cả các ứng dụng ICS.

**5.2.5.17.1 Phát hiện virus và mã độc**

Các sản phẩm phát hiện mã độc và phần mềm độc hại đánh giá các tệp trên các thiết bị lưu trữ của máy tính dựa trên một danh sách các tệp chữ ký phần mềm đã biết. Nếu một trong các tệp trên máy tính khớp với hồ sơ của một loại virus đã biết, virus sẽ được loại bỏ thông qua quá trình tiệt trùng (ví dụ: cách ly, xóa) để ngăn không cho nó lây nhiễm các tệp địa phương khác hoặc truyền qua mạng để lây nhiễm các tệp khác. Phần mềm antivirus có thể triển khai trên các máy trạm, máy chủ, tường lửa và thiết bị di động.

***Khuyến nghị và hướng dẫn cụ thể cho ICS***

Công cụ antivirus chỉ hoạt động hiệu quả khi được cài đặt, cấu hình, hoạt động liên tục và bảo trì đúng cách theo trạng thái của các phương pháp tấn công và gói tin đã biết. Trong khi công cụ antivirus là thực hành an toàn phổ biến trong các hệ thống máy tính IT, việc sử dụng chúng với ICS có thể đòi hỏi áp dụng các thực hành đặc biệt bao gồm kiểm tra tính tương thích, vấn đề quản lý thay đổi và các chỉ số tác động hiệu suất. Những thực hành đặc biệt này nên được sử dụng mỗi khi cài đặt các chữ ký mới hoặc phiên bản mới của phần mềm antivirus.

Các nhà cung cấp ICS hàng đầu khuyến nghị và thậm chí hỗ trợ việc sử dụng các công cụ antivirus cụ thể. Trong một số trường hợp, nhà cung cấp hệ thống điều khiển có thể đã thực hiện kiểm tra đảo ngược trên toàn bộ dòng sản phẩm của họ cho các phiên bản được hỗ trợ của một công cụ antivirus cụ thể và cung cấp tài liệu cài đặt và cấu hình liên quan. Cũng có nỗ lực phát triển một tập hợp các nguyên tắc và thủ tục kiểm tra chung tập trung vào tác động hiệu suất ICS để điền vào những khoảng trống nơi không có hướng dẫn từ ICS và nhà cung cấp antivirus

Nói chung:

- Hệ thống Windows, Unix, Linux, vv. được sử dụng như các bảng điều khiển, máy trạm kỹ thuật, bộ lưu trữ dữ liệu, HMIs và máy chủ SCADA đa mục đích có thể được bảo mật giống như các thiết bị IT thương mại: cài đặt phần mềm antivirus và quản lý bản vá tự động với các bản vá được phân phối thông qua máy chủ antivirus và máy chủ quản lý bản vá được đặt trong mạng điều khiển quá trình và tự động cập nhật từ mạng IT.

- Tuân thủ các khuyến nghị của nhà cung cấp trên tất cả các máy chủ và máy tính khác (DCS, PLC, các thiết bị đo lường) có mã nguồn phụ thuộc vào thời gian, được sửa đổi hoặc mở rộng hệ điều hành hoặc bất kỳ sự thay đổi nào khác làm cho nó khác với bất kỳ máy tính tiêu chuẩn nào có thể mua ở cửa hàng văn phòng hoặc cửa hàng máy tính. Kỳ vọng nhà cung cấp phát hành bảo trì định kỳ bao gồm các bản vá bảo mật.

**5.2.5.17.2 Phát hiện và ngăn chặn xâm nhập**

Hệ thống phát hiện xâm nhập (IDS) giám sát các sự kiện trên một mạng, chẳng hạn như mô hình lưu lượng, hoặc trên một hệ thống, chẳng hạn như các lỗi đăng nhập hoặc truy cập tệp, nhằm xác định kẻ xâm nhập xâm nhập hoặc cố gắng xâm nhập vào hệ thống IDS đảm bảo rằng các hoạt động bất thường như các cổng mở mới, mô hình lưu lượng không bình thường hoặc thay đổi các tệp hệ điều hành quan trọng được đưa ra cho nhân viên bảo mật thích hợp.

Hai loại IDS phổ biến nhất là:

- IDS dựa trên mạng: Hệ thống này giám sát lưu lượng mạng và tạo ra cảnh báo khi nhận dạng lưu lượng được coi là cuộc tấn công.

- IDS dựa trên máy chủ: Phần mềm này giám sát một hoặc nhiều loại đặc điểm của một hệ thống, chẳng hạn như các mục nhập tệp nhật ký ứng dụng, thay đổi cấu hình hệ thống và truy cập vào dữ liệu nhạy cảm trên một hệ thống và phản ứng bằng cảnh báo hoặc biện pháp phòng ngừa khi người dùng cố gắng vi phạm bảo mật.

***Khuyến nghị và hướng dẫn cụ thể cho ICS***

Triển khai hiệu quả IDS thường bao gồm cả IDS dựa trên máy chủ và IDS dựa trên mạng. Trong môi trường ICS hiện tại, IDS dựa trên mạng thường được triển khai giữa mạng điều khiển và mạng doanh nghiệp kết hợp với tường lửa; IDS dựa trên máy chủ thường được triển khai trên các máy tính sử dụng hệ điều hành đa dụng hoặc ứng dụng như HMIs, máy chủ SCADA và máy trạm kỹ thuật. Đúng cấu hình, IDS có thể cải thiện đáng kể khả năng của nhóm quản lý bảo mật trong việc phát hiện các cuộc tấn công xâm nhập hoặc rời khỏi hệ thống, từ đó nâng cao tính bảo mật. Chúng cũng có thể cải thiện hiệu suất mạng điều khiển bằng cách phát hiện lưu lượng không cần thiết trên mạng. Tuy nhiên, ngay cả khi IDS được triển khai, nhân viên an toàn chủ yếu có thể nhận ra các cuộc tấn công cá nhân, thay vì các mẫu tấn công tổ chức theo thời gian. Giám sát an toàn mạng và hiểu rõ trạng thái bình thường của mạng ICS có thể giúp phân biệt các cuộc tấn công so với các điều kiện tạm thời, và cung cấp thông tin về các sự kiện nằm ngoài trạng thái bình thường.

Các sản phẩm IDS và IPS hiện tại hiệu quả trong việc phát hiện và ngăn chặn các cuộc tấn công trên Internet được biết đến, nhưng cho đến gần đây, chúng chưa đề cập đến các cuộc tấn công vào giao thức ICS. Các nhà cung cấp IDS và IPS đang bắt đầu phát triển và tích hợp các chữ ký tấn công cho các giao thức ICS khác nhau như Modbus, DNP3 và ICCP

**5.2.5.17.3 Quản lý bản vá**

Các bản vá là các đoạn mã bổ sung đã được phát triển để khắc phục các vấn đề hoặc lỗ hổng cụ thể trong phần mềm hiện có. Các lỗ hổng là những sai sót có thể bị khai thác, cho phép truy cập trái phép vào hệ thống IT hoặc cho phép người dùng có quyền truy cập cao hơn so với quyền được phép.

Một phương pháp quản lý và sử dụng bản vá phần mềm có hệ thống có thể giúp tổ chức cải thiện tổng thể bảo mật của hệ thống IT của họ một cách hiệu quả về mặt chi phí. Các tổ chức quản lý và sử dụng bản vá phần mềm một cách tích cực có thể giảm khả năng các lỗ hổng trong hệ thống IT của họ bị khai thác; ngoài ra, họ còn tiết kiệm thời gian và tiền bạc có thể được chi trả để đáp ứng các sự cố liên quan đến lỗ hổng.

Tài liệu hướng dẫn tham chiếu theo TCVN thực tế cung cấp hướng dẫn cho các nhà quản lý an toàn tổ chức có trách nhiệm thiết kế và triển khai các chương trình quản lý bản vá bảo mật và lỗ hổng, và kiểm tra hiệu quả của các chương trình này trong việc giảm thiểu các lỗ hổng. Hướng dẫn này cũng hữu ích cho quản trị viên hệ thống và nhân viên vận hành có trách nhiệm áp dụng và kiểm tra bản vá, và triển khai các giải pháp cho các vấn đề lỗ hổng.

***Khuyến nghị và hướng dẫn cụ thể cho ICS***

Áp dụng bản vá cho các thành phần hệ điều hành tạo ra tình huống khác trong môi trường ICS, nơi cần thực hiện các biện pháp cẩn trọng đáng kể. Bản vá nên được kiểm tra đầy đủ (ví dụ: ngoại tuyến trên một ICS tương tự) để xác định tính chấp nhận được của các tác động phụ. Kiểm thử hồi quy được khuyến nghị. Thường xảy ra việc bản vá có tác động tiêu cực đối với phần mềm khác. Một bản vá có thể loại bỏ một lỗ hổng, nhưng cũng có thể đem lại nguy cơ lớn hơn từ phối cảnh sản xuất hoặc an toàn. Việc vá lỗ hổng cũng có thể thay đổi cách thức hoạt động của hệ điều hành hoặc ứng dụng với các ứng dụng điều khiển, gây mất một số chức năng của ứng dụng điều khiển. Vấn đề khác là nhiều hệ thống ICS sử dụng các phiên bản cũ hơn của hệ điều hành không được hỗ trợ bởi nhà cung cấp. Do đó, các bản vá có sẵn có thể không áp dụng. Tổ chức nên triển khai quy trình quản lý bản vá ICS hệ thống có hệ thống, có trách nhiệm và được tài liệu hóa để quản lý rủi ro với lỗ hổng.

Sau khi quyết định triển khai một bản vá, có các công cụ khác giúp tự động hóa quy trình này từ một máy chủ tập trung và xác nhận rằng bản vá đã được triển khai đúng. Cân nhắc tách quy trình tự động cho việc quản lý bản vá ICS khỏi quy trình tự động cho các ứng dụng không phải ICS. Việc vá lỗ hổng nên được lên kế hoạch để diễn ra trong thời gian gián đoạn ICS đã được lên lịch trước

5.2.5.18 Quản lý chương trình

Các biện pháp bảo mật nằm trong Phần quản lý chương trình (PM) tham chiếu theo TCVN thực tế tập trung vào các yêu cầu bảo mật thông tin phạm vi toàn tổ chức, độc lập với bất kỳ hệ thống thông tin cụ thể nào và là cần thiết để quản lý các chương trình bảo mật thông tin.

Các tổ chức ghi lại các biện pháp quản lý chương trình trong kế hoạch chương trình bảo mật thông tin. Kế hoạch chương trình bảo mật thông tin phạm vi toàn tổ chức bổ sung cho các kế hoạch bảo mật cá nhân được phát triển cho mỗi hệ thống thông tin tổ chức. Ngoài việc ghi lại các biện pháp quản lý chương trình bảo mật thông tin, kế hoạch chương trình bảo mật cung cấp một phương tiện cho tổ chức, trong một kho chứa trung tâm, để ghi lại tất cả các biện pháp bảo mật đã được chỉ định là các biện pháp chung (tức là các biện pháp bảo mật được kế thừa bởi các hệ thống thông tin tổ chức).

Bảo vệ quyền riêng tư của thông tin cá nhân cụ thể (PII) được thu thập, sử dụng, duy trì, chia sẻ và xử lý bởi các chương trình và hệ thống thông tin là rất quan trọng trong bối cảnh sự tiến bộ của công nghệ thông tin và ứng dụng của công nghệ đó. Quyền riêng tư hiệu quả cho cá nhân phụ thuộc vào các biện pháp bảo vệ được áp dụng trong các hệ thống thông tin tổ chức đang xử lý, lưu trữ và truyền tải PII. Tổ chức không thể có được quyền riêng tư hiệu quả mà không có một nền tảng bảo mật thông tin. Tuy nhiên, quyền riêng tư không chỉ liên quan đến bảo mật mà còn bao gồm các nguyên tắc về sự minh bạch, thông báo và sự lựa chọn.

Các biện pháp kiểm soát quyền riêng tư tập trung vào quyền riêng tư thông tin như một giá trị riêng biệt, nhưng rất liên quan chặt chẽ đến bảo mật thông tin.

5.2.5.19 Kiểm soát quyền riêng tư

Các biện pháp kiểm soát quyền riêng tư là các biện pháp hành chính, kỹ thuật và vật lý được áp dụng trong tổ chức để bảo vệ và đảm bảo xử lý đúng đắn của (PII). Có tám nhóm biện pháp kiểm soát quyền riêng tư tham chiếu theo TCVN thực tế. Các nhóm biện pháp kiểm soát quyền riêng tư có thể triển khai ở cấp tổ chức, bộ phận, cơ quan, văn phòng, chương trình hoặc cấp độ hệ thống thông tin.

Các biện pháp kiểm soát quyền riêng tư được thiết kế chủ yếu để sử dụng bởi Người Đại diện Cấp cao về Quyền riêng tư (SAOP)/Quản lý Quyền riêng tư chính (CPO) của một tổ chức khi làm việc với các quản lý chương trình, nhà phát triển hệ thống thông tin và nhân viên an toàn thông tin để xác định cách tốt nhất để tích hợp các biện pháp bảo vệ và thực tiễn quyền riêng tư hiệu quả trong các chương trình và/hoặc hệ thống đó. Các biện pháp kiểm soát này giúp tạo điều kiện cho tổ chức tuân thủ các yêu cầu về quyền riêng tư ảnh hưởng đến các chương trình và/hoặc hệ thống đó thu thập, sử dụng, duy trì, chia sẻ hoặc xử lý PII. Điều này thúc đẩy sự hợp tác gắn kết giữa các quan chức về quyền riêng tư và an toàn trong chính phủ liên bang để giúp đạt được các mục tiêu của các nhà lãnh đạo cấp cao trong việc thi hành các yêu cầu trong các luật quyền riêng tư liên bang, chính sách, quy định, chỉ thị, tiêu chuẩn và hướng dẫn.

Có 8 biện pháp kiểm soát quyền riêng tư bao gồm:

* Quyền hành và Mục đích (AP).
* Trách nhiệm, Kiểm toán và Quản lý Rủi ro(AR).
* Chất lượng và Chính xác Dữ liệu (DI).
* Giảm thiểu và Duy trì Dữ liệu(DM).
* Sự tham gia của Cá nhân và Cải thiện (IP).
* Bảo mật (SE).
* Sự minh bạch(TR).
* Hạn chế sử dụng (UL).

**Thư mục tài liệu tham khảo**

“NIST Special Publication (SP) 800-82r2” của Viện Tiêu chuẩn và Công nghệ Quốc gia Mỹ.