BỘ THÔNG TIN VÀ TRUYỀN THÔNG

**CỤC AN TOÀN THÔNG TIN**

**THUYẾT MINH DỰ THẢO TIÊU CHUẨN**

**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

[1. Mở đầu 5](#_Toc153976264)

[1.1. Tên dự thảo tiêu chuẩn 5](#_Toc153976265)

[1.2. Mục tiêu xây dựng 5](#_Toc153976266)

[2. Tình hình tiêu chuẩn hóa 6](#_Toc153976267)

[2.1. Thế giới 6](#_Toc153976268)

[2.2. Trong nước 6](#_Toc153976269)

[3. Phương pháp xây dựng tiêu chuẩn 7](#_Toc153976270)

[4. Giới thiệu tiêu chuẩn tham chiếu (tiêu chuẩn gốc) 7](#_Toc153976271)

[5. Giới thiệu dự thảo tiêu chuẩn 11](#_Toc153976272)

[6. Kết luận 13](#_Toc153976273)

[7. Tài liệu tham khảo 15](#_Toc153976274)

1. Mở đầu
   1. Tên dự thảo tiêu chuẩn

“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”

* 1. Mục tiêu xây dựng

Luật An toàn thông tin đã đưa ra khái niệm về hệ thống thông tin quan trọng và giao Bộ Thông tin và Truyền thông phối hợp với các bộ ngành xây dựng Danh mục hệ thống thông tin quan trọng trình Thủ tướng Chính phủ ban hành. Cụ thể hóa các nhiệm vụ được giao, Bộ Thông tin và Truyền thông đã trình Thủ tướng Chính phủ ban hành các văn bản mang tính quy phạm pháp luật như:

- Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Quyết định số 632/QĐ-TTg ngày 10/5/2017 về Ban hành danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia.

Ngoài ra, Bộ Thông tin và Truyền thông đã ban hành nhiều Thông tư, hướng dẫn như:

Thông tư số 12/2022/TT-BTTTT ngày 12/08/2022 quy định chi tiết và hướng dẫn một số điều của nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ.

- Công văn số 713/CATTT-TĐQLGS về việc hướng dẫn xác định và thực thi bảo vệ hệ thống thông tin theo cấp độ.

Đặc biệt, Bộ Thông tin và Truyền thông đã xây dựng Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ về việc bảo đảm an toàn hệ thống thông tin, trong đó có các nội dung liên quan đến hệ thống thông tin quan trọng.

Để có bức tranh tổng thể nhất và đưa ra được các tiêu chí cụ thể cần thực hiện các bước nghiên cứu như:

- Nghiên cứu tình hình tiêu chuẩn hóa quốc tế và trong nước đối với các cơ sở hạ tầng quan trọng áp dụng cho hệ thống điều khiển công nghiệp ICS

- Nghiên cứu, đánh giá thực trạng việc bảo đảm an toàn hệ thống thông tin các cơ sở hạ tầng quan trọng áp dụng cho hệ thống điều khiển công nghiệp ICS tại Việt Nam.

- Nghiên cứu, rà soát việc quản lý các hạ tầng quan trọng thuộc lĩnh vực các hệ thống điều khiển công nghiệp ICS cần được bảo đảm an toàn thông tin tại Việt Nam

- Xây dựng tiêu chuẩn quốc gia về bảo đảm an toàn hệ thống thông tin các cơ sở hạ tầng quan trọng thuộc lĩnh vực các hệ thống điều khiển công nghiệp ICS dựa trên tiêu chuẩn NIST SP 800-82r2 và tiêu chuẩn TCVN 11930:2017.

Xây dựng tiêu chuẩn quốc gia về bảo đảm an toàn hệ thống thông tin các cơ sở hạ tầng quan trọng áp dụng cho hệ thống điều khiển công nghiệp ICS tại Việt Nam sẽ làm cơ sở để chủ quản của các hệ thống thông tin tổ chức triển khai các phương án bảo đảm an toàn thông tin cho các hệ thống cơ sở hạ tầng quan trọng một cách triệt để.

1. Tình hình tiêu chuẩn hóa
   1. Thế giới

Xác định được tầm quan trọng của các cơ sở hạ tầng, đặc biệt là việc bảo đảm an toàn, an ninh mạng cho các cơ sở hạ tầng quan trọng thuộc các hệ thống điều khiển công nghiệp ICS, các quốc gia hàng đầu trên thế giới đều ban hành các tiêu chuẩn quốc gia như:

Hoa Kỳ: Đã phát triển một chương trình bảo vệ hệ thống thông tin cơ sở hạ tầng quan trọng (CIIP) nhằm tăng cường khả năng ứng phó với các mối đe dọa bảo mật mạng

Liên minh Châu Âu: Đưa ra các hướng dẫn về bảo vệ cơ sở hạ tầng quan trọng và yêu cầu các quốc gia thành viên triển khai các chính sách an ninh mạng. Các hướng dẫn này bao gồm các tiêu chuẩn an ninh mạng, chính sách bảo mật và đào tạo nhân viên.

Canada: Đưa ra các hướng dẫn và tiêu chuẩn về an ninh mạng cho các cơ sở hạ tầng quan trọng.

Nhật Bản: Ban hành nhiều tiêu chuẩn khác nhau về yêu cầu áp dụng đối với các cơ sở hạ tầng quan trọng của Nhật Bản và đảm bảo các yêu cầu về khả năng đối phó với các mối đe dọa về an toàn, an ninh mạng.

* 1. Trong nước

Nhận thức được tầm quan trọng và ảnh hưởng nghiêm trọng đến quốc phòng, an ninh, Luật An toàn thông tin mạng đã đưa ra các quy định về bảo vệ hệ thống thông tin. Trong đó, phân loại ra thành 5 cấp độ an toàn hệ thống thông tin từ cấp độ 1 đến cấp độ 5. Các hệ thống thông tin cấp độ 5 là cần mức độ bảo vệ cao nhất và là hệ thống thông tin quan trọng quốc gia, bên cạnh đó Bộ Thông tin và Truyền thông đã trình Thủ tướng Chính phủ ban hành các văn bản quy định, điều chỉnh lĩnh vực này như:

- Quyết định của Thủ tướng số 632/QĐ-TTg ngày 10/5/2017 về Ban hành danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia.

- Nghị định của Chính phủ số 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ và Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ đã trình bày hướng dẫn chung về cấp độ an toàn hệ thống thông tin cho các hệ thống thông tin, cả hệ thống ICT và ICS, trong đó cấp độ 5 là hệ thống quan trọng quốc gia.

Tuy nhiên, tại Việt Nam chưa có tiêu chuẩn riêng để hướng dẫn áp dụng về bảo đảm an toàn hệ thống thông tin cho các hệ thống thông tin thuộc các lĩnh vực cơ sở hạ tầng quan trọng, đặc biệt là cho các hệ thống điều khiển công nghiệp ICS. Vì vậy cần xây dựng Tiêu chuẩn quốc gia về bảo đảm an toàn hệ thống thông tin cho các hệ thống điều khiển công nghiệp ICS. Vì các hệ thống điều khiển công nghiệp ICS có nhiều điểm khác và đặc thù hơn so với các hệ thống thông tin thuần túy.

1. Phương pháp xây dựng tiêu chuẩn

Qua tham khảo các tiêu chuẩn đối với bảo đảm an toàn các cơ sở hạ tầng quan trọng, NIST SP 800-82r2 của NIST, Hướng dẫn bảo mật hệ thống điều khiển công nghiệp (ICS), cung cấp hướng dẫn về cách bảo mật Hệ thống điều khiển công nghiệp (ICS), bao gồm hệ thống Kiểm soát 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 khả trình (PLC), đồng thời giải quyết các yêu cầu về hiệu suất, độ tin cậy và an toàn độc đáo của chúng. SP 800-82 cung cấp cái nhìn tổng quan về ICS và cấu trúc liên kết hệ thống điển hình, xác định các mối đe dọa và lỗ hổng điển hình đối với các hệ thống này, đồng thời cung cấp các biện pháp đối phó bảo mật được khuyến nghị để giảm thiểu rủi ro liên quan.

Trên cơ sở đó, để xây dựng tiêu chuẩn quốc gia về bảo đảm an toàn các cơ sở hạ tầng quan trọng và áp dụng tại Việt Nam, nhóm nghiên cứu lựa chọn “NIST Special Publication (SP) 800-82, Guide to Industrial Control Systems (ICS) Security” là tài liệu tham chiếu để xây dựng qua hình thức chấp nhận nguyên vẹn, chỉnh sửa một số nội dung cho phù hợp với Việt Nam.

1. Giới thiệu tiêu chuẩn tham chiếu (tiêu chuẩn gốc)

Khung nội dung chính của tiêu chuẩn này như sau:

|  |
| --- |
| 1. Introduction  1.1. Purpose and Scope  1.2. Audience  1.3. Document Structure  2. Overview of Industrial Control Systems  2.1. Evolution of Industrial Control Systems  2.2. ICS Industrial Sectors and Their Interdependencies  2.2.1. Manufacturing Industries  2.2.2. Distribution Industries  2.2.3. Differences between Manufacturing and Distribution ICS  2.2.4. ICS and Critical Infrastructure Interdependencies  2.3. Package conformance claim  2.3.1. ICS System Design Considerations  2.3.2. SCADA Systems  2.3.3. Distributed Control Systems  2.3.4. Programmable Logic Controller Based Topologies  2.4. Comparing ICS and IT Systems Security  2.5. Other Types of Control Systems  3. ICS Risk Management and Assessment  3.1. Risk Management  3.2. Introduction to the Risk Management Process  3.3. Special Considerations for Doing an ICS Risk Assessment  3.3.1. Safety within an ICS Information Security Risk Assessment  3.3.2. Potential Physical Impacts of an ICS Incident  3.3.3. Impact of Physical Disruption of an ICS Process  3.3.4. Incorporating Non-digital Aspects of ICS into Impact Evaluations  3.3.5. Incorporating the Impact of Safety Systems  3.3.6. Considering the Propagation of Impact to Connected Systems  4. ICS Security Program Development and Deployment  4.1. Business Case for Security  4.1.1. Benefits  4.1.2. Potential Consequences  4.1.3. Resources for Building Business Case  4.1.4. Presenting the Business Case to Leadership  4.2. Build and Train a Cross-Functional Team  4.3. Define Charter and Scope  4.4. Define ICS-specific Security Policies and Procedures  4.5. Implement an ICS Security Risk Management Framework  4.5.1. Categorize ICS Systems and Networks Assets  4.5.2. Select ICS Security Controls  4.5.3. Perform Risk Assessment  4.5.4. Implement the Security Controls  5. ICS Security Architecture  5.1. Network Segmentation and Segregation  5.2. Boundary Protection  5.3. Firewalls  5.4. Logically Separated Control Network  5.5. Network Segregation  5.5.1. Dual-Homed Computer/Dual Network Interface Cards (NIC)  5.5.2. Firewall between Corporate Network and Control Network  5.5.3. Firewall and Router between Corporate Network and Control Network  5.5.4. Firewall with DMZ between Corporate Network and Control Network  5.5.5. Paired Firewalls between Corporate Network and Control Network  5.5.6. Network Segregation Summary  5.6. Recommended Defense-in-Depth Architecture  5.7. General Firewall Policies for ICS  5.8. Recommended Firewall Rules for Specific Services  5.8.1 Domain Name System (DNS)  5.8.2 Hypertext Transfer Protocol (HTTP)  5.8.3 FTP and Trivial File Transfer Protocol (TFTP)  5.8.4 Telnet  5.8.5 Dynamic Host Configuration Protocol (DHCP)  5.8.6 Secure Shell (SSH)  5.8.7 Simple Object Access Protocol (SOAP)  5.8.8 Simple Mail Transfer Protocol (SMTP)  5.8.9 Simple Network Management Protocol (SNMP)  5.8.10 Distributed Component Object Model (DCOM)  5.8.11 SCADA and Industrial Protocols  5.9 Network Address Translation (NAT)  5.10 Specific ICS Firewall Issues  5.10.1 Data Historians  5.10.2 Remote Support Access  5.10.3 Multicast Traffic  5.11 Unidirectional Gateways  5.12 Single Points of Failure  5.13 Redundancy and Fault Tolerance  5.14 Preventing Man-in-the-Middle Attacks  5.15 Authentication and Authorization  5.15.1 ICS Implementation Considerations  5.16 Monitoring, Logging, and Auditing  5.17 Incident Detection, Response, and System Recovery  6. Applying Security Controls to ICS  6.1 Executing the Risk Management Framework Tasks for Industrial Control Systems6-1  6.1.1 Step 1: Categorize Information System  6.1.2 Step 2: Select Security Controls  6.1.3 Step 3: Implement Security Controls  6.1.4 Step 4: Assess Security Controls  6.1.5 Step 5: Authorize Information System  6.1.6 Step 6: Monitor Security Controls  6.2 Guidance on the Application of Security Controls to ICS  6.2.1 Access Control  6.2.2 Awareness and Training  6.2.3 Audit and Accountability  6.2.4 Security Assessment and Authorization  6.2.5 Configuration Management  6.2.6 Contingency Planning  6.2.7 Identification and Authentication  6.2.8 Incident Response  6.2.9 Maintenance  6.2.10 Media Protection  6.2.11 Physical and Environmental Protection  6.2.12 Planning  6.2.13 Personnel Security  6.2.14 Risk Assessment  6.2.15 System and Services Acquisition  6.2.16 System and Communications Protection  6.2.17 System and Information Integrity  6.2.18 Program Management  6.2.19 Privacy Controls |

1. Giới thiệu dự thảo tiêu chuẩn

Dự thảo tiêu chuẩn “Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn công nghệ thông tin – Các yêu cầu bảo đảm an toàn thông tin trong hệ thống điều khiển công nghiệp” gồm có 09 phần chính, cấu trúc cụ thể như sau:

|  |
| --- |
| Lời nói đầu  1 Phạm vi áp dụng  2 Tài liệu viện dẫn  3 Thuật ngữ và định nghĩa  4 Ký hiệu và thuật ngữ viết tắt  5 Tổng quan về hệ thống điều khiển công nghiệp ICS  5.1 Sự phát triển của các Hệ thống Điều khiển Công nghiệp  5.2 Các lĩnh vực công nghiệp của ISC và sự tương thuộc lẫn nhau của chúng  5.4 Sự hoạt động và các thành phần của ICS  5.5 So sánh ICS và hệ thống bảo mật công nghệ thông tin  5.6 Các loại hệ thống điều khiển khác  6 Xây dựng phương án về đánh giá và quản lý rủi ro cho các hệ thống điều khiển công nghiệp ICS  6.1 Quản lý rủi ro  6.2 Giới thiệu về quy trình quản lý rủi ro  6.3 Cân nhắc đặc biệt khi thực hiện đánh giá rủi ro  6.4 An toàn trong đánh giá rủi ro bảo mật thông tin ICS  6.5 Tác động vật lý tiềm tàng của một sự cố ICS  6.6 Tác động vật lý gián đoạn quy trình ICS  6.7 Kết hợp các khía cạnh phi kỹ thuật số của ICS vào đánh giá tác động  6.8 Kết hợp tác động của các hệ thống an toàn  6.9 Xem xét việc lan truyền tác động đến các hệ thống được kết nối.  7. Xây dựng phương án quản lý vận hành bảo đảm an toàn thông tin cho các hệ thống điều khiển công nghiệp ICS.  7.1 Trường hợp áp dụng cho các tổ chức kinh doanh về bảo mật  7.2 Xây dựng và đào tạo nhóm đa chức năng  7.3 Xác định điều lệ và phạm vi  7.4 Xác định các thủ tục và chính sách bảo mật dành riêng cho ICS  7.5 Triển khai khung quản lý rủi ro bảo mật ICS  8. Xây dựng khung kiến trúc bảo đảm an toàn thông tin cho các hệ thống điều khiển công nghiệp ICS.  8.1 Phân đoạn và phân tách mạng  8.2 Bảo vệ vùng mạng biên  8.3 Tường lửa  8.4 Mạng điều khiển tách biệt hợp lý  8.5 Phân tách mạng  8.6 Kiến trúc chiều sâu phòng ngự được khuyến nghị  8.7 Chính sách tường lửa chung cho ICS  8.8 Quy tắc tường lửa được đề xuất cho các dịch vụ cụ thể  8.9 Dịch địa chỉ mạng (NAT)  8.10 Các vấn đề về tường lửa ICS cụ thể  8.11 Cổng một chiều  8.12 Điểm lỗi đơn lẻ  8.13 Tình trạng dư thừa và khả năng chịu lỗi  8.14 Ngăn chặn các cuộc tấn công trung gian  8.15 Xác thực và uỷ quyền  8.16 Giám sát, Ghi nhật ký và Kiểm tra  8.17 Phát hiện sự cố, ứng phó và khôi phục hệ thống  9. Nghiên cứu, xây dựng phương án áp dụng các biện pháp kiểm soát bảo mật cho các hệ thống điều khiển công nghiệp ICS.  9.1 Thực hiện nhiệm vụ của Khung Quản lý Rủi ro cho các Hệ thống Kiểm soát Công nghiệp  9.2 Hướng dẫn về việc áp dụng các biện pháp kiểm soát an ninh cho ICS  9.2.1 Kiểm soát truy cập  TÀI LIỆU THAM KHẢO |

1. Kết luận

Có thể thấy, trong bối cảnh phát triển nóng của thị trường thông tin truyền thông, cùng vai trò tác động ngày càng sâu rộng của các hệ thống thông tin và mạng đối với việc vận hành hiệu quả các cơ sở hạ tầng quan trọng của quốc gia , cần phải xây dựng những biện pháp, giải pháp đồng bộ nhằm tăng cường quản lý và bảo vệ cơ sở hạ tầng quan trọng đối với hệ thống ICS tại Việt Nam

Xây dựng tiêu chuẩn quốc gia về bảo đảm an toàn hệ thống thông tin các cơ sở hạ tầng quan trọng áp dụng cho hệ thống điều khiển công nghiệp ICS tại Việt Nam sẽ làm cơ sở để chủ quản của các hệ thống thông tin tổ chức triển khai các phương án bảo đảm an toàn thông tin cho các hệ thống cơ sở hạ tầng quan trọng một cách triệt để.

1. Tài liệu tham khảo
2. Tiêu chuẩn NIST- SP 800-82r2, Guide to Industrial Control Systems (ICS) Security
3. Tiêu chuẩn Việt Nam TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn – Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ về việc bảo đảm an toàn hệ thống thông tin
4. Tiêu chuẩn TCVN ISO/IEC 27001 (ISO/IEC 27001:2013) – Công nghệ thông tin – Các kỹ thuật an toàn – Hệ thống quản lý an toàn thông tin - Các yêu cầu