فصلنامه آموزش مهندسی ایران، شماره ۳۲، سال هشتم، ص ۱۰۳-۸۷

کاربرد فناوری اطلاعات در امنیت سیستم‌های کنترل صنعتی

ابوالقاسم دائی‌چیان و فریدون شعبانی‌نیا
دانشکده مهندسی، دانشگاه شیراز

چکیده: قرن حاضر را قرن اطلاعات نامیده‌اند. فناوری اطلاعات یکی از رشته‌هایی است که ابداع شده است تا چگونگی جمع‌آوری, پردازش و توزیع اطلاعات را به‌صورت علمی بررسی کند. یکی از شاخه‌های مهمی که در فناوری اطلاعات وجود دارد، امنیت اطلاعات است. یک شبکه پایه و اساس یک سیستم کنترل صنعتی در دهه‌های اخیر بوده است. در گذشته، امنیت شبکه‌های کنترل صنعتی بر پایه مجزا کردن شبکه‌های کنترل صنعتی بوده است. امروزه، با گسترش شبکه‌های کنترل صنعتی و اتصال آنها به اینترنت, امنیت آنها به بحث بسیار مهمی تبدیل شده است. هرگونه نفوذ به سیستم‌های کنترل صنعتی می‌تواند بسیار خطرناک باشد, به خصوص در صنایع حیاتی برای یک دولت. در این مقاله سیستم‌های کنترل صنعتی و ساختار شبکه در آنها و نیز راه‌های افزایش امنیت این سیستم‌ها بررسی شده است.

واژه‌های کلیدی: فناوری اطلاعات، امنیت اطلاعات، کنترل صنعتی و کنترل هوشمند.

۱. مقدمه

موسسه جهانی استاندارد (NIST)[1] گروهی را به نام PCSRF[2] به منظور کار بر روی امنیت شبکه‌های کنترلی دیجیتالی, به خصوص شبکه‌های کنترل صنعتی, تشکیل داده است. تلاش این گروه بر بهبود امنیت سیستم‌های کنترل کامپیوتری که در فرایندهای صنعتی مانند سیستم‌های الکتریکی، سوخت‌رسانی، آب‌رسانی، جمع‌آوری زباله، پتروشیمی، دارویی، مواد معدنی و... که در واقع سیستم‌های حیاتی یک کشور هستند، متمرکز شده است.

البته، سازمان‌های دیگری مانند ISA[3], NERC[4] و IEC نیز در این زمینه فعالیت می‌کنند و هرکدام تاکنون استانداردهایی را ارائه کرده‌اند.

۲. سیستم‌های کنترل کامپیوتری فرایندها

کامپیوترهایی که برای کاربرد در کنترل سیستم‌های صنعتی طراحی می‌شوند، معمولاً دارای خواصی متفاوت از سیستم‌های تجاری معمول هستند. این سیستم‌ها به‌گونه‌ای طراحی شده‌اند که به‌صورت زمان حقیقی (Real Time) و با بازده بالا به فرایندها پاسخ دهند و این مسئله‌ای حیاتی است. امنیت اطلاعات معمولاً در این سیستم‌ها، در زمان طراحی، به عنوان یک پارامتر اصلی در نظر گرفته نمی‌شود و در نتیجه، برای به‌دست آوردن امنیت زمان کمی از منابع سیستم در اختیار است و معمولاً رسیدن به امنیت مطلوب در تناقض با کارکرد مناسب سیستم کنترلی قرار می‌گیرد.

سیستم‌های کنترل صنعتی می‌توانند به‌صورت process-based یا discrete-based باشند. کنترل‌های process-based برای مواردی که یک فرایند پیوسته داریم مناسب است، مانند

---

1 . National Institute of Standard and Technology

2 . Process Control Security Requirements Forum

3 . Instrumentation Systems and Automation Society

4 . North-American Electric Reliability Council

جریان سوخت یا بخار در یک نیروگاه یا جریان نفت در یک پالایشگاه. کنترل‌های discrete-based در مواردی که فرایندی گسسته وجود دارد، استفاده می‌شود.

نتایجی که در زمینه سیستم‌های پیوسته به‌دست می‌آید، به راحتی قابل تعمیم به سیستم‌های گسسته است و در نتیجه، فقط به بررسی سیستم‌های پیوسته خواهیم پرداخت.

اجزای اصلی سیستم کنترل صنعتی به طور معمول عبارت است از : حلقه کنترلی[1]، واسط بین انسان ـ ماشین (HMI)[2] و عیب‌یابی و نصب از راه دور[3] (شکل ۱). حلقه کنترلی نیز از فرایندی که قرار است کنترل شود، تعدادی حسگر، عملگر[4] و کنترل‌کننده تشکیل شده است. در حلقه کنترلی مقادیر اندازه‌گیری شده توسط حسگرها به کنترل‌کننده ارسال می‌شود و کنترل‌کننده سیگنال کنترلی مربوط را به عملگر ارسال می‌کند. HMI این امکان را فراهم می‌کند که اپراتور مقادیر دلخواه، الگوریتم کنترل یا پارامترهای کنترل‌کننده را تغییر دهد. HMI همچنین، مقادیر اندازه‌گیری شده توسط حسگرها و وضعیت کنترل‌کننده را نیز به کاربر نشان می‌دهد. ابزار عیب‌یابی و نصب نیز معمولاً از طریق مودم یا اینترنت اطلاعات و وضعیت سیستم را به مهندسان کنترل، اپراتورها یا فروشندگان ارائه می‌دهند و آنها نیز می‌توانند تغییراتی را در وضعیت عملگرها یا خصوصیات حسگرها اعمال کنند.

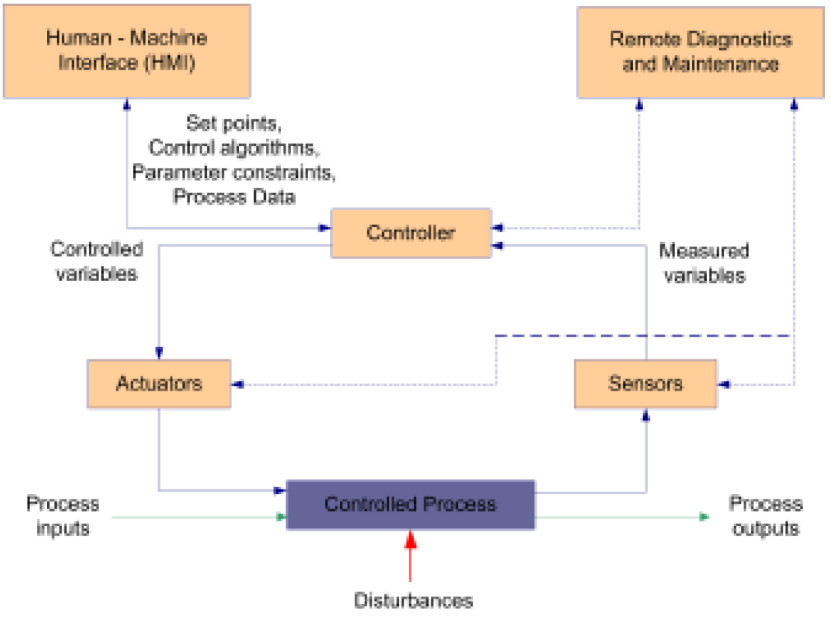
در شرکت‌ها و سیستم‌هایی که چندین فرایند کنترلی را در مناطق مختلف از نظر جغرافیایی باید کنترل کنند، امنیت اطلاعات در ارتباط بین مناطق مختلف مطرح می‌شود. در این سیستم‌ها اطلاعات بین مناطق مختلف توسط اینترنت یا یک WAN مبادله می‌شود. سیستم‌های در این سطح را می‌توان به دو دسته تقسیم کرد: یکی سیستم‌های DCS[5] و دیگری SCADA[6].

سیستم DCS برای کنترل فرایندهای بزرگ و پیچیده مانند نیروگاه، پالایشگاه یا

---

1 . Control Loop
2 . Human-Machine Interface
3 . Remote Diagnostics and Maintenance Utilities
4 . Actuator
5 . Distributed Control Systems
6 . Supervisory Control And Data Acquisition systems

پتروشیمی که معمولاً در یک محل قرار می‌گیرند، استفاده می‌شود. سیستم SCADA برای مواردی که سیستم به‌صورت توزیع شده و گسترده است و پردازش متمرکز داده‌ها به اندازه کنترل آنها اهمیت دارد، مورد استفاده قرار می‌گیرد و مواردی مانند سیستم آب‌رسانی، گاز رسانی و خطوط برق از این قبیل هستند. بلوک دیاگرامی کلی از این سیستم‌ها را می‌توان در شکل‌های ۲ و ۳ ملاحظه کرد.



شکل ۱: سیستم کنترل در حالت کلی

بررسی اجمالی بر روی سیستم‌های بر مبنای DCS و SCADA نشان می‌دهد که عملکرد دو سیستم در سطح بالا مشابه یکدیگر است. در این قسمت معمولاً اجزای عمومی مانند پایگاه‌های داده[1]، پرینترها، سرورها و کنترل‌کننده‌های حوزه[2] قرار می‌گیرند. ارتباط با

---

1 . Plant Database
2 . Domain Controllers

خارج نیز به کمک Firewall به اینترنت یا WAN خارجی صورت می‌گیرد. معمولاً تعدادی مودم نیز برای امکان دسترسی از راه دور در سیستم قرار می‌گیرد.

سیستم DCS از یک لایه کنترل کننده ناظر[1] و چندین کنترل‌کننده توزیع شده تشکیل شده است. کنترل کننده ناظر بر روی سرور کنترل اجرا می‌شود و با کمک یک شبکه peer-to-peer در ارتباط با اجزای دیگر قرار می‌گیرد. کنترل کننده ناظر مقادیر مورد نیاز برای هر فرایند را به کنترل‌کنندههای محلی ارسال و داده‌های حسگرهای آنها را دریافت می‌کند. کنترل‌کنندههای محلی نیز فرایند تحت کنترل خود را بر مبنای درخواست‌هایی که از کنترل‌کننده ناظر دریافت شده است و همچنین، اطلاعات جمع‌آوری شده از حسگرها کنترل خواهد کرد. معمولاً کنترل‌کنندههای محلی برای ارتباط با عملگرها و حسگرها از یک شبکه فیلدباس[2] محلی استفاده می‌کنند که به کابل‌کشی بین کنترل‌کننده و اجزای مربوط نیاز است. در این سیستم‌ها کنترل‌کنندههای متفاوتی مانند کنترل تک حلقه، PLC و کنترل‌کننده‌های فرایندها را می‌توان استفاده کرد. معمولاً امکان دسترسی مستقیم به کنترل‌کنندههای محلی و توزیع شده از طریق مودم به منظور رفع عیب و سرویس‌دهی برای فروشنده نیز وجود دارد.

یک سیستم بر مبنای SCADA معمولاً از یک CMS[3] و تعدادی ایستگاه در دوردست[4] تشکیل شده است. در اتاق CMS سرورهای کنترل‌کننده و روترهای مورد نیاز برای یک شبکه peer-to-peer قرار می‌گیرد. CMS اطلاعات گرفته شده توسط ایستگاه‌های مختلف را جمع‌آوری و فرمان مناسب را تولید می‌کند. هر ایستگاه شامل یک RTU[5] یا PLC است که عملگرها را کنترل و مقادیر اندازه‌گیری شده توسط حسگرها را دریافت می‌کند. در این سیستم‌ها به یک محیط ارتباطی بین ایستگاه‌های مختلف و CMS نیاز است. این محیط به کمک خطوط تلفن، کابل یا ارتباط رادیویی فراهم می‌شود.

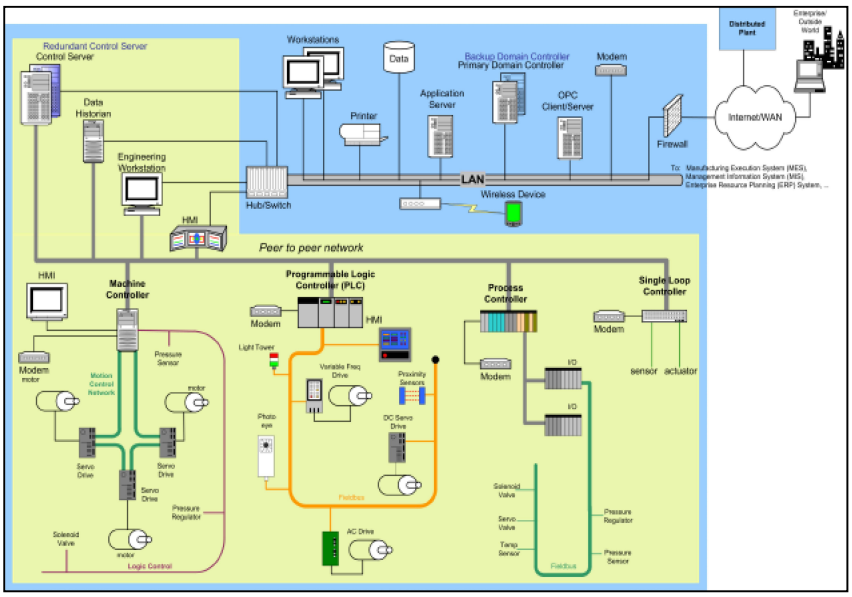
---

1 . Supervisory Controller
2 . Field Bus
3 . Central Monitoring System
4 . Remote Stations
5 . Remote Terminal Unit

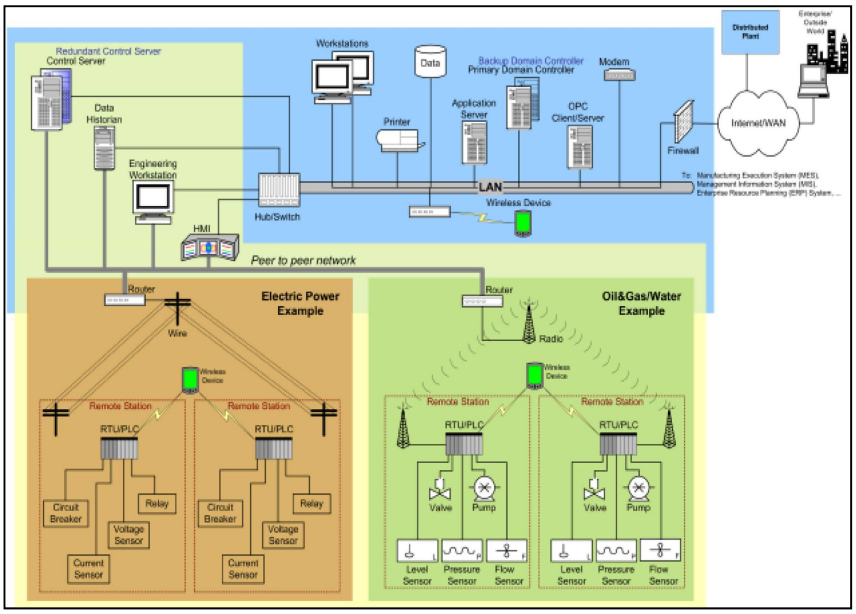
در سیستم‌های صنعتی با توجه به نوع و میزان پراکندگی سیستم، کنترل به صورت DCS و یا SCADA صورت می‌گیرد. برای مثال، در یک سیستم الکتریکی که شامل مراحل تولید، انتقال و توزیع است، در مرحله تولید که در نیروگاه صورت می‌گیرد به دلیل تمرکز تجهیزات، کنترل به صورت DCS و در مراحل انتقال و توزیع که پراکندگی زیادی وجود دارد، کنترل SCADA مناسب‌تر است. به همین ترتیب، در سیستم سوخت‌رسانی یا آب‌رسانی نیز می‌توان کنترل مناسب را انتخاب کرد.

۳. آسیب‌پذیری سیستم‌های کنترل صنعتی

امنیت اطلاعات سیستم‌های کنترل صنعتی در گذشته چندان اهمیت زیادی نداشت، زیرا سیستم‌های صنعتی بر مبنای بازده بالا، قابلیت اطمینان و قابلیت انعطاف بالا طراحی می‌شدند و معمولاً به‌صورت فیزیکی از شبکه های دیگر مجزا بودند و از سخت افزار مجزا استفاده می‌کردند. امروزه، با ورود اینترنت در طراحی سیستم‌های کنترل صنعتی آسیب‌پذیری این سیستم‌ها افزایش یافته است. در بسیاری از موارد شبکه‌های DCS و SCADA به شبکه های خارجی متصل می‌شوند و این موجب ساده‌تر شدن حمله به این سیستم‌ها و حتی انهدام آنها می‌شود.


Redundant Control Server
Control Server
Workstations
Data
Backup Domain Controller
Primary Domain Controller
Modem
Application Server
OPC Client/Server
Printer
Data Historian
Engineering Workstation
Hub/Switch
LAN
Wireless Device
Firewall
Internet/WAN
Distributed Plant
HMI
Peer to peer network
Machine Controller
Programmable Logic Controller (PLC)
Process Controller
Single Loop Controller
sensor
actuator
Logic Control
Fieldbus

شکل ۲: DCS



شکل ۳: SCADA

حملات خرابکارانه می‌تواند از منابع مختلفی مانند دشمنان یک دولت، گروه‌های تروریستی، کارمندان ناراضی در شرکت، نفوذگرها, اشتباهات مدیر شبکه, خرابکاری‌های تصادفی یا ناشی از یک حادثه طبیعی باشد. به طور معمول, آسیب به یک سیستم کنترلی می‌تواند به یکی از روش‌های زیر انجام شود:

۱. Command sequence

در صورتی که یک کاربر سیستم یا متجاوزی[1] که به نحوی برای ورود به سیستم مجوز گرفته است دستوری نادرست در یک سیستم کنترل صنعتی صادر کند, می‌تواند موجب

---

1 . Intruder

وقوع حوادث خطرناکی شود. برای مثال، دستورهایی شبیه به دستورهای زیر می‌تواند باعث رخ‌دادن حوادث خطرناکی شود:

- تمام دریچه‌های یک سد باز شود.
- دو ماده خطرناک در یک سیستم شیمیایی ترکیب شوند.
- مخزن آب خنک کننده در یک نیروگاه تخلیه شود.

۲. Halting Processors

ویروس‌ها می‌توانند با ارسال فرمان‌هایی به پردازنده سیستم باعث کند شدن پردازنده در اجرای محاسبات اصلی سیستم و وقوع خطا در سیستم شوند.

۳. تغییرات در سیستم

یک متجاوز به سیستم می‌تواند با اعمال تغییرات بر روی نقاط تنظیم[1] در سیستم, باعث ایجاد حادثه شود. برای مثال، فرض کنید که برای یک سیستم کنترل کننده فشار:

- برنامه را به نحوی تغییر دهد که فشار را همیشه مقدار کمی بخواند.
- کنترل سیستم را بدین صورت تغییر دهد: اگر فشار از حد مجاز بیشتر شد، آنگاه فشار را افزایش بده.
- همچنین، می‌تواند مقدار حد مجاز برای فشار را افزایش دهد.

٤.امنیت در شبکه

در یک سیستم کنترل صنعتی, در لایه پایین, یکی از انواع شبکه‌های کنترل صنعتی مانند Field bus قرار می‌گیرد. تعدادی Process station وجود دارد که اطلاعات را از حسگرها, کنترلرها و محرک‌ها جمع‌آوری می‌کند و همگی به Operator station ارسال می‌شود. امنیت در شبکه‌های کنترل صنعتی در این قسمت, که اطلاعات مبادله می‌شود, مطرح است. امروزه، برای تبادل اطلاعات در شبکه‌های کنترلی از شبکه‌های تجاری موجود مانند

---

1 . Set Points

اینترنت یا WAN استفاده می‌شود.

اصول اساسی ایجاد امنیت در یک شبکه عبارت‌اند از:

تعریف Permission و Right برای کاربران

با تعیین دقیق میزان دسترسی هر کاربر به منابع سیستم می‌توان از بروز خطرهای خرابکارانه جلوگیری کرد. Permission و Right در واقع، دو مفهوم مجزا هستند؛ Permission تعیین میزان دسترسی کاربر به صورت خواندن, نوشتن و تغییر[1] است، در حالی‌که Right تعیین کننده میزان دسترسی کاربر به اجرای یک برنامه یا مدیریت یک سری ویژگی‌هاست[2].

☒ تصدیق (Authentication)

عمل Authentication تشخیص هویت واقعی یک شخص, وسیله یا سرویس است. معمول‌ترین روش برای تشخیص هویت استفاده از Password است. هرچه تعداد کاراکترهای Password بیشتر باشد، امکان کشف آن کمتر است و معمولاً بین ۸ تا ۱۴ کاراکتر هستند. در صورتی‌که بخواهیم از کلمه عبوری با امنیت بیشتر استفاده کنیم, Digital key پیشنهاد می‌شود. در این موارد یک کارت دیجیتالی کلمه عبور شما را که تعداد کاراکترهای بیشتری دارد, نگهداری می‌کند. برای اطمینان می‌توان یک کلمه رمز ۴ حرفی را نیز به منظور استفاده از Digital key قرار داد. کارت‌های هوشمند نیز نمونهٔ دیگری هستند که دارای حافظه RAM برای نگهداری رمز هستند. در صورتی‌که نیاز به امنیت بیشتری داشته باشیم، می‌توانیم از روش‌های دیگری مانند استفاده از اثر انگشت[3], استفاده از نمونه صدای کاربر[4] یا نمونه شبکیه و عنبیه[5] کاربر استفاده کرد.

---

1 . Read, Write and change

2 . Run and Manage some feature

3 . Fingerprints

4 . voice patterns

5 . eye retinas and irises

☒ رمزنگاری (Cryptography)

رمزنگاری؛ یعنی اینکه اطلاعات را با کمک یک کلید به‌گونه‌ای تغییر دهیم که برای هیچ‌کس قابل تشخیص نباشد, مگر اینکه کلید را داشته باشد. رمزنگاری به دو صورت Symmetric یا Common key و Asymmetric یا Public key انجام می‌شود.

در روش Common یک کلید مخفی وجود دارد که فقط فرستنده و گیرنده به آن دسترسی دارند و هر دو اطلاعات خود را با آن رمزنگاری و رمزگشایی می‌کنند. در این روش امنیت سیستم به مخفی بودن کلید بستگی دارد.

در روش Asymmetric دو کلید وجود دارد: Public key و Private key. کلید Public به‌صورت عمومی منتشر می‌شود و کلید Private به‌صورت مخفی فقط در اختیار فرستنده و گیرنده است. اطلاعاتی که با کمک یکی از این کلیدها کد شده باشد, فقط با کمک کلید دیگر قابل رمزگشایی است. از این روش در Signature Digitalها نیز استفاده می‌شود. متنی که یک شخص با کمک Private key مخصوص خود رمز کرده است, فقط توسط Public key مربوط به آن شخص رمزگشایی خواهد شد و بدین ترتیب, اعتبار آن متن مشخص می‌شود.

میزان امنیت روش‌های مختلف رمزنگاری به طول کلید مورد استفاده و بازده الگوریتم رمزنگاری بستگی دارد.

☒ گواهی کردن (Certification)

در این مورد در ابتدا هویت کاربر تشخیص داده می‌شود و سپس، با توجه به نوع Public key میزان دسترسی‌های کاربر نیز مشخص می‌شود.

☒ ارتباطات مخفی (Secured Link)

به منظور برقراری یک ارتباط با امنیت بالا بر روی اینترنت در بسیاری از موارد نیاز به VPN[1] است. ایجاد یک VPN با کمک پروتکل‌های جدید مانند IPSec یا PPTP

---

1 . Virtual Private Network

امکان‌پذیر است.

☒ دیواره آتش (Firewalls)

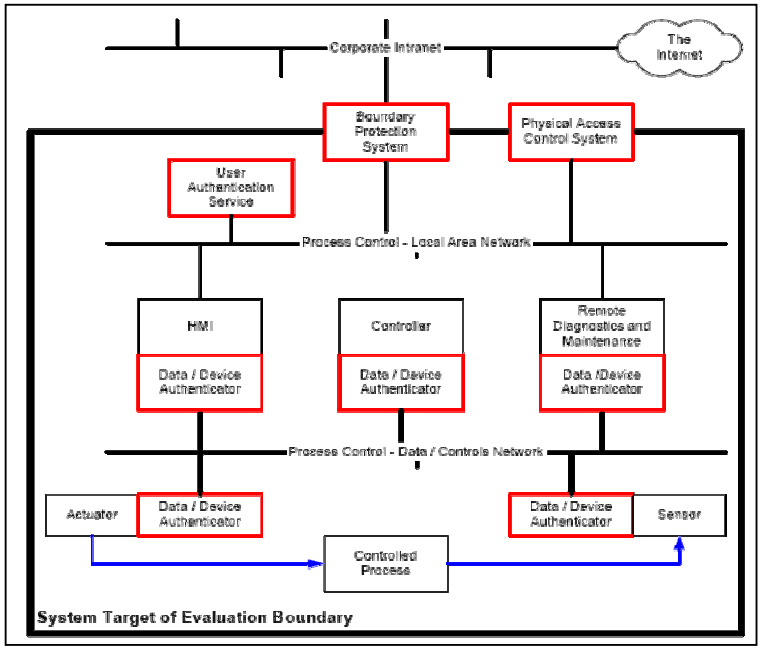
یکی دیگر از مهم‌ترین موارد در امنیت سیستم‌ها استفاده از دیواره‌های آتش است. سه نمونه دیواره آتش وجود دارد: Routing Firewalls, Application Level Firewalls و Circuit-Level Gateways. دیواره‌های آتش با توجه به سیاستگذاری‌های شبکه و بررسی بسته‌های دریافتی یا ارسالی, بسته‌های غیرمجاز را نابود می‌کند و بسته‌های مجاز را به مقصد می‌رساند.

☒ حسابرسی (Audit)

در سیستم‌های صنعتی باید حتماً عمل Audit انجام شود. در این عمل با بررسی تاریخچه دستورهای اعمالی می‌توان تعداد تلاش‌های ناموفق برای ورود به سیستم, جستجو در باره اطلاعات کلی سیستم, دستورهای مشکوک یا تغییرات مشکوک در فایل‌های سیستم را بررسی کرد.

SPP/ICS .۵

هدف این است که از درستی اطلاعات و در دسترس بودن سیستم بدون آسیب رسیدن به ایمنی سیستم حفاظت شود. بدین منظور، یک سیستم کنترلی را که در حالت کلی در شکل ۱ رسم شده است، مطابق با شکل ۴ تغییر می‌دهیم. System Target of Evaluation Boundary وظیفه حفاظت سیستم را برعهده دارد. هرگونه ورود یا خروج اطلاعات به فرایند باید با نظارت Boundary Protection System صورت گیرد.



شکل ٤

در استاندارد SPP/ICS سه سطح شبکه در سیستم تعریف می‌شود:

- Process Control – Data/Control Network: استانداردهای شبکه برای سیستم‌های کنترل صنعتی مانند Field Bus در این قسمت استفاده می‌شود.

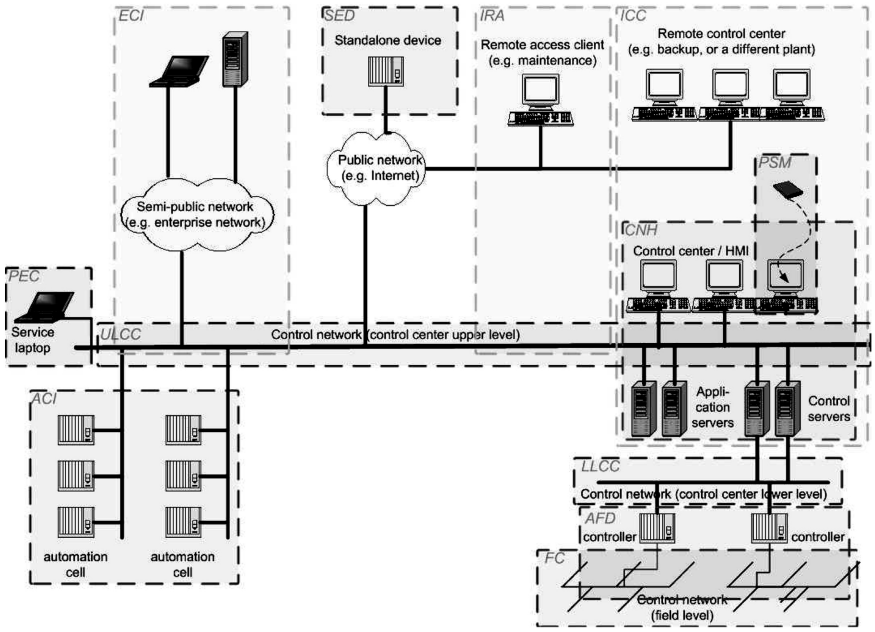
- Process Control – Local Area Network: این شبکه برای اتصال سیستم‌های کامپیوتری که کنترل‌کننده فرایندها هستند، مورد استفاده قرار می‌گیرد. توجه کنید که این شبکه نیز به صورت داخلی در محل فرایند قرار دارد.
- Corporate Intranet: این قسمت شبکه داخلی شرکت است که می‌تواند چندین فرایند را به یکدیگر مرتبط کند. همچنین، می‌تواند به شبکه اینترنت نیز متصل شود.

برای ایجاد امنیت, در هر قسمت بلوک‌های زیر به سیستم اضافه می‌شود:

- Data/Devise Authentication: این قسمت وظیفه تشخیص و تأیید هویت داده‌ها و دستورهای کنترلی را بر عهده دارد. این بلوک بر روی تمام بلوک‌ها در یک سیستم کنترلی قرار می‌گیرد.
- User Authentication Service: این بلوک وظیفه کنترل دسترسی به فرایند, توسط HMI یا Remote Diagnostics and maintenance را برعهده دارد.
- Physical Access Control System: این بلوک تشخیص و تأیید هویت اشخاصی را که قصد دسترسی فیزیکی به سیستم را دارند، بر عهده دارد.

IEC.٦

مدل ایجاد امنیت در سیستم‌هایی که بر مبنای IEC طراحی می‌شوند، مطابق شکل ۵ است.



شکل ۵

در این مدل نیز، برای ایجاد امنیت در شبکه کنترلی، چندین قسمت اساسی قرار گرفته است:

۱. ECI1: این قسمت وظیفه ایجاد امنیت در انتقال اطلاعات به‌صورت non-real-time و عموماً یکطرفه بین شبکه کنترلی و شبکه شرکت مورد نظر را بر عهده دارد.

۲. IRA2: وظیفه ایجاد امنیت در موارد دسترسی از راه دور به سیستم را برعهده دارد. دسترسی از راه دور ممکن است برای مهندسان سیستم یا برای فروشندگان قطعات به‌منظور رفع عیب سیستم صورت گیرد که می‌تواند با کمک مودم یا از طریق اینترنت

---

1 . Enterprise Control net Interconnect
2 . Interactive Remote Access

باشد.

۳. ICC [1]: به منظور ایجاد امنیت در ارتباط بین مراکز کنترلی مختلف استفاده می‌شود.

۴. SED [2]: برای ایجاد امنیت برای وسیله‌هایی که در یک منطقه امن قرار ندارند، مورد استفاده قرار می‌گیرد.

۵. بلوک‌های دیگری نیز وجود دارد که اغلب بلوک‌های کنترلی در سطح پایین هستند.

۷. نتیجه‌گیری

امروزه، در طراحی سیستم‌های کنترل صنعتی، امنیت سیستم یکی از پارامترهای اجتناب‌ناپذیر سیستم است و باید این پارامتر به عنوان یکی از پارامترهای اساسی مد نظر باشد و هر سیستم حتماً تحت نظارت متخصصان امنیت باشد تا از حملات خرابکارانه در امان باشد. یکی از راه‌های افزایش امنیت سیستم‌های کنترل صنعتی استفاده از آخرین استانداردها در امنیت سیستم‌ها و حتی تعریف پروژه‌های تحقیقاتی در این زمینه است. در این مقاله سعی شد تا با بررسی مشکلات ناشی از کمبود امنیت در سیستم‌های کنترل و بررسی استانداردهای جدید در این زمینه راهکارهای مناسبی برای افزایش امنیت سیستم‌ها ارائه شود. صنایع و به‌خصوص صنایع حیاتی کشور باید این مسئله را به عنوان یکی از مسائل اساسی خود مد نظر داشته باشند.

مراجع

1. Keith Stouffer, Joe Falco & Fred Proctor, "The NIST Process Control Security Requirements Forum (PCSRF) and the Future of Industrial Control System Security," Atlanta, Georgia, May 3-5, 2004.
2. Joe Falco, Keith Stouffer, Albert Wavering & Frederick Proctor, "IT Security for Industrial Control Systems," National Institute of Standards

---

1 . Inter Control center Connect

2 . Stand-alone Embedded Device

and Technology.
3. Martin Naedele, “Standardizing Industrial IT Security - A First Look at the IEC approach,” ABB Corporate Research, CH-5405 Baden-D¨attwil, Switzerland, 2005.
4. Joona Nikunen, “Security Considerations on Wide Area Networking Industrial Solutions,” Tampere University of Technology Department of Automation, January 2001.
5. David Williams, “Securing Process Control Systems - IT Security,” European Parliament, Brussels 10 September 2003.
6. Joseph Falco, James Gilsinn & Keith Stouffer, “IT Security for Industrial Control Systems: Requirements Specification and Performance Testing,” NDIA Homeland Security Symposium & Exhibition Hyatt Regency, Crystal City, Virginia, May 25-27, 2004.
7. G. Dondossola, O. Lamquet & M. Masera, "Emerging Standards and Methodological Issues for The Security Analysis of Power System Information Infrastructures,” Securing Critical Infrastructures, Grenoble, October 2004.
8. Alan Gunnerson, “Information Technology (IT) Security for Supervisory Control and Data Acquisition (SCADA) Systems,” University of Dallas, Summer 2003.

(تاریخ دریافت مقاله:۱۳۸۵/۵/۲۱)