

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشگاه صنعت آب و برق (شهید عباسپور)
دانشکده مهندسی برق

پایان نامه کارشناسی ارشد (مهندسی برق-کنترل)

عنوان پایان نامه

ارزیابی سیستم کنترل نیروگاه سیکل ترکیبی طرح نیام شرکت مپنا
(Teleperm-XP)، از نظر آسیب پذیری در مقابل بدافزارهای رایانه‌ای و ارائه
راهکارهای مناسب

تحقیق و تدوین:

وهاب حاجی حاجی

استاد راهنما:

جناب آقای دکتر محسن منتظری

بهمن ۱۳۹۰



دانشگاه صنعت آب و برق (شهید عباسپور)
دانشکده مهندسی برق

پایان نامه کارشناسی ارشد رشته مهندسی برق-کنترل آقای وهاب حاجی حاجی
تحت عنوان

ارزیابی سیستم کنترل نیروگاه سیکل ترکیبی طرح نیام شرکت مپنا (Teleperm-XP)، از
نظر آسیب پذیری در مقابل بدافزارهای رایانه‌ای و ارائه راهکارهای مناسب

در تاریخ ۱۳۹۰/۱۱/۳۰ توسط کمیته تخصصی زیر مورد بررسی و تصویب قرار گرفت.

- | | |
|-------|-------------------------------|
| امضاء | ۱- استاد راهنمای پایان نامه |
| امضاء | ۲- استاد داور داخلی |
| امضاء | ۳- استاد داور مدعو |
| امضاء | سرپرست تحصیلات تکمیلی دانشکده |

مشکرو قدردانی

پس از حمد و ستایش درگاه حضرت دوست، بر خود لازم می‌دانم از راهمبانی‌های بی‌دریغ و ارزشمند استاد عزیزم جناب آقای دکتر محسن منطری کمال مشکرو قدردانی را به عمل آورم. ایشان علاوه بر ایفای نقش استاد راهمنا، به عنوان الگویی اخلاق‌نیز، همواره سرمشق بنده

بوده‌اند.

به نام خدا

تعهدنامه اصالت اثر:

اینجانب وهاب حاجی حاجی تاکید می‌کنم که مطالب مندرج در این پایان‌نامه، حاصل کار پژوهشی اینجانب می‌باشد و به دستاوردهای پژوهشی دیگران که در این نوشته از آنها استفاده شده است مطابق مقررات ارجاع گردیده است.

این پایان‌نامه قبلاً برای احراز هیچ مدرک هم‌سطح، پایین‌تر و بالاتر ارائه نشده است. کلیه حقوق مادی و معنوی این اثر متعلق به دانشگاه صنعت آب و برق (شهید عباسپور) می‌باشد.

وهاب حاجی حاجی

تقدیم به

پدر و مادر عزیزتر از جانم

و

خواهر و برادر دوست داشتنی ام

فهرست مطالب

۲	فصل اول: مقدمه.....
۳	۱-۱- ضرورت بحث.....
۴	۲-۱- تهدیدات رایج امنیتی.....
۵	۳-۱- نتایج حملات امنیتی در سیستم‌های کنترل صنعتی.....
۶	۴-۱- اهداف امنیتی.....
۶	۵-۱- مروری بر کارهای صورت گرفته.....
۱۱	۶-۱- ترتیب فصل‌ها (ساختار کلی).....
۱۳	فصل دوم: آشنایی با نیروگاه سیکل ترکیبی.....
۱۴	۱-۲- مقدمه.....
۱۴	۲-۲- نیروگاه سیکل ترکیبی.....
۱۷	۳-۲- مشخصات نیروگاه سیکل ترکیبی طرح نیام مپنا.....
۱۹	۴-۲- اجزاء تشکیل دهنده سیکل ترکیبی.....
۱۹	۱-۴-۲- توربین گاز.....
۲۰	۲-۴-۲- بویلر.....
۲۰	۳-۴-۲- بویلر بازیاب حرارتی (HRSG).....
۲۲	۴-۴-۲- توربین بخار.....
۲۳	۵-۴-۲- چگالنده.....
۲۴	۶-۴-۲- دی‌اریتور.....
۲۵	۷-۴-۲- سایر اجزای سیکل ترکیبی.....
۲۶	فصل سوم: ساختار کنترلی نیروگاه سیکل ترکیبی (Teleperm XP).....
۲۷	۱-۳- مقدمه.....
۲۷	۲-۳- ساختار کلی.....

۳۰	۳-۳- زیر سیستم اتوماسیون AS620
۳۰	۳-۳-۱- ساختار سیستم اتوماسیون AS620B
۳۱	۳-۳-۲- ساختار سیستم اتوماسیون AS620F
۳۲	۳-۳-۳- ساختار سیستم اتوماسیون AS620T
۳۳	۳-۳-۴- ماژول‌های کنترلی (SIM و FUM)
۳۳	۳-۴-۱- اعضای خانواده FUM-B
۳۳	۳-۴-۲- اعضای خانواده FUM-F
۳۴	۳-۴-۳- اعضای خانواده SIM-B
۳۴	۳-۴-۴- اعضای خانواده SIM-F
۳۴	۴-۳- زیر سیستم مدیریت و کنترل فرآیند (OM650)
۳۶	۳-۴-۱- بسته‌های عملیاتی (بسته‌های توابع)
۳۸	۳-۴-۲- ساختار و نحوه عملکرد OM650
۳۹	۳-۴-۳- واسط انسان و ماشین (HMI)
۴۱	۳-۴-۴- تجزیه و تحلیل خرابی (Fault Analysis)
۴۱	۳-۴-۵- ثبت وقایع (Logging)
۴۱	۳-۴-۵-۱- ثبت وقایع قابل پیکربندی OM
۴۲	۳-۴-۵-۲- ثبت وقایع پیکربندی شده توسط ES
۴۳	۳-۴-۵-۳- ثبت وقایع Online
۴۳	۳-۴-۶- مدیریت داده‌ها
۴۳	۳-۴-۶-۱- انواع رخدادهای مربوط به اپراتور
۴۴	۳-۴-۶-۲- انواع رخدادهای مربوط به مهندس کنترل و ابزار دقیق
۴۴	۳-۴-۷- بایگانی کوتاه مدت
۴۵	۳-۴-۸- بایگانی بلند مدت
۴۵	۳-۴-۹- مستندات بازبینی یک رویداد (SDAT)

۴۶آمارها ۱۰-۴-۳
۴۶سرویس و نگهداری دستگاه‌های نیروگاه ۱۱-۴-۳
۴۶مقادیر مشخصه ۱۲-۴-۳
۴۷حفاظت در برابر دسترسی غیر مجاز ۱۳-۴-۳
۴۷(Engineering System) ES680 زیر سیستم مهندسی ۵-۳
۴۸پیکربندی سیستم اتوماسیون AS620 ۱-۵-۳
۴۹پیکربندی زیر سیستم مدیریت و کنترل OM650 توسط سیستم مهندسی ES ۲-۵-۳
۵۰پیکربندی سخت‌افزار سیستم و تجهیزات حوزه فیلد ۳-۵-۳
۵۰پیکربندی گذرگاه ارتباطی ۴-۵-۳
۵۱زیر سیستم تشخیص خطا (Diagnostic System) ۶-۳
۵۲وظایف DS670 ۱-۶-۳
۵۲جریان داده ۲-۶-۳
۵۴فصل چهارم: گذرگاه ارتباطی در سیستم کنترل نیروگاه سیکل ترکیبی
۵۵مقدمه ۱-۴
۵۵ساختار کلی و ویژگی‌های شبکه ارتباطی ۲-۴
۵۷پروتکل‌های تبادل داده و تجهیزات ارتباطی ۳-۴
۵۹نحوه تبادل داده OM650 با سیستم‌های خارجی ۴-۴
۶۱پروتکل‌ها و قالب‌های تبادل داده ۱-۴-۴
۶۱دسترسی به سیستم کنترلی Teleprm XP از طریق صفحات وب (WEB4TXP) ۵-۴
۶۴اطلاعات کاربران Web4txp ۱-۵-۴
۶۵استفاده از OPC سرور جهت تبادل داده ۶-۴
۶۷سایر واسط‌های موجود جهت تبادل داده ۷-۴
۷۰فصل پنجم: امنیت اطلاعات در شبکه‌های کنترل صنعتی

- ۷۱-۱-۵- مقدمه ۷۱
- ۷۱-۲-۵- تمایز امنیت در شبکه‌های کنترل صنعتی با شبکه‌های IT ۷۱
- ۷۳-۳-۵- استانداردهای موجود جهت برقراری امنیت شبکه‌های صنعتی ۷۳
- ۷۵-۱-۳-۵- استاندارد امنیت سیستم‌های کنترل فرآیندهای صنعتی ، ISA-TR 99.00.01 ۷۵
- ۷۵-۱-۱-۳-۵- روش‌های تصدیق هویت و مجوز دسترسی ۷۵
- ۷۷-۲-۱-۳-۵- تکنولوژی‌های کنترل دسترسی / فیلتر کردن / مسدود نمودن جریان داده ۷۷
- ۷۸-۳-۱-۳-۵- محرمانگی اطلاعات ۷۸
- ۸۰-۴-۱-۳-۵- ابزار و تجهیزات نظارت، اندازه‌گیری و بازرسی ۸۰
- ۸۱-۵-۱-۳-۵- نرم‌افزارهای کامپیوتر ۸۱
- ۸۲-۶-۱-۳-۵- کنترل و امنیت فیزیکی ۸۲
- ۸۲-۴-۵- مراحل ارزیابی یک ساختار امنیتی ۸۲
- ۸۴-۱-۴-۵- طراحی و برنامه ریزی ۸۴
- ۸۵-۲-۴-۵- جمع‌آوری داده ۸۵
- ۸۷-۳-۴-۵- تحلیل ریسک ۸۷
- ۸۷-۱-۳-۴-۵- تحلیل تهدیدات ۸۷
- ۸۸-۲-۳-۴-۵- تحلیل آسیب‌پذیری ۸۸
- ۸۸-۳-۳-۴-۵- نگاشت آسیب‌پذیری/تهدیدات/دارایی‌ها ۸۸
- ۸۸-۴-۳-۴-۵- ارزیابی شدت تأثیر و احتمال ریسک ۸۸
- ۸۹-۵-۳-۴-۵- تحلیل نتایج ریسک ۸۹
- ۸۹-۴-۴-۵- شناسایی و انتخاب تجهیزات امنیتی مناسب ۸۹
- ۹۰-۵-۴-۵- بکارگیری و نظارت ۹۰
- ۹۰-۵-۵- انواع حملات در شبکه کنترلی صنعتی ۹۰
- ۹۱-۶-۵- مروری بر سیاست‌ها و ساختار امنیتی پیاده‌سازی شده در یک سیستم کنترلی عمومی ۹۱
- ۹۱-۶-۵-۱- ساختار کلی سیستم کنترلی PCS 7 ۹۱

۹۲	۵-۶-۲- برخی از سیاست‌های امنیتی به کار گرفته شده در سیستم کنترلی PCS 7
۹۶	فصل ششم: ارزیابی امنیتی سیستم کنترل نیروگاه سیکل ترکیبی
۹۷	۶-۱- مقدمه
۹۷	۶-۲- مدل مرجع (وظیفه)
۱۰۰	۶-۲-۱- سطح فیلد
۱۰۱	۶-۲-۲- تجهیزات حوزه کنترل فرآیند
۱۰۱	۶-۲-۲-۱- تجهیزات حوزه کنترل فردی
۱۰۲	۶-۲-۲-۲- سطح کنترل گروهی
۱۰۲	۶-۲-۳- سطح کنترل فرآیند
۱۰۴	۶-۲-۳- حوزه مدیریتی و تجاری
۱۰۴	۶-۲-۴- بکارگیری مدل
۱۰۵	۶-۲-۴-۱- امنیت داده
۱۰۶	۶-۲-۴-۲- سیستم کنترلی و طبقه‌بندی آن
۱۰۷	۶-۲-۴-۳- کانال‌های تبادل داده
۱۰۸	۶-۲-۴-۴- وظایف بیکربندی سیستم
۱۰۸	۶-۲-۴-۵- وظایف خطایابی سیستم
۱۰۸	۶-۲-۴-۶- عملکرد و بیکربندی
۱۰۸	۶-۳- مدل سرویس‌گرا
۱۱۲	۶-۴- استفاده از مدل سرویس‌گرا- وظیفه‌گرا
۱۱۴	۶-۵- شناسایی آسیب‌پذیری و تهدیدات
۱۱۸	۶-۶- استفاده از درخت حمله جهت ارزیابی امنیت سیستم کنترلی Teleperm XP
۱۱۹	۶-۶-۱- روش ارزیابی توسط درخت حمله
۱۲۱	۶-۶-۲- ارزیابی کمی سیستم کنترل نیروگاه سیکل ترکیبی Teleperm XP
۱۳۲	۶-۷- ارائه راه کارهای مناسب جهت اصلاح امنیت اطلاعات

۱۳۵ فصل هفتم: نتیجه گیری و پیشنهادات
۱۳۶ ۱-۷- جمع بندی و نتیجه گیری
۱۳۷ ۲-۷- پیشنهادات
۱۳۹ پیوست ۱: استفاده از نرم افزار CSET جهت ارزیابی امنیتی سیستم کنترلی Teleperm XP
۱۴۴ منابع و مراجع

فهرست تصاویر و نمودارها

- شکل (۲-۱): ساختار کلی نیروگاه بخار ۱۵
- شکل (۲-۲): ساختار کلی یک نیروگاه گازی ۱۶
- شکل (۲-۳): ساختار کلی نیروگاه سیکل ترکیبی ۱۶
- شکل (۲-۴): ساختار کلی سیکل ترکیبی ۱۸
- شکل (۲-۵): نحوه ارتباط واحد گازی، بویلر بازیاب حرارتی و واحد بخار ۲۱
- شکل (۲-۶): نمای یک نمونه توربین بخار ساخت شرکت زیمنس مربوط به نیروگاه های سیکل ترکیبی ۲۳
- شکل (۲-۷): نحوه ی عملکرد دی اریتور ۲۵
- شکل (۳-۱): سطوح اتوماسیون در TELEPERM XP ۲۸
- شکل (۳-۲): زیر سیستم های تشکیل دهنده TELEPERM XP ۲۹
- شکل (۳-۳): سیستم اتوماسیون AS620B ۳۱
- شکل (۳-۴): مازول های متمرکز و توزیع شده ۳۴
- شکل (۳-۵): ساختار کلی OM650 ۳۵
- شکل (۳-۶): استفاده از چندین اتاق کنترل به همراه یک کنترل مرکزی ۳۶
- شکل (۳-۷): نمایش وضعیت بخشی از نیروگاه ۴۰
- شکل (۳-۸): ساختار Logها ۴۱
- شکل (۳-۹): طبقه بندی و ارزیابی انواع رویدادها ۴۵
- شکل (۳-۱۰): زیر سیستم مهندسی و نحوه ارتباط آن با سایر سیستم ها ۴۸
- شکل (۳-۱۱): نحوه ارتباط سیگنال ها میان دیاگرام وظایف و نمایش های نیروگاه ۴۹
- شکل (۳-۱۲): ساختار تجهیزات پیکربندی OM ۴۹
- شکل (۳-۱۳): دیاگرام توپولوژی جهت پیکربندی سیستم گذرگاه ارتباطی ۵۰
- شکل (۳-۱۴): شیوه نظارت و خطایابی در Teleperm XP ۵۲
- شکل (۳-۱۵): (الف) سیستم خطایابی با ترمینال مرکزی. (ب) سیستم خطایابی با ترمینال های توزیع شده ۵۳
- شکل (۴-۱): تجهیزات متصل شده به گذرگاه ارتباطی Teleperm XP ۵۶
- شکل (۴-۲): تبادل داده میان PU و سیستم خارجی نمونه ۵۹
- شکل (۴-۳): انتقال داده به سیستم OM650 ۶۰
- شکل (۴-۴): استفاده از Web4txp جهت دستیابی به سیستم کنترلی ۶۲
- شکل (۴-۵): ساختار مورد استفاده Web4txp ۶۳

۶۳ شکل (۴-۶): صفحه تایید کاربر جهت ورود به سیستم Web4txp
۶۴ شکل (۴-۷): صفحه شروع برنامه Web4txp
۶۵ شکل (۴-۸): اطلاعات جمع آوری شده از کاربران
۶۶ شکل (۴-۹): نحوه پیکربندی OPC جهت تبادل داده با سیستم کنترلی Teleperm XP
۶۷ شکل (۴-۱۰): پایش و کنترل چندین واحد در TXP توسط سرور OPC
۶۸ شکل (۴-۱۱): پیکربندی شبکه به همراه سرور پست
۶۹ شکل (۴-۱۲): ذخیره داده‌ها و گزارشات بر روی محیط‌های مختلف
۸۴ شکل (۵-۱): مراحل کلی ارزیابی ریسک امنیتی
۹۲ شکل (۵-۲): ساختار کلی سیستم کنترلی PCS 7
۹۴ شکل (۵-۳): نواحی امنیتی در سیستم کنترلی PCS7
۹۸ شکل (۶-۱): نمونه ای از مدل سازی بر اساس وظایف اشیاء (Object-role)
۹۹ شکل (۶-۲): مدل مرجع برای سیستم کنترلی Teleperm XP
۱۰۰ شکل (۶-۳): ساختار سیستم کنترلی Teleperm XP
۱۰۹ شکل (۶-۴): توصیف سیستم در قالب ارتباط میان زیرسیستم، تجهیزات و سرویس‌ها
۱۱۰ شکل (۶-۵): قسمت‌های اصلی زیر سیستم مدیریت و نظارت
۱۱۱ شکل (۶-۶): ارتباط میان سرویس‌های ارائه شده توسط OT، SU و PU
۱۱۲ شکل (۶-۷): نحوه ارتباط کاربر از طریق صفحات وب با سیستم کنترلی Teleperm XP
۱۱۳ شکل (۶-۸): ارائه مدل وظیفه‌گرا- سرویس‌گرا جهت توصیف ساختار سیستم کنترلی Teleperm XP
۱۱۹ شکل (۶-۹): (الف) برگ حمل به همراه عملگر AND. (ب) برگ حمل به همراه عملگر OR
۱۲۲ شکل (۶-۱۰): فرآیند ارزیابی ضریب آسیب پذیری سیستم
۱۲۳ شکل (۶-۱۱): درخت حمله برای سیستم کنترلی Teleperm XP
۱۲۶ شکل (۶-۱۲): آسیب پذیری محاسبه شده برای هر برگ
۱۲۸ شکل (۶-۱۳): آسیب پذیری محاسبه شده برای هر سناریو حمله
۱۳۰ شکل (۶-۱۴): درخت حمله و اقدامات امنیتی اصلاحی برای سیستم کنترلی Teleperm XP
۱۳۱ شکل (۶-۱۵): آسیب پذیری برگ حمله قبل و بعد از اصلاح امنیتی
۱۳۱ شکل (۶-۱۶): اصلاح آسیب پذیری برای هر برگ حمله
۱۳۱ شکل (۶-۱۷): آسیب پذیری سناریوهای حمله قبل و بعد از اصلاح امنیتی
۱۳۲ شکل (۶-۱۸): اصلاح آسیب پذیری برای هر سناریو حمله

- شکل (۶-۱۹): مکانسیم دفاع در عمق برای سیستم کنترلی Teleperm XP ۱۳۳
- شکل (پ-۱): مراحل ارزیابی در نرم افزار CSET ۱۳۳
- شکل (پ-۲): ساختار Teleperm XP پیاده سازی شده در نرم افزار CSET ۱۳۳
- شکل (پ-۳): نتایج حاصل از ارزیابی امنیتی توسط نرم افزار CSET ۱۳۳
- شکل (پ-۴): نتایج حاصل از ارزیابی امنیتی توسط نرم افزار CSET بعد از به کارگیری اصلاحات امنیتی ۱۳۳

چکیده:

در گذشته سیستم‌های کنترل نیروگاهی هیچ گونه تبادل داده یا اشتراک اطلاعاتی با دیگر سیستم‌ها نداشتند. اما امروزه با توجه به نیازمندی جهت بهبود کارایی، بهینه‌سازی و تصمیم‌گیری‌های سریع تجاری، این گونه سیستم‌های صنعتی جزئی از دنیای "بزرگ به هم متصل" شده‌اند و اطلاعات آنها توسط شبکه‌های داخلی، تجاری و یا حتی اینترنت قابل دست‌یابی می‌باشند. این ارتباط و انتقال داده، راه‌ها و فرصت‌های جدیدی را برای تهدید و حملات خرابکارانه علیه این گونه سیستم‌های کنترلی ایجاد نموده است. از طرفی پس از حادثه ۱۱ سپتامبر شرایط امنیتی مورد تحمل، دچار تغییرات شدیدی شده است. لذا امروزه مباحث مربوط به امنیت در شبکه‌های کنترل صنعتی و سایر زیرساخت‌های بحرانی، یکی از بحث‌های مهم و چالش برانگیز دولت‌ها می‌باشد. از طرف دیگر یکی از سیستم‌های کنترل نیروگاه‌های سیکل ترکیبی رایج در کشور، سیستم کنترلی Teleperm XP ساخت شرکت زیمنس می‌باشد. هدف از این پژوهش بیان نمودن دلایل اهمیت امنیت اطلاعات در سیستم‌های کنترل نیروگاه‌های سیکل ترکیبی با تاکید بر روی Teleperm XP، تحلیل و شناخت تمایز میان امنیت این گونه سیستم‌ها با سیستم‌های رایج IT، ارزیابی کمی و کیفی وضعیت امنیت در سیستم کنترلی Teleperm XP، راه کارها و سیاست‌های امنیتی موجود جهت بهبود امنیت اطلاعات در این سیستم کنترلی می‌باشد.

به منظور ارائه یک ارزیابی صحیح از وضعیت امنیتی سیستم کنترلی Teleperm XP از یک مدل‌سازی سرویس-گرا- و وظیفه‌گرا استفاده شده است. این مدلی که بسیار مناسب سیستم‌های کنترل صنعتی و از جمله سیستم کنترلی Teleperm XP می‌باشد، برای اولین بار و در این پایان‌نامه پیشنهاد شده است. این مدل برخلاف مدل‌های وظیفه‌گرا و یا سرویس‌گرا که به تنهایی نمی‌توانند ارتباط دقیق میان زیر سیستم‌ها، تجهیزات و سرویس‌ها را ارائه نمایند و یا اینکه دارای پیچیدگی بسیار بالا می‌باشند، ضمن داشتن سادگی لازم به خوبی می‌تواند ارتباط میان زیر سیستم‌ها، تجهیزات و سرویس‌ها را نشان دهد. بر اساس این مدل پیشنهادی اقدام به مدل‌سازی سیستم کنترلی و بررسی دقیق ارتباط میان زیر سیستم‌ها، تجهیزات و سرویس‌ها نموده و سپس با شناسایی آسیب‌پذیری‌های سیستم کنترلی و تعریف سناریوهای حمله و با استفاده از درخت حمله اقدام به ارزیابی کمی محاسبه آسیب‌پذیری کل سیستم کنترلی نموده‌ایم. نتایج حاصل از ارزیابی امنیتی سیستم کنترلی Teleperm XP نشان دهنده ضعف امنیتی آشکار در این ساختار کنترلی و عدم به کارگیری تجهیزات و سیاست‌های امنیتی مناسب، می‌باشد. قابل ذکر است که این ارزیابی براساس استانداردهای موجود در حوزه سیستم‌های کنترل صنعتی و برای اولین بار است که بر روی سیستم کنترل نیروگاه سیکل ترکیبی، Teleperm XP، موجود در کشور صورت می‌گیرد. در نهایت با توجه به اقدامات امنیتی موجود و با توجه به آسیب‌پذیری‌های شناسایی شده، اقدام به ارائه راه کارهای مناسب، جهت اصلاح امنیتی سیستم کنترلی Teleperm XP نموده‌ایم. که بایستی در به کارگیری این سیستم کنترلی مد نظر قرار گیرد.

کلمات کلیدی: سیستم کنترل نیروگاه، سیکل ترکیبی، امنیت اطلاعات، حملات خرابکارانه

فصل اول:

مقدمه

1-1- ضرورت بحث

در گذشته سیستم‌های کنترلی که شامل تمامی سیستم‌های کنترل صنعتی، کنترل فرآیند، کنترل نظارتی (SCADA¹) و کنترل توزیع شده (DCS²) و اتوماتیک می‌باشند، در یک محیط مجزا یا ایزوله شده به کار خود می‌پرداختند و هیچ گونه تبادل داده یا اشتراک اطلاعاتی با دیگر سیستم‌ها نداشتند. این گونه سیستم‌ها دارای یک سخت‌افزار، نرم‌افزار و پروتکل اختصاصی مربوط به خود بوده که جهت پایش و کنترل فرآیندهای حساس طراحی شده بودند. به دلیل محدودیت شدید در دسترسی به اطلاعات این نوع سیستم‌های کنترلی و دانش محدود درباره پروتکل‌های بکارگرفته شده جهت تبادل داده در آنها، تلاش برای برقراری امنیت شبکه‌های کنترل سیستم بسیار کم بوده و تمرکز اصلی روی خود عملیات کنترل بوده است.

امروزه به دلیل نیازمندی به تبادل داده و اطلاعات، جهت تصمیم‌گیری‌های تجاری و مالی سریع، درخواست برای دسترسی به اطلاعات بلادرنگ فرآیندها در هر نقطه و مکانی بسیار زیاد می‌باشد. این نیاز و درخواست باعث شده است تا سیستم‌های کنترل جزئی از دنیای "بزرگ و به هم متصل" شوند، جایی که اطلاعات کنترل بلادرنگ می‌تواند بسادگی توسط مدیران تجاری، مهندسین، متخصصین تعمیر و نگهداری و فروشندگان و البته توسط شبکه‌های تجاری و یا حتی اینترنت مورد استفاده قرار گیرند. این افزایش در ارتباطات خود مستلزم پذیرش و رعایت استانداردها در پروتکل‌ها و تکنولوژی بکارگرفته شده و همچنین سیستم عامل‌های مورد استفاده، می‌باشد.

اکثر سیستم‌های کنترل مدرن امروزی به شدت به سیستم عامل‌های تجاری و استانداردهای باز همانند: اترنت و تکنولوژی وب وابسته می‌باشند. از طرفی دیگر این استانداردها و ابزار ذاتاً برای محیط‌های تجاری توسعه یافته‌اند، در نتیجه این ارتباط و وابستگی باعث به وجود آمدن خطرات و تهدیداتی خواهد شد که در گذشته برای سیستم‌های صنعتی وجود نداشته است.

در سال‌های اخیر جهش زیادی در نیاز به حفظ این گونه تأسیسات صنعتی و کنترلی در مقابل فعالیت‌های تهدید آمیز موجود توسط تروریست‌ها، سازمان‌های جاسوسی یا گروه‌های تندرو بوده است. به عبارت دیگر، شرایط امنیتی مورد تحمل بعد از حملات ۱۱ سپتامبر دچار تغییرات شدیدی شده است. از طرفی دیگر، گسترش استفاده از تکنولوژی ارتباطات و انتقال، راه‌های جدیدی را برای حملات خرابکارانه باز می‌گذارد.

تجربه Stuxnet خود نشان دهنده تحولی بزرگ در فعالیت‌های تهدیدآمیز موجود برای سیستم‌های کنترل صنعتی را نشان می‌دهد. این بدافزار در اواسط تیرماه ۱۳۸۹ در سراسر جهان انتشار یافت. نخستین بار کارشناسان کامپیوتری بلاروس متوجه وجود ویروسی شدند که هدف آن سامانه‌های هدایت گر تأسیسات صنعتی با سیستم عامل

¹ Supervisory Control and Data Acquisition

² Distributed Control System

ویندوز می‌باشد. کارشناسان معتقدند طراحان این بدافزار یک منطقه جغرافیایی خاص را مدنظر داشته‌اند. طبق گزارشات منتشر شده توسط متخصصین هدف از طراحی این بدافزار دستیابی به اطلاعات صنعتی ایران می‌باشد. این بدافزار برای جلوگیری از شناسایی شدن خود از امضای دیجیتال شرکت‌های معتبر استفاده می‌کند.

با توجه به موارد ذکر شده نیاز به حفظ این گونه تأسیسات صنعتی و کنترلی در مقابل فعالیت‌های تهدیدآمیز موجود توسط تروریست‌ها، سازمان‌های جاسوسی یا گروه‌های تندرو بسیار ضروری می‌باشد. به طوری که افراد و گروه‌های مختلفی سعی در ارزیابی و تحلیل آسیب‌پذیری‌های این قبیل سیستم‌های کنترلی در مقابل حملات اطلاعاتی داشته‌اند و اقدام به بررسی و ارزیابی امنیتی سیستم‌های کنترل صنعتی و ارائه راه کارهای مناسب برای ارتقاء امنیت اطلاعات در آن، نموده‌اند.

با توجه به اهمیت امنیت اطلاعات در سیستم‌های کنترل صنعتی و از طرفی دیگر، وضعیت کشور نیازمند تحقیق و پژوهش فراوان در این حوزه امنیتی می‌باشیم. ولی متأسفانه به دلیل عدم اطلاع کافی افراد و متخصصین موجود در حوزه صنعت درباره اهمیت امنیت اطلاعات در سیستم‌های کنترل صنعتی و نتایج وخیم حاصل از حملات اطلاعاتی، این حوزه تحقیقاتی و پژوهشی مورد توجه قرار نگرفته است. از طرفی یکی از متداول‌ترین سیستم‌های کنترلی نیروگاه سیکل ترکیبی در کشور، سیستم کنترلی Teleperm XP ساخت شرکت زیمنس بوده و همواره تعداد آنها در کشور روبه افزایش می‌باشد. بنابراین با توجه به تهدیدات موجود برای این گونه سیستم‌های کنترل صنعتی و نیروگاهی، شناخت هرچه بیشتر این سیستم‌ها و تحلیل آسیب‌پذیری‌های امنیتی مربوط به آن بسیار ضروری می‌باشد. لذا در این پروژه سعی شده است تا ضمن بررسی ساختار سیستم کنترلی Teleperm XP اقدام به ارزیابی امنیتی، شناسایی آسیب‌پذیری‌ها و تهدیدات احتمالی آن در مقابل حملات اطلاعاتی بنماییم. سپس اقدامات و توصیه‌های امنیتی لازم جهت رفع و یا کاهش آسیب‌پذیری‌های این سیستم کنترلی را ارائه نماییم.

۱-۲- تهدیدات رایج امنیتی

تهدیدات امنیتی به صورت مجموعه‌ای از رویدادها یا وقایع با پتانسیل ایجاد تخریب، فاش نمودن اطلاعات محرمانه، تغییر دادن داده‌ها و یا انکار سرویس، از داخل و خارج سازمان تعریف می‌شوند. تهدیدات داخلی دارای دو منبع اصلی می‌باشند [۱]:

- رویدادهای تصادفی زمانی ایجاد می‌شوند که یک فرد ناآگاه، آموزش ندیده و یا بی‌دقت یک عملیات غیر عمدی را انجام دهند. در اکثر موارد، این گونه حوادث ناشی از سیاست‌ها یا فرآیندهای غلط، تصدیق هویت و محدودیت دسترسی نادرست و یا اشتراک نام کاربری و کلمه عبور، می‌باشند.
- رویدادهای برنامه ریزی شده که توسط افراد یا گروه‌ها و با یک برنامه‌ریزی و آگاهی کافی از سیستم کنترلی مورد نظر صورت می‌گیرد.

تهدیدات خارجی سیستم‌های کنترلی به صورت زیر طبقه‌بندی می‌شوند:

- نرم‌افزارهای مخرب^۱: تمامی سیستم‌های اطلاعاتی و سیستم‌های کنترلی به طور بالقوه در معرض آسیب-پذیری ناشی از ویروس‌ها، کرم‌ها، تروجان‌ها و نرم‌افزارهای جاسوسی می‌باشند. حملات ناشی از این قبیل تهدیدات می‌تواند باعث مسدود کردن و خرابی مسیر تبادل داده، نصب نرم‌افزارهای خارجی و یا خاموشی اجباری در سیستم‌های کنترل صنعتی شود.
- هکر^۲: افرادی که علاقه‌مند به جست و جو مراکز اطلاعاتی، ایجاد مزاحمت و کنترل سیستم‌ها به منظور ایجاد مشکل و یا کسب شهرت می‌باشند.
- تروریست^۳: این قبیل تهدیدات خارجی، سیستم‌های بحرانی را شناسایی کرده و اطلاعات آنها را به سرقت برده و یا تخریب می‌نمایند. این نوع تهدید خارجی، بزرگ‌ترین نگرانی دولت‌ها می‌باشند.

۱-۳- نتایج حملات امنیتی در سیستم‌های کنترل صنعتی

ارزیابی پیامدها و نتایج حملات اطلاعاتی در محیط‌های صنعتی به سادگی یک برآورد مالی ناشی از یک واقعه نمی‌باشد. برای سیستم‌های کنترل نیروگاهی و تولیدی که اغلب به طور مستقیم به شبکه‌های انتقال و تولید انرژی الکتریکی و فرآیندها متصل شده‌اند وقوع یک رویداد امنیتی می‌تواند نتایج وخیمی از قبیل خطرات امنیت عمومی، زیست محیطی و یا از دست رفتن اطلاعات محرمانه، از دست رفتن محصول و تولید، تخریب تجهیزات و از دست رفتن اعتماد عمومی گردد. این باعث می‌شود تا نتایج یک حمله اطلاعاتی به تجهیزات صنعتی بسیار بیشتر از یک ضرر مالی باشد. اگر چه تأثیرات مستقیم مالی (مانند از دست رفتن تولید و یا خرابی دستگاه) وجود دارد ولی برای اغلب کمپانی‌ها، ضربه وارده به اعتبار و آبروی آنها با اهمیت‌تر از هزینه‌های حاصل از قطع تولید می‌باشد. ضربه به سلامت و اعتبار نشان تجاری یک کمپانی می‌تواند بسیار زیان‌بار باشد. از جمله برخی دیگر از پیامدهای حملات اطلاعاتی به سیستم کنترل نیروگاهی سیکل ترکیبی می‌توان به موارد زیر اشاره نمود:

- عدم دسترسی به منابع، از قبیل شبکه تجاری و یا شبکه کنترل نیروگاهی
 - از دست رفتن اختیار تجهیزات و کنترل کننده‌ها
- گسترش ویروس به کل سیستم می‌تواند باعث از دست رفتن کنترل HMI و یا تخریب بایگانی فرآیند و یا با ارائه یک تصویر غلط از وضعیت نیروگاه منجر به از دست رفتن کنترل و حتی به خطر افتادن جان افراد گردد. در نتیجه شدت این نتایج، کاملاً واضح است که تلاش جهت حفاظت سیستم‌های کنترل صنعتی و نیروگاهی بسیار ضروری می‌باشد.

¹ Malware

² Hacker

³ Terrorist