Security of industrial control systems without human operator

Mohammad hosien Eslamian [1], Ali Yazdani [2], Ali Soltanirenani [3], Mohsen Jafarzadeh [4], Vahid Farhadian [2]

[1] Department of civil Engineering, Shahed University of Tehran, Tehran, Iran
[2] Department of Electrical Engineering, Shahed University of Tehran, Tehran, Iran
[3] Faculty of Humanities, Department of Industrial Management, Shahed University of Tehran, Tehran, Iran
[4] Islamic azad university, ilam branch, ilam, iran
E-mails: mhossein.eslamian@shahed.ac.ir, alisepahani7799@gmail.com, alisoltanirenani.1999@gmail.com, jafarzadehmosen@yahoo.com, vahidfarhadiyanbabadi@gmail.com

Abstract
The emergence and increasing development of industrial control systems and their increasing use in important industrial facilities and units as well as large factories make the need to manage, operate and control them with minimal human intervention one of the most important and debatable issues in This field has become. One of the important topics in this field is the issue of threats against the network of industrial control systems and cyber attacks. The purpose of this article is a general introduction to the types of cyber threats and attacks on industrial infrastructures as well as The methods to deal with it are so that the importance of establishing a security system for industrial units is better understood by the readers. Also, considering the increase in the use of automatic industrial control systems and the reduction of the intervention of human factors, the emphasis of this article on the systems It is fully automatic.

Keywords
Industrial Control Systems, Programmable Logic Controller, SCADA, Sensors.

امنیت سیستم های کنترل صنعتی بدون اپراتور انسانی

محمدحسین اسلامیان[۱] ، علی یزدانی باغملکی[۲]، علی سلطانی رنانی[۳]، محسن جعفرزاده[۴]، وحید فرهادیان[۲]

[۱] دانشگاه شاهد تهران، دانشکده فنی و مهندسی، گروه مهندسی عمران

[۲] دانشگاه شاهد تهران، دانشکده فنی و مهندسی، گروه مهندسی برق

[۳] دانشگاه شاهد تهران،دانشکده علوم انسانی،گروه مدیریت

[۴] دانشگاه آزاد اسلامی،واحد ایلام،گروه مهندسی کامپیوتر

ایمیل نویسندگان: mhossein.eslamian@shahed.ac.ir, alisepahani7799@gmail.com, alisoltanirenani.1999@gmail.com, jafarzadehmosen@yahoo.com, vahidfarhadiyanbabadi@gmail.com

چکیده

ظهور و توسعه روز افزون سیستم های کنترل صنعتی و بکارگیری بیش از پیش آنها در تاسیسات و واحد های مهم صنعتی و همچنین کارخانجات بزرگ،نیاز به مدیریت،بهره بداری و کنترل آنها با کمترین دخالت انسانی را به یکی از مسائل مهم و قابل بحث در این حوزه تبدیل کرده است.یکی از مباحث مهم در این زمینه،موضوع تهدیدات علیه شبکه سیستم¬های کنترل صنعتی و حملات سایبری می باشد.هدف از این مقاله،یک آشنایی کلی با انواع تهدیدات سایبری و حملات به زیر ساخت های صنعتی و نیز روش های مقابله با آن می باشد تا اهمیت برقراری یک سیستم امنیتی برای برای واحد های صنعتی بهتر و بیشتر برای خوانندگان درک شود.همچنین با توجه به افزایش استفاده از سیستم های اتوماتیک کنترل صنعتی و کاهش دخالت عوامل انسانی،تاکید این مقاله بر سیستم های از نوع تمام اتوماتیک می باشد.

کلمات کلیدی

سیستم های کنترل صنعتی، کنترل کننده های منطقی، اسکادا، سنسورها.

نام نویسنده مسئول: محمدحسین اسلامیان

ایمیل نویسنده مسئول: mhossein.eslamian@shahed.ac.ir

تاریخ ارسال مقاله: ۱۴۰۲/۰۳/۲۰

تاریخ(های) اصلاح مقاله: ۱۴۰۲/۰۳/۳۱

تاریخ پذیرش مقاله: ۱۴۰۲/۰۴/۰۱

۱- مقدمه

امروزه با توسعه سیستم های کنترل صنعتی و کاربرد های بیش از پیش آن در صنایع، پیشرفت های زیادی در سرعت،دقت و بهروری در زیرساخت های اساسی و حیاتی یک کشور مانند تامین انرژی،آب،بخش حمل و نقل،فناوری اطلاعات و ... را می توان مشاهده کرد .وجود یک سیستم اتوماتیک کنترل و پایش در تاسیسات مذکور، مدیریت بهینه ای را فراهم می سازد.بسیاری از این زیرساخت ها نقش حیاتی را در یک کشور را بازی میکنند و کوچکترین اختلال در انها میتواند عواقب جبران ناپذیری را در اقتصاد و امنیت یک کشور وارد آورد. ساختار کنترل سیستم های صنعتی،به منظور افزایش کارایی و قابلیت اطمینان از طریق اتوماسیون شبکه و به صورت هوشمند انجام می پذیرد اما استفاده از این قابلیت باعث در معرض قرار گرفتن این سیستم در برابر حملات سایبری و بدافزارها می شود. از این رو توسعه سیستم های کنترل صنعتی که در در برابر این گونه حملات ایمن هستند بسیار حائز اهمیت است[۱]برای حل چالشهای موجود در حوزه اتوماسیون و کنترل صنعتی، صنایع از فناوری های در حال توسعه در سیستمهای کنترلی به منظور افزایش راندمان،تولید کارآمد و سایر فرایند های تولیدی استفاده می کنند. این مسئله نیاز به سیستم های کنترل با کیفیت بالا و قابل اعتماد را آشکار می سازد. روش ها و مدلهای جدید اتوماسیون صنعتی با جدیدترین دستگاههای کنترل و پروتکلهای ارتباطی برای کنترل دستگاه هایی با کاربرد های میدانی مانند شیرهای کنترل ونیز سایر عناصر کنترل نهایی سروکار دارند. برخی از دستگاهها و ابزارهای هوشمند مورد استفاده در صنایع اتوماتیک توانایی کنترل فرایندها و همچنین قابلیت های ارتباطی رابط بدون ارتباط با سایر دستگاههای کنترل سطح میدانی مانند سیستم های کنترلگر منطقی برنامه پذیر(PLC) را دارند. شبکه های قدرت، سیستم هایی هستند که در آن حلقه های کنترل بر روی شبکه های ارتباطی بسته می شوند، یک کلاس مهم از سیستم های کنترل شبکه ای (NCS) را نشان می دهند. برخلاف سایر سیستم‌های فناوری اطلاعات که امنیت سایبری عمدتاً شامل رمزگذاری و حفاظت از داده‌ها است، در اینجا حملات سایبری ممکن است فرآیندهای فیزیکی را از طریق کنترل‌کننده‌های دیجیتال تحت تأثیر قرار دهند. بنابراین تمرکز بر رمزگذاری داده ها به تنهایی ممکن است برای تضمین امنیت کلی سیستم، به ویژه اجزای فیزیکی آن کافی نباشد. به منظور افزایش انعطاف پذیری این سیستم ها، نیاز به ابزارهای مناسب برای درک و سپس محافظت از NCS در برابر حملات سایبری است.

عواملی که موجب اختلال در عملکرد عادی این سیستم ها می شود، به دو دسته تقسیم می شوند که شامل عوامل عمدی و غیرعمدی می شوند. اما اصلی ترین تهدید علیه این سیستم ها عوامل عمدی هدف دار است که در گذشته به صورت فیزیکی و امروزه به صورت سایبری انجام می پذیرد.مفهوم عبارت فناوری عملیاتی (OT) به مجموعه ای از فناوری ها، نرم افزارها و سخت افزارها اطلاق می شود که به طور مستقیم با تولید، حمل و نقل و تحول دارایی¬ها در ارتباط هستند. در واقع، این موضوع به هر آنچه که مربوط به حوزه سیستم های نظارت و کنترل سیستم های تولیدی بوده و همچنین با اختصارات دیگر به عنوان

سیستم کنترل نظارت و جمع آوری داده (SCADA) و PLC مشخص شده است ، اشاره دارد. طی چند سال گذشته، OT به طور گسترده ای از فناوری¬های IT (فناوری اطلاعات) پیشی گرفته است، و به تدریج به دلیل ارائه راه حل¬های مبتنی بر ساختارهای عمل گرایانه توانایی بالاتر خود را اثبات کرده است. همانطور که، مشابه مزایای انکارناپذیری که در زندگی روزمره خود از نظر بهبود کیفیت ، تولید و مقرون به صرفه بودن و نیز تولیداتی متفاوت از موارد پیشین مشاهده کرده ایم، آسیب پذیری و تهدیدهای ذاتی فناوری اطلاعات در حوزه OT امری ملموس و قابل تامل است. مسئله مورد بررسی این است که فرایند های OT دارای چندین ویژگی است که انتقال اقدامات حفاظتی که معمولاً برای سیستم های IT اتخاذ می شود را آسان نمی کند. به عنوان مثال، شبکه های قدرت از طریق سیستم های SCADA که با مجموعه ای از نرم افزارهای کاربردی خاص تکمیل می شود، که معمولاً سیستم های مدیریت انرژی (EMS) نامیده می شوند، اداره می شوند. EMS مدرن پشتیبانی اطلاعاتی را برای انواع برنامه های مربوط به نظارت و کنترل شبکه قدرت ارائه می دهد. برآوردگر وضعیت سیستم قدرت (PSSE) یک برنامه کاربردی آنلاین است که از اندازه گیری های اضافی و یک مدل شبکه استفاده می کند تا یک تخمین وضعیت دقیق را در همه زمان ها به EMS ارائه دهد. PSSE به ابزاری جدایی ناپذیر برای EMS تبدیل شده است، به عنوان مثال برای جریان بهینه توان با محدودیت اقتضایی. PSSE همچنین اطلاعات مهمی را برای الگوریتم های قیمت گذاری ارائه می دهد. سیستم های اسکادا داده ها را از واحدهای پایانه راه دور (RTUs) نصب شده در پست های مختلف جمع آوری می کنند و اندازه گیری های جمع آوری شده را به ایستگاه اصلی مرکزی واقع در مرکز کنترل رله می کنند. چندین حمله سایبری به سیستم های SCADA در شبکه های قدرت عامل گزارش شده است و خاموشی های عمده، به عنوان خاموشی شمال شرق آمریکای شمالی در اوت ۲۰۰۳، با سوء استفاده از سیستم های SCADA بدتر شده است. خاموشی سال ۲۰۰۳ همچنین نیاز به برآوردگرهای قوی حالت را برجسته کرد که در چنین شرایط شدید به طور دقیق و سریع همگرا شوند تا اقدامات پیشگیرانه لازم را بتوان به موقع انجام داد.آسیب پذیری های متعددی در معماری سیستم SCADA وجود دارد، از جمله دستکاری مستقیم RTU ها، پیوندهای ارتباطی از RTU به مرکز کنترل، و نرم افزار فناوری اطلاعات و پایگاه های داده در مرکز کنترل [۴].

۲- مانواع تهدیدات سیستم های کنترل صنعتی

امنیت،در سیستم کنترل کننده های منطقی یا به اختصار PLC، سامانه های کنترل توزیع شده(DSC) و پروتکل های ارتباطی در شبکه های سامانه های کنترل صنعتی و SCADA که تمرکز اصلی آنها در جهت افزایش سرعت و سادگی تامین امنیت طراحی شده است، به اندازه کافی در ساختار آنها مورد توجه واقع نشده و در مقابل حملات سایبری بسیار اسیب پذیراند و به همین دلیل استفاده ی روز افزون از سیستم های کنترل صنعتی وهچنین استفاده از ان در زیرساخت های حیاتی یک کشور موجب جلب توجه هرچه بیشتر مهاجمین شده است که می توان تعدادی از این تهدیدات را که به شرح زیر است نام برد:

- بدافزار ها و ویروس ها
- هکرها و افراد سودجو که از راه دور به سیستم دسترسی پیدا می کنند
- رخنه به درون سامانه های اپراتوری سیستم

-

از طرفی باید خاطر نشان کرد که عوامل ایجاد تهدید نیز می تواند غیر عمدی باشد مانند:

- اسیب دیدن سیستم ها در اثر حوادث طبیعی(زلزله، سیل و...)
- خطا های اپراتوری در زمان استفاده از سیستم
- اشتباهات در هنگام نصب، تعمیر و نگهداری

۱-۲- انواع روش های آسیب رسانی به واحد ها

۱-عملیات فریب (تزریق داده های غلط)

در این نوع از حمله، مهاجم با دستکاری خروجی سنسورها می تواند سیستم کنترل را فریب دهد و این سیستم ،داده های نادرست را به کنترل کننده ها ارسال کند و باعث اختلال در عملکرد درست این سسیستم شود. این نوع عملیات ها برای اولین بار توسط اقای Liu برای آسیب رسانی به سیستم قدرت و سامانه های تشخیص داده های غلط آن طرح ریزی شد[۲,۳]. در منابع[۴,۵] گفته شده است که حتی مهاجمان با داشتن اطلاعات نسبی می توانند یک آسیب رسانی با درصد موفقیت بالا را نیز طرح ریزی کنند. منبع [۶] به ما می گوید که برای حفاظت از سیستم،رمزگذاری تمامی داده های خروجی عملی مقرون به صرفه نیست و میتوان فقط با حفاظت از تعدادی از این داده های خروجی از حمله ی موفقیت امیز تزریق داده ی غلط جلوگیری کرد.

۲-عملیات بازسازی اطلاعات

در این نوع از آسیب رسانی، عملگر آسیب رسان داده های دریافتی از سنسور های سیستم را در شرایط نرمال آن دریافت و ذخیره کرده و در زمان وقوع عملیات، اطلاعات را برای شبکه ی کنترل ارسال می کند[۷]. بدینگونه سیستم کنترلی، فریب خورده و سیستم به حالتی می رود که بروز خطا و آسیب به تجهیزات حتمی می باشد.یکی از راههای مقابله با این گونه از حملات، اضافه کردن ورودی های تصادفی با میانگین صفر به ورودی سیستم است[۸]. ورودی تصادفی نوعی پالس تایید هویت است و سعی بر این است که به صورتی بهینه طراحی شود تا کمترین تاثیر را روی راندمان سیستم داشته باشد[۹].

۳- عملیات آسیب زایی نهان

در این نوع از عملیات ها، خروجی آن به صورت حلقه بسته بازسازی می شود تا تاثیر آن بر اطلاعات دریافتی از سنسور ها از بین برود و عملیات به صورت مخفیانه باقی بماند. در این نوع از رخنه ها، سیستم نفوذ کننده باید شناخت کافی از مدل فیزیکی سیستم داشته باشد تا بتواند مدلی مشابه آن را شبیه سازی کند. سیستم آسیب زا،مدل شبیه سازی شده و کنترل کننده ی مورد نظر را بین سیستم وکنترل کننده ی اصلی قرار داده و با ارسال همزمان پالس های دلخواه به ورودی کنترل کننده ی اصلی و سیستم تحت کنترل،عملیات را مخفی نگه می دارد[۱۰].

۴- ایجاد اخلال در مسیر ارسال اطلاعات در شبکه کنترل و حذف امکان کنترل اپراتورهای سیستم کنترل به شبکه

۵- ایجاد تغییرات غیرمجاز در برنامه PLCها، RTUها، DCS، یا اسکادا

۶- دخالت در عملکرد سیستم های ایمنی

۳- روش های مقابله با تهدیدات

برای اسیب رساندن به سیستم باید دسترسی فیزیکی یا شبکه ای به سیستم کنترل صنعتی داشته باشیم تا بتوانیم کنترل ان را در اختیار بگیریم. بنابراین مهم ترین هدف مقابله با تهدید جلوگیری کردن از دسترسی غیرمجاز است که راهکار های متعددی برای این کار وجود دارد. از جمله راههای مفید که اخیرا استفاده شده است، استفاده از ابزارهای مبتنی بر هوش محاسباتی می¬باشد . یک اقدام امنیتی مرسوم استفاده از ارتباطات رمزگذاری شده است، اما کلیدهای رمزنگاری می توانند شکسته یا دزدیده شوند، یا مهاجم می تواند مستقیماً به عناصر فیزیکی سیستم حمله کند، بدون اینکه ارتباطات را برباید. چنین حملاتی زمانی امکان پذیر است که حسگرها و محرک ها در مکان های دور توزیع شده باشند. بنابراین، دانش سیستم و امنیت سایبری برای اطمینان از عملکرد ایمن سیستم های فیزیکی-سایبری (CPS) ضروری است. در ادامه

تعدادی از این راه کارها بیان شده است.

۱-۳- راهکارهای مرتبط با سیستم کنترل

در این قسمت برخی راهکارهای موجود جهت استفاده در سیستم¬های کنترل صنعتی بیان شده¬اند.

-استفاد از سیستم عامل های امن و مطمئن مانند لینوکس

-استفاده از نرم افزار و سخت افزارهای معتبر

-استفاده از روش های رمزنگاری

در ادامه برخی روش های مرتبط با شبکه بیان می¬شوند.

– جداکردن شبکه داخلی سیستم از اینترنت

– استفاده از پروتکل‌های ارتباطی امن

– استفاده از پروتکل‌های اختصاصی در موارد بسیار حساس

راهکارهای مرتبط با افراد

-اموزش پرسنلین

-نظارت مستمر بر پرسنلین

-واکنش و نظارت بر رفتارهای مشکوک

۴- پایش سیستم و تخمین وضعیت

نظارت سیستم برای اطمینان از عملکرد قابل اعتماد شبکه های انرژی ضروری است. این اطلاعات مربوط به وضعیت یک شبکه برق بر اساس قرائت کنتورهای قرار داده شده در اجزای مهم یک شبکه برق، مانند پست ها، ارائه می دهد. اندازه‌گیری‌های کنتور ممکن است شامل ولتاژ شین، تزریق توان واقعی و راکتیو شین، و جریان‌های توان راکتیو انشعاب در هر زیرسیستم شبکه برق باشد.

این اندازه‌گیری‌ها معمولاً به یک مرکز کنترل منتقل می‌شوند، جایی که کارکنان مرکز کنترل، با کمک رایانه‌ها، داده‌های مهم سیستم را جمع‌آوری می‌کنند و قابلیت نظارت و کنترل متمرکز را برای شبکه برق فراهم می‌کنند. اندازه گیری ها معمولاً در یک سیستم تله متری ذخیره می شوند که به نام سیستم کنترل نظارت و جمع آوری داده (SCADA) نیز شناخته می شود[۲]. (CPS) سیستم هایی با هماهنگی دقیق بین عناصر محاسباتی و فیزیکی هستند [۱] . چنین سیستم هایی اغلب از شبکه های توزیع شده از حسگرها و محرک های تعبیه شده استفاده می کنند که با محیط فیزیکی تعامل دارند و توسط یک سیستم کنترل نظارتی و جمع آوری داده ها (SCADA) نظارت و کنترل می شوند. کنترل ترافیک هوایی (ATC)، نظارت پزشکی، و غیره.

تخمین حالت از مدل های جریان توان استفاده می کند. مدل جریان برق مجموعه ای از معادلات است که جریان انرژی را در هر خط انتقال یک شبکه برق نشان می دهد. مدل جریان برق AC یک مدل جریان توان است که هم توان واقعی و هم توان راکتیو را در نظر می گیرد و با معادلات غیر خطی فرموله می شود. تخمین حالت با استفاده از مدل جریان برق AC می تواند از نظر محاسباتی گران باشد و همیشه به یک راه حل همگرا نمی شود.[۱۱-۱۷]

۵- نتیجه گیری

در این مقاله قصد ما بررسی مهم‌ترین مسائل مربوط به امنیت سیستم های کنترل صنعتی بوده است. با توجه به گسترش ویروس کرونا مسئله استفاده از سیستم های کنترل صنعتی با کمترین دخالت و حضور انسان بیش از پیش احساس شده است و با گسترش این سیستم ها و استفاده از از انها در زیرساخت های حیاطی کشور، مسأله‌ی امنیت سیستم های کنترل صنعتی نیز بیش پیش احساس خواهد شد بنابراین استفاده از هر سیستم کنترل صنعتی، در هر واحد صنعتی حساس، نیازمند بررسی‌های امنیتی سخت‌گیرانه می‌باشد.و هرگونه خلل یا اسیب به این سیستم می تواند عواقب جدی را متوجه کشور کند که این امر باعث با اهمیت شمرده شدن مسئله امنیت این سیستم ها می شود.

مراجع

[1] G. Manimaran, A. Hann, and P. Sauer, “Cyber-physical systems security for smart grid,” Future Grid Initiative White Paper, Power systems engineering research center publication (PSERC), 2012.

[2] Liu, Yao, Peng Ning, and Michael K Reiter, “False Data Injection Attacks against State Estimation in Electric Power Grids”, ACM Transactions on Information and System Security (TISSEC), 2011. Vol. 14, No. 1, pp. 13.

[3] Yao Liu, Peng Nin, Michael K. Reiter, “False Data Injection Attacks against State Estimation in Electric Power Grids”, National Science Foundation (NSF), 2009.

[4] Teixeira, André, Saurabh Amin, Henrik Sandberg, Karl Henrik Johansson, and Shankar S. Sastry, “Cyber Security Analysis of State Estimators in Electric Power Systems” 49th IEEE Conference on Decision and Control (CDC), 2010, pp. 5991-5998,.

[5] Liu, Xuan and Zuyi Li, "Local Load Redistribution Attacks in Power Systems with Incomplete Network Information", IEEE Transactions On Smart Grid, July 2014, Vol. 5, pp. 1665-1676.

[6] Bobba, Rakesh B., Katherine M. Rogers, Qiyan Wang, Himanshu Khurana, Klara Nahrstedt, and Thomas J. Overbye, "Detecting False Data Injection Attacks on dc State Estimation”, Preprints of the First Workshop on Secure Control Systems, CPSWEEK, 2010.

[7] Mo, Yilin and Bruno Sinopoli. “Secure Control against Replay Attacks”, 47th Annual Allerton Conference on Communication, Control, and Computing, 2009, pp. 911-918

[8] Bruno Sinopoli, Yilin Mo, “Secure Control against Replay Attacks”, Trust Autumn 2009 Conference, 2009.

[9] Chabukswar, Rohan, Yilin Mo, and Bruno Sinopoli, “Detecting Integrity Attacks on SCADA Systems”, Proceedings of the 18th IFAC World Congress, Milano, Italy, 2011, pp. 11239-11244

[10] Smith, Roy S., “A Decoupled Feedback Structure for Covertly Appropriating Networked Control Systems”, Network, Vol. 6, 2011.

[11] Mohammadi F, Mohammadi-Ivatloo B, Gharehpetian GB, Ali MH, Wei W, Erdinç O, Shirkhani M. Robust control strategies for microgrids: A review. IEEE Systems Journal. 2021 Jun 8.

[12] Aazami R, Heydari O, Tavoosi J, Shirkhani M, Mohammadzadeh A, Mosavi A. Optimal Control of an Energy-Storage System in a Microgrid for Reducing Wind-Power Fluctuations. Sustainability. 2022 May 19;14(10):6183..

[13] Iranmehr H, Aazami R, Tavoosi J, Shirkhani M, Azizi AR, Mohammadzadeh A, Mosavi AH, Guo W. Modeling the price of emergency power transmission lines in the reserve market due to the influence of renewable energies. Frontiers in Energy Research. 2022 Jan 13;9:944..

[14] Huang H, Shirkhani M, Tavoosi J, Mahmoud O. A new intelligent dynamic control method for a class of stochastic nonlinear systems. Mathematics. 2022 Apr 22;10(9):1406 .

[15] Tavoosi J, Shirkhani M, Azizi A, Din SU, Mohammadzadeh A, Mobayen S. A hybrid approach for fault location in power distributed networks: Impedance-based and machine learning technique. Electric Power Systems Research. 2022 Sep 1;210:108073 .

[16] Danyali S, Aghaei O, Shirkhani M, Aazami R, Tavoosi J, Mohammadzadeh A, Mosavi A. A New Model Predictive Control Method for Buck-Boost Inverter-Based Photovoltaic Systems. Sustainability. 2022 Sep 19;14(18):11731.

[17] Tavoosi J, Shirkhani M, Abdali A, Mohammadzadeh A, Nazari M, Mobayen S, Asad JH, Bartoszewicz A. A new general type-2 fuzzy predictive scheme for PID tuning. Applied Sciences. 2021 Nov 5;11(21):10392.

[18] Guo X, Shirkhani M, Ahmed EM. Machine-Learning-Based Improved Smith Predictive Control for MIMO Processes. Mathematics. 2022 Oct 9;10(19):3696.

[19] Tavoosi J, Shirkhani M, Azizi A. Control engineering solutions during epidemics: A review. International Journal of Modelling, Identification and Control. 2021;39(2):97-106.