دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۱، جلد ۲۰، شماره ۱ (۱۰-۱۷)
https://monadi.isc.org.ir

ارائه‌شده در هجدهمین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه اصفهان، ۱۰ و ۱۱ شهریور ۱۴۰۰

الزامات امنیت سایبری پست‌های فوق توزیع بدون اپراتور★

اعظم مظفری*، لیلا ظفری و نگین حامیان

پژوهشگاه نیرو، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
الزامات امنیت سایبری
پست‌های فوق توزیع بدون اپراتور

dor: 20.1001.1.24763047.1401.11.1.2.9

نوع مقاله: پژوهشی

چکیده

بهره‌برداری پست‌های فوق توزیع بدون اپراتور، اگرچه از منظر اقتصادی و فنی مورد توجه مدیران صنعت برق است، فرصت مناسبی است که از نظر امنیت سایبری مورد بررسی دقیق قرار گیرد. در این مقاله ضمن بیان اهمیت توجه به امنیت سایبری مراکز اسکادا، الزامات امنیت سایبری دو نوع DCS و سنتی پست‌های فوق توزیع، ارتباطات این نوع پست‌ها و مرکز اسکادا مربوطه مورد بررسی قرار گرفت. در این مقاله سعی شد بر اساس مستندات و استانداردهای امنیت سایبری صنعتی و صنعت برق، الزامات امنیتی پست‌ها و ارتباطات آنها با مراکز مربوطه استخراج گردد و این الزامات بر اساس شناخت از صنعت و اهمیت بخش‌ها و فرایندهای موجود اولویت‌بندی گردید. ضمن آنکه با توجه به عدم اجرای الزامات امنیتی در پست‌های فشار قوی در کشور، توجه به ملاحظات امنیتی این حوزه از جمله انجام مدیریت مخاطرات امنیتی، توجه به آموزش نیروی انسانی و دریافت تاییدیه‌های امنیتی تاکید گردید.

© ۱۴۰۱ انجمن رمز ایران

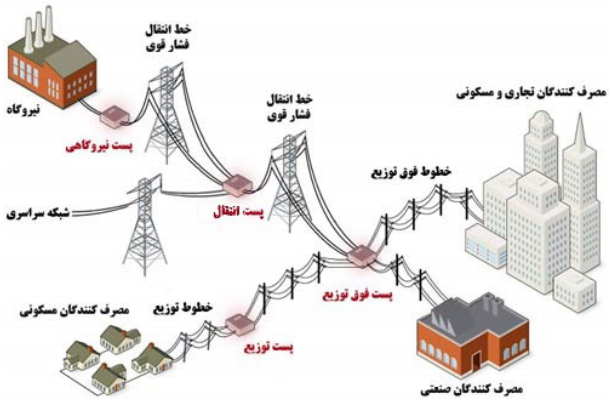
۱ مقدمه

خودکارسازی عملیات در کلیه صنایع من‌جمله صنعت برق همواره مدنظر بوده و امروزه با توجه به رویکرد شبکه هوشمند در صنعت برق بیش از پیش مورد توجه و انتظار است. یکی از مواردی که از سالها قبل و با توسعه هوشمندسازی شبکه برق مورد توجه قرار گرفته، بهره‌برداری از پست‌های فوق توزیع بدون حضور اپراتور [1] است. این بدین معنا است که با استفاده از زیرساخت‌های مخابراتی و توانمندی حوزه IT و برنامه‌های متعدد هوشمندسازی، این پست‌ها بدون اپراتور بهره‌برداری گردند و پایش وضعیت موجود در پست و در صورت لزوم اعمال فرامین کنترلی جهت بهره‌برداری صحیح پست از مرکز مرتبط و بدون حضور نیروی انسانی صورت گیرد.

پست‌های انتقال، به عنوان مهمترین پست‌ها در صنعت برق از ابتدا توسط نرم‌افزار اسکادا پایش و نظارت شده و علاوه بر آن اپراتور مسئول، در پست حضور شبانه‌روزی داشته است. در این پست‌ها در صورت لزوم به اعمال فرمان، این دستور که از مرکز اسکادا صادر می‌گردد، توسط مسئول یا اپراتور حاضر در پست اجرا می‌گردد. علیرغم بهره‌برداری تعداد محدودی از پست‌های فوق توزیع بدون حضور اپراتور در کشور، در بیشتر پست‌های فوق توزیع با توجه به اهمیت آنها و سطح پوشش برق‌رسانی مشترکین توسط این پست‌ها، اپراتور در پست حضور دارد و در صورت وقوع حادثه، با هماهنگی و دستور مرکز کنترل عملیات مورد نیاز را انجام می‌دهد. اما از مدت‌ها قبل، پیشنهاد بهره‌برداری بدون اپراتور پست‌های فوق توزیع همانگونه که برای پست‌های توزیع انجام می‌گردد، در شرکت توانیر مطرح شده و یکی از دلایل این امر مدیریت هزینه‌ها با کاهش نیروی انسانی مستقر در پست بوده است. در طول یک شیفت کاری

★از کمیته علمی هجدهمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول
آدرس‌های رایانامه: amozafari@nri.ac.ir (اعظم مظفری)، lzafari@nri.ac.ir (لیلا ظفری)، nhamain@nri.ac.ir (نگین حامیان)
© ۱۴۰۱ تمامی حقوق متعلق به انجمن رمز ایران است.

[1] unmanned



شکل ۱. جایگاه پست‌های فوق توزیع در شبکه برق

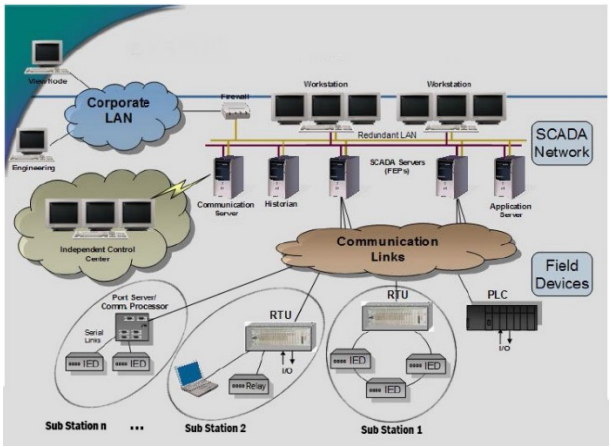
در پست‌های فشارقوی معمولی، اپراتورهایی با سطوح مختلف مهارتی، مشغول به انجام وظیفه هستند که امکان اشتباه و خطای انسانی نیز در آن‌ها وجود دارد و این در حالی است که کنترل پست‌ها به صورت متمرکز و به صورت خودکار، خطای انسانی را کاهش داده و انجام دستورات کنترلی را سریع‌تر امکان‌پذیر می‌سازد. نکته مثبت دیگر این سیاست، امکان بهره‌برداری از نیروی متخصص مستقر در پست در مراکز کنترل و دیگر موقعیت‌هایی است که نیاز به دانش آن‌ها وجود دارد [۱].

شکل ۱ جایگاه پست‌های فوق توزیع را در شبکه برق ازسطح تولید تا مصرف نشان می‌دهد.

در بهره‌برداری بدون اپراتور از پست‌های فوق توزیع، توجه به این نکته مهم است که با حذف اپراتور در این نوع از پست‌ها، اهمیت پایش منظم و دقیق آنها توسط مراکز کنترل از اهمیت بیشتری برخوردار می‌گردد. در این حالت حساسیت فرامین مراکز کنترل بیشتر شده و بالطبع بار مسئولیت و حساسیت کار اپراتورهای مراکز نیز افزایش خواهد یافت. در پست‌های بدون اپراتور عملیات پایش و کنترل باید به صورت خودکار و بدون اپراتور انجام شود. در این حالت و از آنجا که انجام بسیاری از فرامین به حالت خودکار تغییر یافته، امنیت در این نوع پست‌ها نیز از اهمیت بیشتری برخوردار می‌گردد؛ زیرا در پست‌های با اپراتور، انجام فرامین توسط اپراتور انجام می‌گیرد و این امر باعث بررسی مجدد فرمان توسط اپراتور می‌گردد، در صورتی که در پست‌های بدون اپراتور، در صورت تغییر دستورات و فرامین در حین انتقال مشکلات عدیده‌ای به وجود خواهد آمد.

بحث پیرامون امنیت سایبری پست‌های فوق توزیع بدون اپراتور، بحث بسیار مبسوط، مهم و در برخی موارد بسیار پیچیده است. پیچیدگی آن از این جهت است که از ابتدا بحث امنیت سایبری در سامانه دیسپاچینگ فوق توزیع مورد توجه نبوده است و اکنون با حذف اپراتور در این پست‌ها، نباید تنها به الزامات امنیتی پستی که اپراتور در آن حضور ندارد، پرداخت؛ بلکه پارامترها و عوامل بسیاری که قبلا به آن توجه نشده است، به عنوان عوامل تاثیرگذار حضور دارند و بررسی موضوع را پیچیده می‌نمایند.

در این مقاله، ابتدا کلیاتی از سامانه اسکادای فوق توزیع و اهمیت امنیت در کلیه اجزاء ارائه شده، سپس انواع پست‌های فوق توزیع بیان



شکل ۲. اجزای سامانه اسکادای فوق توزیع

شده و به بررسی الزامات امنیتی انواع پست‌ها و ارتباطات آنها پرداخته شده است. در انتها توصیه‌های امنیتی جهت ارتقاء جایگاه امنیت در این سامانه مورد بررسی قرار گرفته و پیشنهادات لازم ارائه گردیده است.

۲ سامانه اسکادای فوق توزیع

قبل از آنکه الزامات امنیت سایبری پست‌های فوق توزیع مورد بررسی قرار گیرد و از آنجا که این پست‌ها در یک سامانه جامع پایش و کنترل مورد بهره‌برداری هستند، به طور خلاصه اجزای مرتبط با پست‌های فوق توزیع بیان می‌گردند و امنیت سایبری آنها به صورت خلاصه مورد توجه قرار می‌گیرد.

همانطور که در شکل ۲ مشاهده می‌گردد، سه جزء اساسی سامانه اسکادای فوق توزیع، مرکز کنترل، پست‌های فوق توزیع و کانال مخابراتی یا ارتباطی هستند. برای دستیابی به امنیت سایبری در این سامانه لازم است که امنیت پست‌های فوق توزیع، کانال‌های مخابراتی پست‌ها و مرکز کنترل مورد توجه قرار گیرد؛ به بیان دیگر، برای در امان ماندن بخش پست از تهدید هکرها و حملات سایبری توجه به امنیت بخش مرکز و همچنین ارتباطات پست با مرکز کنترل مربوطه اهمیت زیادی دارد؛ زیرا که اگر امنیت هر یک از این بخش‌ها دچار اختلال گردد، آنگاه امنیت پست نیز به خطر می‌افتد.

مرکز کنترل به عنوان قلب تپنده و مهم‌ترین بخش سامانه اسکادای فوق توزیع می‌باشد و توجه به الزامات امنیتی و پیاده‌سازی این الزامات در مرکز از بیشترین اهمیت برخوردار است. الزامات امنیتی در مرکز علاوه بر بررسی امنیت نرم‌افزار اصلی، شامل امنیت دیگر اجزاء موجود و به خصوص امنیت شبکه می‌باشد که از آن طریق می‌توان بیشترین آسیب را به مرکز و سامانه اسکادا وارد آورد.

در حالت بهره‌برداری بدون اپراتور از پست‌ها نیز نقش مراکز بیش از پیش اهمیت می‌یابد؛ زیرا در صورتی که حمله‌ای به مرکز اتفاق بیفتد نه تنها کنترل یک پست بلکه کنترل تمامی پست‌های تحت پوشش آن مرکز دچار اختلال شده و این پتانسیل وجود دارد که کلیه پست‌های تحت پوشش

به کنترل مهاجم در آیند. لذا امنیت مراکز دیسپاچینگ از نظر جداسازی شبکه ارتباطی از شبکه عمومی مرکز، امنیت نرم‌افزارهای مورد استفاده، پایش و کنترل دسترسی کاربران به بخش‌های مهم و حیاتی مرکز کنترل، پایش و ثبت کلیه فعالیت‌های انجام‌شده، سخت‌سازی سخت‌افزارها و محدود نمودن کلیه منابع مرکز به نحوی که قابلیت سوء استفاده مهاجمان را به کمترین سطح ممکن کاهش دهد، ضروری است. اگر چه که اهمیت امنیت سایبری مرکز یا مراکز در این ساختار بسیار مهم و تاثیر گذار است و می‌تواند کلیه پست‌های منطقه و یا شبکه فوق توزیع را تحت تاثیر قرار دهد، اما چون الزامات امنیتی مرکز که شامل بخش‌های شبکه، سرورها و تجهیزات مبتنی بر IT است، بیشتر متاثر از امنیت سایبری در فضای IT است و در آن حوزه تجارب مناسبی مشابه سیستم‌های بانکی و دیگر سیستم‌های اطلاعاتی در کشور وجود دارد و با توجه به گستردگی محدوده مورد بررسی در اسکادای فوق توزیع، در این مقاله فقط به آن اشاره شده است و در بخش‌های اصلی مقاله به بررسی الزامات امنیت سایبری پست‌های فوق توزیع و ارتباطات آنها پرداخته شده است.

۳ پست‌های فوق توزیع

پست‌های فوق توزیع در مراکز توزیع بار، داخل شهرها یا شهرك‌ها و مناطق شهرنشین یا روستاهای پر جمعیت ساخته و سطح ولتاژ این پست‌ها عموماً شامل سطوح ۱۳۲ یا ۶۳ کیلوولت می‌باشد و تأمین‌کننده انرژی شبکه توزیع و مصارف صنعتی، تجاری و خانگی می‌باشند. اطلاعات مهم و اساسی در این پست‌ها به صورت دوره‌ای به مرکز مربوطه ارسال می‌گردد و اگر تغییر حالتی در اطلاعات تنظیم شده در پست وجود داشته باشد، به صورت خودکار به مرکز منتقل می‌گردد.

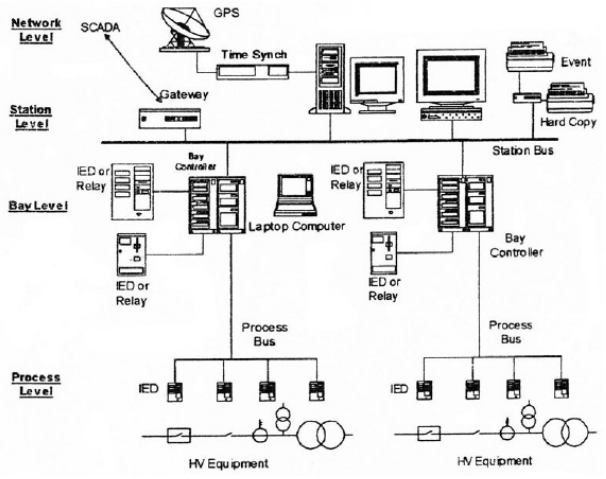
از نظر ساختار داخلی، این پست‌ها به دو دسته زیر تقسیم می‌شوند:

(۱) پست‌های سنتی
(۲) پست‌های DCS

۱.۳ ساختار پست‌های سنتی

در این پست‌ها برای هر بی[۱]، یك تابلو مارشالینگ تعریف می‌گردد که ارتباط تمام تجهیزات آن بی از طریق این تابلو برقرار خواهد شد. از طریق کابل‌های کنترلی ارتباط بی با اتاق کنترل و اتاق حفاظت برقرار و تمام سیگنال‌ها و فرامین بین آنها تبادل می‌گردد. در اتاق کنترل، تابلوهای کنترل نصب شده‌اند که توسط آنها می‌توان از وضعیت بریکرها، سکسیونرها، آلارم‌ها و ... مطلع و در صورت لزوم فرامین لازم را ارسال نمود. در اتاق حفاظت تابلوهای حفاظت شامل رله‌ها قرار دارند که با توجه به تنظیمات اعمال شده بر روی آنها اهداف حفاظتی محقق می‌گردد (در پست‌های فوق توزیع معمولا اتاق حفاظت و کنترل مشترك بوده و به

[۱] هر پست معمولا از تعدادی واحدهای مداری نسبتا مشابه به نام بی تشکیل شده که شامل بخشی از باسبار، دیژنکتور، سکسیونر، برقگیر، راکتور و ... است. در حقیقت بی یک مفهوم فیزیکی است تا الکتریکی؛ و فضایی است که تعدادی از تجهیزات با آرایش خاص برای تشکیل قسمتی از مدار شبکه تشکیل می‌دهند.



شکل ۳. ساختار پست DCS، اجزاء و شبکه‌های ارتباطی

اختصار اتاق کنترل نامیده می‌شود). همانطور که در شکل ۲ نمایش داده شده، (Sub Station 1& 2) در این نوع پست‌ها تجهیز RTU، یا پایانه راه دور وجود دارد. در پست‌های سنتی، تمامی اطلاعات مورد نیاز از نقاط مختلف پست جمع‌آوری شده و به RTU جهت انتقال از طریق سیستم‌های مخابراتی به مرکز کنترل ارسال می‌گردد. از آنجا که تمام ارتباطات در این نوع پست‌ها از طریق RTU با مرکز کنترل برقرار می‌گردد، لذا امنیت سایبری RTU در این نوع پست‌ها بسیار با اهمیت است.

۲.۳ ساختار پست DCS

پست DCS را می‌توان اجرای کامل زیرسیستم‌های حفاظت، کنترل و نظارت بر پایه فناوری شبکه و مفاهیم انتقال و پردازش اطلاعات دیجیتال دانست. ساختار کلی این پست‌ها سیستم خودکارسازی بر مبنای مسیر انتقال و پردازش اطلاعات است و بر این اساس سیستم کنترل دیجیتال پست به چهار سطح تقسیم می‌شود که عبارتند از [۲]:

(۱) سطح عملکرد
(۲) سطح بی
(۳) سطح ایستگاه
(۴) سطح شبکه

این سطح‌بندی و جزئیات آن‌ها در شکل ۳ نشان داده شده است.

این پست‌ها معمولا از استاندارد IEC 61850 (زبان توصیف پیکربندی برای ارتباط در پست‌های برق) پیروی می‌کنند که با استفاده از میکروپروسسور و درگاه‌های مخابراتی با یکدیگر ارتباط دارند. IEDها قادرند داده‌ها و فرمان‌های کنترلی اصلی شامل پایش، کنترل و خودکارسازی، ذخیره‌سازی و آنالیز داده‌ها را تبادل نمایند و به تجهیزات بالا دست خود ارسال کنند.

در این پست‌ها سیستم کنترل و حفاظت در یك اتاقك که محوطه سوئیچ‌دار می‌باشد، نصب گردیده است و می‌توان از همانجا نسبت به کنترل و انجام مانورها روی بی مذکور اقدام نمود. همچنین با استفاده

از سیستم‌های ارتباطی و پروتکل‌های تعریف شده نسبت به ارسال تمام رویدادها (فرامین و عملکردها) به اتاق کنترل اقدام می‌گردد که معمولا ارسال توسط فیبر نوری انجام می‌شود. در اتاق کنترل توسط سیستم کنترل مرکزی که بر روی یك کامپیوتر نصب گردیده است می‌توان تمام وقایع و رویدادها را ثبت و در صورت لزوم فرامین لازم را جهت کنترل و انجام مانورها صادر نمود. در این پست‌ها به دلیل نوع ساختاری که گفته شد میزان کابل‌های کنترلی بسیار کم و به تبع آن اشکالات کمتری به وجود خواهد آمد. ارسال سیگنال به مرکز کنترل و کنترل از راه دور پست نیز در این نوع از پست‌ها راحت‌تر و از طریق Gateway انجام می‌پذیرد. این نوع طراحی با توجه به ابعاد بزرگ پست‌های لایه انتقال، مناسب‌تر بوده و بیشتر مورد استفاده قرار می‌گیرد [۲].

۴ الزامات امنیتی پست‌های فوق توزیع

همانگونه که در بخش قبل بیان گردید، ساختار و معماری پست‌های فوق توزیع سنتی و DCS کاملا متفاوت هستند و لذا الزامات متفاوتی باید برای هر یک از این دو نوع پست مورد توجه قرار گیرد. روش‌های مختلفی برای استخراج الزامات امنیتی وجود دارد و یکی از مهمترین روش‌ها استفاده از استانداردها و مستندات پایه است که برای هر حوزه استخراج شده است. در صنعت برق با توجه به اهمیت امنیت در این حوزه، نیز مستندات مختلفی تهیه شده و مورد استفاده قرار می‌گیرد [۳، ۴]، اما یکی از جامع ترین این مستندات، [۵] است که به بیان الزامات امنیتی در حوزه‌های مختلف شبکه هوشمند برق پرداخته است. در ادامه و در بخش الزامات امنیتی هر نوع از پست‌های فوق توزیع با توجه به الزامات کلی بیان‌شده در مراجع عنوان شده، الزامات امنیتی بر اساس اجزاء و فرایندهای مورد بهره‌برداری در پست استخراج گردیده است و مبنای آن شناخت ساختار عملکردی پست‌های سنتی و DCS می‌باشد.

مجددا تاکید می‌گردد که عدم توجه مناسب به امنیت سایبری در پست‌ها تا کنون منجر به این فرض در مقاله شده که امنیت سایبری در پست‌ها وجود نداشته و باید در دو حالت با حضور اپراتور و بدون اپراتور این الزامات مورد توجه قرار گیرد.

۱.۴ الزامات امنیتی پست‌های DCS

همانگونه که در شکل ۳ نشان داده شده، پست‌های DCS دارای شبکه‌های متعدد بوده و ارتباط اجزاء با استفاده از شبکه‌های ارتباطی در سطوح مختلف برقرار می‌شود، این ساختار موجب می‌گردد که آسیب‌پذیری‌های بیشتر امنیتی وجود داشته و احتمال وقوع حملات سایبری بیشتر باشد و در نتیجه برای ارتقاء امنیتی، الزامات متفاوت و بیشتری برای این نوع از پست‌ها مدنظر می‌باشد که در ادامه این الزامات با توجه به درجه اهمیت ارائه می‌گردد:

امن‌سازی شبکه پست و استفاده از فایروال جهت ارتباط با خارج از پست: با توجه به ساختار پست‌های DCS شاید اولین و مهمترین الزام امنیتی، امنیت شبکه در این پست‌ها باشد. در امنیت شبکه جداسازی ترافیک داخل شبکه از خارج از شبکه بسیار اهمیت دارد، لذا در پست نیز لازم است از فایروال جهت جداسازی ترافیک داخل پست از شبکه خارجی استفاده شود. در این ارتباط استفاده از فایروال صنعتی که قابلیت ارتباط با انواع پروتکل ارتباطی موجود و مورد استفاده در این ارتباطات را داشته باشد، باید مورد توجه قرار گیرد. این الزام در صورت بهره‌برداری از پست‌ها به صورت بدون اپراتور باید بیشتر مورد توجه قرار گیرد.

تنظیم رمز عبور قوی جهت تنظیمات سوئیچ‌ها و ادوات شبکه: از آنجا که با ارتباطات مخابراتی امکان نفوذ به شبکه پست‌ها وجود دارد، این امر می‌تواند در پست‌ها موارد امنیتی متعددی را به وجود آورد. یکی از این امور تغییر رمز عبور تنظیم سوئیچ‌هاست. در صورتی که رمز عبور پیش فرض بر روی سوئیچ‌ها و ادوات شبکه در این تجهیزات تغییر نکرده باشد، با دسترسی به پست چه حضوری و چه مجازی، به راحتی می‌توان این تجهیز را از سرویس خارج نموده و شبکه ارتباطی پست را از وضعیت سرویس‌دهی خارج نمود. همچنین پروتکل‌های ارتباطی متن‌باز تجهیزات شبکه باید غیرفعال شوند تا امکان نفوذ به تجهیزات شبکه وجود نداشته باشد [۶].

سخت‌سازی و محدودسازی کامپیوترها، سرورها و کلیه تجهیزات: وجود سرورها و کامپیوترها در سطح ایستگاه در پست‌های DCS، امکان نفوذ به پست را به راحتی امکان‌پذیر می‌سازد. در صورتی که شبکه سطح ایستگاه در پست امن‌سازی شده و از ورود بدافزارها ممانعت به عمل آورد، اما درگاه‌های باز بر روی کامپیوتر وجود داشته باشد، امکان ورود برنامه‌ها و فایل‌های آلوده به شبکه پست وجود داشته و می‌تواند شرایط را برای نفوذ مهاجمان فراهم سازد. حتی در صورت بسته شدن درگاه‌های فیزیکی، باید کلیه قابلیت‌های غیرضرور در پست غیرفعال شده و امکان استفاده از آنها برای هر سوءاستفاده، غیر ممکن شود. این امر برای دیگر تجهیزات هوشمند مانند رله‌های هوشمند قابل تعمیم بوده و در کلیه تجهیزات، باید رمزهای عبور پیش فرض تغییر یافته و قابلیت‌های بدون استفاده غیرفعال گردند. استفاده از Flash Memoryهای تخصیص داده شده به هر پروژه و بستن پورت‌های غیر ضروری و USB در زمان راه‌اندازی از دیگر الزاماتی است که باید به آن توجه نمود [۷].

لاگ‌گیری و ثبت اطلاعات: هر گونه تغییر اطلاعات، کلیه فعالیت‌ها و تنظیمات در پست باید ثبت و ضبط شود. این امر با در نظر گرفتن ملاحظات زمان دقیق انجام مورد نظر است که از نظر تأخر و تقدم قابل شناسایی باشد. در واقع لازم است هر تغییر یا اصلاحی با برچسب زمانی دقیق ثبت گردد.

بروزرسانی نرم‌افزارها: با توجه به اینکه هر روزه هزاران آسیب‌پذیری امنیتی جدید شناسایی می‌شوند و سازندگان تجهیزات برای رفع این مشکل تلاش می‌نمایند، استفاده از نرم‌افزارها و میان‌افزارهای جدید و بروز و یا وصله‌های منتشر شده که امنیت بیشتری را در اختیار می‌گذارند، می‌تواند در دستیابی به سطح امنیتی بالاتر کمک‌کننده باشد.

تعریف کردن VLAN: تعریف کردن VLAN جهت ارتباطات در پست‌های فوق توزیع DCS می‌تواند امنیت شبکه در این پست‌ها را ارتقا دهد. در صورتی که از سوئیچ‌های مشترک در ارتباطات لایه‌های مختلف استفاده می‌شود، راهکار استفاده از شبکه‌های مجازی مختلف می‌تواند امنیت بالاتری را فراهم سازد. ضمن آنکه با تنظیمات سوئیچ‌ها از ارتباطات بین شبکه‌های مجازی جلوگیری شود.

تعیین و تنظیم سطح دسترسی: کاربران مختلف با نقش‌های مختلف جهت دسترسی به تجهیزات و انجام امور مختلف، چه از راه دور و چه به صورت محلی باید سطوح دسترسی مختلفی داشته باشند. به طور مثال، فردی که فقط نقش اپراتور قرائت‌کننده را دارد، نباید بتواند تنظیمات تجهیزات را تغییر دهد. لذا تعیین سطوح دسترسی برای افراد با نقش‌های مختلف باید متفاوت تعریف شده و متفاوت پیاده‌سازی گردد.

۲.۴ الزامات امنیتی پست‌های سنتی

همانگونه که در بخش ۱.۳ بیان گردید، پست‌های سنتی دارای تجهیزات مختلف فشار قوی هستند، ولی تجهیزات کنترلی محدودی در این نوع پست‌ها وجود دارد که احتمال نفوذ و حمله از طریق آنها وجود داشته باشد. در این نوع پست‌ها چون ارتباط با مرکز و ارسال اطلاعات از طریق تجهیز RTU انجام می‌گیرد، امن‌سازی سایبری پست بیشتر به امن‌سازی و وجود قابلیت‌های امنیتی آن بستگی دارد، اما در ادامه مهمترین الزامات امنیتی که باید در پست‌های سنتی به آن توجه داشت، بیان می‌گردند.

سخت‌سازی تجهیز RTU: سخت سازی[1] یا هاردنینگ سیستم‌های موجود از جمله RTU در پست (شامل غیرفعال کردن پورت‌ها و سرویس‌های غیر کاربردی) لازم است. همچنین لازم است درگاه‌های فیزیکی و منطقی استفاده‌نشده و یا غیرضروری برای جلوگیری از اتصال غیرمجاز دستگاه‌ها، غیرفعال شوند و در طراحی کل سیستم، به اجرا درآوردن سیاست فعال‌سازی حداقل قابلیت‌ها در نظر گرفته شود.

سخت‌سازی و محدود سازی لپ‌تاپ‌ها و کامپیوترهای تنظیم کننده: ورود کامپیوترها یا لپ‌تاپ‌ها به داخل پست جهت انجام اموری از جمله تغییر تنظیمات، می‌تواند بسیار آسیب‌پذیر باشد، از این رو در صورت امکان استفاده از لپ‌تاپ یا کامپیوتری مخصوص این امر که قابلیت جابجایی نداشته باشد و یا فقط جهت این امر مورد استفاده شود، آسیب‌پذیری‌های این حوزه را کاهش خواهد داد؛ زیرا یک لپ‌تاپ عادی که ممکن است توسط پیمانکار به پست وارد شود، می‌تواند عامدانه یا سهوی آلوده به ویروس یا بدافزار شده و به سامانه پست نفوذ کند. در صورتی که لپ‌تاپ مورد استفاده جهت تنظیمات سخت شده باشد، از ورود برخی از حملات جلوگیری می‌گردد و سطح بالاتر امنیتی حاصل خواهد شد.

لاگ‌گیری و ثبت اطلاعات: این الزام در پست‌های سنتی نیز مانند پست‌های DCS مهم و ضروری است اما این واقعیت که امکان ثبت و لاگ‌گیری تا چه میزان در این پست‌ها قابل انجام است، باید مورد توجه قرار گیرد که تا حد زیادی به قابلیت RTU وابسته می‌باشد.

نکته: الزامات دیگر امنیتی در پست‌های سنتی از جمله تنظیم سطوح دسترسی مختلف در RTU، امکان انجام احراز اصالت و یا رمزنگاری نیز به قابلیت‌های تجهیزات و RTU بکار رفته در پست بستگی دارد که در هنگام خرید این محصول باید مورد توجه قرار گیرد.

۵ الزامات امنیتی ارتباطات

برای بهره‌برداری بدون اپراتور پست‌ها، لازم است که پست‌ها توسط مرکز کنترل، پایش شده و کنترل لازم بر روی آنها انجام گیرد و این امر توسط کانال‌های مخابراتی که این ارتباطات را برقرار می‌نمایند، صورت می‌گیرد. به طور کلی می‌توان گفت که برای اجرای خودکارسازی پست‌ها که لازمه بدون اپراتور کردن آنها است، علاوه بر وجود تجهیزات مورد نیاز در پست، مرکز کنترل و یا نرم‌افزار اسکادا، شبکه مخابراتی امن و مطمئن نیز از جمله الزامات اساسی است که علاوه بر انتقال داده پست به مرکز، فرامین و دستورات مرکز را نیز به پست منتقل نماید.

در صنعت برق انواع روش‌های ارتباطی که مورد استفاده قرار می‌گیرد شامل ارتباطات بی‌سیم، ارتباطات ماهواره‌ای، ارتباطات شبکه‌های عمومی مخابرات، ارتباطات خطوط انتقال[2] (PLC) و ارتباطات فیبر نوری می‌باشد.

اگر چه در ارتباطات در سطح فوق توزیع، عموماً از شبکه‌های فیبرنوری و PLC استفاده می‌شود و این شبکه‌ها با توجه به اختصاصی بودن از امنیت بالاتری برخوردارند، اما این امر از یک شرکت برق منطقه‌ای به شرکت دیگر و حتی در یک شرکت برق منطقه‌ای می‌تواند متفاوت باشد. لذا بررسی الزامات امنیتی ارتباطات باید به صورت کلی و بدون در نظر گرفتن ارتباطات اختصاصی مورد توجه قرار گیرد.

هر کدام از فن‌آوری‌های ارتباطی سیمی، بی‌سیم و یا فیبرنوری، دارای مزایا و معایب خاص خود می‌باشند که بسته به موقعیت پست و محدودیت‌های موجود انتخاب می‌گردند، اما از نظر امنیتی، داشتن مسیر پشتیبان مخابراتی از اهمیت ویژه‌ای برخوردار است. لذا در پست‌هایی که در مسیر شبکه فیبرنوری صنعت برق قرار ندارند و یا به هر طریقی، مسیر پشتیبان برای آنها وجود ندارد، تأمین مسیر پشتیبانی که مستقل از مسیر پیش فرض است، لازم می‌باشد.

علاوه بر مسیر پشتیبان که دسترس‌پذیری و در نتیجه امنیت بالاتری را به دنبال خواهد داشت، مفاهیم محرمانگی و یکپارچگی اطلاعات نیز در بخش ارتباطی پست و مرکز کنترل از اهمیت بسیاری برخوردار هستند. این دو الزام امنیتی بخصوص در پست‌هایی که بدون اپراتور بهره‌برداری می‌شوند، بیش از پیش اهمیت داشته و باید با دقت نظر بیشتری مورد مطالعه و بررسی قرار گیرند. این از آن جهت است که بدون حضور اپراتور در پست، فرمان‌های ارسالی از مرکز کنترل می‌توانند قطع و وصل خطوط

[1] hardening

[2] power line carrier

و یا عملیات حفاظتی را به دنبال داشته باشند و اگر فرامین مهم در میان راه تغییر یافته و یا به درستی دریافت نگردند، تاثیرات مخربی را ایجاد نموده و آسیب‌های بسیاری را می‌توانند به دنبال داشته باشند. لذا در بحث امنیت ارتباطات دو الزام مهم و اساسی باید مد نظر قرار گیرد، که در ادامه در مورد هر یک توضیحات مختصری ارائه می‌گردد.

احراز اصالت جهت تضمین یکپارچگی اطلاعات: در ارتباطات مرکز کنترل و پست از پروتکل‌های ارتباطی استفاده می‌شود. از جمله پروتکل‌های ارتباطی بین مراکز کنترل و پست‌ها می‌توان به پروتکل‌های ذیل اشاره کرد:

- **IEC 61870-5-101:** جهت ارتباط و کنترل از راه دور پایانه‌های دور دست و مرکز کنترل اسکادا به کار می‌رود.
- **IEC 61870-5-104:** این پروتکل نسخه مبتنی بر IP از استاندارد IEC870-5-101 است.
- **DNP3:** این پروتکل مجموعه‌ای از پروتکل‌های ارتباطی است که بین اجزای بکار رفته در سیستم اتوماسیون بکار رفته است.

این پروتکل‌ها بخصوص در ارتباطات پست‌های بدون اپراتور و مرکز کنترل باید از نوع امن باشند. در پروتکل‌های امن، یکپارچگی ارتباطات مورد توجه خاص قرار می‌گیرد و حملاتی مانند تکرار و مردی در میانه امکان وقوع نخواهند داشت.

احراز اصالت یکی از مهمترین ابزارهای جلوگیری از نفوذ در استانداردهای امنیتی صنعتی است. لذا باید کلیه دسترسی‌ها به تجهیزات در پست چه به صورت محلی و چه به صورت از راه دور اعتبارسنجی شده و پس از احراز اصالت، دسترسی فراهم گردد. با توجه به تنوع الگوریتم‌های احراز اصالت، الگوریتم HMAC [1] طبق منابع [۸] و [۹] می‌تواند امنیت مناسب را فراهم ساخته ضمن آن که امکان شکستن الگوریتم‌های هش غیرممکن باشد.

رمزنگاری ترافیک ارتباطی: زیرساخت‌های ارتباطی همچون مایکروویو، فیبر نوری مخابرات، شبکه عمومی مخابرات و غیره به منظور برقراری ارتباط پست و مرکز کنترل، بسترهای ارتباطی خارج از صنعت برق هستند که بعضا در ارتباطات پست‌های فوق توزیع و مراکز کنترل استفاده می‌شوند. این بسترهای عمومی، مسیر بالقوه‌ای برای دستیابی یک مهاجم به اطلاعات هستند. علاوه بر بسترهای عمومی مخابراتی، در بسترهای فیبرنوری و PLC اختصاصی صنعت برق نیز همچنان رمزنگاری این ارتباطات و عدم ارسال به صورت رمز نشده، امنیت سایبری را ارتقا خواهد داد. اگرچه در استانداردهای [۸، ۹] رمزنگاری ارتباطات، الزام نشده است، این قابلیت می‌تواند به صورت اختیاری در ارتباطات پست و مرکز اسکادا در نظر گرفته شود. لازم به ذکر است که با بکارگیری رمزنگاری، از محرمانگی نشست‌های برقرار شده از راه دور نیز حفاظت می‌گردد. لازم است که برای جلوگیری از افشای غیرمجاز اطلاعات، برای تبادل پارامترهای امنیتی مهم (به عنوان مثال کلیدهای رمزنگاری، کلمات عبور، پیکربندی‌های امنیتی) از رمزنگاری استفاده شود [۳]. در مورد الگوریتم‌های رمزنگاری مطمئن نیز در کاربردهای صنعت برق، می‌توان به مراجع [۸، ۹] مراجعه نموده و بر اساس آنها به اطمینان کافی در زمینه محرمانگی اطلاعات و ارتباطات دست یافت.

۶ ملاحظات امنیتی

مدیریت مخاطرات امنیتی: اگر چه در این مقاله سعی گردید که الزامات امنیتی بدون اپراتور کردن پست‌های فوق توزیع، بر اساس مراجع و استانداردهای بین المللی و بهترین تجارب کشورهای پیشرفته ارائه گردد، اما یکی از اصولی‌ترین روشهای ارتقاء امنیت، انجام مدیریت مخاطرات امنیتی است. در این روش که با توجه به محدودیت بودجه و زمان در امن‌سازی بسیار مورد توجه قرار می‌گیرد، تهیه سند مدیریت مخاطرات امنیتی است که در این سند با توجه به دارایی‌های موجود در سامانه، آسیب‌پذیری‌های این دارایی‌ها استخراج شده و بر اساس ارزش دارایی، ارزش و سطح آسیب‌پذیری‌های مرتبط با هر دارایی، تأثیر تهدیدات و احتمال آنها برای سوءاستفاده از آسیب‌پذیری‌های مورد نظر، مخاطرات مرتبط با هر دارایی استخراج شده و سپس بر اساس اهمیت مخاطرات مرتبط با هر دارایی، کنترل‌ها و راهکارهای امنیتی با اولویت‌بندی میزان تاثیر بر ارتقاء امنیت و هزینه اجرا، پیشنهاد می‌گردد که انجام این روش به عنوان ادامه فعالیت در این حوزه پیشنهاد می‌گردد.

آموزش نیروی انسانی: توجه به آموزش نیروی انسانی یکی از الزامات مهم و اساسی جهت ارتقاء امنیت سایبری است؛ چرا که بسیاری از حملات از طریق نیروی انسانی ناآگاه انجام شده و دسترسی به سیستم فراهم می‌گردد. در پست‌های بدون اپراتور، عدم حضور اپراتور می‌تواند از آسیب‌پذیری‌های این حوزه بکاهد، اما نیروی انسانی پیمانکاران، گروه‌های مانور و ... هنوز جزء مهمی از سامانه بدون اپراتور پست‌ها هستند که باید جهت آگاهی دادن و آموزش به آنها برنامه‌های آموزشی مناسب تهیه و اجرا گردد.

پایش مستمر: نکته مهم در مورد ارتقاء امنیت سایبری که باید همواره به آن توجه داشت، پایش مستمر آن است. لازم است که به صورت دوره‌ای امنیت سایبری سامانه مورد بررسی و ارزیابی امنیتی قرار گیرد. این امر جدا از زمانی است که تغییراتی در ساختار سامانه و یا افزودن و کاستن بخش‌هایی در سامانه اتفاق می‌افتد که باید کلیه الزامات امنیتی در شرایط تغییر یافته، مورد بررسی و ملاحظه قرار گیرد.

۷ نتیجه‌گیری

با افزایش هر روزه حملات سایبری و جایگزینی جنگ‌های نرم بجای درگیری‌های نظامی و از آنجا که صنعت برق به عنوان یکی از صنایع پایه و مهم همواره مورد توجه مهاجمان و معاندان بوده است، توجه به الزامات امنیتی در پست‌های فوق توزیع بخصوص در حالت بدون اپراتور

[1] HMAC: Keyed-Hashing for Message Authentication

از اهمیت بسیاری برخوردار است. در این مقاله سعی شد که به مهمترین موضوعات امنیت سایبری در پست‌های بدون اپراتور پرداخته شود، هر چند که بسیاری از این موارد در حالت بهره‌برداری پست با اپراتور و بدون اپراتور مشترک است، اما توجه به کلیه این الزامات جهت ارتقاء امنیت این سامانه از اهمیت بالایی برخوردار است. علاوه بر الزامات امنیتی در دو نوع پست‌های سنتی و DCS، الزامات امنیتی ارتباطات پست‌های فوق توزیع و مرکز کنترل مورد توجه قرار گرفت و اهمیت توجه به احراز اصالت داده‌های متبادله با هدف عدم تغییر دستورات دریافتی از مرکز و یا اطلاعات پست به مرکز در میانه راه بیان گردید. در بخش الزامات ارتباطی علیرغم عدم الزام رمزنگاری ارتباطات در استانداردهای مرتبط با سامانه‌های کنترل صنعتی، بر وجود این قابلیت برای افزایش محرمانگی اطلاعات تبادل شده، تاکید گردید.

در بخش ملاحظات امنیتی، بر اهمیت تهیه سند مدیریت مخاطرات امنیتی در سامانه اسکادای فوق توزیع جهت اولویت‌بندی کنترل‌های امنیتی تاکید شد. اما در این مقاله با توجه به تجارب کسب شده در پروژه‌های مشابه، ملاحظات امنیتی ارائه شده اولویت‌بندی گردید.

اگر چه امنیت پست‌های فوق توزیع در این بررسی مورد توجه قرار گرفته، اما ساختار اسکادا در سطوح انتقال و توزیع نیز مشابه این ساختار در سطح فوق توزیع است که می‌تواند تصور امنیت در این سطوح ولتاژی را نیز تا حد زیادی فراهم سازد. پیچیدگی، تعداد ادوات الکتریکی، کنترلی و حفاظتی پست‌های انتقال و توزیع از پست‌های فوق توزیع متفاوت است، اما در انواع DCS و سنتی پست‌ها در سطوح مختلف ولتاژی، شباهت‌های بسیاری وجود دارد که می‌تواند زمینه را برای استخراج الزامات امنیتی پست‌های انتقال و توزیع نیز فراهم آورد. علاوه بر موارد فوق، نکته بسیار مهمی که باید در تصمیم‌گیری در مورد سیستم‌های حیاتی و مهم مانند صنعت برق به آن توجه ویژه نمود، دریافت تاییدیه‌های نهادهای بالادستی، از جمله مرکز راهبردی افتای ریاست جمهوری و سازمان پدافند غیرعامل در اجرایی نمودن سیاست‌هایی از قبیل بهره‌برداری بدون اپراتور پست‌های فوق توزیع است که باید قبل از اجرا از منظر امنیت فیزیکی و سایبری به صورت جامع مورد بررسی قرار گرفته و قبل از اجرا، مورد تایید مقامات مجاز قرار گیرد.

مراجع

[۱] هژبری، حمیدرضا و رستمی، ثریا. تحلیل فنی و اقتصادی بدون اپراتور کردن پست‌های فوق توزیع. در بیست و هشتمین کنفرانس بین المللی برق، ۱۳۹۲.

[۲] صادق‌پور، حسن. اتوماسیون شبکه‌های انتقال قدرت و چالش‌های پیش رو. در بیست و هشتمین کنفرانس بین المللی برق، ۱۳۹۴.

[3] Guide to industrial control systems (ics) security. tech. rep., National Institute of Standards and Technology, US Department of Commerce, 2014.

[4] Cyber security assessments of industrial control systems. tech. rep., Homeland Security, April 2011.

[5] C. S. W. G. -T. S. G. I. Panel. Guidelines for smart grid cybersecurity: Volume 1 - smart grid cybersecurity strategy, architecture, and high-level requirements. (NISTIR 7628), 2014.

[۶] مظفری، اعظم. راه کارهای امنیتی حوزه شبکه در سیستم‌های کنترل صنعتی. در سی‌امین کنفرانس بین المللی برق، ۱۳۹۴.

[۷] حسن پور، جواد و تدین، شبنم. معرفی الزامات امنیت سایبری در سیستم‌های اتوماسیون متناسب با سطح برخورداری از فن‌آوری‌های جدید. در کنگره اتوماسیون صنعت برق، ۱۳۹۱.

[8] IEC/TR 62351-3. Power systems management and associated information exchange – data and communications security–part 3: Security for iec 60870-5 and derivatives, 2009. Edition 1.0.

[9] IEC/TR 62351-3. Power systems management and associated information exchange – data and communications security–part 3: Communication network and system security profiles including tcp/ip, 2007. Edition 1.0.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2022, Volume 20, Number 1 (pp. 10–17)
https://monadi.isc.org.ir

Presented at the ISCISC 2021 in University of Isfahan, Isfahan, Iran

Unmanned Cyber Security Requirements in sub-Transmission Substation★

Azam Mozafari *, Leila Zafari and Negin Hamian

Niroo Research Institute (NRI), Tehran, Iran

ARTICLE INFO.

Keywords:
unmanned cyber security
sub-transmission substation

dor: 20.1001.1.24763047.1401.11.1.2.9

Type: research paper

ABSTRACT

As an economic and technical point of view, operation of without operator or unmanned substations is of interest to power industry managers, so it is an opportunity to investigate cyber security carefully at this time. In this article, while studying the importance of SCADA (Supervisory Control and Data Acquisition) centers cyber security, the cyber security requirements of two types of DCS (Distribution Control System) and traditional substations and the communication of these types of substations and the corresponding SCADA center were examined. In this article, based on the documents and standards of industrial cyber security and power industry, the security requirements of substations and their communications with the relevant centers were extracted, and these requirements were prioritized based on knowledge of the industry and the importance of existing departments and processes. In addition, due to the non-implementation of security requirements in high power substations, it was emphasized to pay attention to the cyber security considerations of this area, such as preparing security risk management documents, paying attention to personnel training and receiving security approvals.

© 2022 ISC

★ The ISCISC 2021 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: amozafari@nri.ac.ir (Azam Mozafari), lzafari@nri.ac.ir (Leila Zafari), nhamain@nri.ac.ir (Negin Hamian)
© 2022 ISC. All rights reserved.