فصلنامه علمی-ترویجی پدافند غیرعامل
سال نهم، شماره ۲، تابستان ۱۳۹۷، (پیاپی ۳۴): صص ۹-۱

بررسی انواع راه‌کارهای افزایش امنیت در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی

احمد افشار[۱*]، عاطفه ترمه‌چی[۲]، عارفه گلشن[۳]، آزاده آقائیان[۴]، حمیدرضا شهریاری[۵]، ساجده سلیمانی[۶]

تاریخ دریافت: ۱۳۹۵/۰۳/۰۴
تاریخ پذیرش: ۱۳۹۶/۰۹/۲۷

چکیده

امروزه توسعه اقتصادی و سیاسی یک جامعه در گرو کارآمدی زیرساخت‌های حیاتی نظیر انرژی، آب، فن‌آوری اطلاعات و ارتباطات، بانکداری، آموزش و پژوهش، حمل و نقل، بهداشت و درمان و ... است. کنترل و پایش در زیرساخت‌های حیاتی و واحدهای صنعتی، توسط یک سیستم کنترل تحت شبکه و هوشمند انجام می‌گیرد. بزرگترین تهدید برای این سیستم‌ها، حملات هدف‌دار مانند حملات سایبری است که در آن مهاجم، راه‌برد حمله خود را با هدف آسیب‌رساندن به سیستم تحت کنترل متناسب می‌کند. به‌منظور دست‌یابی به جامعه‌ای امن، توسعه زیرساخت‌های حفاظت‌شده، امن‌سازی اطلاعات حیاتی و تولید سیستم‌های کنترل مقاوم در برابر حملات سایبری بسیار حائز اهمیت است. راه‌برد کلان بیشتر اسناد مهم و پرکاربرد در زمینه امنیت سیستم‌های کنترل صنعتی برمبنای "راه‌برد دفاع در عمق" استوار است. به‌منظور اجرای راه‌برد کلان دفاع در عمق، راه‌کارهای گسترده‌ای پیشنهاد شده است. بنابراین، هدف این مقاله، بحث و توضیح این راه‌کارها در قالب دو دسته پایه‌ای و ساختاری و با بررسی استانداردهای بین‌المللی و مستندات معتبر از جمله مقاله‌های علمی است. توجه به اشتباهات رایج در اتخاذ تدابیر امنیتی و اجتناب از آن‌ها به منظور دست‌یابی به یک سیستم امن، بسیار حائز اهمیت است. از این‌رو در بخش انتهایی مقاله، به برخی از آن‌ها اشاره می‌شود.

کلیدواژه‌ها: سیستم کنترل صنعتی و زیرساخت حیاتی، مقابله با حملات سایبری، دفاع در عمق، راه‌کارهای پایه‌ای، راه‌کارهای ساختاری

۱- دانشیار دانشگاه صنعتی امیرکبیر aafshar@aut.ac.ir - نویسنده مسئول
۲- دانشجوی دکتری - دانشگاه صنعتی امیرکبیر
۳- دانشجوی کارشناسی ارشد - دانشگاه صنعتی امیرکبیر
۴- دانشجوی کارشناسی ارشد - دانشگاه صنعتی امیرکبیر
۵- استادیار - دانشگاه صنعتی امیرکبیر
۶- دانشجوی کارشناسی ارشد - دانشگاه صنعتی امیرکبیر

۱- مقدمه

در دنیای امروز، توسعه سیاسی و اقتصادی یک جامعه به واسطه کارآمدی زیرساخت‌های آن یعنی انرژی، آب، فن‌آوری اطلاعات و ارتباطات، بانکداری، آموزش و پژوهش، حمل‌ونقل، پست، بهداشت و درمان و... امکان‌پذیر می‌شود. در این میان، برخی از زیرساخت‌ها نقشی حیاتی در منافع ملی یک کشور دارند و اختلال هر چند کوتاه مدت در عملکرد آن‌ها می‌تواند منجر به ایجاد آسیب جدی در اقتصاد، سیاست، امنیت و ایمنی آن کشور شود. کنترل و پایش[1] در زیرساخت‌های حیاتی و واحدهای صنعتی، توسط یک سیستم کنترل تحت شبکه و هوشمند انجام می‌گیرد. استفاده از فن‌آوری اطلاعات در این سیستم‌ها، به هدف افزایش کارایی و قابلیت اطمینان صورت گرفت ولی از سویی دیگر، آن‌ها را در معرض حمله‌های سایبری و بدافزاری قرار داد. از این‌رو، توسعه سیستم‌های کنترل صنعتی[2] مقاوم در برابر حملات سایبری، جهت دست‌یابی به یک جامعه امن بسیار حائز اهمیت است. در گذشته، راه‌حل‌های مطرح‌شده مقابله با حملات سایبری در این سیستم‌ها، تنها بر مبنای امن‌سازی "اطلاعات و سرویس‌ها و ابزارهای فن‌آوری اطلاعات" استوار بودند [۱]، اما حملات سایبری در سال‌های اخیر نشان دادند که سیستم‌های کنترل صنعتی باید اصول امنیتی و مقاوم‌بودن را در درون خود نیز جای دهند. تلاش‌های زیادی جهت حل مسئله امنیت در سیستم‌های کنترل صنعتی در قالب مقالات، استانداردها، توصیه‌نامه‌ها و بهترین شیوه‌ها[3] انجام گرفته است که به برخی از آن‌ها در [۲] اشاره شده است. راه‌برد کلان بیشتر اسناد مهم و پرکاربرد در این زمینه، برمبنای "راه‌برد دفاع در عمق" استوار است. با توجه به گستردگی بسیار زیاد راه‌کارهای پیشنهادی به‌منظور اجرای این راه‌برد کلان، در این مقاله آن‌ها در دو دسته پایه‌ای و ساختاری تقسیم‌بندی و به‌طور خلاصه به برخی از آن‌ها اشاره می‌شود.

در این مقاله، در بخش دوم به بررسی اصل دفاع در عمق پرداخته می‌شود. سپس در بخش سوم راه‌کارهای اجرای راه‌برد دفاع در عمق به منظور افزایش امنیت در سیستم‌های کنترل صنعتی، تقسیم‌بندی و بررسی می‌شوند. در بخش چهارم مقاله، به اشتباهات رایجی که معمولاً در ضمن اجرای راهکارهای امنیتی در صنعت دیده می‌شوند، اشاره می‌شود. در نهایت نتیجه‌گیری ارائه می‌گردد.

1- Monitoring

۲- در این مقاله سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی به اختصار سیستم کنترل صنعتی خوانده می‌شوند.

3- Best Practices

۲- اصل دفاع در عمق[4]

دفاع در عمق به معنای مهیاکردن حفاظت‌های امنیتی چندگانه، به‌خصوص به شکل لایه‌ای، با هدف ایجاد تأخیر (در صورت عدم امکان جلوگیری از حمله) در یک حمله است. این دفاع از یک راه‌برد نظامی نشأت گرفته است که هدف آن به تأخیر انداختن یک حمله با ایجاد زمان کافی برای پاسخی مؤثر است [۳]. بنابراین، دفاع در عمق مؤثر، موجب عدم پیشرفت حمله و یا منجر به شکست تهاجم به علت وجود زمان کافی برای شناسایی و پاسخ به حمله می‌شود. برخی از محققین معتقدند که همواره باید از ابزار و تولیدات شرکت‌های مختلف در لایه‌ها استفاده شود تا سیستم در برابر حمله مقاوم‌تر گردد [۵-۴].

باید توجه نمود که دفاع در عمق به لایه‌های مختلف حفاظتی اشاره دارد که ویژگی‌های زیر را فراهم می‌کند [۶]:

(۱) مهاجمان با این مسئله مواجه هستند که باید هر لایه را بدون این که شناسایی شوند، پشت سر گذارند.

(۲) یک نقص امنیتی در یک لایه می‌تواند به‌وسیله قابلیت‌های موجود در دیگر لایه‌ها کاهش پیدا کند.

پیش‌تر در مرجع [۷] توضیح داده می‌شود که سیستم‌های کنترل صنعتی، خود نیز با ساختاری لایه‌ای توصیف می‌شوند که هر لایه عملکرد متفاوتی دارد. آسیب‌پذیری‌های این لایه‌ها نسبت به حملات سایبری نیز گسترده و متفاوت بوده و به تبع آن هر لایه نیازمند اقدامات امنیتی متفاوتی نیز است. از این‌رو، راه‌برد کلان دفاع در عمق به‌منظور حفاظت از سیستم‌های کنترل صنعتی مطرح و بسیار مورد توجه قرار گرفته است. به‌طوری‌که بیشتر اسناد مهم و پرکاربرد در زمینه امنیت سیستم‌های کنترل صنعتی از جمله منابع [۵-۴ و ۱۶-۸] برمبنای راه‌برد دفاع در عمق استوار هستند. به‌منظور اجرای راه‌برد کلان دفاع در عمق، راه‌کارهای زیادی پیشنهاد شده است که در بخش بعد، این راه‌کارها در قالب دو دسته راه‌کار پایه‌ای و ساختاری تقسیم‌بندی می‌شوند.

۳- دسته‌بندی راه‌کارهای افزایش امنیت در سیستم‌های کنترل صنعتی

همان‌طور که بیان شد با توجه به گستردگی بسیار زیاد راه‌کارهای پیشنهادی به‌منظور اجرای راه‌برد کلان دفاع در عمق و افزایش امنیت در سیستم‌های کنترل صنعتی، در این بخش سعی شده است که آن‌ها در دو دسته پایه‌ای و ساختاری تقسیم‌بندی و مورد بررسی قرار

4- Defense in Depth

گیرند. راه‌کارهای پایه‌ای، راه‌کارهایی هستند که با توجه به موقعیت اجزای سیستم و میزان درجه اهمیت امنیت آن‌ها تدوین می‌شوند. راه‌کارهای ساختاری، راه‌کارهایی هستند که براساس ماهیت اجزای تشکیل‌دهنده سیستم اتخاذ می‌شوند. لازم به ذکر است این دو دسته راه‌کار را می‌توان مکمل همدیگر در راستای اجرای کامل راهبرد دفاع در عمق در نظر گرفت.

۳-۱- راه‌کارهای پایه‌ای

همان‌طور که بیان شد، راه‌کارهای پایه‌ای، راه‌کارهایی هستند که با توجه موقعیت اجزای سیستم، میزان درجه اهمیت امنیت آن‌ها تدوین می‌شوند، این راه‌کارها به دو دسته زیر تقسیم می‌شوند:

- کنترل و سنجش محدوده‌های الکترونیکی
- کنترل و سنجش محدوده‌های فیزیکی

۳-۱-۱-کنترل و سنجش محدوده‌های الکترونیکی

محدوده‌های امنیت الکترونیکی (ESP)[1] حریم‌های منطقی هستند که یک شبکه و یا گروهی از زیرشبکه‌ها را احاطه می‌نمایند. ESP ها برای قطعه‌بندی شبکه بر اساس ارتباطات الکترونیکی آن‌ها به کار می‌روند و تمامی این قطعه‌ها باید ناحیه‌های مطمئنی باشند. کلیه نقاط دسترسی الکترونیکی شامل اترنت[2]، فیبر و هر اتصال بی‌سیم و یا باسیم به یک ESP باید شناسایی‌شده و به طرز مناسبی حفاظت گردد. در دیدگاه دفاع در عمق، لایه‌لایه و یا سلسله مراتبی‌بودن ESP بسیار مهم است [۴، ۱۱ و ۱۷] و به‌طور کلی، ESP متشکل از سه لایه اول، دوم و سوم مناسب است [۱۷].

ESP اول، باید تمامی نواحی قابل اطمینان را احاطه نماید. اتصالات به این لایه جزء اتصالات خارجی محسوب می‌شوند و معمولاً تنها نقاط قابل دسترسی یک مهاجم از راه دور می‌باشند. بدین ترتیب حفاظت از آن‌ها بسیار مهم بوده و نقاط دسترسی به ESP اول، نیازمند اجرای سازوکارهای حفاظتی اضافی، سازوکارهای رمزنگاری پیچیده‌تر و سازوکارهای دسترسی سختگیرانه‌تر است. دسترسی به ESP اول را می‌توان به کمک منطقه حائل[3] محدود کرد. منطقه حائل، تمامی ارتباطات بین نواحی مورد اطمینان (قسمت‌های داخل ESP اول) با ناحیه‌های نامطمئن را محدود و کنترل می‌نماید. هر ابزاری که به یک ناحیه نامطمئن وصل می‌شود، باید در این منطقه قرار گیرد. دیوارهای آتش دو ناحیه نامطمئن و مورد اطمینان را به هم مربوط می‌نمایند. در ساختاری ایده‌آل، تنها یک اتصال بین منطقه حائل و ناحیه مورد اطمینان و همچنین تنها یک اتصال بین منطقه حائل و ناحیه نامطمئن وجود دارد. اگر اتصالات یک طرفه باشد می‌توان یک دیود داده نصب نمود. دسترسی به اینترنت به‌طور مستقیم از منطقه حائل، ESP و یا یک ناحیه مورد اطمینان ممنوع است.

هیچ ESP دومی نباید نقطه ارتباطی با شبکه‌های خارجی داشته باشد. تمامی اتصالات خارجی به آن باید ابتدا از لایه اول عبور نمایند. ESP های این لایه می‌توانند به یکدیگر و یا به نقاط دسترسی به ESP های اول متصل شوند. البته نقاط ارتباط بین ESP های دوم نقاط دسترسی داخلی محسوب می‌شوند و نیازمند کنترلی مؤثر و مقاوم هستند. دسترسی الکترونیکی به هر ESP دوم، از طریق هر نقطه دسترسی باید از طریق دیوار آتش ساختاریافته صورت پذیرد و تمامی دسترسی‌ها باید ثبت شوند. هر تلاشی جهت دسترسی غیرمجاز لازم است پایش، شناسایی و هشدار داده شود.

در بیشتر مواقع، مدیران امنیتی ESP سوم را تعریف نمی‌کنند و یا درصورت تعریف، هیچ محافظتی از آن نمی‌شود که امری اشتباه است. محدوده‌های امنیت الکترونیکی این لایه، آخرین مرحله دفاع از ابزارهای در معرض حمله محسوب می‌شوند. این لایه نیازمند کنترل و محافظتی در حد ESP های دوم است. تمامی ابزارهای سایبری که احتمال خطر بسیار بالایی دارند، در یک ESP سوم قرار می‌گیرند. دسترسی بین ابزار و یا ESP های سوم باید محدود گردد.

دیدگاه لایه‌لایه‌ای به ESP، روشی مناسب برای اجرای دفاع در عمق است که امکان جداسازی یک ESP از ESP دیگر در هنگام خطر را تسهیل می‌نماید.

۳-۱-۲- کنترل و سنجش محدوده‌های فیزیکی

محدوده‌های امنیت فیزیکی (PSP)[4] برای قطعه‌بندی یک واحد صنعتی براساس ارتباطات و دسترسی‌های فیزیکی آن به کار می‌روند و تمامی این قطعه‌ها باید ناحیه‌های مطمئنی باشند. PSP ها در دیدگاه دفاع در عمق، لازم است ماهیتی لایه‌لایه‌ای داشته باشند [۴]. در اکثر استانداردها، درنظرگرفتن سه لایه برای PSP ها مناسب تشخیص داده شده است [۹ و ۱۸].

لایه اول PSP، تمامی واحد صنعتی و همه لایه‌های پایین‌تر PSP را فرا می‌گیرد. نقاط دسترسی به یک PSP اول، خط اول دفاع در برابر حمله‌ها بوده که می‌توانند فیزیکی، سایبری و یا بدافزاری باشند. نقاط دسترسی باید در حد امکان به گونه‌ای محدود شوند که تنها یک نقطه دسترسی برای پرسنل، یک یا دو نقطه دسترسی برای دیگر موارد مورد نیاز وجود داشته باشد. این نقاط نیازمند استفاده از سازوکارهای محافظتی بیشتری می‌باشند. دوربین‌ها، نگهبانان،

1- Electronic Security Perimeter (ESP)
2- Ethernet
3- Demilitarized Zone (DMZ)
4- Physical Security Perimeter (PSP)

کاغذهای امضاء، تأیید ID، همگی باید بخشی از فرآیند دسترسی باشند. دسترسی به PSP اول باید از طریق منطقه حائل محدود گردد. منطقه حائل فیزیکی، معمولاً به شکل دروازه ورودی و یا سیم‌های خاردار است که بعد از آن محوطه عظیمی به صورت فضای باز وجود دارد و در نهایت، واحد صنعتی قرار می‌گیرد. هدف استفاده از منطقه حائل فیزیکی، ایجاد زمان کافی برای نگهبانان است تا بتوانند به ورود غیرمجاز پاسخ مناسب دهند. همچنین، لازم است دوربین‌های نظاره‌گر این منطقه مخفی شوند. پس از عبور از منطقه حائل، فرد با استفاده از ابزارهای امنیتی، مورد بررسی قرار گرفته و سپس اجازه ورود به واحد، به او صادر می‌شود.

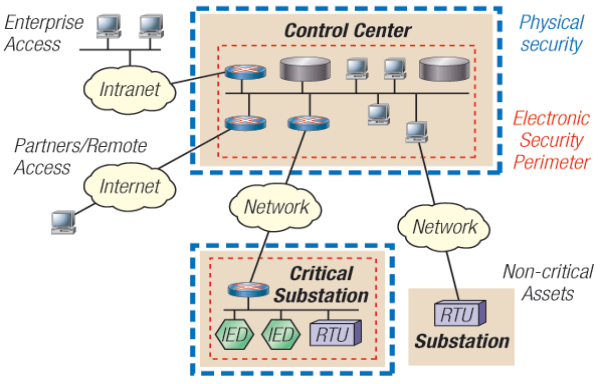
نقاط دسترسی به PSP های دوم (مانند یک در یا یک اتاق در یک واحد صنعتی)، نیازمند اعمال محافظتی مقاوم و مؤثر می‌باشند. دسترسی بین PSP های دوم نیز باید محدود گردد. به منظور دسترسی به هر محدوده فیزیکی دوم، حداقل باید از دو فاکتور تأیید صلاحیت استفاده شود. تمامی دسترسی‌ها باید ثبت گشته و همچنین تلاش‌های غیرمجاز برای ورود باید پایش شده تا تشخیص داده شود و در نهایت، هشدار اعلام گردد.

موقعیت ویژه‌ای که استفاده از PSP سوم در آن ضروری به نظر می‌رسد، نقاط دسترسی به اتاق‌های کنترل مرکزی است. بیشتر اپراتورها در برابر استفاده از سیستم‌های دسترسی رمزی مقاومت می‌کنند. زیرا در مواقع ضروری، باید بتوانند به راحتی به هرجا که لازم باشد، رفته و به هر وسیله مورد نیاز دسترسی داشته باشند. یک راه‌حل، استفاده از دوربین‌هایی است که نقاط دسترسی را نظاره می‌نمایند. در شرایط عادی، پرسنل امنیتی می‌توانند افرادی را که وارد اتاق کنترل می‌شوند را نظاره کرده و راه‌های ورود دیگر به اتاق کنترل را قفل کنند. در شرایط اضطراری، درها باید قابلیت باز و بسته‌شدن دستی را داشته باشند تا تعارضی میان امنیت فیزیکی و محدودکردن اپراتورها وجود نداشته باشد. دسترسی بین ابزارها و یا PSPهای سوم نیز باید محدود گردد. مثالی از PSPهای سوم می‌تواند اتاقک‌های قفل‌شده‌ای باشد که در آن ماژول[1]های سیستم توزیع کنترل (DCS[2]) قرار دارند و معمولاً در داخل یک اتاق امنیتی و یا PSP دوم قرار می‌گیرند. PSP های سوم تنها برای ابزارهای در معرض حمله با بالاترین احتمال خطر تعریف می‌شوند که بسته به نوع هر سیستم تغییر می‌یابد.

هنگام اعمال حفاظت فیزیکی به ابزارهای سیستم، لازم است آن‌ها را به روشی طبقه‌بندی نمود. به‌عنوان مثال، همه ماژول‌های DCS را در یک اتاق حفاظت‌شده قرار داد. به طور کلی، کلیه وسایلی که از درجه اهمیت زیادی برخوردار هستند، لازم است در یک اتاق قفل‌شده قرار بگیرند. سوئیچ‌های شبکه عموماً قفل نشده هستند که این مسأله امری اشتباه است. چاپگرها باید در یک اتاق و یا در یک تأسیسات بزرگ‌تر تحت حفاظت باشند. بهتر است محل قرارگیری آن‌ها در یک ناحیه پر رفت‌وآمد باشد تا کارکنان به‌راحتی هر اتفاق مشکوکی را تشخیص دهند. تمامی کنترل‌کننده‌های برنامه‌پذیر منطقی، صرف‌نظر از درجه اهمیت‌شان، لازم است در یک محوطه بسته و حتی در صورت امکان، در یک اتاق قفل شوند. تمامی ثبات‌ها، رله‌ها و سایر وسایل اترنتی مشابه باید به نحوی از حفاظت فیزیکی برخوردار باشند.

هدف مقاوم‌سازی با حفاظت فیزیکی، به حداقل‌رساندن احتمال یک حمله محلی با بازدارنده‌های محلی ساده مانند ایستگاه‌های نگهبانی، سیم خاردار و دوربین‌های امنیتی است، تا هرگونه حمله قریب‌الوقوع با راه‌بردهای طبقه‌بندی‌شده به تأخیر بیافتد و همچنین، سازوکارهایی به‌کار گرفته شود که هرگونه تلاش برای دسترسی غیرمجاز را پایش و تشخیص دهد.

اگر ابزاری به صورت محلی در معرض خطر قرار گیرد، ضروری است که آن را مجدداً طراحی کرد تا خطرات مربوط به حمله‌ای مشابه به حداقل برسد. در هنگام تصمیم‌گیری در مورد نحوه مقاوم‌سازی یک PSP باید بین عملکرد، در دسترس‌پذیری و امنیت آن تعادلی برقرار شود. به عنوان مثال، افراد دارای صلاحیت در مواقع ضروری نباید توسط موانع امنیتی فیزیکی معطل شوند. اهداف مقاوم‌سازی فیزیکی می‌تواند شامل اتاق‌ها، محیط‌های بسته، اتاق‌های کنترل، پنل‌ها و ... باشد و هر دسته از اهداف، چالش طراحی منحصر به فردی را می‌طلبد. در تعیین اولویت اهداف و میزان مقاوم‌سازی هر هدف، طبقه‌بندی ابزار به همراه تخمین‌های آسیب‌پذیری محیط، می‌تواند نقش اساسی ایفا نماید. به طور کلی، مقاوم‌سازی فیزیکی کامل یک واحد صنعتی، کار نسبتاً بزرگی است.



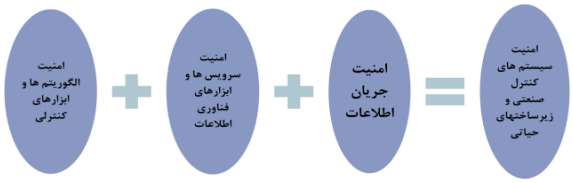
شکل (۱): نمونه‌ای از اجرای امنیت فیزیکی و الکترونیکی [۱۹]

1- Module
2- Distributed Control System

۳-۲- راه‌کارهای ساختاری

سیستم‌های کنترل صنعتی، وظیفه هدایت وکنترل فرآیندهای فیزیکی را برعهده دارند. این سیستم‌ها معمولاً متشکل از مجموعه‌ای از اجزای متعددی شامل حسگرها، عملگرها، واحدهای پردازش داده مانند کنترل‌کننده‌های منطقی قابل برنامه‌ریزی (PLCs[1])، شبکه‌های ارتباطی و رایانه‌های مرکزی می‌باشند.

در شکل (۲)، رابطه‌ی امنیت سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی با توجه به ماهیت اجزای تشکیل‌دهنده این سیستم‌ها بیان می‌شود.

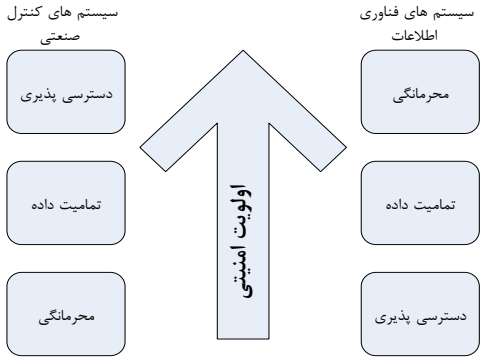


شکل (۲): رابطه امنیت سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی

راه‌کارهای ساختاری با توجه به رابطه بیان‌شده در شکل (۲)، به بررسی چگونگی حفاظت از سه لایه جریان اطلاعات، سرویس‌ها و ابزارهای فن‌آوری اطلاعات و الگوریتم‌ها و ابزارهای کنترلی و اجرای اصل دفاع در عمق می‌پردازند.

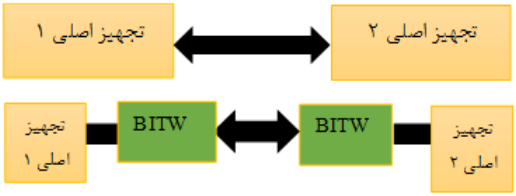
۳-۲-۱- حفاظت از جریان اطلاعات

سیستم‌های کنترل صنعتی دارای خصوصیات ویژه‌ای هستند که آن‌ها را از سیستم‌های فن‌آوری اطلاعات متمایز می‌کند. تفاوت در اولویت امنیتی در سیستم‌های کنترل صنعتی و سیستم‌های فناوری اطلاعات در شکل (۳)، نمایش داده شده است.



شکل (۳): اولویت‌های امنیت در سیستم‌های IT و کنترل صنعتی [۲۰]

به طور معمول، به منظور حفاظت از جریان اطلاعات، ابزارهایی نظیر امضای دیجیتال، رمزنگاری و تأیید هویت و ... پیشنهاد می‌شوند. ولی با توجه به اهمیت بسیار زیاد عدم تأخیر و دسترس‌پذیری در سیستم‌های کنترل صنعتی، این ابزارها باید متناسب با محدودیت‌های این سیستم‌ها طراحی شوند. برای مثال رمزنگاری ابزاری مشترک برای زیرساخت‌های کنترل صنعتی و فن‌آوری اطلاعات محسوب می‌شود، اما اجرای آن در این سیستم‌ها نیازمند تطبیق آن با مشخصات خاص سیستم‌های کنترل صنعتی است. اگرچه در مراجعی نظیر [۲۳-۲۱] توصیه‌هایی به این منظور ارائه شده است اما به طور کلی، می‌توان گفت معمولاً بازنگری در پروتکل‌ها و سیستم‌های قدیمی به سادگی امکان‌پذیر نیست. بنابراین، روش رمزنگاری BITW[2] برای رمزنگاری سیستم‌های قدیمی پیشنهاد شده است [۲۴]. مرجع [۲۵] نشان می‌دهد که راه‌کار BITW میزان تأخیر ناشی از رمزنگاری را به حداقل می‌رساند. تجهیزات BITW در هر دو سوی یک انتقال داده بین دو تجهیز قرار می‌گیرند. شکل (۴)، مسیر ارتباطی قبل و بعد از استفاده از BITW را نشان می‌دهد:



شکل (۳): تجهیزات BITW [۲۵]

مطابق شکل (۴)، دو تجهیز به دو سر ارتباط افزوده می‌شوند و در واقع، تجهیزات اصلی فقط با تجهیز BITW خودش در ارتباط هستند. ارتباطات بین BITW بدون نیاز به ایجاد تغییرات و به‌روزرسانی در تجهیزات اصلی شبکه، به صورت رمز انجام می‌گیرد. تجهیزات BITW برای دسته گسترده‌ای از شبکه‌ها (RS-232، Ethernet و...) موجود است، مانند:

- CEP5 LC SCADA Network Encryptor محصول شرکت Alutech
- Senetas certified high-speed encryptor محصول شرکت Senetas

امضاء دیجیتالی برای تأیید هویت پیام‌ها، دستورات، و یا بخش‌هایی از نرم‌افزار استفاده می‌شود. به عنوان مثال، در یک سیستم اسکادا[3]، اگر اطلاعات فرستاده‌شده توسط حسگر و یا ماژول حسگر امضاء دیجیتالی شود، RTU[4] که دریافت‌کننده اطلاعات است

1- Programmable logic controllers

2- Bump-In-The-Wire
3- SCADA(Supervisory Control And Data Acquisition)
4- Remote Terminal Unit

می‌تواند تأیید نماید که این اطلاعات از حسگری تأیید شده و واقعی رسیده است و اطلاعات دروغینی از یک مهاجم نیست. امضاء دیجیتالی امکان پاسخ به این سوال را فراهم می‌کند که یک بسته نرم‌افزاری و یا به‌روزرسانی نرم‌افزار از منبعی قابل اطمینان آمده است یا خیر. در مرجع [۲۶]، روش‌های تأیید هویتی ارائه شده است که با کمک الگوریتم‌های مدل‌سازی مجدد می‌تواند برای مدت‌زمان زیادی در یک سیستم به‌کار گرفته شود. در مورد حمله استاکس‌نت، کدهای مخرب به یک PLC تزریق و موجب تغییر سرعت درایوها شده بودند. اما اگر تغییراتی که در کدهای PLC رخ داده بود و یا هرگونه به‌روزرسانی نرم‌افزاری آن، در ابتدا نیاز به تأیید دیجیتالی داشت، این حمله توسط PLC تشخیص داده می‌شد و لذا عملیات تغییر کد صورت نمی‌گرفت. امضاء دیجیتالی می‌تواند حتی سیستم را از تغییرات در پیکربندی سخت‌افزاری محافظت نماید. به عنوان مثال، مهاجم ممکن است که کالیبراسیون حسگر را تغییر دهد. بروز این اتفاق برای سیستم‌های کنترل صنعتی که ناحیه جغرافیایی وسیعی را در برمی‌گیرند، احتمال بیشتری دارد. زیرا در این سیستم‌ها نمی‌توان دسترسی فیزیکی به حسگرها را کاملاً تحت کنترل قرار داد. استفاده از امضاء دیجیتالی این مشکل را تا حد زیادی حل می‌نماید و می‌تواند برای تأیید سخت‌افزارها نیز استفاده شود. به عنوان مثال، زمانی‌که RTU به یک شبکه اسکادا متصل است، با استفاده از امضاء دیجیتالی می‌توان از هویت سخت‌افزاری که داده‌هایی را به اسکادا می‌فرستد، اطمینان حاصل کرد.

۳-۲-۱-۱- افزایش امنیت پروتکل‌های صنعتی

امروزه پروتکل‌های ارتباطی بسیار زیادی در سیستم‌های کنترل صنعتی استفاده می‌شوند. در اکثر آن‌ها توجه ویژه‌ای به همگام‌سازی[1]، پشتیبانی از عملیات بلادرنگ و صرفه اقتصادی شده است و در هر یک، درجه‌های مختلفی از امنیت و قابلیت اطمینان ذاتی وجود دارد که باید در هنگام ایجاد امنیت در آن‌ها در نظر گرفته شود. اما عموماً این پروتکل‌ها از ویژگی‌های امنیتی نظیر احراز اصالت و رمزنگاری صرف‌نظر کرده‌اند. از سوی دیگر در جهت پشتیبانی از نیازهای رو به رشد تجاری و به منظور اتصال به شبکه‌های اینترنت و پروتکل اترنت اصلاح شده‌اند، بنابراین، در برابر حملات سایبری بسیار آسیب‌پذیر می‌باشند. از سویی دیگر، در یک سیستم کنترل صنعتی، نوع پروتکل‌های در حال اجرا نقش مهمی در تعیین نحوه حفاظت از سیستم دارد. بدین ترتیب، به منظور امن‌کردن این پروتکل‌ها، ابتدا باید آسیب‌پذیری‌ها و خطرات پیش‌روی آن‌ها بررسی شده سپس توصیه‌هایی برای ایمن‌سازی آن‌ها ارائه گردد. در انتخاب پروتکل ارتباطی در یک واحد صنعتی، باید توجه داشت که تمامی ابزارها و کنترل‌کننده‌ها با یک پروتکل سازگار باشند تا بتوان از هزینه‌ها و پیچیده‌شدن روند امن‌سازی آن‌ها کاست. با این حال، این مهم همواره عملی نیست و نمی‌توان همیشه از یک پروتکل سازگار استفاده کرد.

۳-۲-۲- حفاظت از سرویس‌ها و ابزارهای فن‌آوری اطلاعات

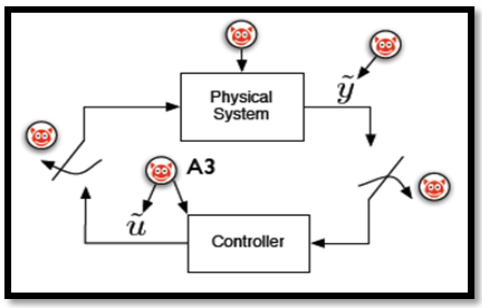
سرویس‌ها و ابزارهای فن‌آوری اطلاعات مانند رایانه‌ها، سرورها، چاپگرهای دارای سیستم عامل و غیره که در سیستم‌های کنترل صنعتی استفاده می‌شوند در معرض حملات سایبری و بدافزاری بیشتری می‌باشند. اگر مهاجم به یک تجهیز یا سرویس دسترسی یابد، معمولاً می‌تواند کلیه ارتباطاتی که از طریق این تجهیز صورت می‌گیرد را تحت کنترل خود درآورد. حفاظت‌های اعمال‌شده به این سرویس‌ها و ابزارها به عوامل گوناگونی بستگی دارند. حفاظت‌ها به‌طور کلی با سطح ریسک و یا حیاتی‌بودن تجهیز تغییر می‌یابند. استفاده از سرورهای امن، دیوار آتش، سیستم‌های تشخیص نفوذ و غیره برای حفاظت از این سرویس‌ها و تجهیزات توصیه می‌گردد.

۳-۲-۳- حفاظت از الگوریتم‌ها و ابزارهای کنترلی

تفاوت اصلی سیستم‌های کنترل صنعتی با سیستم‌های فن‌آوری اطلاعات، تعامل آن‌ها با دینامیک فیزیکی است. ابزارهای رایج مقابله با حملات سایبری می‌توانند تا حدودی سازوکارهای لازم برای امن‌سازی سیستم‌های کنترل صنعتی را ارائه دهند اما این سازوکارها به تنهایی برای اجرای راهبرد دفاع در عمق کافی نمی‌باشند [۹]. پیشتر تحقیقات در حوزه مقابله با حملات سایبری بر روی حفاظت از جریان اطلاعات، سرویس‌ها و تجهیزات فن‌آوری اطلاعات متمرکز شده‌اند و متاسفانه چگونگی اثر حملات بر روی ابزارها، تخمینگرها و الگوریتم‌های کنترل را در نظر نگرفته‌اند. بنابراین، این تحقیقات چگونگی اثر حملات بر دنیای فیزیکی را بررسی نکرده‌اند. مهاجم ممکن است بتواند کدهای نامطلوب خود را مخفی کند و از روش‌های پیچیده‌ی فن‌آوری اطلاعات برای حمله به سیستم کنترل صنعتی استفاده کرده و به‌طور مرتب روش‌های خود را به‌روزرسانی کند، اما در نهایت، نمی‌تواند هدف نهایی خود "ایجاد صدمه و اثر منفی بر روی سیستم فیزیکی" را پنهان نماید. مهاجم هدف نهایی خود را از سه طریق زیر انجام می‌دهد:

۱. صدمه به حسگر و یا ارسال داده اندازه‌گیری غلط و مخرب از حسگر به کنترل‌کننده، به این ترتیب کنترل‌کننده را در تصمیم‌گیری دچار خطا نموده است.
۲. ایجاد تغییرات مخرب در خروجی کنترل‌کننده و یا خود کنترل‌کننده
۳. صدمه به عملگر و یا اختلال در سیستم ارتباطی عملگر

1- Synchronization



شکل (۴): حمله‌های سایبری به سیستم کنترل [۲۷]

به‌طور کلی، می‌توان گفت مهاجم سعی دارد با صدمه به یکی از اجزای کنترل یعنی حسگر، عملگر، کنترل‌کننده و یا سیستم ارتباطی آن‌ها و همچنین تحت تأثیر قراردادن الگوریتم کنترل، هدف خود را تحقق بخشد. از این‌رو، حفاظت از این تجهیزات و ارتباطات آن‌ها بسیار حیاتی است. از سویی دیگرریال برای اطمینان از قابلیت تحمل سیستم‌های کنترل صنعتی در برابر حملات برنامه‌ریزی‌شده بدافزاری، مقاوم‌سازی الگوریتم‌های کنترلی ضروری است. مفهوم انعطاف‌پذیری در سال‌های اخیر جهت بهبود پاسخ و بازیابی سریع در مواجه با حوادث غیرمنتظره و اختلال‌های عمدی و غیرعمدی سیستم‌های کنترل صنعتی، مطرح شده است. طبق تعریف، یک سیستم کنترل انعطاف‌پذیر باید در صورت مواجه با اختلالات، اثرات آن‌ها را کاهش داده و عملکرد مطلوب سیستم را برآورده نماید [۲۹-۲۸]. در یک سیستم قدرت، مدیریت عیب و بازیابی دو امر مهم تلقی می‌شوند. هنگامی‌که در اثر اختلال، وقفه‌هایی در توزیع برق اتفاق می‌افتد، سیستم باید بتواند به‌طور سریع بازیابی شود. با بهره‌گیری از مفهوم انعطاف‌پذیری در این زمینه، قابلیت اطمینان و هماهنگی در کنترل و حفاظت شبکه بیشتر گشته و سیستم می‌تواند در برابر اختلالات موجود انعطاف‌پذیر گردد [۳۰].

۳-۲-۳-۱- حفاظت از تجهیزات سیستم کنترل

همان طور که بیان شد، حمله سایبری که لایه فیزیکی یک سیستم کنترل صنعتی را نشانه می‌گیرد، معمولاً تمرکز اصلی خود را روی حسگرها، عملگرها و یا کنترل‌کننده‌ها می‌گذارد، مانند آنچه در حمله استاکس‌نت رخ داد. توصیه‌های زیر مثال‌هایی برای اعمال حفاظت‌ها به چند تجهیز کنترلی است.

کنترل‌کننده‌های منطقی قابل برنامه‌ریزی (PLC)

بسیاری از کنترل‌کننده‌های منطقی قابل برنامه‌ریزی فاقد برنامه‌های حفاظتی می‌باشند. بدین ترتیب، حفاظت‌های درونی برای آن‌ها محدود است و وسایل حفاظتی جانبی مانند TSA[1] [۳۱] مورد نیاز است. توجه شود که بعضی تولیدکنندگان، سازوکارها و تجهیزات حفاظتی ویژه‌ای را نیز پیشنهاد می‌کنند.

1- Tofino Security Appliance

ماژول‌های سیستم کنترلی گسترده (DCS)

تا چندی پیش، ماژول‌های DCS پیشرفت زیادی در زمینه حفاظت نداشتند. به تازگی سازندگان DCSهای پیشرفته (مانند شرکت‌های Siemens [۳۲]، ABB [۳۳]، Emerson [۳۴] و غیره) ادعا می‌نمایند که ابزارهای مورد قبولی ساخته‌اند که در حفاظت از این وسایل استفاده می‌شوند. اعمال کنترل‌های حفاظتی به یک ماژول DCS ممکن است بسته به طول عمر دستگاه دشوار بوده و در مواردی نیز به یک سخت‌افزار اضافی نیاز باشد.

عملگرها و حسگرهای هوشمند

با توجه به افزایش استفاده از عملگرها و حسگرهای هوشمند، راه نفوذ مهاجم به سیستم از طریق این تجهیزات گشوده شده است. بنابراین، طراحی و نصب ماژول‌های شناسایی و تشخیص نفوذ به حسگر و عملگر (مانند آنچه در [۲۷ و ۳۵] رفته است) جهت حفاظت از این تجهیزات، ضروری است.

۳-۲-۳-۲- افزایش قابلیت تحمل الگوریتم‌های کنترلی در برابر حمله

مرکز کنترل با استفاده از داده‌های اندازه‌گیری شده و مدل سیستم، حالت‌های درونی آن را تخمین می‌زند و دستورات کنترلی را صادر می‌کند. اگر داده‌های ارسالی از ابزارهای لایه فیزیکی در محدوده قابل قبول نباشند، مرکز کنترل متوجه می‌شود. اما مهاجم هوشمند ممکن است به نحوی داده‌ها را دستکاری کند که آن‌ها همچنان در محدوده قابل قبول بمانند. از آن‌جایی‌که سیستم‌های کنترلی معمول توانایی تشخیص این دستکاری هوشمندانه را ندارند، براساس این داده‌ها تصمیم‌گیری نموده و امکان بروز حوادث جبران‌ناپذیر وجود خواهد داشت. الگوریتم‌های کنترلی با قابلیت تحمل بالا در برابر حملات سایبری، الگوریتم‌هایی هستند که با تشخیص و شناسایی حملات، اثرات نامطلوب آن‌ها را بر روی سیستم تحت کنترل کاهش داده و همچنین قابلیت بازگشت به شرایط کاری عادی در مدت زمان کوتاهی بعد از حمله را دارند. بدین ترتیب، به منظور اجرای کامل راه‌برد دفاع در عمق، ضروری است سیستم‌های کنترل صنعتی طراحی و ساخته شوند:

۱) قابلیت تشخیص و شناسایی حملات سایبری و اثرات آن‌ها را داشته باشد (تهیه ساختارهای مناسب به منظور تشخیص نفوذ براساس مدل کیفی یا کمی سیستم تحت کنترل).

۲) دارای الگوریتم‌های کنترلی هوشمندی باشند که اثرات حمله را کاهش دهند. همچنین دارای قابلیت بازیابی سریع باشند.

در مرجع [۲] به نمونه‌هایی از تلاش‌های صورت‌گرفته به منظور دستیابی به سیستم‌های کنترل صنعتی با قابلیت تحمل بالا نسبت به حملات سایبری، اشاره شده است.

۴- اشتباهات رایج

با اجرای دسته‌ای از نکات امنیتی نمی‌توان از امن‌بودن سیستم کنترل صنعتی اطمینان داشت و باید ارزیابی‌های مجدد در بازه‌های زمانی مختلف صورت پذیرد. به طور کلی، حتی درصورت اتخاذ تدابیر امنیتی، اشکالاتی نظیر اطمینان کاذب، عدم پیکربندی مناسب، اجرای کورکورانه مقررات و استانداردها، عدم اتخاذ ظرفیت و محدوده تحت بررسی و ... همچنان وجود دارند [۳۶].

۴-۱- اطمینان کاذب[1]

در اکثر موارد تصور می‌شود که با یک بار تلاش برای ارزیابی وضعیت امنیتی سیستم و رفع نواقص و آسیب‌پذیری‌های تشخیص داده شده، دیگر نگرانی درخصوص امنیت سیستم بی‌معنا است. درصورتی‌که با توجه به وجود آسیب‌پذیری‌های ناشناخته (Zero-Day) و گسترش رو به رشد آسیب‌پذیری‌ها، به هیچ وجه نمی‌توان از امنیت سیستم اطمینان داشت. به منظور رفع این مشکل می‌توان ارزیابی منظم و مرتب را در دستور کار قرار داد و از تمام توان فنی و تشخیصی برای جلوگیری و تشخیص تهدیدات استفاده کرد.

۴-۲- عدم پیکربندی مناسب[2]

عدم پیکربندی مناسب ناشی از پیاده‌سازی معیوب است. طبق بررسی‌های صورت‌گرفته، حدود ۱۶ ٪ از حملات، ناشی از عدم پیکربندی مناسب است [۳۶] و در مراجعی نظیر NERC CIP [۱۵]، CFATS [۱۱]، NRCRG5.71 [۱۶] و NIST SP800 [۱] توصیه‌های امنیتی در ارتباط با مدیریت و کنترل پیکربندی مطرح شده است. عدم پیکربندی مناسب موارد زیر را تحت پوشش قرار می‌دهد:

- عدم تغییر رمز عبورهای پیش‌فرض.
- عدم پایش مناسب امنیت داخلی ناحیه‌ها.
- تغییر آگاهانه تدابیر امنیتی. به عنوان مثال، امکان برقراری ارتباط شبکه خارجی با شبکه کنترل به منظور به‌روز بودن داده‌های شبکه مالی و تجاری.

۴-۳- اجرای دقیق مقررات بدون بررسی نتایج آن

اگرچه هدف از وضع قوانین، استانداردها و دستورالعمل‌ها تأمین امنیت بهتر برای سیستم است، اما ممکن است در هنگام پایش کارآمدی آن‌ها، سیستم کنترل صنعتی دچار مشکل شود. باید توجه داشت که در مورد سیستم‌های کنترل صنعتی اولویت اول، بررسی قابلیت اعمال مقررات و یا روش‌های تست آن‌ها روی سیستم کنترل صنعتی مورد نظر است تا عملکرد سیستم دچار اخلال نشود.

۴-۴- عدم توجه به ظرفیت و محدوده مورد بررسی

یکی از اشکالات از دید امنیتی در سیستم‌های کنترل صنعتی، عدم توجه به ویژگی‌های منحصر به فرد سیستم کنترل صنعتی است. از جمله این ویژگی‌ها لزوم دسترسی‌پذیری، ارتباط پیوسته (هرچند غیرمستقیم)، این سیستم‌ها با شبکه‌های دیگر است. به‌طور کلی، لازم است وضعیت امنیتی سیستم‌های کنترل صنعتی به‌طور مداوم بررسی شود حتی اگر سیستم بدون تغییر باشد زیرا شبکه‌هایی که با آن در ارتباط هستند، مدام در حال به‌روزرسانی و تحول هستند. همچنین، ضروری است در هنگام ارزیابی وضعیت امنیتی و امن‌کردن این سیستم‌ها، ویژگی‌های منحصر به فرد آن‌ها مانند دسترسی‌پذیری، مورد توجه قرار گیرد.

۵- نتیجه‌گیری

در این مقاله به بررسی راه‌کارهای ارائه‌شده در زمینه امنیت سایبری سیستم‌های صنعتی، حول راه‌برد کلان دفاع در عمق، پرداخته شد. لازمه اجرای راه‌برد دفاع درعمق در سیستم‌های کنترل صنعتی، درنظرگرفتن اصول امنیتی و مقاوم‌بودن در لایه‌های مختلف سیستمی آن‌ها است. معمولاً سیستم‌های کنترل صنعتی و به خصوص لایه فیزیکی آن‌ها، به گونه‌ای طراحی شده‌اند که فقط توانایی مقابله با دسته‌ای از نقص‌های غیرعمدی و تصادفی را دارند. اما این ویژگی به تنهایی برای مقابله در برابر نقص‌های برنامه‌ریزی‌شده که ناشی از کدهای مخرب هستند، کافی نیست. با توجه به گستردگی راه‌کارهای مطرح در زمینه مقابله با حملات سایبری در سیستم‌های کنترل صنعتی، در این مقاله یک دسته‌بندی کلان پیشنهاد و در قالب این دسته‌بندی به بحث و بررسی این راه‌کارها پرداخته شد.

۶- 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. A. Afshar, A. Termehchy, A. Golshan, A. Aghaeeyan, and H. Shahriyari, “Survey on Cyber Security of Industrial Control Systems,” Journal of Control, vol. 8, no. 1, Spring 2014. (in Persion)
3. http://searchsecurity.techtarget.com/definition/defense-in-depth, accessed on 07/07/2018.
4. P. Wade, P. Malkewicz, and J. Novak, “Industrial Cyber Security: From the Perspective of the Power Sector,” Presented at DEFCON 18, Riviera Hotel, Las Vegas NV, July 29th-August 1st 2010.
5. U.S. Department of Homeland Security (DHS), “Recommended Practice: Improving Industrial Control Systems Cybersecurity

1- Complacency
2- Misconfiguration

with Defense-In-Depth Strategies," Control Systems Security Program (CSSP), US-CERT Defense in Depth, October 2009.

6. ISA, "ANSI/ISA–62443-1-1 (99.01.01) Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models," 2007.
7. A. Afshar, A. Termehchy, A. Golshan, A. Aghaeeyan, S. Soleimani, and H. Shahriyari, "Comprehensive Conceptual Model of Control System's Vulnerabilities," journal of Passive Defence, vol. 24, no. 6, pp. 23-32, winter 2015. (in Persion)
8. ISA, "ANSI/ISA-62443-1-1, (ANSI/ISA-99.00.01-2007) Security for Industrial Automation and Control Systems Terminology, Concepts and models," 2007.
9. Stouffer, Keith, Joe Falco, and Karen Scarfone, "Guide to Industrial Control Systems (ICS) Security," NIST special publication 800.82, 2011.
10. http://isa99.isa.org, ISA99: Developing the Vital ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security, accessed on 07/07/2018.
11. U.S. Department of Homeland Security (DHS), "Chemical Facility Anti-Terrorism Standards (CFATS)," 2006.
12. IEC, TR, "62210: Power system control and associated communications–Data and communication security," International Electrotechnical Commission, 2003.
13. PA Consulting Group, "NISCC: Good Practice Guide: Process Control and SCADA Security," October 2005.
14. American Chemistry Council's Chemical Information Technology Council (ChemITC) ™, "Chemical Sector Cyber Security Program; Guidance for Addressing Cyber Security in the Chemical Industry," Version 3.0, 2006.
15. http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx, accessed on 07/07/2018.
16. U.S. Nuclear Regulatory Commission, "Cyber security programs for nuclear facilities," Regulatory Guide 5.71, 2010.
17. NERC-CIP Cyber Security Standards, "Standard CIP-005-3a-Cyber Security- Electronic Security Perimeter(s),".
18. NERC-CIP Cyber Security Standards, "Standard CIP-006-3c-Cyber Security-Physical Security of Critical Cyber Assets,".
19. http://www.bomara.com/G arrett/wp_nerc_cip_compliance.html, accessed on 07/07/2018.
20. http://embedded.communit ies.intel.com, accessed on 07/07/2018.
21. F. Igor Nai, A. Carcano, M. Masera, and A. Trombetta, "Design and implementation of a secure modbus protocol," Critical Infrastructure Protection III, Springer Berlin Heidelberg, pp. 83-96, 2009.
22. I. Eusgeld, F. Freiling, and R. H. Reussner, "Dependability Metrics: GI-Dagstuhl Research Seminar; Dagstuhl Castle, Germany; October 5-November 1, 2005," Advanced Lectures, vol. 4909, Springer 2008.
23. IEEE Standards Association; WGC6; P1711 - Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.
24. Department of Homeland Security, "Control Systems Communications Encryption Primer," U.S. Department of Homeland Security (DHS), 2009.
25. P. Tsang Patrick and W. S. Sean, "YASIR: A low-latency, high-integrity security retrofit for legacy SCADA systems," In Proceedings of The Ifip Tc 11 23rd International Information Security Conference, Springer US, pp. 445-459, 2008.
26. C. Rasika, C. Hauser, and D. E. Bakken, "Long-lived authentication protocols for process control systems," International Journal of Critical Infrastructure Protection, vol. 3, no. 3, pp. 174-181, 2010.
27. A. Saurabh, "On cyber security for networked control systems," Ph.D. Thesis, University of California, Berkeley, 2011.
28. D. Wei. and K. Ji, "Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights," IEEE 3rd International Symposium on Resilient Control Systems (ISRCS), 2010.
29. C. G. Rieger, D. I. Gertman, and Miles A. McQueen, "Resilient control systems: next generation design research," IEEE 2nd Conference on Human System Interactions, 2009.
30. R. Arghandeh, Alexandra. Von Meier, L. Mehrmanesh, and Lamine Mili, "On the definition of cyber-physical resilience in power systems," Renewable and Sustainable Energy Reviews 58, pp. 1060-1069, 2016.
31. https://www.tofinosecurity.com/products/tofino-security-appliance, accessed on 07/07/2018.
32. http://www.siemens.com/entry/cc/en/, accessed on 07/07/2018.
33. http://www.abb.com/, accessed on 07/07/2018.
34. http://www.emerson.com/Accessed on 07/07/2018.
35. Termehchy, Atefeh, "Control of cyber attacks damages to critical infrastructure," M.Sc. Thesis, Amirkabir University of Technology, Iran, 2013.(in Persion)
36. D. Knapp Eric and J. T. Langill, "Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems," Syngress, 2014.

تشکر و قدردانی

این مقاله در ضمن اجرای فاز مطالعاتی پروژه " طراحی و پیاده‌سازی سامانه جامع مقابله با بدافزارها در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی" تهیه شده است و در راستای طرح کلان ملی "معماری و راه‌اندازی مرکز ملی دفاع سایبری و سامانه‌های زیرساختی فضای سایبری"، در پژوهشکده پدافند غیرعامل دانشگاه صنعتی امیرکبیر اجرا شده است.

Review of the Types of Strategies to Improve Security of Industrial Control Systems and Critical Infrastructure

A. Afshar[*], A. Termechi, A. Golshan, A. Aghaeian, H. R. Shahriari, S. Soleymani

Abstract

Nowadays, economic and political development of a society depends on the performance of critical infrastructure such as energy, water, ICT, banking, research and education, transportation, health and treatment, etc. Control and monitoring of critical infrastructure and industrial systems are performed by intelligent network control systems. Major threats to critical infrastructure and industrial control systems are targeted attacks such as cyber ones in which the attacker tailors its strategy for industrial control systems. In order to achieve a secure community, development of protected infrastructure, securing the critical information, and construction of intrinsically secure control systems are absolutely essential. There are a vast number of solutions to security of industrial control systems. The aim of this paper is to classify the solutions into two categories, namely basic strategies and structural strategies. Moreover, some of the common pitfalls and mistakes in the employment of security solutions are addressed.

Key Words: *Industrial Control System and Critical Infrastructure,Cyber Attack, Defense in Depth- Basic Strategies,Structural Strategies*

[*] Amirkabir University of Technology - (aafshar@aut.ac.ir) - Writer-in-Charge