فصلنامه علمی امنیت ملی
سال چهاردهم، شماره پنجاه و یکم، بهار ۱۴۰۳
مقاله ششم از صفحات ۱۹۸-۱۵۷

مقاله پژوهشی: ارائه الگوی راهبردی بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور

مجید غیوری ثالث[۱]، ناصر مدیری[۲]، محمدرضا موحدی صفت[۳]، علیرضا سقایی[٤]

تاریخ دریافت: ۱۴۰۱/۰۸/۲۸ تاریخ پذیرش: ۱۴۰۱/۱۲/۱۳

چکیده

امروزه تهدیدهای سایبری سامانه‌های کنترل صنعتی که به‌طور فزاینده‌ای در زیرساخت‌های حیاتی استفاده می‌شوند، پیچیده‌تر از آن هستند که به‌سادگی بتوان با آن‌ها مقابله کرد. از این‌رو امنیت این سامانه‌ها از اضطراری‌ترین نگرانی‌های بازیگران صنعتی، از جمله دولت‌ها محسوب می‌شود. بر این اساس، ارائه الگوی راهبردی به‌کارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی (هدف این پژوهش) از ضروریت‌ها است. در این پژوهش محقق با مراجعه به ارکان جهت‌ساز حوزه سایبری، اسناد بالادستی کشور، اسناد و اقدامات راهبردی سایر کشورها، بررسی مدل‌ها و طرح‌های داخلی و بین‌المللی و با تحلیل خبرگی، اقدام به طراحی مدل مفهومی و استخراج ابعاد، مؤلفه‌ها و شاخص‌های تحقیق نموده و سپس برای پاسخ به سؤالات تحقیق، نسبت به طراحی پرسشنامه محقق ساخته مبتنی بر مصاحبه با خبرگان و اسناد مورد اشاره اقدام نموده‌است. نتایج این تحقیق نشان می‌دهد که الگوی راهبردی به‌کارگیری امن دارای۳ بعد، ۱۲ مؤلفه و ٦٧ زیرمؤلفه می‌باشد که مهمترین مؤلفه‌ها در بعد فرایند به ترتیب اولویت، ساختارها و نظامات، سیاست‌گذاری، قوانین و مقررات، به‌کارگیری و راهبری، در بعد فناوری به ترتیب سازماندهی امنیت، اقدامات پیشگیرانه، تحلیل و مدیریت حوادث، اقدامات تشخیصی و اقدامات بازیابی و در بعد منابع انسانی به ترتیب ظرفیت‌سازی و مدیریت منابع انسانی می‌باشند.

کلیدواژه: زیرساخت حیاتی، سامانه کنترل صنعتی، به‌کارگیری امن سامانه کنترل صنعتی

۱ .استادیار دانشکده برق و کامپیوتر دانشگاه جامع امام حسین(ع)
۲ .استادیار گروه کارشناسی ارشد مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد زنجان
۳.دانشیار دانشگاه عالی دفاع ملی
٤.دانش‌آموخته مقطع دکتری دانشگاه عالی دفاع ملی، (نویسنده مسئول)، رایانامه: alisaghaei@yahoo.com

مقدمه و بیان مسئله

سامانه‌های کنترل صنعتی از جمله سامانه‌های کنترل نظارت و جمع‌آوری داده[1]، سامانه‌های کنترل توزیع شده[2]، سامانه‌های کنترل فرایند[3]، سامانه‌های فیزیکی-سایبری[4] یا کنترل کننده‌های منطقی قابل برنامه‌ریزی[5] هستند که اغلب در بخش‌های صنعتی و زیرساخت‌های حیاتی یافت می‌شوند، این سامانه‌ها اساساً سامانه‌های کنترلی بوده که در صنایعی مانند برق، آب و فاضلاب، نفت و گاز، شیمیایی، حمل و نقل، داروسازی، خمیر و کاغذ، مواد غذایی و آشامیدنی استفاده و عملیات تأسیسات صنعتی را برای مدیریت فرایندهای صنعتی مانند تولید، جابجایی و توزیع، کنترل و مدیریت می‌کنند (آنی، واتسون و نورس، ۲۰۱۹)[6]. افزایش اتصال شبکه‌های کنترل صنعتی به شبکه‌های سازمانی و استفاده از سیستم عامل‌های استاندارد، خطر بالقوه‌ای را برای امنیت و ایمنی زیرساخت‌های حیاتی ایجاد کرده است (تیمسونا و مرادیان، ۲۰۱۸)[7]. تهدیدات امنیت سایبری از افزایش پیچیدگی و اتصال سیستم‌های زیرساخت حیاتی سوء استفاده کرده و امنیت، اقتصاد، ایمنی و سلامت عمومی کشورها را در معرض خطر قرار می‌دهند (بنیادملی استاندارد و تکنولوژی آمریکا، ۲۰۱۸)[8]. اقدامات متداول که در شبکه‌های سازمانی برای کاهش خطر مرتبط با فناوری‌ها اجرا می‌شوند، اغلب در محیط‌های سامانه‌های کنترل صنعتی کارایی نداشته و متأسفانه، هیچ راه میانبر یا راه‌حل ساده، برای برطرف نمودن آسیب‌پذیری‌های

---

[1] SCADA

[2] DCS

[3] PCS

[4] CPS

[5] PLC

[6] Uchenna D Ani, Jeremy D McK. Watson, Jason R C Nurse Al Cook.and.Carsten, Maple

[7] Timpsona,Dominic.And.Moradian, Esmiralda

[8] NIST.CSWP

امنیت سایبری در سامانه‌های کنترل صنعتی وجود ندارد. از دیگر سو معماری سیستم کنترل مدرن، نیازهای تجاری و هزینه اقدامات کنترل، منجر بـه افـزایش ادغـام معمـاری فنـاوری اطلاعات شرکت‌های بزرگ و سامانه‌های کنترل صـنعتی مـی‌شـود. در ایـن راسـتا جـدایی فیزیکی به تنهایی دیگر امنیت فراهم نمی‌کند (وزارت امنیت داخلی آمریکا، ۲۰۱۶). پـیش-بینی می‌شود حملات امنیتی به سـامانه‌های کنترل صنعتی، به دلیل عقب مانـدگی ده سـاله امنیت این سامانه‌ها از امنیت فناوری اطلاعات، به‌طور فزاینده‌ای توسـط مهاجمـان افـزایش یابـد (سـوفوس، ۲۰۱۵).[1] مـدرن‌سـازی سـامانه‌هـای کنتـرل صـنعتی، استانداردسـازی پروتکـل‌های ارتباطی و افزایش ارتباط متقابل، حملات سـایبری بـه آن‌هـا را بـه شـدت افزایش داده است (یاداو و پاولا، ۲۰۲۱).[2] امنیت سایبری سیستم‌های کنتـرل صـنعتی تبـدیل بـه یـک نگرانـی مهـم‌تـر و گسـترده‌تـر شـده و مسـتلزم دسـتورالعمل‌هـا و رویـه‌هـای ساختارمندتری برای تعریف امنیت سایبری در اتوماسیون صنعتی و سیستم‌های کنترل است (استاندارد۱-۱-۶۲۴۴۳).[3] در کشور ما اسکاداهای غیربومی مصداق بـارز مـدخل تهدیـدات سایبری در زیرساخت‌های حیاتی هستند که ایـن زیرسـاخت‌هـا را بـا دقـت بـالا کنتـرل و مدیریت می‌کنند (تقی‌پور و همکاران، ۱۳۹۸). درحال حاضر، زیرساخت‌های حیاتی هریک تاحدی به فضای سایبری وابسته بوده و این وابستگی ضمن آن‌کـه مـی‌توانـد عـاملی بـرای تسهیل فعالیت زیرساخت‌ها در ارائه خدمات به مشتریان خود باشد، می‌تواند بسـتری بـرای شکل‌گیری تهدیدهای متنوع نیز باشد (گابریل، ۲۰۱۷).[4] از دیگرسو تخریب زیرساخت‌هـای حیاتی و یا ناتوانی آن‌ها در ارائه خدمات مـی‌تواند تأثیر منفی بر امنیت فیزیکی، اقتصـادی و یا ایمنی و سلامت عمومی بگذارد (وزارت امنیت داخلی آمریکا، ۲۰۱۹). لذا حفاظـت از آن‌ها جزء مسائل کلان و راهبردی محسوب می‌شـود و در برنامـه راهبـردی سـایبری اکثـر

[1] Sophos

[2] Yadav, Geeta.and Paul, Kolin

[3] IEC62443-1-1

[4] Gabriel

کشورها وجود دارد، در کشور ما نیز این فرایند در سیاست‌های کلی ابلاغی مقام معظم رهبری (مدظله‌العالی) در حوزه افتا و سایر اسناد بالادستی کشور مورد تأکید قرار گرفته است. حال با در نظر گرفتن اهمیت زیرساخت‌های حیاتی و تهدیدات، مشکلات، تنگناها، ناکارآمدی‌ها و ضعف‌های مورد اشاره، مهم‌ترین مسئله تحقیق، چگونگی الگوی راهبردی بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور و سعی بر این است که با شناخت حوزه‌های مرتبط با تهدیدات و آسیب‌پذیری‌های سایبری سامانه‌های کنترل صنعتی به‌کار رفته در زیرساخت‌های حیاتی ابعاد، مؤلفه‌ها وشاخص‌های مرتبط با سامانه‌های کنترل صنعتی امن احصاء و ارتباط بین مؤلفه‌ها و شاخص‌های شناسایی شده، مشخص گردد تا بتوان با توجه به آن، یک الگوی راهبردی برای به‌کارگیری امن این سامانه‌ها، در زیرساخت‌های حیاتی کشور ارائه داد. نتایج این مطالعه می‌تواند به عنوان اولین گام در یک تلاش راهبردی برای کمک به ذینفعان سامانه‌های کنترل صنعتی در مورد بکارگیری امن این سامانه‌ها عمل کرده و همچنین می‌تواند به توسعه دستورالعمل‌های امنیتی سامانه‌های کنترل صنعتی پیشرفته کمک کند تا بتوانند رابطه بین امنیت و بکارگیری امن را ایجاد نمایند. انتظار می‌رود ارائه چنین الگوی راهبردی بتواند باعث ایجاد همگرائی و هم‌افزائی شده و مشخص کند کجا باید دنبال آسیب‌پذیری‌های سامانه‌های موصوف بوده و چگونه می‌توان تهدیدات مترتب بر آن‌ها را مدیریت کرد تا بدینوسیله بتوان سامانه‌های کنترل صنعتی را در زیرساخت‌های حیاتی به‌صورت امن بکارگیری کرد.

اهمیت و ضرورت تحقیق:

انجام این تحقیق از آن جهت حائز اهمیت است که با ارائه الگوی راهبردی بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی مزیت‌های زیر حاصل می‌شود.

۱- می‌توان نسبت به ایجاد همگرائی و هم‌افزائی مبتنی بر یک نگاه واحد در خصوص بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی اقدام نمود.

۲- می‌توان نسبت به تسهیل فرایند مدیریت، تصمیم‌سازی و تصمیم‌گیری‌های مناسب، مؤثر و منطقی در راستای مدیریت تجهیزات مرتبط با سامانه‌های کنترل صنعتی موجود در زیرساخت‌های حیاتی، با رویکرد بکارگیری امن اقدام نمود.

۳- می‌توان نسبت به ایجاد یک رویکرد پیشگیرانه، جهت‌دهی هدفمند فعالیت‌ها در راستای مدیریت تهدیدات مرتبط با سامانه‌های کنترل صنعتی اقدام نمود.

همچنین ضرورت انجام این تحقیق با رویکرد سلبی این است که:

۱- برای مقابله با موج جدید قدرت‌طلبی و هژمونی جریان سلطه، اتکا به منابع و مدیریت سنتی قدرت، کافی نیست و عدم وجود یک الگوی راهبردی در بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی در رویارویی هم‌تراز، از طریق فضای سایبر موجب شکست و ایجاد هزینه به کشور می‌شود.

۲- با توجه به تهدید علنی دشمن به جنگ سایبری، نداشتن الگوی راهبردی درخصوص بکارگیری امن سامانه‌های کنترل صنعتی باعث جامع نبودن، نگاه بخشی و محدودنگری، عدم توجه به الزامات و نیازمندی‌های اهداف راهبردی در مباحث زیرساخت‌های حیاتی می‌شود.

۳- فقدان یک الگوی راهبردی و عدم کسب تمهیدات لازم در خصوص بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی، می‌تواند ضمن تحمیل هزینه‌های زیاد، اعتبار و اقتدار ملی را در سطح بین‌المللی خدشه‌دار کند.

پیشینه تحقیق:

میریوسفی و غفارپور (۱۳۹۹)، با بررسی مفاهیم مرتبط با زیرساخت‌های حیاتی و الزام محافظت از آن‌ها، به لزوم تغییر نگرش نسبت به مفاهیم حفاظت و تاب‌آوری زیرساخت‌های حیاتی اشاره و عملا در زمینه حملات سایبری و بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های سایبری اقدامی صورت نپذیرفته است. محمودزاده و همکاران (۱۳۹۷)، نسبت به احصاء و ارائه راهبردهای تأمین امنیت سایبری سامانه‌های

کنترل صنعتی در زیرساخت‌های حیاتی و رتبه‌بندی آن‌ها اقدام نموده‌اند. در این پژوهش ضمن اهمیت به نقش فضای سایبر به عنوان نهاد تأثیرگذار جهت تداوم فعالیت زیرساخت حیاتی، نسبت به امن‌سازی سامانه‌های کنترل صنعتی اقدام شده است ولی در خصوص ارائه مدل و نیز بکارگیری امن این سامانه‌ها اقدامی صورت نگرفته است. یاداو و پل (۲۰۲۱)، سعی می‌کنند با بررسی و پیوند دادن جنبه‌های مختلف امنیت اسکادا ضمن در نظر گرفتن نقاط ضعف شناخته شده آن‌ها و توضیح ارتباط بین معماری اسکادا و پروتکل‌های ارتباطی، به این سؤال پاسخ دهند که «کجا باید به‌دنبال آسیب‌پذیری‌های امنیتی بود؟» در این تحقیق ضمن بررسی معماری سیستم‌های اسکادا و حملات صورت گرفته به آن‌ها، نسبت به برجسته کردن نیازهای امنیتی در سیستم‌های اسکادا اقدام شده و عملا بدون ارائه یک مدل راهبردی، اشاره‌ای نیز نسبت به بکارگیری امن سامانه‌های کنترل صنعتی نمی‌شود. خاوالا (۲۰۱۹)[1] نسبت به بررسی ادغام سیستم‌های کنترل صنعتی با سیستم‌های تجاری اقدام نموده است. در این تحقیق، برروی مطالعه روش دفاع در عمق و کاربرد آن در سیستم‌های یکپارچه کنترل صنعتی تمرکز نموده و یک روش جدید تقسیم‌بندی برای سیستم‌های کنترل صنعتی پیشنهاد داده ولی به‌صورت خاص نسبت به بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی اقدامی صورت نپذیرفته است. ماگلاراس (۲۰۱۸)[2] یک معماری مبتنی بر سیستم تشخیص نفوذ محیط بلادرنگ را پیشنهاد می‌کند، که توانایی تجزیه و تحلیل و شناسایی سایبری را فراهم کرده و مسئولیت ارزیابی مداوم و محافظت از محیط امنیتی الکترونیکی را دارد. در این پژوهش، محقق جهت ارتقاء امنیت سامانه‌های اسکادا بیشتر بر مباحث فنی و تکنیکی تمرکز داشته تا مباحث راهبردی که موردنظر پژوهش حاضر است. تیمسونا و مرادیان (۲۰۱۸)، با بررسی چالش‌های سامانه‌های کنترل صنعتی، نسبت به ارائه یک مدل جهت همگام‌سازی ایمنی و امنیت در سامانه‌های پیشگفته اقدام نموده و سعی دارد بیان کند برای همسوسازی اقدامات

[1] Es-Salhi,Khaoula.

[2] Maglaras,Leandros.

امنیتی و ایمنی به اقداماتی فراتر از اقدامات فنی نیاز می‌باشد. علی‌رغم اینکه در این تحقیق بحث مناسبی در خصوص ناکافی بودن اقدامات فنی صورت گرفته و مدلی نیز در این زمینه ارائه شده ولی مشخصاً اشاره‌ای به بحث بکارگیری امن سامانه‌های کنترل صنعتی نشده است.

نوآوری تحقیق:

در برخی از تحقیقات، به تأثیر فناوری‌های نوین، مخصوصا فناوری اطلاعات و ارتباطات در زیرساخت‌های حیاتی پرداخته شده، نگاه غالب در پژوهش‌های صورت گرفته اذعان به آسیب‌پذیر بودن سامانه‌های کنترل صنعتی و یافتن راهی برای بهبود امنیت آن‌ها می‌باشد. در تحقیقات صورت‌گرفته پیشین روش بکارگیری امن این سامانه‌ها در زیرساخت‌های حیاتی با توجه به آسیب‌پذیر بودنشان به‌طور خاص بررسی نشده است. نوآوری ویژه این تحقیق را می‌توان به ارائه راه‌حل‌هایی جامع با درنظر گرفتن کلیه نهادهای مرتبط سامانه‌های مذکور (افراد، فرایند و فناوری)، پرداختن به آسیب‌پذیری‌های سامانه‌های کنترل صنعتی و نیز مفهوم‌سازی، شناخت ماهیت، ابعاد، چرایی، چیستی و الزامات سامانه‌های کنترل صنعتی برای شکل‌دهی یک الگوی راهبردی بکارگیری امن این سامانه‌ها، در زیرساخت‌های حیاتی درنظر گرفت.

۱. مبانی نظری:

۱-۱-مفاهیم و مبانی زیرساخت‌های حیاتی

زیرساخت حیاتی: سیستم‌ها و دارایی‌های فیزیکی و سایبری که ناتوانی یا تخریب آن‌ها می‌تواند تأثیر منفی بر امنیت فیزیکی یا اقتصادی و یا ایمنی و سلامت عمومی بگذارد، زیرساخت حیاتی گفته می‌شود. این زیرساخت‌های حیاتی کشور، خدمات اساسی جامعه را

فراهم می‌کنند و به ۱٦ بخش اساسی تقسیم‌بندی می‌شوند (وزارت امنیت داخلی آمریکا، ۲۰۱۹).

۱-۱-۱-وابستگی زیرساخت‌های حیاتی به فضای سایبر

فضای سایبر: شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده (جاگذاری شده)، کنترل‌گرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به‌منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات می‌باشد. این فضا ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه شده باشد (سندراهبردی پدافندسایبری، ۱۳۹٤). امروزه، تمام سیستم‌هایی که در زیرساخت‌های حیاتی استفاده می‌شوند به شبکه‌ها و سرویس‌های فناوری اطلاعات و ارتباطات متکی هستند (ویگانو، لویی و یغمایی، ۲۰۱۹).[1] مهم‌ترین بخش وابستگی در هر کشوری به فضای سایبر، وابستگی زیرساختی است. درحال حاضر، زیرساخت‌های حیاتی هریک تاحدی به فضای سایبر وابسته‌اند. این وابستگی ضمن آن‌که می‌تواند عاملی برای تسهیل فعالیت زیرساخت‌ها در ارائه خدمات به مشتریان خود باشد، می‌تواند بستری برای شکل‌گیری تهدیدهای متنوع نیز باشد (گابریل، ۲۰۱۷).

[1] Viganò,Eleonora;Loi,Michele.and.Yaghmaei,Emad

۲-۱-۱-حفاظت از زیرساخت‌های حیاتی کشور در اسناد بالادستی

توجه ویژه به فضای سایبر کشور و به‌خصوص مصون‌سازی زیرساخت‌های حیاتی در برابر هرگونه تهدید، از مواردی است که در اسناد بالادستی مورد توجه قرارگرفته است. از جمله مهم‌ترین اسناد می‌توان به موارد ذیل اشاره کرد.

-سیاست‌های کلی ابلاغی مقام معظم رهبری (مدظله‌العالی) در حوزه افتا

-سند راهبردی امنیت فضای تبادل اطلاعات کشور

-قانون برنامه پنج ساله ششم توسعه کشور ماده ۱۰۶ و ماده ۱۰۹

-سند راهبردی پدافند سایبری کشور

۳-۱-۱-گزاره‌های نقش‌ساز و جهت‌ساز در اسناد بالادستی

برخی از گزاره‌های بیان شده در اسناد بالادستی که نقش‌ساز وجهت‌ساز در فعالیت‌های مرتبط با امنیت و بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی دارند به شرح ذیل در جدول ۱ بیان می‌گردند.

جدول۱ گزاره‌های نقش ساز و جهت ساز در اسناد بالا دستی

سند/ نهاد	گزاره نقش ساز یا جهت ساز مرتبط با موضوع پژوهش
سیاست‌های کلی ابلاغی مقام معظم رهبری (مدظله-العالی) در حوزه افتا	ارتقاء مداوم امنیت، استمرار خدمات عمومی، پایداری زیرساخت‌های ملی، صیانت از اسرار کشور، ارتقاء دانش، تکیه برفناوری بومی، پایش، پیشگیری، دفاع و ارتقاء بازدارندگی، تعامل مؤثر و سازنده منطقه‌ای و جهانی، تعیین نهادهای متولی، تدوین استانداردهای لازم، افزایش آگاهی و مهارت
سند راهبردی امنیت فضای تبادل اطلاعات کشور	ایجاد نظام مدیریتی، آموزش و آگاهی، ارائه مراکز جمع‌آوری و تحلیل مخاطرات، تشخیص و مقابله با حوادث، امن سازی زیرساخت‌های حیاتی
قانون برنامه پنج ساله پنجم توسعه کشور	ارتقاء پایداری ملی، تدوین استاندارد فنی، ایجاد سامانه پایش، هشدار و خنثی‌سازی تهدیدات، ایمن‌سازی و حفاظت از مراکز حیاتی، ارتقاء امنیت
قانون برنامه پنج ساله	بروزرسانی شبکه‌های امن و پایدار، شبکه‌های تعامل پذیر، سامانه‌های فرماندهی و

ششم توسعه کشور	کنترل، کاهش آسیب‌پذیری زیرساخت‌ها، ارتقاء پایداری ملی، تدوین طرح‌های ایمن-سازی، ایجاد سامانه‌پدافند سایبری، ارتقاء قدرت رصد، پایش و تشخیص تهدیدات، افزایش آموزش سایبری
سند راهبردی پدافند سایبری کشور	مصون‌سازی زیرساخت‌حیاتی، تهدیدات و حملات سایبری، طراحی نظام پدافند سایبری، بومی سازی استانداردها و فرایندها، آموزش، رزمایش، ارتقاء دانش منابع انسانی، رصد و پایش، هشدار، مدیریت و کنترل تهدیدات، بومی‌سازی، تقویت صنعت پدافند سایبری، زیست‌بوم سایبری داخلی، زیرساخت امن، مراکز تحقیقاتی، دفاع حقوقی، نهادها و سازمان‌های بین‌المللی، شناسایی دارایی‌ها

۲-۱-مفاهیم و مبانی سامانه‌های کنترل صنعتی

سامانه‌های کنترل صنعتی به عنوان هسته اصلی فضای سایبر در زیرساخت‌های حیاتی و به عنوان یکی از مهم‌ترین اجزاء آن، اهمیت و اولویت بسیار زیادی دارند (محمودزاده و همکاران، ۱۳۹۷).

۱-۲-۱-تعریف سامانه کنترل صنعتی

سامانه کنترل صنعتی، اصطلاح کلی است که شامل انواع مختلفی از سیستم‌های کنترلی، از جمله سیستم‌های کنترل نظارتی و جمع‌آوری داده‌ها، سیستم‌های کنترل توزیع شده و دیگر پیکربندی‌های سیستم کنترل مانند کنترل کننده‌های منطقی قابل برنامه‌ریزی می‌باشد. این سامانه‌ها اغلب در بخش‌های صنعتی و زیرساخت‌های حیاتی یافت می‌شوند. یک سامانه کنترل صنعتی شامل ترکیبی از اجزای کنترل (به عنوان مثال، الکتریکی، مکانیکی، هیدرولیک، پنوماتیک) است که با هم برای دستیابی به یک هدف صنعتی (به عنوان مثال، ساخت، حمل و نقل ماده یا انرژی) عمل می‌کنند. یک سامانه کنترل صنعتی معمولی شامل حلقه‌های کنترل متعدد، رابط‌های انسانی، و ابزارهای تشخیص و نگهداری از راه دور است که با استفاده از آرایه‌ای از پروتکل‌های شبکه برروی معماری‌های شبکه لایه‌ای ساخته شده‌اند. یک حلقه کنترل از حسگرها، محرک‌ها و کنترل‌کننده‌ها برای دستکاری برخی از

فرایندهای کنترل شده استفاده می‌کند (بنیاد ملی استاندارد و تکنولوژی آمریکا ۸۲-۸۰۰، ۲۰۱۵).[1]

۲-۲-۱-لزوم امنیت سامانه‌های کنترل صنعتی

حملات سایبری درسامانه‌های کنترل صنعتی، نیاز به پیش‌بینی نداشته و این سامانه‌ها به‌طور مداوم و بدون مقاومت زیاد، در معرض حملات مخرب هستند. نقض شبکه، سرقت داده‌ها و انکار سرویس نمونه‌هایی از حملات متداول به سامانه‌های کنترل صنعتی هستند (آنی، دنیل، اولادیپو و همکاران، ۲۰۱۸).[2] با توجه به این‌که فناوری‌های عملیاتی وظیفه انجام فرایندهای اتوماسیون یکپارچه در محیط صنعتی را با پشتیبانی فناوری اطلاعات و شبکه ارتباطی بر عهده دارند تا خدمات زیرساخت حیاتی ملی همیشه در دسترس باشد، لذا با ادغام روزافزون فناوری‌های جدید و افزایش اتصال و دسترسی از راه دور دستگاه‌های اسکادا، آسیب‌پذیری‌های جدیدی بروز و چشم‌انداز تهدید سامانه‌های کنترل صنعتی افزایش می‌یابد (آرا، ۲۰۲۲).[3] این مسئله پرداختن به امن‌سازی آن‌ها را به یک اولویت ملی مهم تبدیل کرده‌است.

۳-۲-۱-تفاوت بین برقراری امنیت در سامانه‌های کنترل صنعتی و فناوری اطلاعات

اصول اولیه امنیت سامانه‌های کنترل صنعتی، از سامانه‌های سنتی فناوری اطلاعات گرفته شده است، اگرچه ماهیت حیاتی بودن فرایندهای آن‌ها در مقایسه با سامانه‌های

---

[1] NIST Special Publication 800-82

[2] Uchenna, D Ani; Nneka, Daniel; Francisca, Oladipo.and Sunday, E Adewumi.

[3] Ara, Anees.

فناوری اطلاعات، الزامات سرویس و امنیت را سخت‌تر می‌کند (آنی، دنیل، اولادیپو و همکاران، ۲۰۱۸). نقض شبکه فناوری اطلاعات یک شرکت می‌تواند تأثیرات نامطلوبی بر عملیات روزمره کسب و کار داشته باشد در مقابل، نقض یک سامانه کنترل صنعتی که به فناوری عملیاتی سرویس می‌دهد می‌تواند تولید را مختل کند، به دارایی‌های فیزیکی آسیب برساند و حتی منجربه جراحت یا مرگ برای کارکنان و عموم مردم شود (زیمنس، ۲۰۱۸).[1] طراحی و اجرای اکثر راه حل‌های امنیتی فناوری اطلاعات براساس فرضیات امنیتی معمولی بنا شده و سپس به همه حوزه‌های کاربردی شامل نرم‌افزار و معماری سخت افزار محصول، سیاست‌های مدیریت ریسک گسترش می‌یابد. این فرضیات برای اغلب سامانه‌های کنترل صنعتی نامعتبر هستند. سامانه‌های کنترل صنعتی به دلیل آسیب‌پذیری‌های امنیت سایبری و پیامدهای بهره‌برداری احتمالی از آن‌ها با شبکه‌های فناوری اطلاعات تفاوت دارند. در جدول ۲ مقایسه‌ی برخی الزامات شبکه سامانه‌های فناوری اطلاعات و شبکه سامانه‌های کنترل صنعتی آورده شده است (اوپادیای و سمپالی، ۲۰۱۹).[2]

جدول ۲ مقایسه برخی الزامات شبکه سامانه‌های فناوری اطلاعات و شبکه سامانه‌های کنترل صنعتی

ردیف	نیازمندی‌ها	شبکه فناوری اطلاعات	شبکه کنترل صنعتی
۱	شرایط محیطی	متوسط (اداری)	شدید (رطوبت، مواد شیمیایی،
۲	چرخه زندگی	۵-۳ سال	۲۵+ سال
۳	تأخیر	شاید قابل قبول باشد	نگرانی جدی
٤	تحمل خطا	کم اهمیت	ضروری
۵	مکانیسم امنیتی	یکپارچگی بالا	در دسترس بودن بالا
٦	مدیریت ریسک	بر یکپارچگی پیام و محرمانه بودن اطلاعات متمرکز است.	بر ایمنی انسان و محافظت از فرایند تمرکز دارد.
۷	پشتیبانی/مدیریت شده	پشتیبانی توسط فروشندگان مختلف	پشتیبانی از فروشندگان مشخص

[1] Siemens.

[2] Upadhyay,Darshana.and.Sampalli,Srinivas.

۸	ارتباطات	پروتکل‌های ارتباطی استاندارد	پروتکل‌های ارتباطی اختصاصی
۹	مدیریت وصله	نصب ساده، از راه دور و بصورت خودکار	نصب توسط نصب کننده خاص و زمان نسبتا طولانی
۱۰	پاسخ حادثه	توسعه و استقرار آسان	بستگی به تجدید سیستم دارد.

٤-۲-۱-دورنمای تهدیدات سامانه‌های کنترل صنعتی

در گزارش کسپرسکی اشاره شده است که ۳۹,٦ درصد کامپیوترهای سامانه‌های کنترل صنعتی در سال ۲۰۲۱ مورد حمله قرار گرفته‌اند. در این گزارش منابع اصلی تهدید برای رایانه‌ها در محیط‌های مربوط‌به سامانه‌های کنترل صنعتی، اینترنت، رسانه‌های قابل جابجایی و پست الکترونیک معرفی شده‌اند (کسپرسکی، ۲۰۲۲).[1] در گزارش دیگری که توسط فورتی‌نت منتشر شده با بررسی تعداد حملات به سامانه‌های فناوری و عملیاتی نتیجه‌گیری شده؛ درحالی‌که اکسپلویت‌های مرتبط با فناوری اطلاعات به وضوح تعداد بیشتری دارند، ولی سطح نسبتاً بالای بهره‌برداری با هدف قرار دادن سامانه‌های عملیاتی نشان دهنده علاقه مداوم بازیگران تهدید برای شناسایی آسیب‌پذیری‌های سامانه‌های عملیاتی و همچنین گنجاندن آسیب‌پذیری‌های مذکور در ابزارهای بهره‌برداری مختلف است که هزینه حمله را کاهش می‌دهد (فورتی‌نت، ۲۰۲۱).[2] در گزارش دفتر فدرال آلمان ده تهدید برتر حوزه سامانه‌های کنترل صنعتی و روند آن‌ها از سال ۲۰۱۹ به شرح جدول ۳ نمایش داده شده است (بی.اس.آی، ۲۰۲۲).[3]

[1] Kasperski.

[2] Fortinet,Global Threat Landscape Report.

[3] BSI-CS 005- Version 1.50.

جدول ۳ ده تهدید برتر سال ۲۰۲۲ و روند آن‌ها از سال ۲۰۱۹

۱۰ تهدید برتر	روند از سال ۲۰۱۹
نفوذ بدافزار از طریق رسانه‌های قابل جابجایی و سیستم‌های تلفن همراه	
آلودگی بدافزار از طریق اینترنت و اینترانت	
خطای انسانی و خرابکاری	
به خطر انداختن اجزای ابر و اکسترانت	
مهندسی اجتماعی و فیشینگ	
حملات منع سرویس[1]	
کنترل اجزای متصل به اینترنت	
نفوذ از طریق دسترسی تعمیر و نگهداری از راه دور	
نقص فنی و فورس ماژور	
آسیب‌پذیری‌های نرم‌افزاری و سخت‌افزاری در زنجیره تأمین	

۵-۲-۱- مطالعه کتشافی و بررسی اجمالی استانداردهای بین‌المللی مرتبط با امنیت سامانه‌های کنترل صنعتی

۵-۲-۱-۱-مطالعه اکتشافی

-انگلستان

چشم‌انداز انگلستان برای سال ۲۰۲۱ این است که در برابر تهدیدهای سایبری، ایمن و تاب‌آور باشد. در این راستا، ایجاد ابزارهایی برای محافظت در برابر تهدیدهای سایبری- پاسخگویی مؤثر به حوادث- اطمینان از تاب‌آوری لازم شبکه‌ها، داده‌ها و سیستم‌های حیاتی در برابر تهدیدات سایبری- افزایش دانش و توانایی شهروندان و شاغلین بخش دولتی برای دفاع از خود در برابر این تهدیدات- ایجاد یک مؤسسه تحقیقاتی جدید برای

[1] Dos

موضوعات مهم، راهبردی است که راهبرد علوم و فناوری سایبر آینده، شکاف‌ها و قابلیت‌ها را مشخص می‌کند. در این راستا سامانه‌های کنترل صنعتی و شهرهای هوشمند حوزه‌های مهمی هستند که باید مورد توجه قرار بگیرند (راهبرد امنیت سایبری ملی انگلستان، ۲۰۲۱-۲۰۱۶).

ساختارها و سازمان‌های مرتبط

مرکز حفاظت از زیرساخت‌های ملی[1] با شرکای مختلفی برای شناسایی خطرات ناشی از آسیب‌پذیری و کاهش آن در زیرساخت‌های حیاتی ملی، همکاری می‌کند. این مرکز با دبیرخانه امور اضطراری مدنی در دفتر کابینه همکاری نزدیک دارد. این بخش برای تقویت توانایی انگلیس در آماده سازی، پاسخ دادن و بهبود شرایط اضطراری، کار و سیاست‌های حفاظت از زیرساخت‌های حیاتی انگلیس را تدوین می‌کند.

مرکز محافظت از زیرساخت‌های ملی انگلستان نسبت به تهیه استانداردها و راهنمایی‌های مختلفی در راستای محافظت از زیرساخت‌ها اقدام نموده است از جمله سندی که با عنوان کنترل فرایند و امنیت سامانه اسکادا که یک راهنمای عملی خوب برای امنیت سیستم‌های کنترل صنعتی است. به‌طور مشخص این سند، نمای کلی از ضرورت امنیت سامانه‌های کنترل صنعتی را ارائه و تفاوت بین امنیت این سامانه‌ها و امنیت فناوری اطلاعات را برجسته می‌کند. همچنین سند دیگری با عنوان استقرار فایروال برای سامانه‌های اسکادا و شبکه‌های کنترل فرآیند که نمونه دیگری از راهنمای عملی است که توسط مرکز

[1] Center for the Protection of National Infrastructure(CPNI)

محافظت از زیرساخت‌های ملی انگلستان تهیه شده‌است (آژانس شبکه و امنیت اطلاعات اروپا[1] ۲۰۱۱).

- آمریکا

آژانس امنیت سایبری و امنیت زیرساخت در سندی با عنوان امن‌سازی سامانه‌های کنترل صنعتی در سال۲۰۲۰، موفقیت پایدار امنیت برای سامانه‌های کنترل صنعتی را مستلزم شناخت کامل این سامانه‌ها و درک اولویت‌های مرتب با آن‌ها دانسه است. در این سند بیان می‌گردد باید به طور موثر، مشارکت‌های قابل اعتماد را در سراسر حوزه‌های مرتبط با سامانه‌های مذکور گسترش و تعمیق داد تا سازمان‌ها و کارشناسان فنی بیشتری با داده‌ها، تخصص و ایده‌های مرتبط برای موفقیت در مأموریت، مشارکت کنند. بایستی با آگاهی، دانش و اعتماد با هم به عنوان یک سازمان واحد و یکپارچه به امنیت پایدار و بادوام در سامانه‌های کنترل صنعتی دست یافته و با سرمایه‌گذاری‌های عاقلانه و آگاهانه، ریسک‌های مرتبط با این سامانه‌ها را مدیریت کرد (آژانس امنیت سایبری و امنیت زیرساخت، ۲۰۲۰). همچنین وزارت امنیت داخلی در سندی دیگری با عنوان بهبود امنیت سیستم کنترل صنعتی با راهبرد دفاع در عمق در سال ۲۰۱٦ به مسئله رو به رشد امنیت سایبری و تأثیر آن بر سامانه‌های کنترل صنعتی زیرساخت‌های حیاتی پرداخته و درک روشنی از چالش‌های امنیتی فعلی و اقدامات متقابل دفاعی خاص را از مسائل مربوطبه امنیت سایبری سامانه‌های کنترل صنعتی دانسته است. در دفاع از تهدیدات و آسیب‌پذیری‌های سایبر تأثیرگذار برروی این سامانه‌ها، یک رویکرد جامع که از اقدامات متقابل مشخصی برای ایجاد یک وضعیت امنیتی مبتنی بر ریسک استفاده می‌کند پیشنهاد داده است (وزارت امنیت داخلی، 2016).

برخی از استانداردها، دستورالعمل‌ها و راهنماهای تهیه شده در ایالات متحده:

[1] ENISA European Network and Information Security Agency

راهنمای بنیاد ملی استاندارد و تکنولوژی آمریکا ۸۲-۸۰۰

راهنمای بنیاد ملی استاندارد و تکنولوژی آمریکا ۵۳-۸۰۰

راهنمای بنیاد ملی استاندارد و تکنولوژی آمریکا ۸۰۸۹

-آلمان

مشکلات احتمالی و نقص در زیرساخت‌های حیاتی و خطرات مترتب آن، یک تهدید غیرمستقیم محسوب می‌شوند زیرا این زیرساخت‌ها به‌طور مرتب در معرض خطرات طبیعی، نقص فنی، خطای انسانی یا اقدامات عمدی قرار می‌گیرند. حفاظت از زیرساخت‌های حیاتی به عنوان یک کار مشترک بسیاری از ذینفعان مختلف دیده می‌شوند. قوانین و مقررات با درجات مختلف، زمینه را برای همکاری آن‌ها ایجاد و یک راهبرد است که موجب تبادل اطلاعات بین کلیه ذینفعان ذیربط می‌شود (آیسمان، ۲۰۱٤). از نظر راهبردی و درسطح عملیاتی، دولت فدرال از یک رویکرد جامع برای حفاظت از زیرساخت‌های حیاتی پیروی می‌کند که در چارچوب آن، طرح اجرای محافظت از زیرساخت‌های حیاتی آلمان[1] درسال ۲۰۰۵و ۲۰۰٦با همکاری اپراتورهای زیرساخت‌های حیاتی تهیه شد. با انتشار طرح اجرایی درسال ۲۰۰۷، این همکاری دولتی-خصوصی که امروزه UP KRITIS نامیده می‌شود، نهادینه شد. هدف مشترک آن بهبود حفاظت از زیرساخت‌های حیاتی در همه بخش‌های تعریف شده است. درسال ۲۰۰۹، وزارت کشور، راهبرد ملی برای حفاظت از زیرساخت‌های حیاتی را منتشر کرد که در آن به خطرات وتهدیدات خاص برای زیرساخت‌های اطلاعاتی نیز اشاره شده است. درسال ۲۰۱۱، «استراتژی امنیت سایبری آلمان» با «حفاظت از زیرساخت اطلاعات حیاتی» به عنوان موضوع اصلی منتشر شد. از آن زمان، بسیاری از فعالیت‌های دیگر مانند تأسیس شورای

[1] KRITIS Umsetzungsplan

امنیت ملی سایبری و مرکز ملی دفاع سایبری سهم قابل توجهی در حفاظت از زیرساخت‌های حیاتی داشته‌اند (سند مشارکت عمومی و خصوصی برای حفاظت از زیرساخت‌های حیاتی آلمان، ۲۰۱٤).

-اقدامات کشورهای مختلف را می‌توان به اقدامات پیشگیرانه و واکنشی به شکل زیرتقسیم کرد:

پیشگیرانه: هشداردهی و آگاهی بخشی، فرهنگ‌سازی (کارگاه‌های آموزشی، دوره‌های آموزشی و غیره)، برآورد نیازهای امنیتی (دسته‌بندی دارایی‌ها و میزان حیاتی بودنشان و تهیه نیازمندی‌ها و الزامات امنیتی)، اقدامات فنی (استفاده از رمزنگاری، ارتقاء تاب‌آوری سامانه‌ها)، استانداردسازی (تنظیم و اعمال استاندارد، ممیزی امنیتی، چک لیست ممیزی امنیتی)، بررسی اثربخشی اقدامات حفاظتی، مدیریت مخاطرات (ارزیابی مدیریت مخاطرات، راه‌اندازی مدیریت مخاطرات، مدیریت بحران و افزایش ظرفیت مخاطره‌پذیری در زیرساخت‌های حیاتی از طریق افزایش تاب‌آوری زیرساخت‌های حیاتی، افزایش مشارکت (مراکز علمی، تحقیقاتی، آزمایشگاهی، شرکت‌های مشاوره امنیت، امنیت اطلاعات، ایجاد شوراهای مشورتی)، همکاری‌های بین‌المللی (توجه به تجارب موفق بین‌المللی و همکاری‌های دو یا چند جانبه بین‌المللی).

واکنشی: پاسخ‌دهی فنی به تهدیدات، گزارش‌گیری (جمع‌آوری، اشتراک‌گذاری و تحلیل آسیب‌پذیری‌های اطلاعاتی در مورد زیرساخت‌های حیاتی)، اعمال مقررات کیفری برای مجرمین سایبری علیه زیرساخت‌های حیاتی.

۲-۱-۲-۵- استانداردهای اختصاصی در زمینه امنیت سایبر و سامانه‌های کنترل صنعتی

شرح مختصری از استانداردهای اختصاصی در زمینه امنیت سایبر و سامانه‌های کنترل صنعتی در جدول٤ قابل مشاهده می‌باشد (گروه بی.اس.آی، ۲۰۱۹)[1]:

جدول ٤ استانداردهای مرتبط با امنیت سایبری سامانه‌های کنترل صنعتی

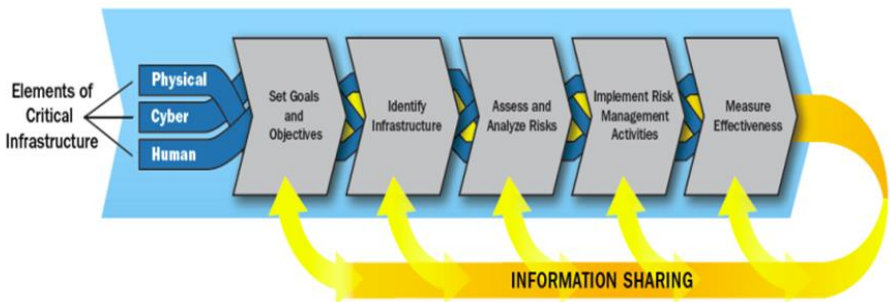
شرح	نام استاندارد
این استاندارد، قادر به حل بسیاری از موضوعاتی است که مختص سامانه‌های کنترل صنعتی هستند. از طرف دیگر، داشتن درجه‌ای از تخصص در سیستم‌های عملیاتی، می‌تواند استاندارد را در هنگام پرداختن به موضوعات عمومی فناوری اطلاعات دقیق‌تر کند.	استاندارد ٦٢٤٤٣
سری 800، مجموعه‌ای از اسناد بنیاد ملی استاندارد و تکنولوژی آمریکا است که سیاست‌ها، رویه‌ها و دستورالعمل‌های امنیتی دولت ایالات متحده را پوشش می‌دهد. در این بین800-82 "راهنمای امنیت سیستم‌های کنترل صنعتی"، از اهمیت ویژه‌ای برخوردار است، زیرا به طور خاص فضای اتوماسیون صنعتی را هدف قرار داده است.	راهنمای بنیاد ملی استاندارد و تکنولوژی آمریکا ۸۲-۸۰۰
بنیاد ملی استاندارد و فناوری، یک بستر آزمایشی عملکرد امنیت سایبری برای سیستم‌های کنترل صنعتی پیشنهاد می‌دهد. هدف از بستر آزمایش، تقلید از سیستم‌های صنعتی دنیای واقعی است و تا حد امکان، بستر آزمایش، انواع سناریوهای صنعتی را شبیه سازی می‌کند.	راهنمای بنیاد ملی استاندارد و تکنولوژی آمریکا ۸۰۸۹
این راهنما نشان می‌دهد چگونه محصولات منبع باز و تجاری در دسترس، می‌توانند در محیط‌های تولیدی برای برآوردن الزامات در چارچوب امنیت سایبری پیاده‌سازی شوند.	راهنمای بنیاد ملی استاندارد و تکنولوژی آمریکا ۸۱۸۳ الف
این راهنما فهرستی از کنترل‌های امنیتی و حریم خصوصی را برای سیستم‌های اطلاعاتی و سازمان‌ها ارائه داده تا از عملیات و دارایی‌های سازمانی، افراد، سازمان‌های دیگر و کشور در برابر مجموعه‌ای از تهدیدها و خطرات محافظت کند.	راهنمای بنیاد ملی استاندارد و تکنولوژی آمریکا ۵۳-۸۰۰

[1] bsigroup

٦-۲-۱-مدل‌های امنیت سایبری در زیرساخت‌های حیاتی و سامانه‌های کنترل صنعتی

-چارچوب مدیریت ریسک در زیرساخت‌های حیاتی

وزارت امنیت داخلی آمریکا چارچوبی را برای حفاظت از تمام بخش‌های زیرساخت حیاتی ایجاد کرد که در برنامه ملی حفاظت از زیرساخت سال ۲۰۱۳ مستند و در شکل ۱ نشان داده شده است.



شکل ۱ چارچوب مدیریت ریسک در زیرساخت‌های حیاتی (آنی، واتسون و نورس، ۲۰۱۹)

این مدل با شناسایی و اولویت‌بندی اقدامات، برای اطمینان از تداوم عملکردها و خدمات ضروری و پشتیبانی از پاسخگویی و بازسازی پیشرفته، امنیت را افزایش داده و انعطاف‌پذیری را تقویت می‌کند. در این مدل به‌طور خاص، سه عنصر زیرساخت حیاتی (فیزیکی، سایبری و انسانی) به صراحت شناسایی و پیشنهاد شده اولویت‌بندی گزینه‌های کاهش ریسک، به عنوان بخشی جدایی ناپذیر از فرایند تصمیم‌گیری، جهت انتخاب فعالیت‌های مدیریت ریسک و محافظت از زیرساخت‌های حیاتی با توجه به هدفی که در خدمت آن هستند طبقه‌بندی شوند.

-چارچوبی برای بهبود امنیت سایبری زیرساخت‌های حیاتی

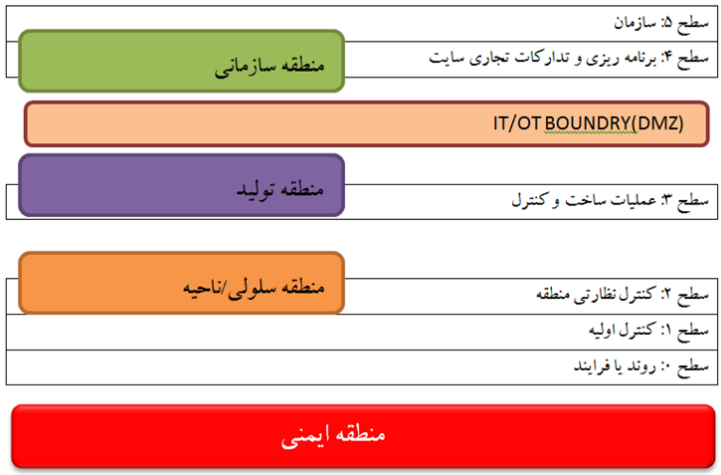
این چارچوب یک رویکرد برای مدیریت ریسک امنیت سایبری است و از سه بخش هسته، لایه‌های پیاده‌سازی و نمایه‌های چارچوب تشکیل شده است. هر جزء چارچوب ارتباط بین کسب و کار/مأموریت را تقویت می‌کند. هسته چارچوب از پنج عملکرد همزمان و پیوسته شناسایی، محافظت، تشخیص، پاسخ و بازیابی تشکیل شده است. هنگامی‌که این توابع با هم در نظر گرفته شوند یک دیدگاه راهبردی و سطح بالاتر از چرخه حیات مدیریت ریسک امنیت سایبری سازمان ارائه می‌دهند. هسته چارچوب مجموعه‌ای از فعالیت‌ها را برای دستیابی به نتایج خاص امنیت سایبری ارائه می‌کند که توسط ذینفعان به عنوان کمک کننده در مدیریت ریسک امنیت سایبری، شناسایی شده است (بنیاد ملی استاندارد و تکنولوژی آمریکا، ۲۰۱۸).

-مدل پوردو[1]

مدل پوردو از مفهوم زون‌بندی یا ناحیه‌بندی، برای تقسیم یک شبکه سازمانی و سیستم کنترل صنعتی، به بخش‌های منطقی که عملکرد مشابهی داشته و یا نیازمندی‌های مشابهی دارند استفاده می‌کند (لوسیانا، ۲۰۱۵)[2] این مدل در شکل ۲ نشان داده شده است.

[1] Purdue model

[2] Luciana



شکل ۲ مدل لایه‌ای پوردو

۲-۱-۷-تعریف عملیاتی بکارگیری امن سامانه‌های کنترل صنعتی

تعریف عملیاتی بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی شامل اعمال حمکروائی[۱] و ارتقاء امنیت و کاهش مخاطرات سایبری، در جهت تشخیص، پیشگیری و مدیریت تهدیدات بیرونی و درونی مرتبط با سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی، از طریق سیاست‌گذاری حاکمیتی، امنیتی، پروتکل‌های امنیتی، الگوریتم‌های رمزنگاری، ممیزی امنیتی، تهیه و ارائه استانداردهای بومی، دستورالعمل‌های عملیاتی جهت اجرا و پیاده‌سازی و نیز طراحی فرایندهای مشارکت ذینفعان برای تهیه دستورالعمل‌های بکارگیری امن پروتکل‌های مرتبط، در سه لایه فرایند، منابع انسانی و فناوری (تکنولوژی) می‌باشد.

[۱] سازماندهی عمل جمعی

۸-۲-۱-گزاره‌های نقش‌ساز و جهت‌ساز در مطالعه اکتشافی

برخی از گزاره‌های بیان شده در استانداردها، دستورالعمل‌ها واسناد مطالعه اکتشافی، که نقش‌ساز و جهت‌ساز در فعالیت‌های مرتبط با بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی می‌باشند در جدول ۵ بیان شده‌اند.

جدول ۵ گزاره‌های نقش ساز و جهت ساز مستخرج از اسناد بین‌المللی

سند/ نهاد	گزاره نقش ساز یا جهت ساز مرتبط با موضوع پژوهش
فورتی‌نت ۲۰۲۱	همگرایی سامانه کنترل صنعتی، درک تهدیدات، بازیگران تهدید
گزارش دفتر فدرال آلمان ۲۰۲۲ (بی.اس.آی، ۲۰۲۲)	خطای انسانی، خرابکاری، نقص فنی، زنجیره تأمین.
بنیاد ملی استاندارد و تکنولوژی آمریکا ۸۰۰	سیاست‌ها و رویه‌ها، معماری سیستم صنعتی، اقدامات متقابل امنیتی، کاهش ریسک، خطای انسانی، نهادهای اطلاعاتی خارجی، کنترل‌های انعطاف‌پذیر، مدیریت ریسک، محصولات قابل اعتماد، پیامدهای نامطلوب، زیرساخت حیاتی، سیستم امن، مهندسی مدیریت پیچیدگی، پیوستگی سامانه‌ها، اجزاء سیستم(ماشین، انسان و فیزیکی)، چرخه حیات سایبری.
بنیاد ملی استاندارد و تکنولوژی آمریکا ۱۰-۱۸۰۰	حملات سایبری پیچیده، ایمنی عوامل انسانی، معماری سایبری، استاندارد امنیت سایبری، تشخیص ناهنجاری، بررسی یکپارچگی فایل، یکپارچگی سامانه‌های فناوری اطلاعات و عملیات، تهدیدات داخلی، ارزیابی ریسک، قابلیت امنیتی.
بنیاد ملی استاندارد و تکنولوژی آمریکا ۲۰۱۸	مدیریت ریسک، برنامه امنیت سایبری سازمان، شناسایی فرصت‌ها، شناسایی-محافظت-تشخیص-پاسخ و بازیابی، دیدگاه راهبردی، چرخه حیات ریسک، سازماندهی اطلاعات، بهبود با یادگیری فعالیت قبلی، مدیریت هویت، استانداردها و دستورالعمل‌ها، درک زمینه کسب و کار، خدمات حیاتی، مهار تأثیر یک رویداد، نظارت مستمر امنیتی.
استاندارد ٦٢٤٤٣	تأمین کنندگان محصول، صاحبان دارایی، بهبود ایمنی، در دسترس بودن، یکپارچگی تجهیزات، کنترل ایمن، بهبود امنیت، شناسایی و رفع آسیب‌پذیری،

	کاهش ریسک، خط مشی‌ها و رویه‌ها، ایجاد برنامه امنیتی، امنیت سایبری مؤثر، مدیریت وصله، ارزیابی ریسک، گروه‌بندی منطقی و فیزیکی دارایی، چرخه عمرتوسعه امنیت، هدایت سازمان، اقدامات متقابل امنیتی، کاهش تهدید.
راهبردهای امنیت سایبری ملی بریتانیا ۲۰۲۱-۲۰۱۶	پاسخگویی مؤثر، اطمینان از تاب‌آوری شبکه‌ها و سیستم‌های حیاتی، افزایش دانش شاغلین و شهروندان، ایجاد مؤسسات تحقیقاتی، علوم و فناوری سایبرآینده، تقویت دفاع از زیرساخت‌های حیاتی، تقویت توانایی در تشخیص و شکست حملات، همکاری با شرکت‌های صاحب زیرساخت، سیستم‌های ایمن و انعطاف‌پذیر، پیاده‌سازی استانداردها.

با درنظر گرفتن اهمیت تهدیدات و آسیب‌پذیری‌های پیش‌گفته مستخرج از مدل‌ها، استانداردها و اسناد بالادستی داخلی و بین‌المللی، مدل مفهومی اولیه بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور، مبتنی بر شناخت حوزه‌های مرتبط با تهدیدات و آسیب‌پذیری‌های سایبری سامانه‌های پیش‌گفته، در ادامه بیان شده-است.

۹-۲-۱-مدل مفهومی بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی

شرکت‌ها باید قابلیت‌های کاری از راه دور و انعطاف‌پذیر را طراحی کرده، فرصت‌ها و چالش‌های پیرامون فناوری‌های افزایش کار و اتوماسیون را درنظر داشته و با ترسیم یک نقشه راه دقیق و بلندمدت نسبت به تغییر فرایندها، ابزارها، فناوری‌ها، آموزش و تغییر فرهنگی اقدام نمایند (گارتنر، ۲۰۲۱).[1] راه‌حل‌های جامع برای امنیت سامانه‌های کنترل

[1] Gartner

صنعتی، باید با نوآوری و بکارگیری رویکردهای خاص، نوعی از اقدامات امنیتی را تعریف کنند که با یک طراحی ویژه در پاسخ به پویایی ریسک‌های امنیتی متحول شوند. این راه-حل‌ها شامل افراد، فرایند و فن‌آوری در سیستم می‌شوند. پرداختن به همه آسیب‌پذیری‌های سه موضوع پیش‌گفته می‌تواند راه‌حل بهتری برای محیط‌های سامانه‌های کنترل صنعتی ارائه دهد (آنی، دنیل، اولادیپو و همکاران، ۲۰۱۸). فناوری با ارائه مجموعه ابزارهایی که می‌تواند خطر را کاهش دهد، حل مسئله را امکان پذیر می‌کند اما بهترین فناوری در جهان مانع از اشتباه عمدی و غیر عمدی انسان‌ها نمی‌شود و سازمان‌ها باید به طور مداوم اقدامات متقابل امنیتی را برای محافظت در برابر تهدیدات شناخته شده و نوظهور تنظیم و اصلاح کنند (وزارت امنیت داخلی آمریکا، ۲۰۱۶). وزارت دفاع امریکا راهبرد دفاعی از جمله دفاع در عمق را ترکیبی از افراد، فناوری، عملیات و آگاهی دشمنان می‌داند و استاندارد ٦٢٤٤٣ از نگاه تهدید، حوزه سایبری را به سه گروه افراد، فرایند و فناوری تقسیم و به عنوان سه ضلع یک مثلث به شرح زیر درنظر می‌گیرد:

• افراد: از جمله مدیریت ارشد، کارمندان، پیمانکاران و سایر پرسنلی که مؤلفه‌های برنامه امنیت سایبری سامانه‌های کنترل صنعتی را توسعه، پیاده سازی، اجرا و مدیریت می‌کنند.

• فرایندها: شامل سیاست‌ها، رویه‌ها، فرم‌ها، فرایندهای تجاری و سایر مستندات مرتبط با سیستم مدیریت امنیت.

• فناوری: شامل کلیه کنترل‌های امنیتی و فنی برای تأمین امنیت.

هدف از این طبقه‌بندی، یادآوری نیاز به تعادل در این سه جنبه است. استاندارد، سه جنبه را به عنوان سه ضلع مثلث نشان می‌دهد. هرگونه اصلاح باید سه جنبه مثلث را به طور مساوی تحت تأثیر قرار دهد.

راهنمای تاب‌آوری و امنیت زیرساخت‌های حیاتی که در سال ۲۰۱۹ توسط وزارت امنیت داخلی امریکا ارائه شده، سه مؤلفه فیزیکی، سایبری و منابع انسانی را به عنوان مؤلفه‌های زیرساخت‌های حیاتی درنظر گرفته است (وزارت امنیت داخلی آمریکا، ۲۰۱۹). حال با اقتباس از این مدل‌ها و بعد از مباحث مرتبط با محیط‌شناسی و بررسی دستورالعمل‌ها و مطالعه اکتشافی، مدل مفهومی این پژوهش با سه بعد منابع انسانی، فرایند و فناوری(تکنولوژی) درنظر گرفته شده، که در جدول ٦ نشان داده شده است.

جدول٦ ابعاد و مؤلفه‌های سامانه‌های کنترل صنعتی

ابعاد	مولفه
منابع انسانی	ظرفیت‌سازی، مدیریت منابع انسانی
فرایند	سیاست‌گذاری، راهبری، قوانین و مقررات، ساختارها و نظامات
فناوری	اقدامات پیشگیرانه، اقدامات تشخیصی، مدیریت حوادث، سازماندهی امنیت

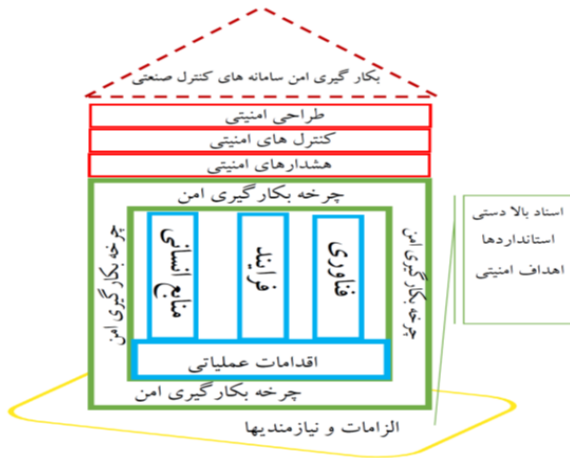
برای تکمیل و اصلاح موارد عنوان شده، با خبرگان حوزه زیرساخت‌های حیاتی و سامانه‌های کنترل صنعتی، در قالب دو گروه متخصصین صنعت و سیاست‌گذاران، در حد اشباع نظری، مصاحبه عمیق به عمل آمد. پس از مصاحبه خبرگی، ابعاد فوق مورد تأکید خبرگان قرار گرفت، همچنین مؤلفه‌های دیگری پیشنهاد و توسط اساتید راهنما و مشاور بررسی شدند. لذا ابعاد و مؤلفه‌های نهایی درجدول ۷ آورده شده است.

جدول۷ ابعاد و مؤلفه‌های نهایی سامانه‌های کنترل صنعتی

ابعاد	مؤلفه
منابع انسانی	ظرفیت‌سازی، مدیریت منابع انسانی
فرایند	سیاست‌گذاری، راهبری، بکارگیری، قوانین و مقررات، ساختارها و نظامات
فناوری	اقدامات پیشگیرانه، اقدامات تشخیصی، تحلیل و مدیریت حوادث، سازماندهی امنیت، اقدامات بازیابی

با توجه‌به مطالب مطرح شده در بخش‌های قبلی و چارچوب مفهومی تحقیق و همچنین ابعاد، مؤلفه‌ها و شاخص‌های آن، مدل مفهومی تحقیق، مطابق شکل ۳ ارائه شده است.

در این مدل، خروجی فرایند (بکارگیری امن سامانه‌های کنترل صنعتی)، ناشی از چرخه بکارگیری امن، برای هریک از اجزای سامانه‌های کنترل صنعتی امن می‌باشد که در تعریف عملیاتی این سامانه‌ها به آن اشاره شده است. اقدامات عملیاتی نیز پس از تحلیل پرسشنامه مشخص و بر روی اجزای سامانه‌ها اعمال می‌گردند.



شکل۳ مدل مفهومی تحقیق

۲. روش‌شناسی تحقیق

این پژوهش باتکیه بر نتایج پژوهش‌های بنیادی و با شناسایی عناصر سامانه‌های کنترل صنعتی و تبیین نقش و عملکرد نهادها و سازمان‌های مختلف، به‌منظور بهره‌برداری امن از این سامانه‌ها در زیرساخت‌های حیاتی کشور مورد استفاده قرار می‌گیرد بنابراین، یک پژوهش کاربردی است. این تحقیق با شناخت ماهیت و رویکردهای مختلف نظری به این مقوله، می‌تواند مقدمه‌ای برای گسترش مرزهای دانش در این زمینه شود. بنابراین این پژوهش، در زمره پژوهش‌های توسعه‌ای محسوب می‌شود. در این تحقیق، هدف، ارائه یک الگوی راهبردی است که بتواند زمینه‌ساز جهت‌گیری راهبردی، برای ارتقاء تاب‌آوری

زیرساخت‌های حیاتی کشور از طریق بکارگیری امن سامانه‌های کنترل صنعتی و استفاده از فرصت‌ها و پیامدهای مثبت ناشی از آن، در تمامی حوزه‌های مرتبط با زیرساخت‌های حیاتی، متناسب با شرایط و مقتضیات کشور شود؛ بنابراین، یک پژوهش راهبردی محسوب می‌شود.

روش انجام تحقیق در این پژوهش ترکیبی و یا آمیخته (کمی و کیفی) است، چون هم از روش کیفی و هم از روش کمی در تحقیق مذکور استفاده شده است. در بخش کیفی این تحقیق برای مستندسازی دانش بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی مراجعه به بیانات ارزشمند مقام معظم رهبری، اسناد بالادستی نظام جمهوری اسلامی ایران، اسناد و اقدامات راهبردی امنیتی کشورهای مختلف و پژوهش‌های علمی مورد بررسی، مضامین پایه استخراج و سپس با بهره‌گیری از روش بررسی خبرگی (مصاحبه با ۱۰ خبره) چارچوب مدل مفهومی تحقیق ایجاد و ابعاد و مؤلفه‌های سامانه‌های کنترل صنعتی امن احصاء گردید. محقق برای رسیدن به اهداف تحقیق یعنی دستیابی به الگوی راهبردی بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی، از پرسشنامه (محقق ساخته) که مبتنی بر مصاحبه با متخصصین و بررسی اسناد بالادستی است استفاده نمود. در این پژوهش پرسشنامه براساس طیف لیکرت به ۵۰ نفر از متخصصین حوزه سامانه‌های کنترل صنعتی ارجاع و نتایج در نرم‌افزار اس.پی.اس.اس[1]تحلیل گردید.

-سنجش روایی(اعتبار) پرسشنامه: در این تحقیق برای افزایش روایی محتوای پرسشنامه از نظرات اساتید راهنما، مشاور، متخصصان و کارشناسان امور پژوهشی، مطالعه پرسشنامه‌های مشابه، مقالات، کتب و مجلات استفاده شد.

- سنجش پایایی پرسشنامه: برای برآورد پایایی پرسشنامه این پژوهش از فرمول ضریب آلفای کرونباخ استفاده شده است، به‌همین منظور تعداد ۱۵ نسخه پرسشنامه تدوینی به‌منظور تعیین میزان پایایی‌پرسشنامه توزیع و همان‌طورکه در جدول ۸ مشاهده می‌گردد،

[1] SPSS

ضریب آلفای محاسبه شده، ۰۹۶ محاسبه گردید. بنابراین می‌توان گفت که پرسشنامه از پایایی کافی برخوردار می‌باشد.

جدول ۸ سنجش پایایی پرسشنامه

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
۰۹۶	۰۹۶	۵۰

۲-۶-نرمالیتی توزیع داده‌ها

باتوجه‌به اطلاعات مندرج در جدول ۹ و با استناد به‌انحراف کم مشاهدات در متغیرهای پژوهش (میزان کجی و کشیدگی متغیرهای پژوهش در بازه عددی ۲+ تا ۲- قرار گرفته است)، فرض نرمالیتی توزیع داده‌ها تأیید می‌گردد.

جدول۹ توصیف کجی و کشیدگی متغیرهای پژوهش

One-Sample Kolmogorov-Smirnov Test				
	ابعاد	منابع انساني	فرآيند	فناوري
	تعداد	۵۰	۵۰	۵۰
Normal Parameters	Mean	۸۶,۲	۹۲,۵	۸۸,۶
	Std. Deviation	۸,۱۸	۱۱,۱۹	۱۱,۰۲
Most Extreme Differen	Absolute	.۳۴۶	.۳۴۱	.۳۷۱
	Positive	.۲۶۵	.۲۸۲	.۲۶۹
	Negative	-.۳۴۶	-.۳۴۱	-.۳۷۱
Kolmogorov-Smirnov Z		۴,۳	۴,۵	۴,۴
(-tailed۲)Asymp. Sig.		.۰۰۰	.۰۰۰	.۰۰۰
Test distribution is Normal				

برای آزمون فرضیات پژوهش از روش‌های آماری پارامتریک رتبه‌ای فریدمن و تی جفت و نیز برای تحلیل آماری ابعاد تحقیق از نرم‌افزار لیزرل استفاده شده است.

۳. تجزیه و تحلیل یافته‌ها

الف–تحلیل آماری پرسشنامه تحقیق در خصوص بعد منابع انسانی به تفکیک مؤلفه‌ها و شاخص‌ها

مطابق شکل ٤ خروجی شاخص‌های برازش مدل معادلات ساختاری بالاتر از ۹۰ نشان می‌دهد که این مدل از برازش قابل قبولی برخوردار می‌باشد.

Chi-Square=۲۴۴.۸۹ df=۵۰ p-value=۰.۰۰۰۰۰ RMSEA=۰.۱۱۴

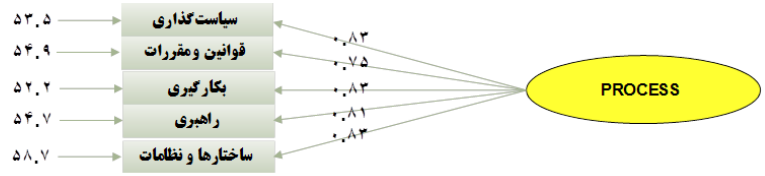
Normed Fit Index (NFI) =95%

شکل ٤ تحلیل بعد منابع انسانی

همچنین با توجه‌به خروجی آزمون خی۲ در تحلیل مدل فوق ۰۲٤٤٪ میزان ارتباط بین متغیرها نرمال می‌باشد. خروجی تحلیل اطلاعات نشان می‌دهد در وضعیت موجود مدیریت منابع انسانی از نظر جامعه خبرگی، نسبت به ظرفیت‌سازی دارای جایگاه بهتری می‌باشد، باتوجه به این‌که ظرفیت‌سازی به‌عنوان مهم‌ترین مؤلفه در بعد اول تحقیق از نظر جامعه‌آماری مورد قبول واقع شده، باید شاخص‌هایی که در این مؤلفه فاصله معناداری نسبت با وضع مطلوب دارند (آگاهی بخشی، مستند سازی تجارب موفق و انتشار آن و تحقیق و توسعه)، مورد توجه بیشتر واقع شوند.

ب–تحلیل آماری پرسشنامه تحقیق در خصوص بعد فرایند به تفکیک مؤلفه‌ها و شاخص‌ها

مطابق شکل ۵ خروجی شاخص‌های برازش مدل معادلات ساختاری بالاتر از ۹۰ نشان می‌دهد که این مدل از برازش قابل قبولی برخوردار می‌باشد.



Chi-Square=۲۳۵.۶۳df=۵۰ p-value=۰.۰۰۰۰۰ RMSEA=۰.۱۱۱

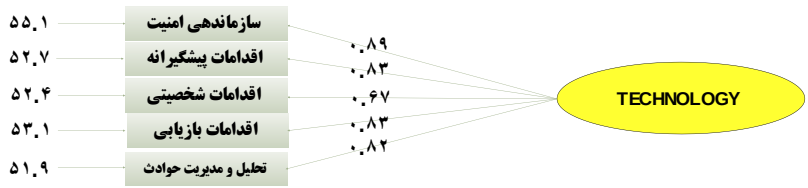
Normed Fit Index (NFI) =95%

شکل۵ تحلیل بعد فرایند

همچنین باتوجه به خروجی آزمون خی۲ در تحلیل مدل فوق ۰۲۳۵٪ میزان ارتباط بین متغیرها نرمال می‌باشد. خروجی تحلیل اطلاعات نشان می‌دهد در وضعیت موجود، مؤلفه ساختارها و نظامات از نظر جامعه خبرگی نسبت به سایر مؤلفه‌ها دارای جایگاه بهتری می‌باشد، باتوجه به این‌که، همین مؤلفه در بعد دوم تحقیق از نظر جامعه آماری به‌عنوان با اهمیت‌ترین مؤلفه تشخیص داده شده، باید شاخص‌هایی که در این مؤلفه فاصله معناداری نسبت با وضع مطلوب دارند (ایجاد ساختار تهیه قوانین و الزامات مربوط به استفاده از فناوری‌های نوین، مدیریت امنیت زنجیره تأمین و ایجاد ساختار وارسی و اعتبارسنجی محصولات)، مورد توجه بیشتر واقع شوند.

ج- تحلیل آماری پرسشنامه تحقیق در خصوص بعد فناوری به تفکیک مؤلفه‌ها و شاخص‌ها

مطابق شکل ٦ خروجی شاخص‌های برازش مدل معادلات ساختاری بالاتر از ۹۰ نشان می‌دهد که این مدل از برازش قابل قبولی برخوردار می‌باشد.



Chi-Square=۵۶۱.۷۳df=۵۰ p-value=۰.۰۰۰۰۰ RMSEA=۰.۱۱۲

Normed Fit Index (NFI) =95%

شکل٦ تحلیل بعد فناوری

باتوجه به خروجی آزمون خی۲ در تحلیل مدل فوق ۰۵۶۱٪ میزان ارتباط بین متغیرها نرمال می‌باشد. خروجی تحلیل اطلاعات نشان می‌دهد در وضعیت موجود مؤلفه سازماندهی امنیت از نظر جامعه خبرگی نسبت به سایر مؤلفه‌ها دارای جایگاه بهتری می‌باشد، باتوجه به این‌که، همین مؤلفه در بعد سوم تحقیق از نظر جامعه آماری به عنوان با اهمیت‌ترین مؤلفه تشخیص داده شده، باید شاخص‌هایی (مدیریت وصله‌های امنیتی، تعیین نیازمندی‌های امنیت سایبری و ایجاد زون بندی درشبکه زیرساخت)، که در این مؤلفه فاصله معناداری نسبت با وضع مطلوب دارند مورد توجه بیشتر واقع شوند.

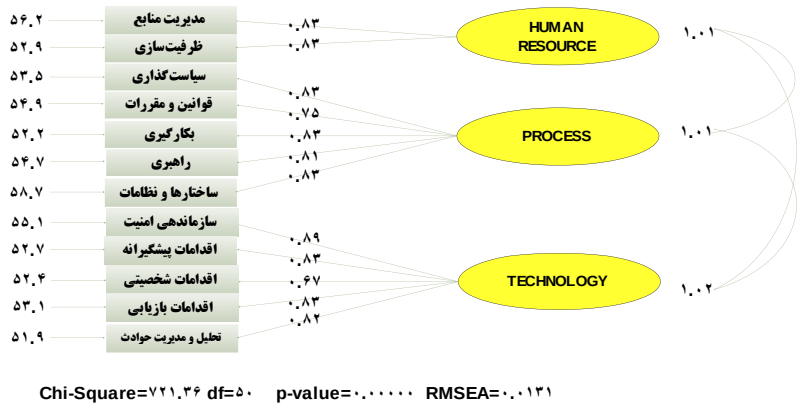
از تحلیل اطلاعات دریافت شده می‌توان نتیجه گرفت، الگوی راهبردی بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور شامل سه بعد با شرایط عنوان شده در جدول ۱۰ و به شرح ذیل می‌باشد.

جدول ۱۰ اطلاعات رتبه‌ای (فریدمن) بعدهای تحقیق با توجه به بار عاملی (میزان تأثیرگذاری خود شاخص)

ردیف	بعد	بارعاملی وضع موجود	بارعاملی وضع مطلوب	اختلاف دو میانگین	اهمیت
۱	بعد منابع انسانی	٥٤,٥	۸۸,۸	۳٤,۲	۳
۲	بعد فرآیند	٥٤,۸	۹۰,۲	۳٥,۸	۱
۳	بعد فناوری	٥۳,٤	۸۹,۸	۳٦,٥	۲

تحلیل عاملی تأییدی اساساً این مطلب را بیان می‌کند که آیا نشانگرهایی که برای معرفی سازه یا متغیر مکنون درنظر گرفته شده‌اند، واقعاً معرف آن‌ها هستند یا خیر، همچنین مشخص می‌نماید که نشانگرهای انتخابی با چه دقتی، معرف یا برازنده متغیر مکنون هستند و ارتباط بین ابعاد و مؤلفه‌ها را مشخص می‌نماید. مطابق شکل ۷ باتوجه به RMSEA=0.0131 در مدل فوق، می‌توان گفت برازش این مدل در سطح خوبی قرار دارد و ارتباط بین ابعاد از ارزیابی قابل قبولی برخوردار می‌باشد. زیرا مدل‌هایی که مقدار

RMSEA آن پایین‌تر از ۱۰٪ باشد، بیانگر این است که مدل از برازش خوبی برخوردار است.



Normed Fit Index (NFI) =95%

شکل۷ تحلیل ابعاد تحقیق

٤. نتیجه‌گیری:

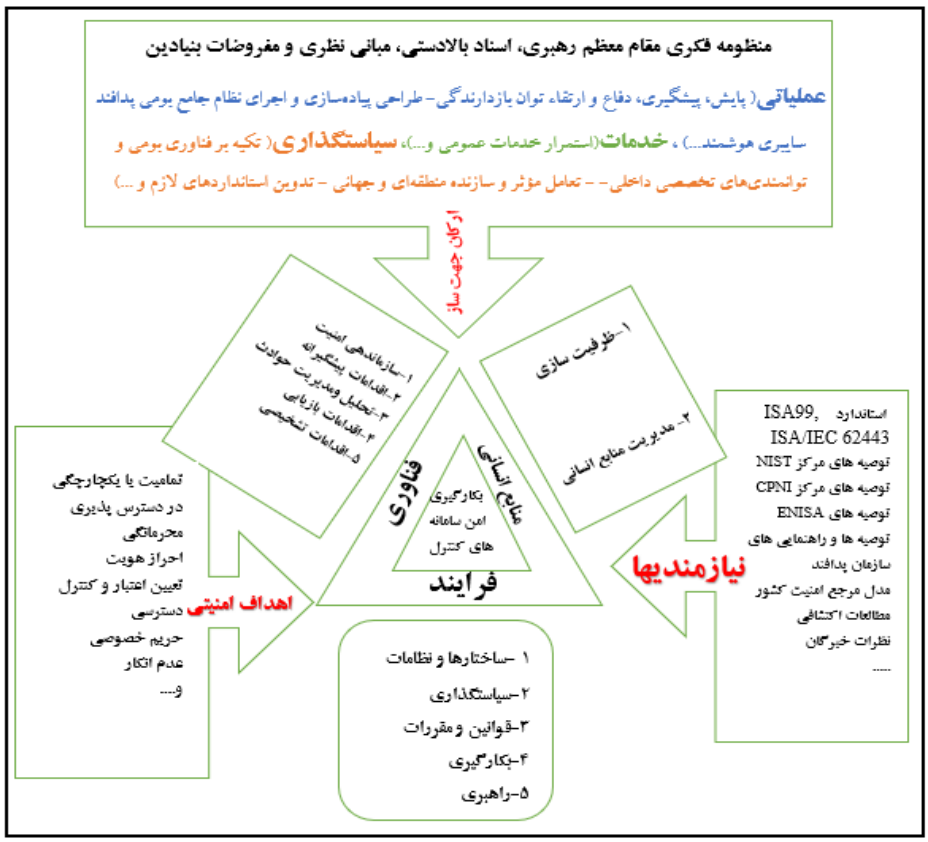
باتوجه به مطالب عنوان شده، بین ابعاد سه‌گانه و مؤلفه‌های آن‌ها ارتباط معناداری برقرار بوده و به‌درستی، موضوع تحقیق را پوشش می‌دهند، همچنین باتوجه به خروجی جدول شماره ۱۰ ترتیب ابعاد تحقیق براساس اهمیت عبارتند از فرایند، فناوری و منابع انسانی، نتایج تحلیل داده‌ها در خصوص بعد اول تحقیق نشان می‌دهد ازنظر جامعه آماری مؤلفه ظرفیت‌سازی با میانگین بارعاملی ۸٦,۹، از اهمیت بالاتری برخوردار است. این مؤلفه دارای اختلاف میانگین بارعاملی ۳٦,۹ بین وضع موجود و مطلوب است که باید در طراحی الگوی راهبردی مورد توجه واقع شود. در این بعد آگاهی بخشی، مستندسازی تجارب موفق و انتشار آن و مدیریت دسترسی کارکنان از شاخص‌هایی هستند که دارای اختلاف میانگین بالایی نسبت به حد مطلوب می‌باشند. در بعد دوم تحقیق با توجه به نتایج به‌دست آمده مؤلفه ساختارها و نظامات با میانگین بارعاملی ۹٤,٤ به‌عنوان با اهمیت‌ترین مؤلفه تشخیص داده شده، این مؤلفه دارای اختلاف میانگین بارعاملی ۳۰,۱ بین وضع موجود و مطلوب است که باید در طراحی الگوی راهبردی مورد توجه قرارگیرد. در این بعد نیز

بیشترین اختلاف میانگین شاخص‌ها در وضعیت جاری و مطلوب مربوط به مدیریت دارایی‌ها، مدیریت هویت و دسترسی و تعیین سنجه‌های آمادگی می‌باشد. در بعد سوم تحقیق سازماندهی و امنیت با میانگین بارعاملی ۹۰,۳ به عنوان مهم‌ترین مؤلفه از نظر جامعه آماری تشخیص داده شده، این مؤلفه دارای اختلاف میانگین بارعاملی ۳۵,۲ بین وضع موجود و مطلوب است که باید در طراحی الگوی راهبردی مورد توجه واقع شود. در این بعد نیز بیشترین اختلاف میانگین شاخص‌ها در وضعیت جاری و مطلوب، مربوط به تهیه سرور پشتیبان، مدیریت وصله‌های امنیتی و رصد و پایش می‌باشد. موارد عنوان شده پایه ارائه الگوی راهبردی بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی می‌باشند. بنابر یافته‌های تحقیق در بعد فرایند با پنج مؤلفه باتوجه به نظر جامعه خبرگان از بالاترین اهمیت عبارتند از: ساختارها و نظامات، سیاست‌گذاری، قوانین و مقررات، بکارگیری و راهبری همچنین زیر مؤلفه‌ها یا شاخص‌ها به ترتیب از بالاترین اهمیت در مؤلفه ساختارها و نظامات عبارتند از: ایجاد استقرار و بهبود فرایندها، ایجاد ساختار بررسی و پیاده‌سازی تجربیات موفق (به‌روش‌ها)، مدیریت تغییرات و ظرفیت، مدیریت منابع مالی، مدیریت امنیت زنجیره تأمین، ایجاد ساختار تهیه قوانین و الزامات مربوطبه استفاده از فناوری‌های نوین، ایجاد ساختار وارسی و اعتبارسنجی محصولات و ایجاد ساختار ممیزی محصولات و ارائه گواهینامه کیفیت. در بعد فناوری با پنج مؤلفه باتوجه به نظر جامعه خبرگان از بالاترین اهمیت عبارتند از: سازماندهی امنیت، اقدامات پیشگیرانه، تحلیل و مدیریت حوادث، اقدامات تشخیصی و اقدامات بازیابی. همچنین زیر مؤلفه‌ها یا شاخص‌ها در مؤلفه سازماندهی امنیت به ترتیب از بالاترین اهمیت عبارتند از: تعیین نیازمندی‌های امنیت سایبری، پیش‌بینی و برآورد تهدید و حمله، تعیین معیارهای ارزیابی خطرات کمی و کیفی، پیاده‌سازی مکانیزم دفاع در عمق، نظارت بر انجام ایزوله‌سازی شبکه زیرساخت، ایجاد زون بندی درشبکه زیرساخت و راه اندازی مرکز عملیات امنیتی. در بعد منابع انسانی با دو مؤلفه مدیریت منابع انسانی و ظرفیت‌سازی با در نظر گرفتن اولویت مؤلفه‌ها از بالاترین اهمیت عبارتند از: ظرفیت‌سازی و مدیریت منابع

انسانی که اولویت زیر مؤلفه‌ها یا شاخص‌ها در مؤلفه ظرفیت‌سازی بـه ترتیـب از بـالاترین اهمیت عبارتند از: حمایت از ایده‌های جدیـد، مسـتندسـازی تجـارب موفـق و انتشـار آن، آگاهی بخشی، تحقیق و توسعه، آموزش سازمانی و مشارکت در رویـدادهای بـین المللـی. همانگونه که پیشتر توضیح داده شد مشخص گردیـد بکـارگیری امـن سـامانه‌هـای کنتـرل صنعتی در زیرساخت‌های حیاتی دارای سه وجه به شکل زیر می‌باشد:

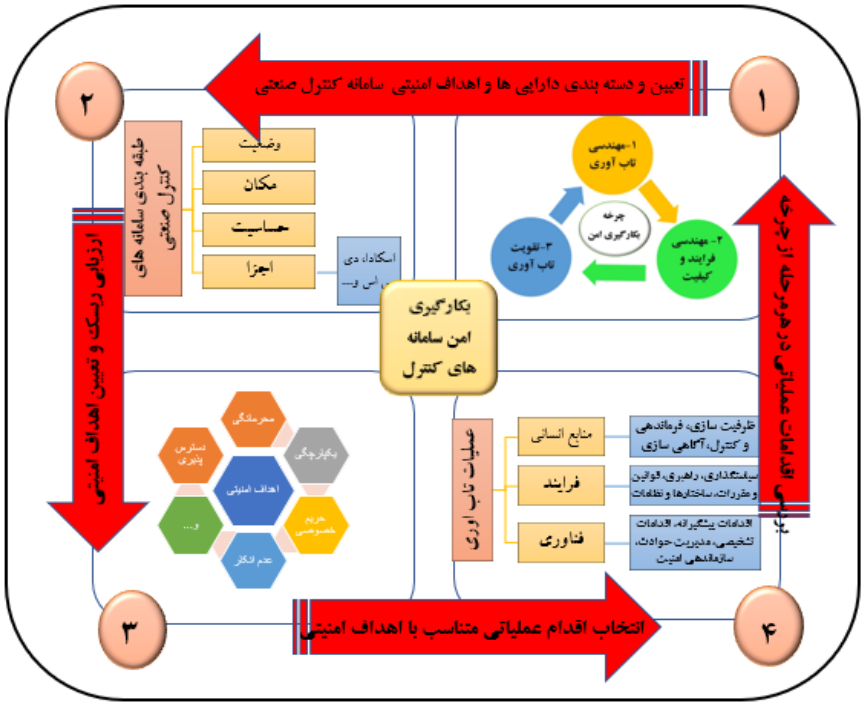
۱- عوامل فرایندی با پنج مؤلفه و بیست و نه زیر مؤلفـه، ۲- عوامـل فنـاوری بـا پـنج مؤلفه و بیست و یک زیرمؤلفه، ۳- عوامل منابع انسانی با دو مؤلفه و چهارده زیرمؤلفه.

به‌طورکلی این الگوی راهبردی شامل ابعاد سه‌گانه (فرایند، فنـاوری و منـابع انسـانی) و دارای دوازده مؤلفه و ٦٤ زیرمؤلفه مطابق با شکل ۸ می‌باشد.



شکل ۸ الگوی راهبردی بکارگیری امن سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور

باتوجه به بررسی‌ها و مطالعات صورت‌گرفته که خلاصه آن در مبانی نظری تحقیق بیان شد، جهت پیاده‌سازی الگوی راهبردی پیشگفته مدل اجرایی به شرح شکل ۹ پیشنهاد می‌گردد.



شکل ۹ مدل اجرایی الگوی راهبردی بکارگیری امن سامانه کنترل صنعتی

فاز یک:

مهندسی تاب‌آوری: در این مرحله باید الزامات سیستم تعریف و تجزیه و تحلیل شوند. الزامات سیستم شامل الزامات تجاری، سازمانی، کاربر، ایمنی و امنیت می‌باشند. درک سازمانی برای مدیریت امنیت سایبری برای سیستم‌ها، افراد، دارایی‌ها، داده‌ها و قابلیت‌ها ایجاد و همچنین میزان تحمل ریسک سازمان مشخص، تا توسط آن بتوان فعالیت‌های سایبری را سازماندهی کرد. مدیریت دارایی، تعیین جایگاه سازمان در زیرساخت حیاتی و بخش صنعت، اولویت بندی مأموریت، اهداف و فعالیت‌ها و همچنین تعیین راهبرد

مدیریت ریسک را می‌توان به عنوان دسته‌ای از خروجی‌های مؤثر این مرحله نام برد.

مهندسی فرایند و کیفیت: زیرساخت لازم برای رسیدن به اهداف تعیین شده، باید تعریف شوند تا الزامات پیاده‌سازی را با درنظر گرفتن رویه‌ها، استانداردها، ابزارها و تکنیک‌های قابل اجرا برآورده کند. هدف از فرایند مهندسی فرایند و کیفیت این است که اطمینان حاصل شود خدمات و پیاده سازی فرایندها، اهداف سازمانی را برآورده می‌کنند.

تقویت تاب‌آوری: یک مکانیسم کنترل فرایند برای توسعه، نظارت، کنترل و بهبود فرایند است. در این مرحله سازمان باید در نتیجه ارزیابی و بازنگری فرایند، بهبودهایی را در فرایندهای خود اعمال کند. داده‌های عملیاتی، فنی و ارزیابی باید جمع‌آوری، تجزیه و تحلیل شوند تا درکی از نقاط قوت و ضعف فرایندهای بکار گرفته شده به‌دست آید. این تجزیه و تحلیل‌ها باید به عنوان بازخورد برای بهبود این فرایندها، توصیه تغییرات در جهت پروژه (یا پروژه های بعدی) و تعیین نیازهای پیشرفت فناوری استفاده شوند.

فاز دو:

اجزاء: نوع دارایی از نظر دسته‌بندی سامانه‌های کنترل صنعتی امن تعیین می‌گردد.

حساسیت: اهمیت امنیتی و اطلاعاتی دارایی تعیین می‌گردد.

مکان و مالکیت: تعیین اینکه دارایی در مالکیت سازمان می‌باشد و یا این‌که از نظر فیزیکی در اختیار سازمان قراردارد؟

وضعیت: تعیین کننده حالت دارایی از نظر آغاز، استمرار یا پایان فعالیت می‌باشد.

فازسه:

براساس خروجی فاز ۱ و ۲ و نیز ارزیابی ریسک صورت پذیرفته، نسبت به انتخاب اهداف امنیتی متناسب با دارایی موردنظر اقدام می‌شود.

فاز چهار:

باتوجه به خروجی فازهای ۱ تا ۳ و اولویت بندی‌های صورت پذیرفته منتج از تحلیل انجام شده در پژوهش، مطابق شکل ۹ اقدام عملیاتی مناسب صورت می‌پذیرد و خروجی مجدداً به فاز اول ارجاع داده شده، تا چرخه بکارگیری امن تکرار و در صورت نیاز به فاز

دوم ارجاع گردد.

پیشنهاد

بر مبنای اهداف مطرح شده، ضمن مفهوم‌سازی بکارگیری امن سامانه‌های کنترل صنعتی، ابعاد، مؤلفه‌ها و شاخص‌های آن با توجه به مبانی نظری، تحلیل محیطی و مصاحبه با خبرگان تعیین و بر این اساس پیشنهادات اجرایی و پژوهشی زیر ارائه می‌گردد.

پیشنهادات اجرایی

۱-یکی از چالش‌های اصلی نگاه فناورانه، وابستگی سامانه‌های کنترل صنعتی به فضای سایبر است. در بعد مدیریتی نیز چالش اصلی، نگاه مسؤلین زیرساخت است که باتوجه به اعتمادشان به محصولات خارجی نگاه مثبتی به محصولات و پروتکل‌های بومی داخلی ندارند. باید با حمایت راهبردی از شرکت‌های دانش‌بنیان نگاه مثبت به محصولات داخلی و استفاده از فناوری‌های نوین در حوزه سامانه‌های کنترل صنعتی تقویت شود (ایجاد ساختار تهیه قوانین و الزامات مربوط‌به استفاده از فناوری‌های نوین، حمایت از ایده‌های جدید).

۲-بسیاری از سامانه‌های کنترل صنعتی، براساس پروتکل‌ها، نرم‌افزارها و سخت‌افزارهای اختصاصی غیر بومی طراحی شده و فعالیت می‌کنند. بنابراین طراحی فرایندهای تطبیق پذیر، اصلی‌ترین چالش بکارگیری امن سامانه‌های موصوف می‌باشد که باید مورد توجه قرارگیرد (ایجاد استقرار و بهبود فرایندها، تعیین چارچوب بومی استانداردها).

۳-تدوین وظایف و مسئولیت‌های سازمان‌های دولتی و مأموریت دستگاه‌های اجرایی و شرکت‌های خصوصی در زمینه اقدامات مرتبط با بکارگیری امن سامانه‌های کنترل صنعتی (ایجاد استقرار و بهبود فرایندها، تعیین چارچوب‌های تبادل داده و ارتباط بین زیرساخت‌های حیاتی).

پیشنهادات پژوهشی

۱-آینده‌پژوهی در زمینه فناوری‌های نوین بنیان‌شکن و هم‌افزا در فضای سایبر و شناسایی پیشران‌های مؤثر و فناوری‌های جهشی در حوزه سامانه‌های کنترل صنعتی.

۲-احصاء راهبردهای متناسب‌سازی رفتار سامانه‌های کنترل صنعتی با تهدیدات مرتبط با این سامانه‌های جهت مدیریت تهدیدات، در راستای بکارگیری امن سامانه‌های کنترل صنعتی.

۳-شناسایی آسیب‌پذیری‌ها و مشکلات ناشی از همگرایی سامانه‌های کنترل صنعتی جدا شده و درج مؤلفه‌های فناوری اطلاعات، در دامنه سامانه‌های کنترل صنعتی جهت مدیریت محیط‌های پیچیده.

فهرست منابع و مآخذ

الف. منابع فارسی

- تقی‌پور، رضا؛ لشکریان، حمیدرضا؛ ناصری، علی و یزدانی، رحیم(زمستان ۱۳۹۸). ***الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران***، فصلنامه امنیت ملی، سال نهم، شماره سی و چهار، ۴۸-۷.
- کمیته دائمی پدافند غیرعامل کشور (۱۳۹٤)، ***سندراهبردی پدافند سایبری کشور***. فرماندهی معظم کل قوا، کمیته دائمی پدافند غیرعامل کشور.
- محمودزاده، ابراهیم؛ حسنی اصل، حمیدرضا؛ قوچانی، محمدمهدی و نیک نفس، علی (تابستان ۱۳۹۷). ***تدوین راهبردهای امنیت سایبری سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور***، فصلنامه مطالعات بین رشته‌ای دانش راهبردی، سال هشتم شماره ۳۱ ، ۲۸۱-۲۵۳.
- میریوسفی، سید محسن و غفارپور، رضا (پاییز ۱۳۹۹). ***راهبردهای نوین حفاظت از زیرساخت‌های حیاتی***، فصلنامه پدافند غیرعامل، سال یازدهم، شماره ۳، صفحات ۱٤-۱.

ب. منابع انگلیسی

- Ara, Anees,(2022)," Security in Supervisory Control and Data Acquisition (SCADA) based Industrial Control Systems: Challenges and Solutions". IOP Conf. Series:Earth and Environmental Science 1026.
- BSI-CS 005 | Version 1.50 ,(2022)," Industrial Control System Security Top 10 threats and countermeasures ". https://www.allianz-fuer-cybersicherheit.de /SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSICS_005E.pdf?__blob= publicationFile&v=5
- BSI-ICS,(2019), "Cybersecurity Assessment Framework" ,https: //www.bsigroup.com/globalassets/localfiles/it-it/csir/resources/whitepaper/bsi-ic-cybersecurity-assessment-framework.pdf.
- CISA,(2020),"Securing Industrial Control Systems ",https://www.cisa.gov/ resources-tools/ resources /securing-industrial-control-systems
- [D.H.S],(2019),"A Guide toCritical Infrastructure Security and Resilience" November 2019,https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security -Resilience-110819-508v2.pdf
- [D.H.S],(2016),"Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems", Cyber Emergency Response Team,https://www.cisa.gov/uscert/ sites /default /files/recommended_practices/NCCIC_ICS_CERT_Defense_in_Depth_2016_ S508C.pdf
- EISMANN,Christine(2014),"TRENDS IN CRITICAL INFRASTRUCTURE PROTECTION IN GERMANY",Technical university of Ostrava, Safety Engineering Series, ISSN 1805-3238.
- Es-Salhi,Khaoula,(2019),"Segmentation and segregation mechanisms and models to secure the integration of Industrial control Systems(ICS) with corporate system", Ecole nationale supérieure Mines-Télécom Atlantique, 2019. English. ffNNT : 2019IMTA0143ff.
- ENISA,(2011),"ICS Security Related Standards, Guidelines and Policy Documents", https://www.enisa.europa.eu/publications/annex-iii
- Fortinet,(2021),"Global Threat Landscape Report A Semiannual Report by FortiGuard Labs",https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-threat-landscape -2021.pdf

- Gabriel, P,(2017),"Global Health Observatory (GHO)": London, Pearson Publication.
- Gartner,(2021),Sumic,Zarko;Foust,Nicole;Cohen,Ethan;Jones,Lloyd.and.Nair, Sruthi,"Top 10 Trends Driving the Utility Industry in 2021".
- IEC 62443-1-1:Industrial communication networks – Network and system security – Part 1-1: Terminology , concepts and models IEC 62443-1-1.
- kasperski,(2022),"Threat landscape for industrial automation systems " .https://ics-cert.kaspersky.com/publications/reports/2022/03/03/threat-landscape-for-industrial-automation -systems-statistics-for-h2-2021/
- Luciana,Obregon,(2015),"Secure Architecture for Industrial Control Systems". SANS Institute InfoSec Reading Room. Available online: https:// www.sans.org /readingroom /whitepapers /ICS/secure-architecture-industrial-control-systems-36327
- Maglaras,Leandros,(2018),"Intrusion Detection in SCADA Systemsusing Machine Learning Techniques", Department of Computing and Informatics University of Huddersfield.
- NIST.CSWP,(2018),"Framework for Improving Critical Infrastructure Cybersecurity". https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.
- NIST Special Publication 800-82 Revision2,(2015),"Guide to Industrial Control Systems (ICS) Security".
- Siemens,(2018),https://assets.new.siemens.com/siemens/assets/api/uuid:2b57b21f-c87f-4dec-8368-90333cedd18e/whitepaper_securityen082018web.pdf
- Sophos,(2015),"Security Threat Trends 2015".https://www.sophos.com/en-us/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf
- Timpsona,Dominic. And.Moradian, Esmiralda (2018),"A Methodology to Enhance Industrial Control System Security".22nd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems.
- Uchenna,D Ani;Jeremy,D McK Watson;Jason R C Nurse;Al Cook.and. Carsten, Maple,(2019),"a review of critical infrastructure protection approaches: improving security through responsiveness to the dynamic modelling landscape", published in PETRAS/IET Conference Living in the Internet of Things: Cybersecurity of the IoT – 2019.

- Uchenna,DAni;Nneka,Daniel;Francisca,Oladipo.and.Sunday,EAdewumi,(2018), "Securing Industrial Control System Environments: The Missing Piece". Journal of Cyber Security Technology Volume 2, 2018 - Issue 3-4.
- Uk National Cyber Security Strategy 2016-2021. https://assets.publishing.service.gov.uk /government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.
- Upadhyay,Darshana.and. Sampalli ,Srinivas, (20۱۹),"SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations".Computers & Security Volume 89, February 2020, 101666.
- UP KRITIS ,(2014),Public-Private Partnership for Critical Infrastructure Protection UP KRITIS,Germany ,2014. https://ccdcoe.org/uploads/2018/10/Germany_UP_KRITIS_Public-Private-Partnership-for-Critical-Infrastructure-Protection_2014_English.pdf
- Viganò,Eleonora;Loi,Michele.and.Yaghmaei,Emad,(2019),"Cybersecurity of Critical Infrastructure "https :// www.researchgate.net /publication /335 752979.
- Yadav,Geeta.and.Paul,Kolin,(2021),"Architecture and Security of SCADA Systems". International Journal of Critical Infrastructure Protection Volume 34, September 2021, 100433.