تعیین روش‌شناسی مناسب درخصوص ارزیابی امنیتی تجهیزات مرتبط با فناوری اطلاعات و ارتباطات صنعت برق

صوفیا آهنج*[1]، مهسا رحمانی[2]، ویدا نوبخت[3] و زهرا صادقی گل[4]

[1] کارشناس ارشد، مرکز توسعه فناوری امنیت اطلاعات و ارتباطات و تجهیزات در صنعت برق، پژوهشگاه نیرو، تهران، ایران
sahanj@nri.ac.ir

[2] کارشناس ارشد، مرکز توسعه فناوری امنیت اطلاعات و ارتباطات و تجهیزات در صنعت برق، پژوهشگاه نیرو، تهران، ایران
rahmani.m87@gmail.com

[3] کارشناس ارشد، مرکز توسعه فناوری امنیت اطلاعات و ارتباطات و تجهیزات در صنعت برق، پژوهشگاه نیرو، تهران، ایران
nobakhtvida@yahoo.com

[4] کارشناس ارشد، مرکز توسعه فناوری امنیت اطلاعات و ارتباطات و تجهیزات در صنعت برق، پژوهشگاه نیرو، تهران، ایران
sadeghigol@gmail.com

چکیده

برقراری امنیت در زیرساخت‌های حیاتی کشور، یکی از مهم‌ترین اقداماتی است که باید به‌منظور ارتقای امنیت کشور به آن پرداخته شود. در این راستا استراتژی امن‌سازی باید مرتب به‌صورت یک چرخه پویا برقرار شود. انجام ارزیابی امنیتی از مهم‌ترین اقدامات در این پروسه است. ارزیابی امنیتی از دو بعد سیستم و محصول مطرح است. نخستین گام در ارزیابی امنیتی یک محصول، تعیین روش‌شناسی ارزیابی است که در این مقاله مورد بررسی قرار می‌گیرد. در این خصوص استانداردهای مختلفی در حوزه ارزیابی فنی امنیتی ICT عمومی وجود دارند. در این مقاله ابتدا به بررسی این استانداردها پرداخته، سپس استانداردها و گزارش‌های مطرح در حوزه صنعتی بررسی و مقایسه و درنهایت نیز بر اساس نتایج حاصله و ملاحظات خاص تجهیزات فناوری اطلاعات و ارتباطات خاص صنعت برق روش‌شناسی مناسب ارائه شده است.

واژگان کلیدی: ISO/IEC 15408، سری استانداردهای ISO/IEC 27001، NIST SP 800-5، NIST 7628T، NIST 800-82، ISO/IEC 27019، سری استانداردهای ISO/IEC62443

۱- مقدمه

مدیریت سازوکارهای مختلف یک آزمایشگاه از زمان عقد قرارداد تا انجام آزمون و تحویل نتایج و درنهایت صدور گواهی، جنبه‌های مختلفی دارد و نیازمند یک روش‌شناسی جامع است که در آن تمامی تعاملات بین اجزاء مختلف آزمایشگاه و مشتری به‌طور شفاف تعریف شده باشد. روش‌شناسی جامع در دو حوزه فنی و مدیریتی در آزمایشگاه مطرح است. بخش فنی در روش‌شناسی ارزیابی امنیت، فرآیند کلی انتخاب آزمون و سایر مواردی را که برای انجام آزمون مورد نیاز است را مشخص می‌کند که شامل نیازمندی‌های امنیتی و سطوح آزمون و نیازمندی‌های مطرح در هر سطح است که در این مقاله مد نظر است.

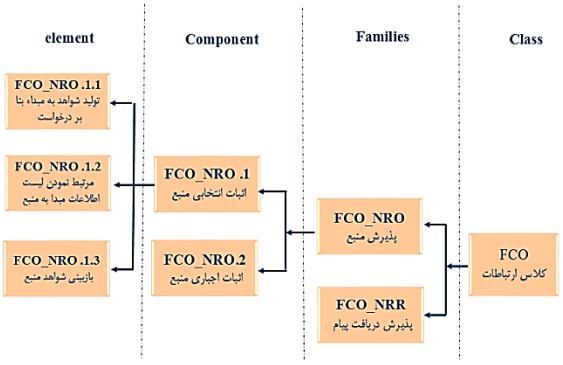
استانداردها و اسناد مختلفی در حوزه امنیت وجود دارند که به بیان این موارد می‌پردازند که از مهم‌ترین آنها می‌توان به ISO/IEC 15408، ISO/IEC 27001، ISA99 یا IEC 63443 و NIST SP 800-53 اشاره کرد. در این مقاله ابتدا به بررسی این استانداردها پرداخته می‌شود، سپس استانداردهای بررسی‌شده، مقایسه شده و درنهایت نیز بر اساس نتایج حاصله و ملاحظات خاص تجهیزات فناوری اطلاعات و ارتباطات خاص صنعت برق روش‌شناسی مناسب تعیین می‌شود.

* نویسندهٔ عهده‌دار مکاتبات: صوفیا آهنج

۲- بررسی روش‌شناسی‌های ارزیابی امنیتی در حوزه فناوری اطلاعات و ارتباطات عمومی استاندارد ISO/IEC 15408

یکی از خانواده استانداردهای مطرح در زمینه ارزیابی امنیت محصولات IT، استاندارد معیارهای مشترک ISO/IEC15408 یا CC[1] به همراه روش‌شناسی به‌کارگیری آن ISO/IEC 18045 یا CEM[2] است. استاندارد CC جهت ارزیابی امنیت محصولات تکنولوژی اطلاعات توسط مؤسسه ISO/IEC پذیرفته و منتشر شده است [۱]. استاندارد ISO/IEC 15408 درواقع به شرح تعارف کلی، نیازمندی‌های عملکردی، نیازمندی‌های تضمین و سطوح امنیتی و نیازمندی‌های آن می‌پردازد. CEM روش‌شناسی را برای ارزیابی امنیت IT با استفاده از CC به‌عنوان پایه ارائه می‌دهد. بسیاری از کشورهای جهان در قاره‌های آمریکا، اروپا و آسیا از این استاندارد بین‌المللی استفاده می‌کنند. این استاندارد به‌عنوان استاندارد ملی نیز در کشور ما پذیرفته شده است.

استاندارد ISO/IEC 15408 الزامات امنیتی عملکردی[3] را در قالب ۱۱ کلاس امنیتی ارائه می‌دهد. ساختار تشکیل‌دهنده کلاس در این استاندارد مطابق شکل زیر است. همانطور که در این شکل نشان داده شده است. نیازمندی‌های امنیتی در قالب کلاس، خانواده، کامپوننت و المان در چهار سطح مطابق شکل (۱) بیان می‌شوند.



(شکل-۱): ساختار تشکیل‌دهنده کلاس در استاندارد ISO/IEC 15408 [1]

همچنین در این استاندارد مفهومی تحت عنوان تضمین[4] بیان شده است، تضمین در این استاندارد زمینه‌ای برای اعتماد است از این منظر که یک محصول فناوری اطلاعات به اهداف امنیتی‌اش می‌رسد یا خیر. ساختار الزامات تضمین نیز مشابه ساختار الزامات عملکردی است.

یکی دیگر از مفاهیمی که در این استاندارد مطرح است، مفهوم سند پروفایل حفاظتی (PP[5]) است. این استاندرد نیازمندی‌های عملکردی و تضمین را به صورت کامل و جامعی ارائه داده است. ولی در این استاندارد نیازمندها برای محصول خاصی طبقه‌بندی و انتخاب نشده است. انتخاب نیازمندی‌ها در سند پروفایل حفاظتی انجام می‌شود. پروفایل حفاظتی مجموعه‌ای از نیازمندهای عملکردی و تضمین برای یک نوع خاص از محصول فناوری اطلاعات است. در واقع پروفایل حفاظتی سند طراحی سیستم است که در ابتدا الزمات امنیتی و سپس راهکارهای کلی برای برآورده کردن این دسته از الزامات را مشخص می‌کند. این سند اصولا توسط نهادهای بالادستی تدوین و برای اجرا در اختیار سازندگان قرار داده می‌شود.

مفهوم دیگری که در این استاندارد مشخص شده است مفهوم سند هدف امنیتی (ST[6]) است. سند هدف امنیتی پایه‌ای برای ارزیابی یک محصول تحت ارزیابی خاص است. این سند به‌طور اصولی توسط سازنده بر مبنای پروفایل حاظتی تدوین می‌شود. یک سند هدف امنیتی می‌تواند بر اساس نیازمندی‌های محصول تحت ارزیابی از یک یا چند سند پروفایل حفاظتی تشکیل شده باشد.

همچنین در این استاندارد ۷ سطح تضمین ارزیابی مشخص شده است. از سطح ۱ تا ۷، در این سطوح برای یک پروفایل حفاظتی خاص نیازمندهای عملکردی می‌توانند تغییری نداشته باشند، ولی برای بدست آوردن اطمینان از پیاده‌سازی درست نیازمندی‌های عملکردی نیازمندی‌های تضمین از سطح ۱ تا ۷ تغییر می‌کنند و افزایش می‌یابند. درواقع سطح ۱، تضمین در حد تست جعبه سیاه را ارائه می‌دهد ولی در سطح ۷ تضمینی بر اساس تمامی اسناد، در حد طراحی فرمال و نیمه فرمال ارائه خواهد شد. به طور مثال در خانواده تضمین Complete Functional Specification که از دسته‌ی الزامات توسعه[7] محصول است و اطلاعاتی در مورد نحوه طراحی و معماری امنیت محصول ارائه می‌دهد. چندین المان وجود دارد که این المانها به ترتیب به سطوح

[1] Common Criteria
[2] Common Evaluation Method
[3] Functional
[4] Assurance
[5] Protection Profile
[6] Security Target
[7] DEVELOPMENT

افزوده می‌شوند. در این مورد در سطح ۱ تنها به سندی نیاز است که خصوصیات همه TSFI[1] را شرح بدهد. در سطح ۲ هدف روش و پارامترهای همه TSFI باید ارائه شود. در سطح ۳ علاوه بر مشخصات توابع اصلی مشخصات کلی TSF پشتیبان نیز باید ارائه شود و این موضوع که آنها جز توابع اصلی نیستند باید مشخص شود. سطح ۴ مشخصات همه توابع TSFI، شامل پشتیبان و non interfering را بیان می‌کند. در سطح پنج مشخصات نیمه رسمی و در سطح ۶ مشخصات رسمی عملیات TSF باید بیان شود.

این استاندارد تنها استانداردی است که با این جزئیات به بیان سطوح تضمین امنیتی می‌پردازد ولی این استاندارد در خصوص قدرت امنیتی (کم، زیاد، متوسط) دسته‌بندی ارائه نمی‌کند.

۲-۱- سند NIST 800-53 و NIST 800-115

نخستین نسخه این استاندارد در سال ۲۰۰۸ منتشر شده است و نسخه نهای draft پنجم آن در سال ۲۰۲۰ تدوین شده است. هدف سند NIST 800-53 فراهم‌کردن مجموعه‌ای از کنترل‌های امنیتی است که می‌توانند سطح و عمق نیازمندی‌های سازمان، فرایندهای تجاری/ مأموریت و سیستم‌های اطلاعاتی را برآورده کنند و سازگار و مکمل سایر استانداردهای امنیت اطلاعات باشد. این سند نگاه سیستمی به مجموعه تحت ارزیابی دارد و تنها بر مبنای محصول به ارزیابی نمی‌پردازد. این سند کنترل‌های امنیتی را در قالب دو کلاس فنی و عملیاتی و ۱۹ خانواده امنیتی بیان می‌کند. در این سند هر خانواده شامل یکسری کنترل‌های امنیتی است. ساختار کنترل‌های امنیتی این سند شامل ۱) یک قسمت کنترل ۲) یک قسمت راهنمایی تکمیلی ۳) یک قسمت کنترل‌های تکمیلی ۴) یک قسمت مرجع و ۵) یک قسمت اولویت و تخصیص پایه است. در واقع این سند ساختار شکست سه لایه‌ای برای بیان الزامات امنیتی دارد [۲].

در این سند کدهای اولویت همراه هر کنترل امنیتی جهت تصمیم‌گیری در پیاده‌سازی آنها بیان شده است. در این استاندارد سه اولویت تعیین شده است. P0، P1 و P2 که به‌ترتیب شماره دارای اولویت بالاتری در پیاده‌سازی می‌باشند. این اولویت‌بندی متوالی کمک می‌کند که کنترل‌های امنیتی اساسی با کنترل‌های وابسته در ابتدا پیاده‌سازی شوند، بر این اساس سازمان قادر خواهد شد از کنترل‌ها در یک حالت ساختار یافته و دوره‌ای مطابق منابع موجود استفاده کند. همچنین در این سند بیان شده است که کدهای اولویت فقط برای پیاده‌سازی متوالی هستند نه برای تصمیمات انتخاب کنترل‌های امنیتی. در این سند تعیین دقیق الزامات را بر اساس مدیریت ریسک و بر اساس سند NIST 800-30 با عنوان "Guide for Conducting Risk Assessments" مشخص کرده است. همچنین این سند دسته‌بندی در خصوص سطوح تضمین امنیتی ارائه نکرده است.

۲-۲- مجموعه استانداردهای ISO/IEC 27000

مجموعه ISO/IEC27000 (که تحت عنوان "خانواده استاندارد "ISMS یا به اختصار "ISO27k" شناخته شده‌است)، شامل استانداردهای امنیت اطلاعات به‌طور مشترک توسط سازمان بین‌المللی استانداردسازی (ISO) و کمیسیون علوم الکترونیکی بین‌المللی (IEC) منتشر شده‌است. این مجموعه بهترین توصیه‌ها را بر پایه تجربیات عملی در مدیریت امنیت اطلاعات، ریسک و کنترل را در کلیه ابعاد سیستم مدیریت امنیت اطلاعات (ISMS[2]) بیان می‌کند. به طور کلی این خانواده دارای ۳ استاندارد الزام‌آوار است که شرکت‌ها می‌توانند در صورت اجرای بندها و الزامات موجود در آنها و طی مراحل ممیزی شخص ثالث، گواهینامه آن استاندارد را دریافت نمایند [۳].

نخستین و معروفترین استاندارد الزام‌آور ISO/IEC 27001 است که به بیان الزامات سیستم مدیریت امنیت اطلاعات می‌پردازد. این استاندارد نیز نگاه سیستمی به بحث ارزیابی امنیتی دارد. دومین استاندارد الزام‌آور استاندارد ISO/IEC 27006 است که الزامات مربوط به شرکت‌های ممیزی‌کننده یا ارائه‌دهنده گواهی (CB) را تبیین می‌کند. استاندارد ISO/IEC 27009 که الزامات پیاده‌سازی ISMS برای حوزه‌های کسب و کاری خاص را تدوین کرده است. سایر استانداردهای این خانواده به عنوان مکمل و راهنمایی برای جنبه‌های مختلف پیاده‌سازی یک سیستم مدیریت امنیت اطلاعات به صورت عمومی و اختصاصی کسب و کارها موجود هستند.

درواقع به غیر از سه استاندارد مذکور، سایر استانداردها نظیر ISO/IEC 27005 یا ISO/IEC 27002 اگر چه به بیان راهنمایی‌هایی درخصوص کنترل‌های

[1] TSF interfaces

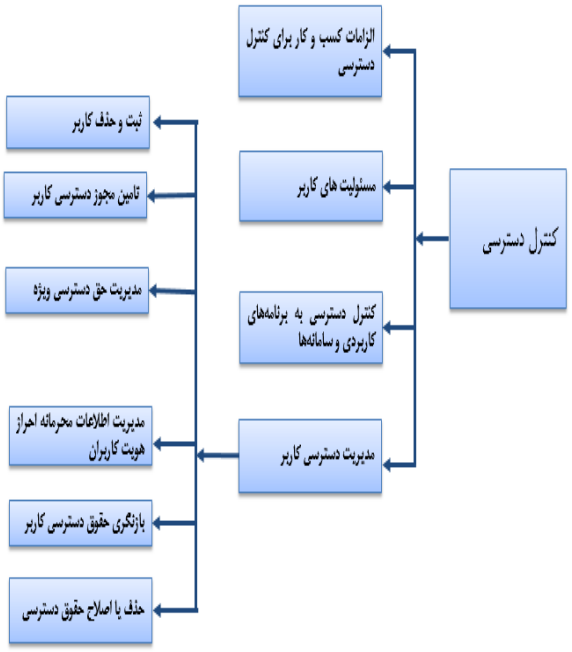
[2] information security management system

امنیتی و نحوه انجام مدیریت ریسک در سازمان می‌پردازند ولی قابلیت دریافت گواهینامه از سوی سازمان‌ها و شرکت‌های مختلف را ندارند.

هدف از تدوین این استاندارد بین‌المللی، تعیین الزامات جهت استقرار، پیاده‌سازی، نگهداری و بهبود مستمر سیستم مدیریت امنیت اطلاعات (ISMS) است. استاندارد ISO/IEC 27001 استاندارد بین‌المللی است که می‌تواند توسط طرف‌های درونی و بیرونی، برای ارزیابی توانایی سازمان در برآورده‌سازی الزامات امنیت اطلاعات خود سازمان به‌کار برده شود.

این استاندارد شامل دو بخش اصلی استاندارد و اهداف کنترلی و کنترل‌ها که پیاده‌سازی بخش اصلی استاندارد برای اجرای سیستم مدیریت مخاطرات الزامی است اما اهداف کنترلی و کنترل‌های مربوطه می‌توانند بنا بر نیاز سازمان به‌کار گرفته شوند. بخش اصلی شامل مواردی است که در سازمانی که سیستم ISMS برقرار است باید به صورت الزامی پیاده‌سازی شوند.

ساختار کنترل‌های امنیتی در این استاندارد نیز به سه سطح مطابق شکل زیر شکسته شده است. در واقع استانداردها در سه سطح به بیان جزئیات می‌پردازد.



(شکل-۲): ساختار کنترل های امنیتی در استاندارد ISO/IEC 27001 [3]

در این سری استاندارد نیز برای هر محصول کنترل امنیتی خاصی ارائه نشده است و انتخاب کنترل‌های امنیتی را به مدیریت امنیت، بر اساس استاندارد ISO/IEC 27005 واگذار کرده است.

۳- استانداردها و گزارشات مرتبط با سیستم‌های کنترل صنعتی

۳-۱- مجموعه استانداردهای SO/IEC 62443

هدف اصلی خانواده استانداردهای ISO/IEC 62443 (ISA99) افزایش ایمنی، دسترس‌پذیری، یکپارچگی و محرمانگی اجزای سامانه‌های به کار رفته برای کنترل و اتوماسیون صنعتی و ارائه معیارهایی برای دستیابی و پیاده‌سازی سامانه‌های کنترل و اتوماسیون صنعتی امن است. از میان این استانداردها با توجه به موضوع مورد بحث استاندارد IEC 62443-3-3، IEC62443-3-2 ، IEC 63443-4-1 و IEC 63443-4-1 در ادامه به‌صورت اجمالی مورد بحث و بررسی قرار خواهند گرفت.

۳-۲- استاندارد IEC 6244-3-3

این استاندارد، هفت الزام پایه (FR[1]) را به مجموعه‌ای از الزامات سامانه (SR[2]) متناظر می‌کند و هر الزام سامانه (SR) یک الزام پایه یا چند الزام افزایشی (RE[3]) برای بهبود و افزایش امنیت دارد. الزامات پایه و افزایشی، در صورت وجود، به سطح امنیتی سامانه کنترلی نگاشت می‌شوند. همچنین در این استاندارد مفهومی تحت عنوان سطح امنیتی هدف وجود دارد. این استاندارد، سطوح امنیت (SLs) را به پنج سطح مختلف (۰، ۱، ۲، ۳ و ۴) تقسیم‌بندی می‌کند. این سطوح و تعاریف آنها عبارتند از:

- SL 0: هیچ الزامات ویژه یا حفاظت امنیتی لازم نیست.
- SL 1: حفاظت در مقابل نقض گاه به گاه یا تصادفی
- SL 2: حفاظت در برابر تخلف عمدی با استفاده از ابزار ساده با منابع و مهارت‌های عمومی کم، و انگیزه پایین
- SL 3: حفاظت از نقض عمدی با استفاده از ابزارهای پیشرفته با منابع متوسط، مهارت‌های خاص IACS و انگیزه متوسط
- SL 4: حفاظت از نقض عمدی با استفاده از ابزار پیشرفته با منابع گسترده، مهارت‌های خاص IACS و انگیزه بالا

تخصیص‌های منحصربه‌فرد SR و RE برای هر FR خاص در سطوح مختلف امنیتی براساس یک افزایش تدریجی در امنیت کلی سیستم کنترل هستند [۴]. لازم

[1] Foundational Requirement
[2] System Requirement (SR)
[3] Requirement Enhancements

به ذکر است این سطوح در خصوص تضمین امنیتی درستی پیاده‌سازی الزامات امنیتی ناست وبیان کننده قدرت مقابله امنیتی می‌باشند.

۳-۲- استاندارد IEC 62443-3-2

از آنجائیکه یک دستور ساده برای چگونگی ایمن‌سازی اتوماسیون صنعتی و سیستم کنترلی (IACS) وجود ندارد، استانداردهای مختلف از انجام مدیریت مخاطرات برای تعیین نحوه امن‌سازی استفاده می‌کنند. در این استاندارد نیز مشابه استاندارد ISMS فرض بر آن است که هر IACS بر اساس تهدیداتی که در معرض آن قرار دارد، احتمال وقوع تهدیدات، آسیب‌پذیری ذاتی در سیستم و پیامد آن در صورت آسیب‌رساندن به سیستم، مخاطرات متفاوتی را به سازمان تحمیل می‌کند و لازم است بر همین اساس الزامات (کنترل‌های امنیتی) مشخص شوند. در این استاندارد ابتدا سیستم تحت ارزیابی تحت یک مدیریت ریسک سطح بالا قرار گرفته و ارزیابی مخاطره برای آن انجام می‌گیرد. سپس بر اساس نتایج حاصله سیستم تحت ارزیابی به مناطق مختلف دسته‌بندی می‌شود. در نهایت ارزیابی ریسک با جزئیات بنا بر روش‌های مرسوم مشابه استاندارد IEC 27000 انجام می‌گیرد و الزامات امنیتی بر این اساس مشخص می‌شود [۵].

۳-۳- استاندارد IEC 62443-4-1

هدف اصلی از این استاندارد فراهم‌کردن یک روش طراحی امن برای ساخت محصولات از درجه صنعتی و سیستم‌های فیزیکی سایبری است. هدف دوم در این استاندارد یکسو کردن فرآیند توسعه با نیازهای امنیتی بالای کاربران صنعتی است. نیازهای تعریف‌شده در این استاندارد در قالب فرآیند بیان شده‌اند. فرآیندهای در نظر گرفته شده در این استاندارد در قالب هشت عمل و فرآیندهای زیر مجموعه آن بیان شده‌اند که عبارتند از:

- مدیریت امنیت (SM[1]): هدف از عمل مدیریت امنیت اطمینان از این است که فعالیت‌های مرتبط با امنیت به اندازه کافی در طول چرخه زندگی محصول برنامه‌ریزی، مستند و اجرایی شوند.
- مشخصات نیازهای امنیتی (SR): فرآیندهای مشخص‌شده توسط این عمل برای مستندسازی قابلیت‌های امنیتی که برای یک محصول که در ارتباط با چهارچوب امنیتی مورد انتظار محصول مورد نیاز است، استفاده می‌شود.
- امنیت به وسیله طراحی(SD)- فرایندهای مشخص‌شده در این عمل برای اطمینان از این‌که استراتژی دفاع در عمق به‌عنوان بخش از طراحی قرار داده شده‌است، استفاده می‌شود.
- پیاده‌سازی امن (SI[2])- فرایندهای مشخص‌شده توسط این عمل برای اطمینان از این استفاده می‌شوند که ویژگی‌ها برای پشتیبانی از استراتژی دفاع در عمق محصول پیاده‌سازی شده‌اند یا خیر .
- تست درستی و اعتبارسنجی امنیتی[3]- فرایندهای مشخص‌شده در این عمل برای مستندسازی تست امنیتی موردنیاز استفاده می‌شود تا اطمینان حاصل کند که تمام نیازهای امنیتی برآورده شده است و امنیت محصول زمانی‌که در چهارچوب امنیتی محصول خود استفاده می‌شود و به منظور بکارگیری استراتژی دفاع در عمق پیکربندی می‌شود، حفظ می‌شود.
- مدیریت نقص امنیتی (DM[4]): فرایندهای مشخص‌شده در این عمل، برای رفع مسائل مرتبط با امنیت یک محصول استفاده می‌شود که برای به‌کارگیری استراتژی دفاع در عمق خود در چهارچوب امنیتی محصول پیکربندی شده است.
- مدیریت به‌روزرسانی امنیتی (SUM [5]): فرآیندهای مشخص شده توسط این عمل برای اطمینان از اینکه به روزرسانی امنیتی مربوط به محصول تست شده و به موقع در اختیار کاربران محصول قرار می‌گیرند، بکار می‌رود.
- دستورالعمل‌های امنیتی (SG[6]): فرایندهای مشخص‌شده در این عمل به این منظور بکار برده می‌شوند تا برای کاربران محصول مستنداتی فراهم کنند که نحوه یکپارچه‌کردن، پیکربندی‌کردن و نگهداری استراتژی دفاع در عمق محصول مطابق با چهارچوب امنیتی محصول خود را شرح دهد.

این الزامات مشابه الزامات تضمین در استاندرد ISO/IEC 15408 می‌باشند اما با ریزدانگی کمتر از CC بیان شده‌اند. همچنین در این استاندارد نحوه اختصاص آنها به سطوح تضمین بیان نشده است [۶].

۳-۴- استاندارد IEC 62443-4-2

این استاندارد نیز مشابه استاندارد IEC 62443-3-3 بـه بیـان الزامات ۷ گانه در سطح تجهیز، سامانه و زیر سـامانه می‌پـردازد

[1] Security management

[2] Secure implementation
[3] Security verification and validation testing (SV)
[4] Security defect management
[5] Security update management
[6] Security guidelines

[۷]. ساختار بیان شده در این استاندارد مشابه استاندارد IEC 62443-3-3 است.

۳-۵- سطوح تضمین بر اساس مستنداتISA Secure

در سال ۲۰۰۶ ISA، (ASCI)[1] به صورت جداگانه به نهاد غیر انتفاعی سازمانی برای پشتیبانی از برنامه برای ارزیابی تطابق استانداردهای مرتبط با اتوماسیون تشکیل داد. در حال حاضر دو مؤسسه زیر بر روی ASCI فعالیت می‌کنند:

- ISA Security Compliance Institute
- ISA 100 Wireless Compliance Institute

ISA ،ISA Security Compliance Institute Secure را مدیریت می‌کند. این مؤسسه محصولات، سیستم‌ها و دارایی‌های تامین کنندگان را بر اساس بهترین روش‌های توسعه چرخه حیات امن ارزیابی می‌کند. اهداف مد نظر ISA Secure را می‌توان به‌طور خلاصه به‌صورت زیر بیان کرد:

- تسهیل آزمون و صدور گواهینامه سیستم‌های کنترل سیستم برای یک مجموعه مشخص از استانداردهای امنیتی سیستم‌های کنترلی
- استفاده از استانداردهای موجود صنعتی امنیتی در خصوص سیستم‌های کنترل صنعتی و توسعه و به‌کارگیری استانداردهای موقت در مواقعی که در این خصوص استانداردی وجود نداشته باشد و پذیرش استانداردهای جدید وقتی تدوین بشوند.
- شتابدهی به توسعه استانداردهای صنعتی که می‌توانند برای تائید سیستم‌های کنترل صنعتی جهت برآورده کردن یک سری از نیازمندی‌های امنیتی بکار گرفته شوند.
- تهیه استانداردها، آزمون‌ها برای سیستم‌های کنترل صنعتی به منظور فراهم‌سازی امنیت مجتمع در آنها. هدف نهایی قرار دادن آزمون‌های انطباق در سیکل تولید محصول است.

این مؤسسه ISCI سه تائیدیه بر اساس چهار سطح مطرح در IEC624443-3-3 می‌دهد که عبارتند از [۸]:

- ISASecure Embedded Device Security Assurance (EDSA) Certification
- ISA Secure System Security Assurance (SSA) Certification
- ISA Secure Security Development Lifecycle Assurance (SDLA) Certification

که هر کدام از این تائیدیه‌ها در چهار سطح تضمین ارائه می‌شوند که بر اساس چهار استاندارد IEC 62443-3-3، IEC62443-3-2، IEC 63443-4-1 و IEC 63443-4-1 می‌باشند. نکته قابل ذکر آن است که اختصاص الزامات تضمین در این استانداردها مطابق برنامه ISA Secure است و به صورت استاندارد در سری استاندارد IEC 62443 بیان نشده است.

[1] Automation Standards Compliance Institute

۳-۶- سند NIST800-82

در این سند، خلاصه‌ای از کنترل‌های مدیریتی، عملیاتی و فنی شناسایی شده در نسخه چهارم استاندارد NIST 800-53 (راهنمای ابتدای برای چگونگی اعمال این کنترل‌ها در سامانه‌های کنترل صنعتی است)، فهرستی از تهدیدها، آسیب‌پذیرها و حوادث رایج در سطح سامانه‌های کنترل صنعتی، فهرستی از فعالیت‌های امنیتی در سطح سامانه‌های کنترل صنعتی، فهرستی از ابزارها و قابلیت‌های امنیتی سامانه‌های کنترل صنعتی بیان شده است. در این سند به صراحت بیان شده است که کنترل‌های امنیتی و سایر ویژگی‌ها مطرح شده در آن بر اساس استاندارد NIST 800-53 می‌باشند و بیان شده است که این کنترل‌ها به اندازه کافی انعطاف‌پذیر هستند که برای انواع سیستم‌های کنترلی کاربرد داشته باشند. این کنترل‌ها مطابق استاندارد NIST 800-53 برای سه دسته سیستم با اثرهای کم، متوسط و بالا بیان شده‌اند [۹].

۳-۷- سند NIST 7628

در این استاندارد در سال ۲۰۱۰ منتشر شده و ویرایش ۱ آن در سال ۲۰۱۴ منتشر شده است. این استاندارد دارای سه بخش است. بخش اول این استاندارد به بیان استراتژی‌های امنیت سایبری، الزامات سطح بالا و معماری شبکه هوشمند می‌پردازد. بخش دوم به بحث حریم خصوص در شبکه هوشمند پرداخته و بخش سوم آن به آنالیزهای پشتیبان لازم برای بحث امنیت شبکه هوشمند و مراجع می پردازد. در ضمیمه A، Vol این سند الزامات این استاندارد بر اساس مراجع زیر بیان شده‌اند [۱۰].

- NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009;
- NERC CIP 002, 003-009, version 3
- Catalog of Control Systems Security: Recommendations for Standards Developers, Department of Homeland Security, March 2010.

با تقریب بسیار خوبی می‌توان گفت الزامات وسایر ویژگی‌های این سند بر اساس سند NIST 800-53 است. حتی نامگذاری کنترلهای نیز بر اساس کنترلهای سند

NIST 800-53 است و تنها SG.CA-3کنترل‌های SG.ID-1، SG.SC-20، SG.AC-16، SG.AC-13، SG.AC-19، SG.CP-4، SG.SC-2، SG.PL-5، SG.MA-2، و SG.PL-4 در سند NIS 800-53 به آنها اشاره نشده است که بیشتر حول محور امنیت سیستمی و شبکه‌ای می‌باشند.

۳-۸- استاندارد ISO/IEC 27019

استاندارد ISO/IEC 27019 استاندارد مدیریت امنیت اطلاعات بر اساس ISO/IEC 27001 برای سامانه‌های کنترل فرآیند ویژه صنعت انرژی است. این مستند در حقیقت به نوعی نگاشت ISMS به حوزه کنترل صنعتی است. کنترل‌های این استاندارد همانطور که از نام آن بر می‌آید منطبق بر استاندارد IEC/ISO 27001 است. البته کنترل‌های جدیدی به این استاندارد علاوه بر کنترل های IEC/ISO 27001 اضافه شده است. با تقریب خوبی می‌توان گفت کنترل‌ها و سایر ویژگی‌های این سند نیز بر اساس سند ISO/IEC 27001 می‌باشند [۱۱].

۴- ملاحظات خاص سامانه‌های کنترل صنعتی صنعت برق

طراحی یک سامانه کنترل صنعتی، شامل اینکه آیا از توپولوژی‌های مبتنی بر سیستم‌های کنترل نظارتی و جمع‌آوری‌داده‌ها، سیستم‌های کنترل توزیع‌شده و یا کنترل‌کننده‌های منطقی برنامه‌پذیر استفاده شده‌است، به بسیاری از عوامل بستگی دارد. این بخش عوامل کلیدی تحریک‌کننده تصمیم‌های طراحی مرتبط با کنترل، ارتباطات، قابلیت اطمینان و ویژگی‌های افزونگی سامانه‌های کنترل صنعتی را معرفی می‌کند. از آنجایی که این عوامل برروی طراحی سامانه‌های کنترل صنعتی بسیار تأثیرگذار هستند، در تعیین نیازهای امنیتی سیستم نیز بسیار اثرگذار خواهند بود. این الزامات عبارتند از [۱۰]:

- الزام‌های عملکردی،
- الزام‌های دسترس‌پذیری (قابلیت اطمینان)
- الزام‌های مدیریت مخاطره
- سیستم عامل
- محدویت منابع
- ارتباطات
- مدیریت تغییر
- پشتیبانی مدیریت شده
- طراحی عمر مؤلفه
- مکان قرارگیری مؤلفه

۵- مقایسه استانداردها و اسناد بررسی شده

بر اساس بررسی‌های انجام شده، به نظر می‌رسد که پایه الزامات امنیتی ارائه شده در تمامی استانداردهای امنیت صنعتی به جزء استاندارد ISO/IEC 62443 که پایه الزامات را مشخص نکرده است، از الزامات استانداردهای مرتبط با سیستم‌های فناوری اطلاعات عمومی است و تنها در این اسناد اشاره شده است که ملاحظات طراحی با توجه به ویژگی‌های سامانه‌های کنترل صنعتی باید در هنگام پیاده‌سازی این الزامات در نظر گرفته شود. لذا مقایسه استانداردها و گزارشات پایه بررسی شده به همراه ISO/IEC 62443 می‌تواند در یافتن استاندارد جامع و مناسب در خصوص سامانه‌های کنترل صنعتی راهگشا باشد. با توجه به این که در انتخاب روش‌شناسی جهت ارزیابی محصول معیارهای مختلفی نظیر پوشش‌دهی کامل الزامات، تعیین قدرت امنیتی، تعیین سطوح تضمین امنیتی، دسته‌بندی دقیق الزامات مطرح است، در این مرحله استانداردهای مختلف از لحاظ با یکدیگر مقایسه شدند.

با توجه به مطالب ارائه‌شده در مورد مقایسهٔ استاندارد NIST 800-53 با استاندارد ISO/IEC 27001 می‌توان گفت که بر طبق مقایسه انجام شده الزامات استاندارد ISO/IEC 27001 به صورت کامل توسط سند NISTIR800-53 پوشش داده می‌شود ولی مواردی بسیاری وجود دارد که در سند NISTIR800-53 وجود دارد ولی در استاندارد ISO/IEC 27001 موجود نیست. از لحاظ سطوح تضمین امنیت هیچ کدام از این دو سند به دسته‌بندی برای تعیین سطح تضمین امنیتی نمی‌پردازند. ضمن آنکه در هر دو سند نگاه سیستمی به ارزیابی وجود دارد. در خصوص تعیین کنترل‌های امنیتی هر دو استاندارد بر مبنای مدیریت ریسک به تعیین کنترل‌های امنیتی می‌پردازند. در خصوص دسته‌بندی سطح امنیت (کم، متوسط و بالا) استاندارد NIST 800-53 برای کنترل‌های امنیتی سه سطح امنیتی برای توسعه محصول ارائه داده است ولی در نهایت انتخاب کنترل‌ها را به مدیریت ریسک بر اساس استاندار NIST 800-30 واگذار کرده است که این دسته‌بندی در استاندارد IEC 27001

وجود ندارد. در کل درخصوص مقایسه این دو استاندارد می‌توان گفت که استاندارد NIST 800-53 به عنوان استانداردی جهت ارزیابی محصولات امنیتی از لحاظ تعداد کنترل‌های امنیتی عملکردی و تضمین و همچنین سطح‌بندی انجام شده، مناسب‌تر است.

درخصوص مقایسه دو سند NIST800-53 و استانداردهای IEC 62443-3-3، IEC 62443-4-1 و IEC 62443-4-2 از لحاظ کنترل‌های امنیتی می‌توان گفت که اکثر کنترل‌های امنیتی IEC 62443-3-3، IEC 62443-4-1 و IEC 62443-4-2 توسط سند NIST 800-53 پوشش داده می‌شوند ولی موارد بسیاری از کنترل‌ها در سند NIST800-53 وجود دارند که در استاندارد IEC62443 موجود نمی‌باشند. همچنین در هر دو سند نگاه سیستمی به بحث ارزیابی وجود دارد. در خصوص دسته‌بندی سطح امنیت، استاندارد NIST 800-53 برای کنترل‌های امنیتی سه سطح امنیتی (کم، متوسط، زیاد) برای توسعه محصول ارائه داده است ولی در نهایت انتخاب کنترل‌ها را به مدیریت ریسک واگذار کرده است. استاندارد IEC 62443-3-3 نیز کنترل‌ها را در چهار سطح امنیتی SL1 تا SL4 دسته‌بندی کرده است ولی در نهایت انتخاب کنترل‌ها را به مدیریت ریسک واگذار کرده است. هر چند که بر اساس اسناد ISA secure این سطوح را می‌توان به سطح تضمین مرتبط کرد، ولی این موارد استاندارد نمی‌باشند. از لحاظ سطوح تضمین امنیت هر دو سند، دسته‌بندی خاصی دراین خصوص ارائه نمی‌دهند هر چند که به الزامات تضمین اشاره می‌کنند. در سند NIST 800-53 الزامات تضمین به نوعی به سطوح قدرت امنیتی مرتبط شده‌اند. در کل در خصوص مقایسه سند NIST800-53 و IEC 62443-3-3 نیز می‌توان گفت سند NIST 800-53 سندی کاملتر از استاندارد IEC 62443 است.

درخصوص مقایسه استاندارد ISO/IEC 15408 در مقایسه با سند NIST800-53 بر اساس توضیحات ارائه شده می‌توان گفت که از نظر تعداد کنترل‌های امنیتی هم الزامات عملکردی و هم الزامات تضمین، هر دو استاندارد پوشش خوبی از کنترل‌های یکدیگر دارند. در هر دو استاندارد کنترل‌هایی یافت می‌شود که در استاندارد دیگر وجود ندارد. کنترل‌های که در سند NIST800-53 و با کنترل‌های استاندارد ISO/IEC 15408 پوشش داده نمی‌شوند، عمدتا از جنس کنترل‌های مدیریت ریسک و یا طرح‌های مربوط به امنیت سازمان (مانند کنترل‌های مدیریت برنامه) یا امنیت شبکه (مانند SC-35 – شانه عسل، SC-26 –کندوهای عسل) هستند و ناشی از نگاه سیستمی این استاندارد به بحث ارزیابی است. با توجه به اینکه استاندارد IEC 15408 نگاه بر پایه محصول به امنیت دارد لذا کنترل‌ها یا الزامات مرتبط با جزئیات بیشتری نسبت به NIST 800-53 بیان شده‌اند. در کل در خصوص پوشش‌دهی دو استاندارد می‌توان گفت اگرچه NIST 800-53 پوشش تقریبا خوبی از کنترل‌های سند IEC 15408 ارائه می‌دهد و حتی در بعضی موارد کنترل‌های اضافه بر استاندارد ISO/IEC 15408 دارد ولی این کنترلهای اضافی بیشتر درخصوص ارزیابی سامانه یا سیستم است و جزئیات بیشتری در استاندارد IEC 15408 برای کنترل‌های حوزه محصول ارائه شده است. در خصوص تعیین کنترل‌های امنیتی در سری NIST 800 تعیین کنترل‌های امنیتی بر مبنای سند NIST 800-30 و تحلیل مخاطرات صورت می‌گیرد و سه سطح کلی تضمین و قدرت امنیتی ارائه شده است در حالیکه در استاندارد IEC 15408 انتخاب کنترل را بر عهده ارزیاب یا نهاد بالادستی در قالب ST یا PP انجام می‌شود. البته این نیاز می‌تواند با انجام مدیریت مخاطرات تامین شود. در خصوص دسته‌بندی کنترهای امنیتی، در استاندارد IEC 15408 قدرت امنیتی برای الزامات عملکردی و تضمین مشخص نشده است، درحالی که سند NIST 800-53 کنترل‌های عملکردی را به سه سطح قدرت و تضمین امنیتی (کم، متوسط، زیاد) دسته‌بندی کرده است. هر چند که در سند NIST 800-53 بیان شده که تعیین دقیق این سطوح امنیت وابسته به نتیجه تحلیل مخاطرات است. در استاندارد IEC 15408 در خصوص دسته‌بندی تضمین امنیتی ۷ سطح تعیین شده است. این دسته‌بندی سطح تضمین امنیتی محصول را مشخص می‌کند. این سطوح از سطح ۱ تا ۷ تضمین بالاتر را به مصرف کننده محصول درخصوص امنیت ارائه می‌دهند. این دسته‌بندی با این جزئیات در دیگر اسناد بررسی شده وجود ندارد. لذا با توجه به نتایج ارائه شده به نظر می‌رسد که استاندارد IEC 15408 سند کاملتری از لحاظ خصوصیات مورد نظر جهت روش‌شناسی ارزیابی محصولات نسبت به NIST800-53 باشد. خلاصه‌ای از مقایسه‌های صورت گرفته در جدول ۱ قابل مشاهده است.

(جدول-۱): خلاصه نتایج مقایسه استانداردها و اسناد مورد بررسی

نام سند پایه امنیتی	ساختار شکست الزامات	الزامات تضمین	سطوح امنیتی	سطوح تضمین	تخصیص الزامات
ISO/IEC 15408	دارای چهار سطح	✓	×	✓	PP ST
NIST 800-53	دارای سه سطح	✓	✓	×	NIST 800-30
IEC/ISO 27001	دارای سه سطح	✓	×	×	IEC/ISO 27005
IEC 63443-3-3 IEC 63443-4-1 IEC 63443-4-2	دارای سه سطح	✓	✓	×	IEC 63443-3-2
NIST800-82	دارای سه سطح	✓	✓	×	NIST 800-30
NIST 7628	دارای سه سطح	✓	✓	×	NIST 800-30
ISO/IEC 27019	دارای سه سطح	✓	×	×	IEC/ISO 27005

۶- نتیجه‌گیری

بر اساس نتایج حاصله تاکنون، چنین حاصل می‌شود که استاندارد IEC/ISO 15408 از لحاظ معیارهای مورد بررسی می‌تواند مرجع روش‌شناسی ارزیابی محصولات صنعتی قرار گیرد. لیکن وجود آزمایشگاه‌های مختلف ISA secure، Wurldtech، Exida، Kema، Tecnalia و... [12-18] که بر اساس استاندارد ISA99 و الزامات دیگر اسناد حوزه صنعتی نظیر NIST800-82، تأئیدیه صادر می‌نمایند که قطعا در جهت تسهیل دهی به امر انجام آزمون تجهیزات کنترل صنعتی است. این تصور را به وجود می‌آورد که کنترل‌های سند ISA99 و یا سند NISTIR7628 حداقل‌های لازم برای سامانه کنترل صنعتی و شبکه هوشمند می‌باشند که قطعا تصور صحیحی است. شایان ذکر است که این موضوع در انتخاب استاندارد IEC 15408 به روش‌شناسی ارزیابی امنیتی محصولات کنترل صنعتی با توجه به تعریف پروفایل حفاظتی (PP) اشکالی به وجود نمی‌آورد زیرا در این استاندارد انتخاب توابع عملکردی، بر عهده نهاد بالادستی یا ارزیاب قرار داده شده است. درحال حاضر با توجه به نداشتن دیگر خصوصیات مد نظر جهت انتخاب به‌عنوان روش‌شناسی جامع (سطوح بیان شده در ISA Secure استاندارد IEC نمی‌باشند) و همچنین روند تکاملی این استانداردها و وجود ساختارهای آزمایشگاهی در کشور بر اساس استاندارد IEC 15408 و با توجه به پوشش کامل الزامات استاندارد IEC62443 توسط استاندارد IEC15408 می‌توان از استاندارد IEC 62443 و سند NISTIR7628 به‌عنوان مبنای برای انتخاب کنترل‌های امنیتی در استاندارد IEC 15408 استفاده کرد. به این طریق می‌توان از ابزارهای تعبیه شده در این خصوص نیز برای ارزیابی امنیت بر اساس استاندارد IEC 15408 تا زمان تکمیل نهایی سری استاندارد های صنعتی استفاده کرد. در کل به عنوان جمع‌بندی مطالب ارائه شده، استاندارد IEC 15408 به عنوان روش‌شناسی مرجع معرفی می‌شود.

۷- مراجع

[1] Common Criteria org, “Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model” ,September 2012, Version 3.1, Revision 4

[2] National Institute of Standards and Technology, NIST Special Publication 800-53, Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations”, http://dx.doi.org/10.6028/NIST.SP.800-53r4, April 2013, Includes Update as of 01-22-2015

[3] Sadid Application Engineering Company, "ISO / IEC 27001 & 27002 Standard 2013", compiled and translated by Reza Taynia, 2016

[4] British Standard was published under the authority of the Standards Policy and Strategy Committee,” BS IEC 62443-3-3, Industrial communication networks — Network and system security, Part 3-3: System security requirements and security levels”, 31 October 2013.

[5] National Institute of Standards and Technology, “ISA-62443-3-2, Security for industrial automation and control systems Security risk assessment and system design”, Draft 6, Edit 2و August 5, 2015

[6] National Institute of Standards and Technology, “ISA-62443-4-1, Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements”, Draft 2, Edit 14 , April 9, 2015

[7] National Institute of Standards and Technology, Initial draft of IEC/NP 62443-4-2 , “Industrial communication networks – Network and system security – Part 4-2: Technical security requirements for IACS components based on ISA-99.04.02”, Draft 1, Edit 1, August 2013
https://isasecure.org/en-US/

[8] National Institute of Standards and Technology, "NIST Special Publication 800-82, Revision 2 Initial Public Draft, Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)”, May 2014

[9] National Institute of Standards and Technology,”NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity Volume 1 - Smart Grid Cybersecurity Strategy,

Architecture, and High-Level Requirements", The Smart Grid Interoperability Panel – Smart Grid Cybersecurity Committee, http://dx.doi.org/10.6028/NIST.IR.7628r1, September 2014

[10] ISO/IEC TR 27019, "Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry", First Edition, 2013

[11] Wurldtech Security Technologies Inc., "Achilles Practices Certification Datasheet", 2016

[12] Embedded Device Security Assurance (EDSA) version 2.0.0 effective 01 July 2016, http://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification

[13] DNV GL - Energy, "DNV GL DLMS Test Suite for Smart Meters", www.dnvgl.com\ "Certification of Smart Meters and Smart Data Concentrators", http://www.tecnalia.es/en/https://www.encs.eu/activities/security-testing/ http://www.dlms.com/conformance/certificationprocess/