

مروری بر استانداردهای امنیتی حوزه فاوا در جهت تعیین متدولوژی مناسب برای ارزیابی امنیتی تجهیزات مرتبط با فناوری اطلاعات و ارتباطات صنعت برق

صوفیا آهنج*، مهسا رحمانی، ویدا نوبخت و زهرا صادقی گل

مرکز توسعه فناوری امنیت اطلاعات و ارتباطات و تجهیزات در صنعت برق، پژوهشگاه نیرو، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:

ISO/IEC 15408

سری استانداردهای ISO/IEC 27001

NIST SP 800-5

NIST 7628T

NIST 800-82

ISO/IEC 27019

سری استانداردهای ISO/IEC 62443

doi: 10.1001.1.24763047.1401.11.1.11.8

نوع مقاله: پژوهشی

چکیده

برقراری امنیت در زیرساخت‌های حیاتی کشور، یکی از مهمترین اقداماتی است که باید به منظور ارتقاء امنیت کشور به آن پرداخته شود. در این راستا استراتژی امن‌سازی باید مرتب به صورت یک فرآیند پویا برقرار شود. انجام ارزیابی امنیتی از مهمترین اقدامات در این فرآیند است. ارزیابی امنیتی از دو بعد سیستم و محصول مطرح می‌باشد. اولین گام در ارزیابی امنیتی یک محصول، تعیین متدولوژی ارزیابی می‌باشد 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 شده است. سپس استانداردها و گزارشات مطرح در حوزه صنعتی مقایسه شده و در نهایت نیز بر اساس نتایج حاصله و ملاحظات خاص تجهیزات فناوری اطلاعات و ارتباطات خاص صنعت برق متدولوژی مناسب ارائه شده است.

© ۱۴۰۱ انجمن رمز ایران

۱ مقدمه

مدیریت ساز و کارهای مختلف یک آزمایشگاه از زمان عقد قرارداد تا انجام آزمون و تحویل نتایج و نهایتاً صدور گواهی، جنبه‌های مختلفی دارد و نیازمند یک متدولوژی جامع است که در آن تمامی تعاملات بین اجزاء مختلف آزمایشگاه و مشتری به طور شفاف تعریف شده باشد. متدولوژی جامع در دو حوزه فنی و مدیریتی در آزمایشگاه مطرح می‌باشد. بخش فنی در متدولوژی 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 می‌باشد.

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 نمود. در این مقاله ابتدا به بررسی این استانداردها پرداخته می‌شود. سپس استانداردهای بررسی شده، مقایسه شده و در نهایت نیز بر اساس نتایج حاصله و ملاحظات خاص تجهیزات فناوری اطلاعات و ارتباطات خاص صنعت برق متدولوژی مناسب تعیین می‌شود.

۲ بررسی متدولوژی‌های ارزیابی امنیتی در حوزه فناوری اطلاعات و ارتباطات عمومی

۱.۲ استاندارد ISO/IEC 15408

یکی از خانواده استانداردهای مطرح در زمینه ارزیابی امنیت محصولات IT، استاندارد معیارهای مشترک ISO/IEC 15408 یا CC به همراه متدولوژی بکارگیری آن ISO/IEC 18045 یا CEM است. استاندارد

*از کمیته علمی هجدهمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول

آدرس‌های رایانامه: sahanj@nri.ac.ir (صوفیا آهنج)، rahmani.m87@gmail.com (مهسا رحمانی)، nobakhtvida@yahoo.com (ویدا نوبخت)، sadeghigol@gmail.com (زهرا صادقی گل)

© ۱۴۰۱ تمامی حقوق متعلق به انجمن رمز ایران است.

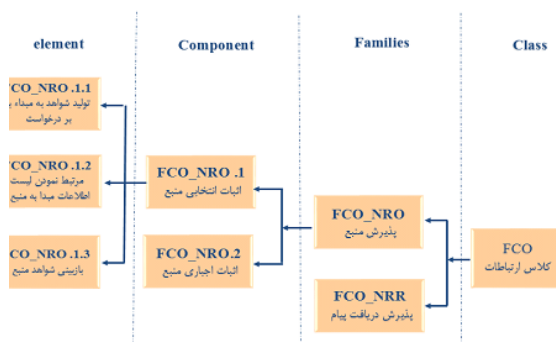
محصول تحت ارزیابی خاص است. این سند اصولاً توسط سازنده بر مبنای پروفایل حالتی تدوین می‌شود. یک سند هدف امنیتی می‌تواند بر اساس نیازمندی‌های محصول تحت ارزیابی از یک یا چند سند پروفایل حفاظتی تشکیل شده باشد. همچنین در این استاندارد ۷ سطح تضمین ارزیابی مشخص شده است. از سطح ۱ تا ۷، در این سطوح برای یک پروفایل حفاظتی خاص نیازمندی‌های عملکردی می‌تواند تغییری نداشته باشند، ولی برای به دست آوردن اطمینان از پیاده‌سازی درست نیازمندی‌های عملکردی نیازمندی‌های تضمین از سطح ۱ تا ۷ تغییر می‌کنند و افزایش می‌یابند. در واقع 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 محصول می‌باشد و اطلاعاتی در مورد نحوه طراحی و معماری امنیت محصول ارائه می‌دهد. چندین المان وجود دارد که این المان‌ها به ترتیب به سطوح افزوده می‌شوند. در این مورد در سطح ۱ تنها به سندی نیاز است که خصوصیات همه TSFI 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 استاندارد می‌باشد که با این جزئیات به بیان سطوح تضمین امنیتی می‌پردازد ولی این استاندارد در خصوص قدرت امنیتی (کم، زیاد، متوسط) دسته‌بندی ارائه نمی‌نماید.

۲.۲ سند NIST 800-53 و NIST 800-115

اولین نسخه این استاندارد در سال ۲۰۰۸ منتشر شده است و نسخه نهایی draft پنجم آن در سال ۲۰۲۰ تدوین شده است. هدف سند NIST 800-53 فراهم کردن مجموعه‌ای از کنترل‌های امنیتی است که می‌تواند سطح و عمق نیازمندی‌های سازمان، فرایندهای تجاری/ماموریت 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 یک سری کنترل‌های امنیتی است. ساختار کنترل‌های امنیتی این سند شامل (۱) کنترل (۲) راهنمایی تکمیلی (۳) کنترل‌های تکمیلی (۴) مرجع و (۵) اولویت و تخصیص پایه می‌باشد. 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 به ترتیب شماره دارای اولویت بالاتری در



شکل ۱. ساختار تشکیل دهنده کلاس در استاندارد ISO/IEC 15408 [۱]

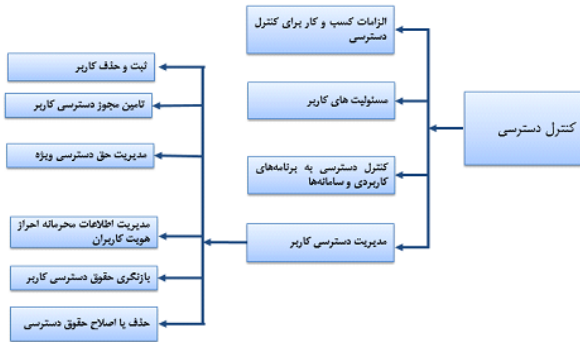
جهت ارزیابی امنیت محصولات تکنولوژی اطلاعات توسط مؤسسه CC ISO/IEC پذیرفته و منتشر شده است [۱]. استاندارد ISO/IEC 15408 در واقع به شرح تعارف کلی، نیازمندی‌های عملکردی، نیازمندی‌های تضمین و سطوح امنیتی و نیازمندی‌های آن می‌پردازد. CEM متدولوژی را برای ارزیابی امنیت IT با استفاده از CC به عنوان پایه ارائه می‌دهد. بسیاری از کشورهای جهان در قاره‌های آمریکا، اروپا و آسیا از این استاندارد بین‌المللی استفاده می‌کنند. این استاندارد به عنوان استاندارد ملی نیز در کشور ما پذیرفته شده است.

استاندارد ISO/IEC 15408 الزامات امنیتی عملکردی را در قالب ۱۱ کلاس امنیتی ارائه می‌دهد. ساختار تشکیل‌دهنده کلاس در این استاندارد مطابق شکل ۱ می‌باشد. 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. همچنین در این استاندارد مفهومی تحت عنوان تضمین 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 می‌باشد.

یکی دیگر از مفاهیمی که در این استاندارد مطرح است، مفهوم سند پروفایل حفاظتی (PP^۱) است. این استاندارد نیازمندی‌های عملکردی و تضمین را به صورت کامل و جامعی ارائه داده است. ولی در این استاندارد نیازمندی‌ها برای محصول خاصی طبقه‌بندی و انتخاب نشده است. انتخاب نیازمندی‌ها در سند پروفایل حفاظتی انجام می‌شود. پروفایل حفاظتی مجموعه‌ای از نیازمندی‌های عملکردی و تضمین برای یک نوع خاص از محصول فناوری اطلاعات است. در واقع پروفایل حفاظتی سند طراحی سیستم است که در ابتدا الزامات امنیتی و سپس راهکارهای کلی برای برآورده نمودن این دسته از الزامات را مشخص می‌کند. این سند اصولاً 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^۲) است. سند هدف امنیتی پایه‌ای برای ارزیابی یک

^۱Protection Profile ^۲Security Target



شکل ۲. ساختار کنترل های امنیتی در استاندارد ISO/IEC ۲۷۰۰۱ [۳]

مخاطرات الزامی می‌باشد اما اهداف کنترلی و کنترل‌های مربوطه می‌توانند بنا بر نیاز سازمان به کار 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.

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 نموده است.

۳ استانداردها و گزارشات مرتبط با سیستم‌های کنترل صنعتی

۱.۳ مجموعه استانداردهای ISO/IEC 62443

هدف اصلی خانواده استانداردهای (ISA99) ISO/IEC 62443 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 می‌باشد. از میان این استانداردها با توجه به موضوع مورد بحث استاندارد IEC 62443-3، IEC62443-3-2، IEC 63443-4-1 و IEC 63443-4-1 در ادامه به صورت اجمالی مورد بحث و بررسی قرار خواهند گرفت.

۱.۱.۳ استاندارد IEC 6244-3-3

این استاندارد، هفت الزام پایه (FR^۱) را به مجموعه‌ای از الزامات سامانه (SR^۲) متناظر می‌کند و هر الزام (SR) یک الزام پایه یا چند الزام افزایشی (RE^۳) 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

^۱Foundational Requirement ^۲System Requirement (SR) ^۳Requirement Enhancements

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 نموده است. همچنین این سند دسته‌بندی در خصوص سطوح تضمین امنیتی ارائه نموده است.

۳.۲ سندهمجموعه استانداردهای ISO/IEC 27000

مجموعه ISO/IEC27000 (که تحت عنوان «خانواده استاندارد ISMS» یا به اختصار ISO27k شناخته شده‌است)، شامل استانداردهای امنیت اطلاعات به طور مشترک توسط سازمان بین‌المللی استانداردسازی (ISO) و کمیسیون علوم الکترونیکی بین‌المللی (IEC) منتشر شده است. 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) بیان می‌کند. به طور کلی این خانواده دارای ۳ استاندارد الزام‌آور 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].

اولین 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 ممیزی کننده یا ارائه دهنده گواهی (CB) را تبیین می‌کند. استاندارد ISO/IEC 27009 که الزامات پیاده‌سازی ISMS برای حوزه‌های کسب و کاری خاص را تدوین نموده 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. در واقع به غیر از سه استاندارد مذکور، سایر استانداردها نظیر ISO/IEC 27005 یا ISO/IEC 27002 اگر چه به بیان راهنمایی‌هایی در خصوص کنترل‌های 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 به کار برده شود.

این استاندارد شامل دو بخش اصلی استاندارد و اهداف کنترلی و کنترل‌ها که پیاده‌سازی بخش اصلی استاندارد برای اجرای سیستم مدیریت

مدیریت امنیت (SM)^۱: 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 مشخص شده 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): فرآیندهای مشخص شده در این عمل برای اطمینان از این‌که استراتژی دفاع در عمق به عنوان بخش از طراحی قرار داده شده‌است، استفاده می‌شود.

پیاده‌سازی امن (SI)^۲: فرآیندهای مشخص شده 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^۳: فرآیندهای مشخص شده در این عمل برای مستندسازی تست امنیتی مورد نیاز 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)^۴: فرآیندهای مشخص شده در این عمل، برای رفع مسائل مرتبط با امنیت یک محصول استفاده می‌شود که برای بکارگیری استراتژی دفاع در عمق خود در چهارچوب امنیتی محصول پیکربندی شده است.

مدیریت بروز رسانی امنیتی (SUM)^۵: فرآیندهای مشخص شده توسط این عمل برای اطمینان از اینکه به‌روزرسانی امنیتی مربوط به محصول تست شده و به موقع در اختیار کاربران محصول قرار می‌گیرند، به کار می‌رود.

دستورالعمل‌های امنیتی (SG)^۶: فرآیندهای مشخص شده در این عمل به این منظور به کار برده می‌شوند تا برای کاربران محصول مستندات 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 استاندارد ISO/IEC 15408 می‌باشند، اما با ریزدنگی کمتر از CC بیان شده‌اند. همچنین در این استاندارد نحوه اختصاص آنها به سطوح تضمین بیان نشده است [۶].

۴.۱.۳ استاندارد IEC 62443-4-2

این استاندارد نیز مشابه استاندارد IEC 62443-3-3 به بیان الزامات هفت‌گانه در سطح تجهیز، سامانه و زیرسامانه می‌پردازد [۷]. ساختار بیان

استاندارد، سطوح امنیت (SLs) را به پنج سطح مختلف (۰، ۱، ۲، ۳ و ۴) تقسیم‌بندی می‌کند. این سطوح و تعاریف آنها عبارتند از:

(۱) SL 0: هیچ الزامات ویژه یا حفاظت امنیتی لازم نیست.

(۲) SL 1: حفاظت در مقابل نقض گاه به گاه یا تصادفی

(۳) SL 2: حفاظت در برابر تخلف عمدی با استفاده از ابزار ساده با منابع و مهارت‌های عمومی کم، و انگیزه پایین

(۴) SL 3: حفاظت از نقض عمدی با استفاده از ابزارهای پیشرفته با منابع متوسط، مهارت‌های خاص IACS و انگیزه متوسط

(۵) 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 به ذکر است این سطوح در خصوص تضمین امنیتی درستی پیاده‌سازی الزامات امنیتی نمی‌باشد و بیان‌کننده قدرت مقابله امنیتی می‌باشند.

۲.۱.۳ استاندارد IEC 62443-3-2

از آنجایی که 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 آسیب رساندن 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 27005 انجام می‌گیرد و الزامات امنیتی بر این اساس مشخص می‌شود [۵].

۳.۱.۳ 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 تعریف شده 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:

^۱Security Management ^۲Secure Implementation ^۳Security verification and Validation testing (SV) ^۴security Defect Management ^۵Security Update Management ^۶Security Guidelines

شده در این استاندارد مشابه استاندارد IEC 62443-3-3 می‌باشد.

۲.۳ 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].

۳.۳ سند NIST800-82

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 راهبردهای 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 می‌پردازد. در ضمیمه Vol A 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 و سایر ویژگی‌های این سند بر اساس سند NIST 800-53 می‌باشد. حتی نام‌گذاری کنترل‌های نیز بر اساس کنترل‌های سند NIST 800-53 است و تنها SG.CA-3، SG.ID-1، SG.SC-20، SG.AC-16، SG.AC-3، SG.MA-2، SG.PL-5، SG.SC-2، SG.CP-4، SG.AC-19، 13، و SG.PL-4 در سند NIS 800-53 به آنها اشاره نشده است که بیشتر حول محور امنیت سیستمی و شبکه‌ای می‌باشند.

۴.۳ استاندارد ISO/IEC 27019

استاندارد ISO/IEC 27019 استاندارد مدیریت امنیت اطلاعات بر اساس ISO/IEC 27001 برای سامانه‌های کنترل فرآیند ویژه صنعت انرژی می‌باشد. این مستند در حقیقت به نوعی نگاهت ISMS به حوزه کنترل

۵.۱.۳ سطوح تضمین بر اساس مستندات ISA Secure

در سال ۲۰۰۶ ISA، (ASCI^۱) 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 موسسه زیر بر روی ISA فعالیت می‌کنند:

- ISA Security Compliance Institute
- ISA 100 Wireless Compliance Institute

ISA Security Compliance Institute، ISA Secure را مدیریت می‌کند. این موسسه محصولات، سیستم‌ها و دارایی‌های تأمین‌کنندگان را بر اساس بهترین روش‌های توسعه چرخه حیات امن ارزیابی می‌کند. اهداف مد نظر ISA Secure را می‌توان به طور خلاصه به صورت زیر بیان نمود:

- (۱) تسهیل آزمون و صدور گواهی‌نامه سیستم‌های کنترل سیستم برای یک مجموعه مشخص از استانداردهای امنیتی سیستم‌های کنترلی
- (۲) استفاده از استانداردهای موجود صنعتی امنیتی در خصوص سیستم‌های کنترل صنعتی و توسعه و بکارگیری استانداردهای موقت در مواقعی که در این خصوص استاندارد وجود نداشته باشد و پذیرش استانداردهای جدید وقتی تدوین بشوند.
- (۳) شتاب‌دهی به توسعه استانداردهای صنعتی که می‌توانند برای تأیید سیستم‌های کنترل صنعتی جهت برآورده کردن یک سری از نیازمندی‌های امنیتی به کار گرفته شوند.
- (۴) 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 موسسه ISCI سه تأییدیه بر اساس چهار سطح مطرح در IEC62443-3-3 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 تأییدیه‌ها در چهار سطح تضمین ارائه می‌شوند که بر اساس چهار استاندارد IEC 62443-3-2، IEC 62443-3-3، 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.

¹Automation Standards Compliance Institute

مرحله استانداردهای مختلف از لحاظ با یکدیگر مقایسه شدند.

با توجه به مطالب ارائه شده در مورد مقایسه‌ی 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 استاندارد NIST 800-30 واگذار نموده است که این دسته‌بندی در استاندارد IEC 27001 وجود ندارد. در کل در خصوص مقایسه این دو استاندارد می‌توان گفت که استاندارد NIST 800-53 به عنوان استاندارد جهت ارزیابی محصولات امنیتی از لحاظ تعداد کنترل‌های امنیتی عملکردی و تضمین و همچنین سطح بندی انجام شده، مناسب تر است.

در خصوص 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 نموده است. استاندارد IEC 62443-3-3 نیز کنترل‌ها را در چهار سطح امنیتی SL1 تا SL4 دسته‌بندی نموده است ولی در نهایت انتخاب کنترل‌ها را به مدیریت ریسک واگذار نموده است. هر چند که بر اساس اسناد ISA secure این سطوح را می‌توان به سطح تضمین مرتبط نمود، ولی این موارد استاندارد نمی‌باشند. از لحاظ سطوح تضمین امنیت هر دو سند، دسته‌بندی خاصی در این 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 می‌باشد.

در خصوص 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

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 کنترل‌های 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 سیستم‌های کنترل صنعتی صنعت برق

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

- (۱) الزام‌های عملکردی
- (۲) الزام‌های دسترس‌پذیری (قابلیت اطمینان)
- (۳) الزام‌های مدیریت مخاطره
- (۴) سیستم عامل
- (۵) محدودیت منابع
- (۶) ارتباطات
- (۷) مدیریت تغییر
- (۸) پشتیبانی مدیریت شده
- (۹) طراحی عمر مؤلفه
- (۱۰) 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 جز استاندارد ISO/IEC 62443 که پایه الزامات را مشخص نکرده است، از الزامات استانداردهای مرتبط با سیستم‌های فناوری اطلاعات عمومی می‌باشد 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 متدولوژی جهت ارزیابی محصول معیارهای مختلفی نظیر پوشش دهی کامل الزامات، تعیین قدرت امنیتی، تعیین سطوح تضمین امنیتی، دسته‌بندی دقیق الزامات مطرح می‌باشد، در این

همچنین بر اساس نتایج حاصله از مقایسه استانداردها و اسناد موجود جهت ارزیابی محصولات بر اساس معیارهای مختلفی نظیر پوشش‌دهی کامل الزامات، تعیین قدرت امنیتی، تعیین سطوح تضمین امنیتی، دسته‌بندی دقیق الزامات، چنین حاصل می‌شود که استاندارد IEC/ISO 15408 از لحاظ معیارهای مورد بررسی کاملترین مرجع می‌باشد.

لیکن وجود آزمایشگاه‌های مختلف Exida, ISAsecure Wurldtech, Tecnalía, Kema و ... که بر اساس استانداردهای ISA99 و الزامات دیگر استانداردها نظیر NIST800-53، تأییدیه صادر می‌نمایند و ابزارهای موجود در این خصوص نظیر Achilles Test Platform این تصور را ایجاد می‌نمایند که شاید کنترل‌های این سند و یا سند NISTIR7628 حداقل‌های لازم برای سامانه کنترل صنعتی و شبکه هوشمند باشند.

این موضوع در انتخاب استاندارد IEC 15408 به عنوان متدولوژی جامع ارزیابی امنیتی سامانه‌های 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 که با توجه به پوشش کامل الزامات (عملکردی و تضمین) توسط استاندارد IEC 15408 می‌تواند با توجه به توصیه‌های دیگر استانداردها نظیر استاندارد مجموعه استانداردهای ISA99 باشد. لذا با توجه به بررسی‌های انجام شده و بستر مناسب موجود در آزمایشگاه‌های کشور، استاندارد ملی IEC 15408 می‌تواند به عنوان مرجع متدولوژی ارزیابی محصولات صنعتی نیز بکار گرفته شود.

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 con-

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، عمدتاً 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 تقریباً 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 در خصوص ارزیابی سامانه یا سیستم و شبکه 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 حالی که 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، در حالی که سند NIST 800-53 کنترل‌های عملکردی را به سه سطح قدرت و تضمین امنیتی (کم، متوسط، زیاد) دسته‌بندی نموده است. هر چند که در سند NIST 800-53 بیان شده که تعیین دقیق این سطوح امنیت وابسته به نتیجه تحلیل مخاطرات می‌باشد. 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 مصرف‌کننده محصول در خصوص 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 متدولوژی ارزیابی محصولات نسبت به NIST800-53 باشد. خلاصه‌ای از مقایسه‌های صورت گرفته در جدول ۲ قابل مشاهده است.

۶ نتیجه‌گیری

به عنوان نتیجه‌گیری می‌توان بیان نمود که پایه الزامات امنیتی ارائه شده در تمامی استانداردهای امنیت صنعتی، از الزامات سیستم‌های فناوری اطلاعات عمومی بوده است و تنها ملاحظات طراحی با توجه به ویژگی‌های سامانه‌های کنترل صنعتی باید در هنگام پیاده‌سازی این الزامات در نظر گرفته شود.

جدول ۱. خلاصه نتایج مقایسه استانداردها و اسناد مورد بررسی

نام سند	ساختار شکست الزامات	الزامات تضمین	سطح امنیتی	سطح تضمین	تخصیص الزامات
ISO/IEC 15408	دارای چهار سطح (با پوشش‌دهی کامل)	✓ (با جزئیات کامل)	✓	✗	PP, ST
NIST 800-53	دارای سه سطح	✓	✓	✗	NIST800-30
ISO/IEC27001	دارای سه سطح	✓	✗	✗	ISO/IEC27005
IEC 63443-3-2, IEC 63443-4-1, IEC 63443-4-2	دارای سه سطح	✓	✓	✗	IEC 63443-3-2
NIST 800-82	دارای سه سطح	✓	✓	✗	NIST 800-30
NIST 7628	دارای سه سطح	✓	✓	✗	NIST 800-30
ISO/IEC 27019	دارای سه سطح	✓	✗	✗	ISO/IEC 27005

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.

- [11] 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.
- [12] Wurdtech Security Technologies Inc., Achilles Practices Certification Datasheet, 2016.
- [13] Embedded Device Security Assurance (EDSA) - version 2.0.0 effective 01 July 2016.
- [14] <http://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification>.
- [15] DNV GL - Energy, DNV GL DLMS Test Suite for Smart Meters, www.dnvgl.com.
- [16] Certification of Smart Meters and Smart Data Concentrators, <http://www.tecnalia.es/en/>.
- [17] <https://www.encs.eu/activities/security-testing/>, <http://www.dlms.com/conformance/certificationproc>.

جدول ۲. بررسی کلی برخی از آزمایشگاه‌ها و استانداردهای مورد استفاده در آنها

نام آزمایشگاه	متدولوژی	زمینه فعالیت
Wurdtech	WIB(IEC27002,NIST80-82,...) ISO/IEC Guide 65, ISA99, NERC/CIP/NIST	ISA/IACS
DNV GL	IEC 15408/ISA99	Energy Utilities, ISA, IACS
Technalia	IEC 15408/ISA99	Smart Metering, ICS Security
ENCS	ISA99	Smart Metering, ICS Security

control systems Security risk assessment and system design, Draft 6, Edit 2, 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.
- [8] <https://isasecure.org/en-US/>.
- [9] 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.
- [10] National Institute of Standards and Technology, NISTIR

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

An Overview of Security Standards in the Field of ICT in order to Determining the Appropriate Methodology for the Security Evaluation of Equipment Related to Information and Communication Technology in the Power Industry★

Sofia Ahanj*, Mahsa Rahman, Vida Nobakht and Zahra Sadeghigol

Niroom Research Institute, Tehran, Iran

ARTICLE INFO.

Keywords:

ISO/IEC 15408
ISO/IEC 27001 series
NIST SP 800-53
NISTIR 7628
NIST 800-82
ISO/IEC 27019
ISA/IEC 62443 series

dor: 20.1001.1.24763047.1401.11.1.11.8

Type: research paper

ABSTRACT

Providing security in the electricity industry, as one of the vital infrastructures of the country, is one of the essential operations that must be taken in order to improve the security of the country. Resistant security strategies need to be regularly implemented as a dynamic process to improve security, and security evaluation is one of the most important steps in this process. Methodology in the field of evaluation in both technical and managerial dimensions is discussed in the laboratory. There are various standards in the field of general ICT technical-security evaluation. The most important are ISO/IEC 15408, ISO/IEC 27001 and NIST SP 800-53. In the present paper, these standards are first examined. Then, the standards and reports in the industrial field have been reviewed and compared, and finally, based on the results and special considerations of information and communication technology equipment in the electricity industry, the appropriate methodology has been presented.

© 2022 ISC

★ The ISCISC 2021 Program Committee effort is highly acknowledged for reviewing this paper.

* Corresponding author

Email addresses: sahanj@nri.ac.ir (Sofia Ahanj), rahmani.m87@gmail.com (Mahsa Rahman), nobakhtvida@yahoo.com (Vida Nobakht), sadeghigol@gmail.com (Zahra Sadeghigol)

© 2022 ISC. All rights reserved.