*فصلنامه مطالعات راهبردی فضای سایبر*
*سال اول، شماره ۲، بهار ۱۴۰۱*
*مقاله ششم، از صفحات ۱۵۲-۱۳۳*

**مقاله پژوهشی:**

# مدل ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری

**علی‌محمد امین زاده[۱]، ابراهیم محمود زاده[۲]، محمدرضا موحدی صفت[۳]، محمدعلی فرقانی[٤]**

**تاریخ دریافت: ۱۴۰۰/۰۵/۱۰** **تاریخ پذیرش: ۱۴۰۰/۱۲/۲**

## چکیده

دو عامل اصلی در توسعهٔ سیستم‌های کنترل صنعتی دفاعی، افزایش بهره‌وری و کیفیت محصولات دفاعی می‌باشد و این توسعه به دلیل بهره‌گیری از تجهیزات سایبر پایه باعث افزایش آسیب‌پذیری‌های سایبری در فرایند تولید سیستم‌های کنترل صنعتی دفاعی شده است. تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری، به معنی ایجاد تمهیدات مناسب پیش از حملهٔ سایبری، حفظ عملیات اصلی سیستم و پایداری مناسب در زمان حملهٔ سایبری و بازگشت به حالات اولیه پس از حملهٔ سایبری یکی از اصلی‌ترین راهبردها در مواجهه با تهدیدات سایبری است؛ در این پژوهش برای ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری به‌عنوان یکی از اصلی‌ترین گام‌ها در تاب‌آوری سایبری، مدل ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری مبتنی بر مدل یکپارچه‌سازی مدل بلوغ توانایی[۵]، برای سه سطح سیستم‌های کنترل صنعتی شامل سطح راهبری، سطح کنترل و سطح عملیات سیستم کنترل صنعتی دفاعی ارائه‌شده است. مدل ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری در پنج سطح بلوغ و سه بعد اصلی سیستم‌های کنترل صنعتی ارائه‌شده است و درمجموع ۵۱ شاخص ارائه‌شده است.

**کلیدواژه‌ها: ارزیابی و تحلیل آسیب‌پذیری‌ها، سیستم‌های کنترل صنعتی دفاعی، تاب‌آوری سایبری**

۱. دانش آموخته مقطع دکتری دانشگاه عالی دفاع ملی (نویسنده مسئول) *am.aminzadeh@sndu.ac.ir*
۲. استاد و عضو هیئت علمی دانشگاه صنعتی مالک اشتر
۳. دانشیار و عضو هیئت علمی دانشگاه عالی دفاع ملی
٤. استادیار و عضو هیئت علمی دانشگاه عالی دفاع ملی

۵. *Capability Maturity Model Integration (CMMI)*

## مقدمه

نگرانی سازمان‌های دولتی، شرکت‌های بخش خصوصی و مؤسسات علمی از تهدیدات خارجی ناشی از دسترسی به اطلاعات حساس، خرابکاری اینترنتی و حملات انکار سرویس توسط طیف هکرها، جنایتکاران، تروریست‌ها و بازیگران دولتی رو به افزایش است. سال ۲۰۱۸ سرشار از حوادث سیستم‌های کنترل صنعتی بود. مطابق با جزئیات منتشر شد در تریتون در خصوص حملات سایبری سال ۲۰۱۸، بدافزارهایی نظیر استاکس نت و اینداستروور، بیشترین حمله را به تجهیزات سیستم‌های کنترل صنعتی را داشته‌اند و علاوه بر این، چندین حمله با مشخصات بالا به شرکت‌های صنعتی ضربه‌های شدیدی را وارد نموده‌اند. بوئینگ اعلام کرد که توسط بدافزار واناکری مورد اصابت قرار گرفت و چند ماه بعد، همین ویروس چندین کارخانهٔ شرکت تولیدی نیمه‌هادی تایوان را خاموش کرد؛ اگرچه این حملات زیرساخت‌های فناوری اطلاعات را مورد هدف قرار داد اما پیامدهای آن‌ها همچنین بر فناوری عملیاتی مورداستفاده برای تولید تأثیر گذاشت؛ درواقع، مهاجمان همیشه به دانش خاصی نیاز ندارند تا بتوانند آن‌ها را مختل کنند (تکنولوژی‌های مثبت[۱]، ۲۰۱۹).

## بیان مسئله

پس از سوءاستفاده از آسیب‌پذیری‌ها در زیرساخت‌های فناوری اطلاعات، هکرها می‌توانند به شبکهٔ صنعتی دسترسی پیدا کنند؛ طبق تحقیقات ما، یک مهاجم داخلی که قبلاً بر روی سیستم اطلاعاتی شرکت دسترسی داشته است، می‌تواند در ۸۲ درصد موارد به شبکهٔ صنعتی نفوذ کند. مهاجمین روش‌های مختلفی برای انجام اقدامات مخرب در برابر اجزای سیستم‌های کنترل صنعتی دارد و متداول‌ترین آن سوءاستفاده از آسیب‌پذیری‌های شناخته‌شده است؛ به همین دلیل شناسایی آسیب‌پذیری‌های موجود در تجهیزات سیستم‌های کنترل صنعتی بسیار مهم است؛ زیرا

۱. positive Technology

این امر به مشاغل اجازه می‌دهد خطرات را به‌موقع ارزیابی کرده و اقدامات حفاظتی مناسبی را انجام دهند (استیو میلر، ایون رایس[۱]، ۲۰۱۸).

سیستم‌های کنترل صنعتی دفاعی به دلیل حساسیت دشمنان نسبت به افزایش توان دفاعی کشور همواره موردتوجه بوده است و وجود آسیب‌پذیری در این سیستم‌ها می‌تواند خسارات جبران‌ناپذیری را ایجاد نماید. این پژوهش به دنبال ارائهٔ پاسخ مناسب در خصوص شناسایی و مدیریت آسیب‌پذیری‌های سیستم‌های کنترل صنعتی دفاعی و ارائهٔ مدل ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری است.

**اهمیت تحقیق**

نیاز به مدل راهبردی مناسب برای تداوم فعالیت‌های اساسی سیستم‌های کنترل صنعتی دفاعی در مواجهه با تهدیدات سایبری – نیاز به مدل راهبردی مناسب در شناسایی مدیریت آسیب‌پذیری‌های، ریسک‌ها و رخدادهای سایبر سیستم‌های خودکارسازی صنعتی دفاع – داشتن برنامهٔ راهبردی مناسب در کاهش ریسک‌های عملیاتی سیستم‌های کنترل صنعتی در مواجهه با تهدیدات سایبری – داشتن برنامهٔ راهبردی مناسب برای بازگشت به حالت اولیه از انجام حملهٔ سایبری احتمالی به سیستم‌های کنترل صنعتی دفاعی.

**ضرورت تحقیق**

هزینه‌های بسیار بالای ناشی از نداشتن مدل راهبردی مناسب در بروز حملات سایبری به سیستم‌های کنترل صنعتی دفاعی- عدم بهره‌گیری مناسب از سیستم‌های کنترل صنعتی دفاعی ناشی از افزایش آسیب‌های مرتب با بهره‌گیری تجهیزات نوین سیستم‌های کنترل و نداشتن مدل راهبری مناسب در مواجهه با تهدیدات سایبری- عدم بهره‌گیری از سیستم‌های کنترل صنعتی دفاعی ناشی از افزایش و تنوع تهدیدات سایبری- به دلیل نداشت مدل راهبری مناسب در مواجههٔ با این تهدیدات.

---

۱. Steve Miller, Evan Reese

هدف اصلی عبارت است از: ارائۀ مدل ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری.

اهداف فرعی عبارتنداز: شناسایی آسیب‌پذیری‌های سیستم‌های کنترل صنعتی دفاعی- شناسایی ابعاد سیستم‌های کنترل صنعتی دفاعی- شناسایی مؤلفه‌های اصلی تاب‌آوری سیستم‌های کنترل صنعتی دفاعی.

مدل ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری **سیستم‌های** کنترل صنعتی دفاعی در مقابل تهدیدات سایبری کدام است؟ به‌عنوان سؤالات اصلی و ۱-آسیب‌پذیری‌های سیستم‌های کنترل صنعتی دفاعی کدامند؟ ۲-ابعاد سیستم‌های کنترل صنعتی دفاعی کدامند. ۳-شاخص‌های اصلی برای ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری کدامند؟ سؤالات فرعی هستند.

**پیشینۀ پژوهش**

در این پژوهش با مرور ادبیات پیشین حوزۀ امنیت سایبری و سیستم‌های کنترل صنعتی و همچنین با بهره‌گیری از نظرات متخصصین این حوزه، انواع حملات سایبری شناسایی گردند و سپس عواملی از زیرساخت‌های حیاتی ازجمله سیستم‌های کنترل صنعتی که تحت تأثیر قرار می‌گیرند و موردحمله واقع می‌شوند، مشخص می‌گردند؛ بنابراین مطالعات صورت‌گرفته در این حوزه تا حدودی توانسته‌اند این عوامل را شناسایی کنند و می‌توان این را از نکات مشترک این پژوهش و مطالعات پیشین در نظر گرفت؛ درحالی‌که در این پژوهش تمامی موارد مهم و ضروری که تحت تأثیر حملات سایبری قرار می‌گیرند از متخصصان و مطالعات پیشین استخراج می‌شود.

## مبانی نظری

تفاوت اساسی بین سیستم‌های کنترل صنعتی و سیستم‌های فناوری اطلاعات سنتی در این است که سیستم‌های کنترل صنعتی با محیط فیزیکی ارتباط برقرار می‌کنند. سیستم‌های کنترل صنعتی و کلیهٔ سیستم‌های زیرساختی سایبری[۱] در سیستم‌های سایبری هستند و به همین دلیل در برابر حملات سایبری آسیب‌پذیر هستند؛ این ارتباط با دنیای فیزیکی، چالش‌ها و فرصت‌های بی‌نظیری را نشان می‌دهد. سیستم‌های کنترل صنعتی منابع محاسباتی، قابلیت‌های ارتباطی، سنجش و تحریک را در تلاش برای نظارت و کنترل فرایندهای فیزیکی ادغام می‌کنند. سیستم‌های کنترل صنعتی در زیرساخت‌های مهم مانند شبکه‌های حمل‌ونقل، سیستم‌های هوایی بدون سرنشین[۲]، تولید برق هسته‌ای، شبکه‌های توزیع برق، شبکه‌های توزیع آب و گاز و سیستم‌های پیشرفتهٔ ارتباطی یافت می‌شود؛ نکتهٔ مهم و قابل‌توجه این است که فناوری اطلاعات در بخش اصلی و میانی فناوری عملیات قرار گرفته است و این همگرایی بین فناوری اطلاعات و فناوری عملیات به همراه گسترش به‌کارگیری انواع حس‌گرهای هوشمند در سطح عملیاتی، باعث افزایش سطح حملات شده است؛ در این محیط جدید سطح حملات از سرقت اطلاعات به سطوح پیچیده‌تری نظیر جرائم سایبری تغییر پیدا کرده است (ادوارد جی. ام کلبرت، الکساندر کوت، ۲۰۱۶).

به‌کارگیری سیستم اسکادا در سطح فرایند تولید با شناسایی دقیق و تجزیه‌وتحلیل آسیب‌پذیری‌های داخلی و خارجی و درنتیجه کاهش خطرات احتمالی فرایند تولید و قرار گرفتن در شرایط بحرانی که می‌تواند در سطح عمومی جامعه باعث بحران‌هایی نظیر قطع برق شود. راهبرد دفاع در عمق[۳] یک استراتژی امنیت اطلاعات است که با به‌کارگیری سه عنصر اصلی افراد، فناوری و عملیات، برای ایجاد موانع لازم را برای نفوذ در لایه‌های مختلف سازمان توصیه می‌شود. اتخاذ رویکرد دفاع در عمق، نیاز به رویکرد چند رشته‌ای در تمامی سطوح سیستم دارد،

---

۱. Cyber-Physical Systems (CPS)

۲. Unmanned Aerial Vehicle Systems (UAS)

۳. defense-in-depth

امکان شناسایی و یا جلوگیری از نقض کامل را فراهم می‌کند و بخشی از یک راهبرد کاهش خطر جامع است. نکتهٔ مهم و اساسی در این رویکرد این است که یک شبکهٔ آگاهانه‌تر می‌تواند مشکلات کاری و امنیتی را شناسایی کند.

**آسیب‌پذیری‌های سیستم‌های کنترل صنعتی**

در سال‌های اخیر علاوه بر آسیب‌پذیری‌های نرم‌افزاری، انواع سخت‌افزاری و سفت‌افزاری نیز به‌شدت موردتوجه کارشناسان امنیت قرار گرفته است؛ این موارد در پردازنده‌ها و قطعات الکترونیکی به‌طور گسترده وجود دارند و حتی در سطوح مخابراتی و یا نظامی نیز یافت می‌شوند؛ نمونهٔ بارزی از این آسیب‌پذیری‌ها، وجود یک نقطهٔ دسترسی مخفی در تراشه‌های ساخت یک شرکت چینی است که در تجهیزات نیروی هوایی آمریکا نیز به کار می‌روند و توسط گروه تحقیقات دانشگاه کمبریج شناسایی شده است. سیستم‌های کنترل شامل تجهیزات الکترونیکی و پردازشی متنوعی است که ازجمله مهم‌ترین این تجهیزات، عملگرها، حس‌گرها، سیستم‌های کنترلی قابل‌برنامه‌ریزی[۱] و واحدهای ارتباط از راه دور[۲] است. مهاجمان با دسترسی به کد نرم‌افزاری و یا سفت‌افزاری این تجهیزات، می‌توانند به‌راحتی به سامانه‌های کنترل نفوذ کرده و کنترل فرایند را در دست بگیرند. در آخرین پژوهش‌های انجام‌شده در دنیا و به‌عنوان نمونه در دانشگاه کارولینای جنوبی که در خصوص آسیب‌پذیری کدهای کنترل‌کننده‌های منطقی برنامه‌ریزی‌شده[۳] از طریق سیستم‌های اسکادا انجام شده است، حاکی از ضعف شدید این ابزارها در حوزهٔ امنیت سایبری است؛ ازجمله آسیب‌پذیری‌های عنوان‌شده برای واحدهای ارتباط از راه دور[٤]، تأیید ورودی نامناسب و غیر ایمن این تجهیز می‌باشد که منجر به نفوذ مهاجم به سیستم کنترل صنعتی می‌گردد. پژوهش مذکور برای استفادهٔ گسترده از سیستم‌های کنترل نظارت و جمع‌آوری داده‌ها (اسکادا[٥]) در تولید خودکار و سایر زمینه‌های زیرساخت و همچنین برنامه‌های

---

۱. PLC

۲. RTU

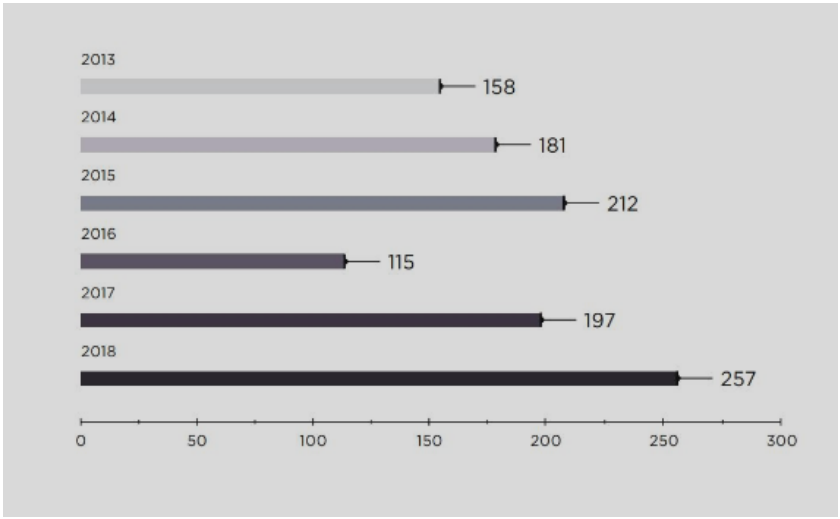
۳. PLC

٤. RTU

٥. SCADA

کاربردی از فرایندهای شیمیایی و تأسیسات تصفیهٔ آب، تولید نفت، گاز، برق و... انجام‌شده است؛ در این پژوهش به دلیل موردتوجه قرار ندادن خطرات امنیتی ناشی از حملات علیه دستگاه‌های جانبی مانند کنترل‌کننده‌های منطقی برنامه‌ریزی‌شده انجام‌شده است؛ در این پژوهش اقدامات سازگار با فناوری‌های کنترل‌کننده‌های منطقی برنامه‌ریزی‌شده توسعه‌یافته است که هر دو اشتباهات نرم‌افزاری عمدی و غیرعملی را مطالعه و روش‌هایی برای جلوگیری از آن‌ها را پیشنهاد کرده است (والن تاین[۱]، ۲۰۱۳).

تعداد آسیب‌پذیری‌های جدید در اجزای سیستم‌های کنترل صنعتی نسبت به سال ۲۰۱۷ معادل ۳۰ درصد افزایش‌یافته است. در زمان این تحقیق، اطلاعات کامل در مورد ۲۴۳ آسیب‌پذیری منتشرشده است که ۱۴ آسیب‌پذیری هنوز در انتظار تحلیل هستند. جدول مقایسهٔ آسیب‌پذیری‌های به تفکیک سال در شکل زیر نشان داده‌شده است.



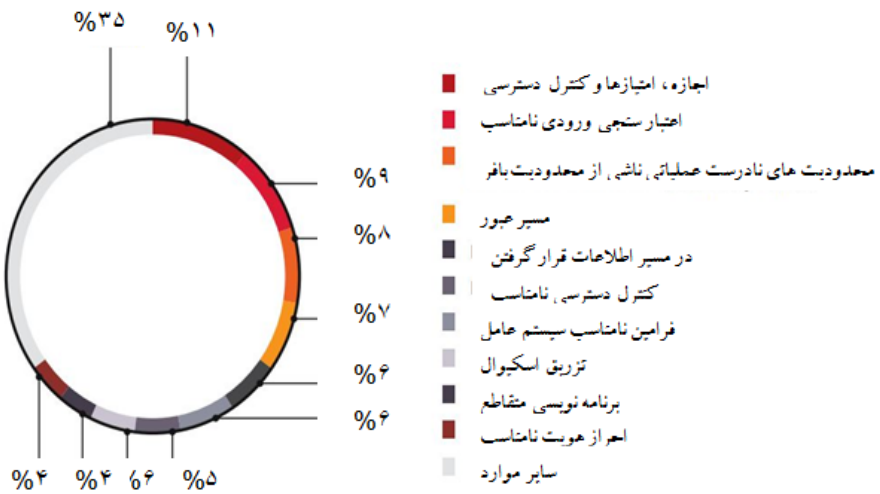

**شکل ۱- تعداد کل آسیب‌پذیری‌های موجود در اجزای سیستم‌های کنترل صنعتی (تکنولوژی‌های مثبت، ۲۰۱۹)**

۱. Valentine

از منظر تعداد آسیب‌پذیری‌های جدید در تجهیزات مورداستفاده، محصولات اشنایدر در سال ۲۰۱۸ همچنان صدرنشین بوده، هرچند که تعداد آسیب‌پذیری‌های موجود در تجهیزات زیمنس در مقایسه با سال گذشته تقریباً دو برابر شده است.

توزیع آسیب‌پذیری‌ها بر اساس نوع مؤلفهٔ سیستم‌های کنترل صنعتی در سال ۲۰۱۸ به‌طور قابل‌توجهی تغییر یافت. در سال ۲۰۱۷، اکثر آسیب‌پذیری‌ها در اجزای اسکادا مشاهده شد اما در سال ۲۰۱۸، آسیب‌پذیری‌ها تقریباً به‌طور مساوی بین اسکادا، آرتی یو / پی آل سی و تجهیزات شبکهٔ صنعتی توزیع شده‌اند. درصد آسیب‌پذیری در اجزای، آرتی یو / پی آل سی نسبت به سال ۲۰۱۷ معادل ۷ درصد افزایش‌یافته است.

بخش قابل‌توجهی از آسیب‌پذیری‌ها شامل احراز هویت نادرست یا امتیازات بیش‌ازحد است؛ بیش از نیمی از این آسیب‌پذیری‌ها (٦٤٪) قابل‌استفاده از راه دور هستند.




**شکل ۲- انواع آسیب‌پذیری در اجزای سیستم‌های کنترل صنعتی (تکنولوژی‌های مثبت، ۲۰۱۹)**

### سطوح سیستم‌های کنترل صنعتی

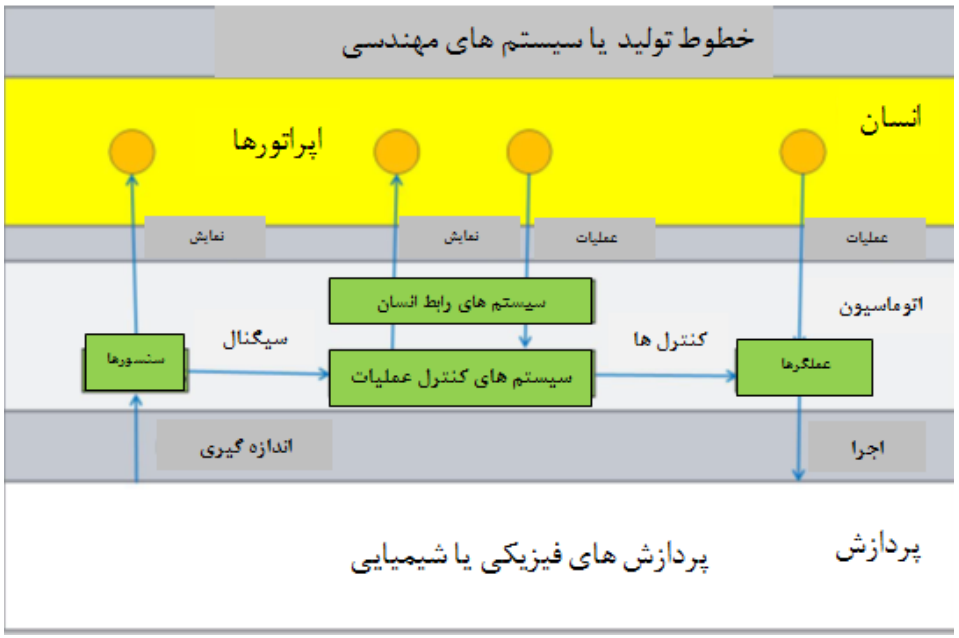
در خط تولید مبتنی بر سیستم‌های مهندسی، سه سطح اصلی سیستم‌های کنترل صنعتی به‌صورت زیر در نظر گرفته می‌شود:

۱- سطح اول که در بالای ساختار قرار دارد، مربوط به نیروهای انسانی یا اپراتورها هستند که وظیفهٔ پایش و نظارت پردازش داده‌ها از طریق حس‌گرها به‌صورت مستقیم و کنترل آن‌ها با استفاده از محرک‌ها را بر عهده دارند؛

۲- سطح دوم که سطح میانی آن است مربوط به لایهٔ خودکارسازی می‌باشد؛ در این لایه، سیستم کنترل صنعتی واقع در مرکز وظیفهٔ جمع‌آوری بی‌وقفهٔ داده‌ها از فرایندهای پردازش‌شده توسط حس‌گرها، ارائهٔ داده‌های وضعیت و تشخیص به اپراتورها از طریق رابط ماشین انسان، دریافت دستورها و تنظیمات از اپراتورها و کنترل فرایندهای کنترل‌شده از طریق حس‌گرها را بر عهده دارد؛

۳- سطح سوم، سطح نهایی است که مرتبط با لایهٔ پردازش یا فرایند است؛ در این لایه، فرایند فیزیکی یا شیمی از طریق حس‌گرها پایش و نظارت می‌شوند و به‌وسیلهٔ محک‌ها کنترل می‌شوند (وی جی[۱]، ۲۰۱۰).

۱. Wei & Ji, ۲۰۱۰




**شکل ۳- مدل سیستم سه سطحی خودکارسازی صنعتی (وی جی،۲۰۱۰)**

با توجه به مدل فوق می‌توان گفت که حوادث نامطلوب تنها محدود به حوادث رخ‌داده در درون سیستم کنترل اطلاعات نیستند، بلکه می‌توانند از طرق لایه‌های دیگر به این سیستم کنترل اطلاعات اعمال گردند؛ به‌عنوان‌مثال حوادث نامطلوب در لایهٔ نیروی انسانی، ارسال اشتباه دستورها یا تنظیمات به سیستم کنترل اطلاعات و در لایهٔ فرایند، شکستگی کابل و نیز در لایهٔ خودکارسازی از طریق آسیب‌دیدگی حس‌گرها می‌توانند به سیستم کنترل اطلاعات اعمال گردند.

## یافته‌های تحقیق

برای تدوین مدل مراحل ذیل انجام پذیرفت:

مرحلهٔ اول: در طراحی مدل پیشنهادی ابتدا بر اساس منابع علمی و پژوهش‌های انجام‌شده برای ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری سه محور اصلی در نظر گرفته شد:

- بر اساس سطوح سیستم‌های کنترل صنعتی (راهبری – کنترل – عملیات) که در سطح سازمان‌های صنعتی معادل سه سطح مدیریت سازمانی (راهبردی - میانی – عملیاتی)

می‌باشد برای نظارت و راهبری سیستم که وابستگی بیشتر به نیروی انسانی خبره و تصمیم‌گیر دارد و سطح کنترل که بیشتر وابسته به ابزارهای کنترلی نظیر سیستم‌های فناوری عملیات و اسکادا[۱] و سیستم‌های کنترلی قابل‌برنامه‌ریزی[۲] می‌باشد و سطح عملیات که دربرگیرندهٔ تجهیزات و دریافت‌کننده‌ها[۳] و عملگرها[٤] است؛

- سطوح بلوغ سازمانی که دربرگیرندهٔ رشد سازمان در مدیریت آسیب‌پذیری‌های با پنج سطح بلوغ (انجام‌شده – برنامه‌ریزی‌شده – مدیریت‌شده – اندازه‌گیری شده – نهادینه‌شده) می‌باشد مبتنی بر مدل یکپارچهٔ بلوغ قابلیت‌های سازمانی در نظر گرفته‌شده است.

مرحلهٔ دوم: برای بررسی و تأیید محورها و مؤلفه‌های در نظر گرفته‌شده با انجام مصاحبهٔ خبرگان تأیید اخذ گردید؛ سپس برای هر سطوح بلوغ مبتنی بر سه بعد اصلی سیستم‌های کنترل صنعتی دفاعی گویه‌های ذیل استخراج گردید:

**جدول ۱- عوامل مؤثر در ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی**

| سطح بلوغ | عوامل مؤثر در ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی |
|---|---|
| یک (انجام‌شده) | • آماده‌سازی برای تجزیه‌وتحلیل آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• شناسایی و تجزیه‌وتحلیل آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• مدیریت آسیب‌پذیری‌های شناسایی‌شدهٔ عوامل انسانی و سازمانی<br>• بررسی علل ریشه‌ای آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• آماده‌سازی برای تجزیه‌وتحلیل آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• شناسایی و تجزیه‌وتحلیل آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• مدیریت آسیب‌پذیری‌های شناسایی‌شدهٔ سیستم‌های کنترل و نظارت<br>• بررسی علل ریشه‌ای آسیب‌پذیری‌های سیستم‌های کنترل<br>• آماده‌سازی برای تجزیه‌وتحلیل آسیب‌پذیری‌های تجهیزات و عملیات |

۱. SCADA

۲. PLC

۳. Sensors

٤. Actuators

| سطح بلوغ | عوامل مؤثر در ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی |
|---|---|
| | • شناسایی و تجزیه‌وتحلیل آسیب‌پذیری‌های تجهیزات و عملیات<br>• مدیریت آسیب‌پذیری‌های شناسایی‌شدهٔ تجهیزات و عملیات<br>• بررسی علل ریشه‌ای آسیب‌پذیری‌های تجهیزات و عملیات |
| دوم (برنامه‌ریزی‌شده) | • برنامه‌ریزی مستند برای مدیریت آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• مدیریت مستند آسیب‌پذیری‌ها<br>• آگاهی نقش ذی‌نفعان برای فعالیت مدیریت آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• شناسایی و اجرای دستورالعمل‌ها و استانداردهای مدیریت آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• برنامه‌ریزی مستند برای مدیریت آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• آگاهی نقش ذی‌نفعان برای فعالیت مدیریت آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• شناسایی و اجرای دستورالعمل‌ها و استانداردهای مدیریت آسیب‌پذیری‌های سیستم‌های کنترل و نظارت برنامه‌ریزی مستند برای مدیریت آسیب‌پذیری‌های تجهیزات و عملیات<br>• آگاهی نقش ذی‌نفعان برای فعالیت مدیریت آسیب‌پذیری‌های تجهیزات و عملیات<br>• شناسایی و اجرای دستورالعمل‌ها و استانداردهای مدیریت آسیب‌پذیری‌های تجهیزات و عملیات |
| سوم (مدیریت‌شده) | • نظارت مدیریتی بر کارایی فعالیت‌های مدیریت آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• به‌کارگیری کارکنان مجرب طبق برنامه‌ریزی انجام‌شده برای آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• تخصیص بودجهٔ مناسب برای مدیریت آسیب‌پذیری‌ها به‌صورت برنامه‌ریزی‌شده برای آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• شناسایی و تحلیل، دفع، نظارت و کنترل ریسک مربوط به‌کارایی فعالیت‌های مدیریت آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• نظارت مدیریتی بر کارایی فعالیت‌های مدیریت آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• به‌کارگیری کارکنان مجرب طبق برنامه‌ریزی انجام‌شده برای آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• تخصیص بودجهٔ مناسب برای مدیریت آسیب‌پذیری‌ها به‌صورت برنامه‌ریزی‌شده برای آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• شناسایی و تحلیل، دفع، نظارت و کنترل ریسک مربوط به‌کارایی فعالیت‌های مدیریت آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• نظارت مدیریتی بر کارایی فعالیت‌های مدیریت آسیب‌پذیری‌های تجهیزات و عملیات |

| سطح بلوغ | عوامل مؤثر در ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی |
|---|---|
| | • به‌کارگیری کارکنان مجرب طبق برنامه‌ریزی انجام‌شده برای آسیب‌پذیری‌های تجهیزات و عملیات<br>• تخصیص بودجهٔ مناسب برای مدیریت آسیب‌پذیری‌ها به‌صورت برنامه‌ریزی‌شده برای آسیب‌پذیری‌های تجهیزات و عملیات<br>• شناسایی و تحلیل، دفع، نظارت و کنترل ریسک مربوط به‌کارایی فعالیت‌های مدیریت آسیب‌پذیری‌های تجهیزات و عملیات |
| چهارم (اندازه‌گیری شده) | • بازنگری و سنجش دوره‌ای مدیریت آسیب‌پذیری‌ها برای اطمینان از اثربخشی آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• بازنگری و سنجش دوره‌ای مدیریت آسیب‌پذیری‌ها برای اطمینان عملکرد طبق برنامه برای آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• آگاه‌سازی مدیریت سطح بالاتر از کارایی مدیریت آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• بازنگری و سنجش دوره‌ای مدیریت آسیب‌پذیری‌ها برای اطمینان از اثربخشی آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• بازنگری و سنجش دوره‌ای مدیریت آسیب‌پذیری‌ها برای اطمینان عملکرد طبق برنامه برای آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• آگاه‌سازی مدیریت سطح بالاتر از کارایی مدیریت آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• بازنگری و سنجش دوره‌ای مدیریت آسیب‌پذیری‌ها برای اطمینان از اثربخشی آسیب‌پذیری‌های تجهیزات و عملیات<br>• بازنگری و سنجش دوره‌ای مدیریت آسیب‌پذیری‌ها برای اطمینان عملکرد طبق برنامه برای آسیب‌پذیری‌های تجهیزات و عملیات<br>• آگاه‌سازی مدیریت سطح بالاتر از کارایی مدیریت آسیب‌پذیری‌های تجهیزات و عملیات |
| پنجم (نهادینه‌شده) | • اتخاذ تعریف استاندارد از فعالیت‌های مدیریت آسیب‌پذیری‌ها برای عملیات منحصربه‌فرد آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• ثبت و اشتراک‌گذاری فعالیت‌های آسیب‌پذیری در سطح سازمان برای آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• اتخاذ تعریف استاندارد از فعالیت‌های مدیریت آسیب‌پذیری‌ها برای عملیات منحصربه‌فرد آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• ثبت و اشتراک‌گذاری فعالیت‌های آسیب‌پذیری در سطح سازمان برای آسیب‌پذیری‌های سیستم‌های کنترل و نظارت |

| سطح بلوغ | عوامل مؤثر در ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی |
|---|---|
| | • اتخاذ تعریف استاندارد از فعالیت‌های مدیریت آسیب‌پذیری‌ها برای عملیات منحصربه‌فرد آسیب‌پذیری‌های تجهیزات و عملیات<br>• ثبت و اشتراک‌گذاری فعالیت‌های آسیب‌پذیری در سطح سازمان برای آسیب‌پذیری‌های تجهیزات و عملیات |

مرحلهٔ سوم: گویه‌های فوق برای تعیین شاخص‌های ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری طی پرسشنامه‌ای برابر ساختار زیر در اختیار خبرگان قرار گرفت و نظر خبرگان اخذ گردید.

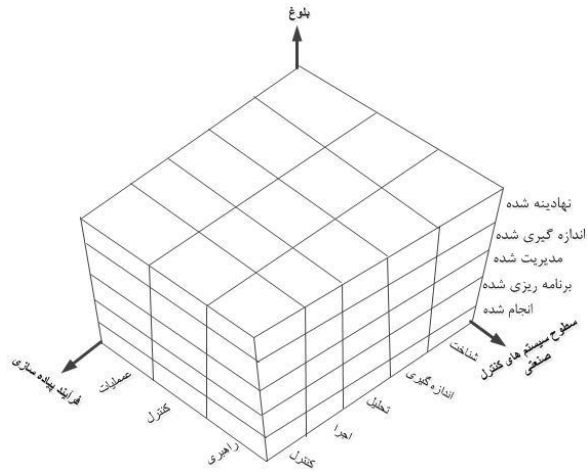
مرحلهٔ چهارم: تدوین مدل: بر اساس شاخص‌های احصاء شده و مبانی پژوهشی بیان‌شدهٔ مدل ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری به شرح ذیل تدوین و ارائه گردید:

**جدول ۲- مدل ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری**

| سطوح سیستم‌های کنترل صنعتی / سطوح بلوغ | راهبری | کنترل | عملیات |
|---|---|---|---|
| یک (انجام‌شده) | • آماده‌سازی برای تجزیه‌وتحلیل آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• شناسایی و تجزیه‌وتحلیل آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• مدیریت آسیب‌پذیری‌های شناسایی‌شده عوامل انسانی و سازمانی<br>• بررسی علل ریشه‌ای آسیب‌پذیری‌ها عوامل | • آماده‌سازی برای تجزیه‌وتحلیل آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• شناسایی و تجزیه‌وتحلیل آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• مدیریت آسیب‌پذیری‌های شناسایی‌شدهٔ سیستم‌های کنترل و نظارت<br>• بررسی علل ریشه‌ای آسیب‌پذیری‌ها سیستم‌های | • آماده‌سازی برای تجزیه‌وتحلیل آسیب‌پذیری‌های تجهیزات و عملیات<br>• شناسایی و تجزیه‌وتحلیل آسیب‌پذیری‌های تجهیزات و عملیات<br>• مدیریت آسیب‌پذیری‌های شناسایی‌شدهٔ تجهیزات و عملیات<br>• بررسی علل ریشه‌ای آسیب‌پذیری‌های تجهیزات و |

| سطوح سیستم‌های کنترل صنعتی / سطوح بلوغ | راهبری | کنترل | عملیات |
|---|---|---|---|
| | انسانی و سازمانی | کنترل و نظارت | عملیات |
| دوم (برنامه‌ریزی‌شده) | • برنامه‌ریزی مستند برای مدیریت آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• مدیریت مستند آسیب‌پذیری‌ها<br>• آگاهی نقش ذی‌نفعان برای فعالیت مدیریت آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• شناسایی و اجرای دستورالعمل‌ها و استانداردهای مدیریت آسیب‌پذیری‌های عوامل انسانی و سازمانی | • برنامه‌ریزی مستند برای مدیریت آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• مدیریت مستند آسیب‌پذیری‌ها<br>• آگاهی نقش ذی‌نفعان برای فعالیت مدیریت آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• شناسایی و اجرای دستورالعمل‌ها و استانداردهای مدیریت آسیب‌پذیری‌های سیستم‌های کنترل و نظارت | • برنامه‌ریزی مستند برای مدیریت آسیب‌پذیری‌های تجهیزات و عملیات<br>• مدیریت مستند آسیب‌پذیری‌ها<br>• آگاهی نقش ذی‌نفعان برای فعالیت مدیریت آسیب‌پذیری‌های تجهیزات و عملیات<br>• شناسایی و اجرای دستورالعمل‌ها و استانداردهای مدیریت آسیب‌پذیری‌های تجهیزات و عملیات |
| سوم (مدیریت‌شده) | • نظارت مدیریتی بر کارایی فعالیت‌های مدیریت آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• به‌کارگیری کارکنان مجرب طبق برنامه‌ریزی انجام‌شده برای آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• تخصیص بودجهٔ مناسب برای مدیریت آسیب‌پذیری‌ها به‌صورت برنامه‌ریزی‌شده برای آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• شناسایی و تحلیل، دفع، | • نظارت مدیریتی بر کارایی فعالیت‌های مدیریت آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• به‌کارگیری کارکنان مجرب طبق برنامه‌ریزی انجام‌شده برای آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• تخصیص بودجهٔ مناسب برای مدیریت آسیب‌پذیری‌ها به‌صورت برنامه‌ریزی‌شده برای آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• شناسایی و تحلیل، دفع، | • نظارت مدیریتی بر کارایی فعالیت‌های مدیریت آسیب‌پذیری‌های تجهیزات و عملیات<br>• به‌کارگیری کارکنان مجرب طبق برنامه‌ریزی انجام‌شده برای آسیب‌پذیری‌های تجهیزات و عملیات<br>• تخصیص بودجهٔ مناسب برای مدیریت آسیب‌پذیری‌ها به‌صورت برنامه‌ریزی‌شده برای آسیب‌پذیری‌های تجهیزات و عملیات<br>• شناسایی و تحلیل، دفع، |

| سطوح سیستم‌های کنترل صنعتی / سطوح بلوغ | راهبری | کنترل | عملیات |
|---|---|---|---|
| | نظارت و کنترل ریسک مربوط به کارایی فعالیت‌های مدیریت آسیب‌پذیری‌های عوامل انسانی و سازمانی | نظارت و کنترل ریسک مربوط به کارایی فعالیت‌های مدیریت آسیب‌پذیری‌های سیستم‌های کنترل و نظارت | نظارت و کنترل ریسک مربوط به کارایی فعالیت‌های مدیریت آسیب‌پذیری‌های تجهیزات و عملیات |
| چهارم (اندازه‌گیری شده) | • بازنگری و سنجش دوره‌ای مدیریت آسیب‌پذیری‌ها برای اطمینان از اثربخشی آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• بازنگری و سنجش دوره‌ای مدیریت آسیب‌پذیری‌ها برای اطمینان عملکرد طبق برنامه برای آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• آگاه‌سازی مدیریت سطح بالاتر از کارایی مدیریت آسیب‌پذیری‌های عوامل انسانی و سازمانی | • بازنگری و سنجش دوره‌ای مدیریت آسیب‌پذیری‌ها برای اطمینان از اثربخشی آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• بازنگری و سنجش دوره‌ای مدیریت آسیب‌پذیری‌ها برای اطمینان عملکرد طبق برنامه برای آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• آگاه‌سازی مدیریت سطح بالاتر از کارایی مدیریت آسیب‌پذیری‌های سیستم‌های کنترل و نظارت | • بازنگری و سنجش دوره‌ای مدیریت آسیب‌پذیری‌ها برای اطمینان از اثربخشی آسیب‌پذیری‌های تجهیزات و عملیات<br>• بازنگری و سنجش دوره‌ای مدیریت آسیب‌پذیری‌ها برای اطمینان عملکرد طبق برنامه برای آسیب‌پذیری‌های تجهیزات و عملیات<br>• آگاه‌سازی مدیریت سطح بالاتر از کارایی مدیریت آسیب‌پذیری‌های تجهیزات و عملیات |
| پنجم (نهادینه‌شده) | • اتخاذ تعریف استاندارد از فعالیت‌های مدیریت آسیب‌پذیری‌ها برای عملیات منحصربه‌فرد آسیب‌پذیری‌های عوامل انسانی و سازمانی<br>• ثبت و اشتراک‌گذاری فعالیت‌های آسیب‌پذیری در سطح سازمان برای آسیب‌پذیری‌های عوامل انسانی و سازمانی | • اتخاذ تعریف استاندارد از فعالیت‌های مدیریت آسیب‌پذیری‌ها برای عملیات منحصربه‌فرد آسیب‌پذیری‌های سیستم‌های کنترل و نظارت<br>• ثبت و اشتراک‌گذاری فعالیت‌های آسیب‌پذیری در سطح سازمان برای آسیب‌پذیری‌های سیستم‌های کنترل و نظارت | • اتخاذ تعریف استاندارد از فعالیت‌های مدیریت آسیب‌پذیری‌ها برای عملیات منحصربه‌فرد آسیب‌پذیری‌های تجهیزات و عملیات<br>• ثبت و اشتراک‌گذاری فعالیت‌های آسیب‌پذیری در سطح سازمان برای آسیب‌پذیری‌های تجهیزات و عملیات |




**شکل ٤. مدل ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری**

## بحث و نتیجه‌گیری

دسترسی مهاجمین سایبری به آسیب‌پذیری‌های سیستم‌های کنترل صنعتی و بهره‌گیری از آن می‌تواند تهدیدات سایبری را برای مراکز دفاعی را ایجاد نماید. برای مدیریت این آسیب‌پذیری‌ها به‌عنوان یکی از پایه‌ای‌ترین اقدامات تاب‌آوری سایبری، در سه سطح راهبری، کنترل و عملیات برای هر سطح بلوغ محورهایی پیشنهاد شد که با بهره‌گیری از مدل سامانمند بهبود فرایندها، مراحل پیاده‌سازی مدیریت آسیب‌پذیری‌ها اجرایی می‌شود و با توجه به به‌کارگیری تجهیزات جدید در سیستم‌های کنترل صنعتی دفاعی و بروز و ظهور آسیب‌پذیری‌های جدید این مدل به‌عنوان مبنای اصلی در به‌کارگیری تجهیزات جدید مورد مدائقه قرار گیرد. سؤالات مطرح‌شده در این پژوهش و پاسخ‌های احصا شده به شرح ذیل ارائه می‌گردد.

**سؤال اصلی:** مدل ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری کدام است؟

**پاسخ:** مدل ارائه‌شده مبتنی بر سطح بلوغ، در سه سطح سیستم‌های کنترل صنعتی دفاعی و ۵۱ شاخص احصاء شده از نظرسنجی خبرگان ارائه شد.

سؤالات فرعی

– آسیب‌پذیری‌های سیستم‌های کنترل صنعتی کدامند؟

آسیب‌پذیری‌های احصا شده در سیستم‌های کنترل صنعتی عبارت است از:

- عدم تعریف مناسب امتیازها و کنترل دسترسی؛
- اعتبار سنجی ورودی نامناسب؛
- در محدودیت‌های نادرست عملیاتی ناشی از محدودیت بافر؛
- مسیر عبور؛
- در مسیر اطلاعات دیگر قرار گرفتن؛
- کنترل دسترسی نامناسب؛
- فرمان‌های نامناسب سیستم‌عامل؛
- تزریق اسکیوال؛
- برنامه‌نویسی متقاطع؛
- احراز هویت نامناسب.

– ابعاد سیستم‌های کنترل صنعتی دفاعی کدامند؟

سیستم‌های کنترل صنعتی در سه سطح نظارت و راهبری – خودکارسازی و کنترل و فرایند و عملیات بر اساس منابع علمی و نظر خبرگان احصا گردید.

– شاخص‌های اصلی برای ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری کدامند؟

برای ارزیابی و تحلیل آسیب‌پذیری‌ها در تاب‌آوری سیستم‌های کنترل صنعتی دفاعی در مقابل تهدیدات سایبری مطابق با نظرسنجی از خبرگان ۵۱ شاخص که مدل ارائه شده است احصا و ارائه شد.

**پیشنهادها**

۱– در سطح بلوغ یک آماده‌سازی برای تجزیه‌وتحلیل آسیب‌پذیری‌ها، شناسایی و تجزیه‌وتحلیل آسیب‌پذیری‌ها، مدیریت آسیب‌پذیری‌های شناسایی‌شده، بررسی علل ریشه‌ای آسیب‌پذیری‌ها انجام پذیرد؛

۲- در سطح بلوغ دو برنامه‌ریزی مستند برای مدیریت آسیب‌پذیری‌ها، مدیریت مستند آسیب‌پذیری‌ها، آگاهی نقش ذی‌نفعان برای فعالیت مدیریت آسیب‌پذیری‌ها انجام پذیرد؛

۳- در سطح بلوغ نظارت مدیریتی بر کارایی فعالیت‌های مدیریت آسیب‌پذیری‌های، به‌کارگیری کارکنان مجرب طبق برنامه‌ریزی انجام‌شده برای آسیب‌پذیری‌ها، تخصیص بودجهٔ مناسب برای مدیریت آسیب‌پذیری‌ها به‌صورت برنامه‌ریزی‌شده برای آسیب‌پذیری‌ها، شناسایی و تحلیل، دفع، نظارت و کنترل ریسک مربوط به کارایی فعالیت‌های مدیریت آسیب‌پذیری‌ها و شناسایی و اجرای دستورالعمل‌ها و استانداردهای مدیریت آسیب‌پذیری‌ها انجام پذیرد؛

٤- در سطح چهارم بلوغ بازنگری و سنجش دوره‌ای مدیریت آسیب‌پذیری‌ها برای اطمینان از اثربخشی آسیب‌پذیری‌ها، بازنگری و سنجش دوره‌ای مدیریت آسیب‌پذیری‌ها برای اطمینان عملکرد طبق برنامه برای آسیب‌پذیری‌ها و آگاه‌سازی مدیریت سطح بالاتر از کارایی مدیریت آسیب‌پذیری‌ها انجام پذیرد؛

۵- در سطح پنجم بلوغ اتخاذ تعریف استاندارد از فعالیت‌های مدیریت آسیب‌پذیری‌ها برای عملیات منحصربه‌فرد آسیب‌پذیری‌ها، ثبت و اشتراک‌گذاری فعالیت‌های آسیب‌پذیری در سطح سازمان انجام پذیرد.

## فهرست منابع و مآخذ:


- BlackEnergy Threatens U. S. Infrastructure. (۲۰۱٤, November ۹). Government Security News. Retrieved from http://www.gsnmagazine.com/node/٤۲۸۸۷.
- Chabinsky, S. R. (۲۰۱۰). Cybersecurity strategy: A primer for policy makers and those on the front line. J. Nat'l Sec. L. & Pol'y, ٤, ۲۷.
- Chaves, A., Rice, M., Dunlap, S., & Pecarina, J. (۲۰۱۷). Improving the cyber resilience of industrial control systems. International Journal of Critical Infrastructure Protection, ۱۷, ۳۰-٤۸.
- Colbert, E. J. M., & Kott, A. (۲۰۱٦). Cyber-security of SCADA and Other Industrial Control Systems. Advances in Information Security, ٦۳. doi:۱۰,۱۰۰۷/۹۷۸-۳-۳۱۹-۳۲۱۲٥-۷.
- Conklin, W. A., & Shoemaker, D. (۲۰۱۷). Cyber-Resilience: Seven Steps for Institutional Survival. EDPACS, ٥٥(۲), ۱٤-۲۲.
- Council, E., Forbes Technology. Cybersecurity Is Dead. Forbes.
- Davis, Z. (۲۰۱٥). Definition of computer security. Encyclopedia. Retrieved ٦ September ۲۰۱٥.
- Edward J.M. Colbert • Alexander Kott, ۲۰۱٦,Cyber-security of SCADA and Other Industrial Control Systems https://www.ptsecurity.com/ww-en/analytics/ics-vulnerabilities-۲۰۱۹/.
- G. Antone. (۲۰۱٤, June ۱٦). Target Top Security O_cer Reporting to CIO Seen as a Mis-take. Retrieved from http://www.cio.com/article/۲۳۷٥٤۸۳/cio-role/target-top-security-o_cer-reporting-to-cio-seen-as-a-mistake.html.
- https://www.fireeye.com/blog/threat-research/۲۰۱۸/۰٦/totally-tubular-treatise-on-triton-and-tristation.html.
- https://www.researchgate.net/publication/۳۲٥۱۰۷٤۷۰_QUALITY_IMPROVEMENT_BY_USING_SIX_SIGMA_IN_AN_AUTOMOTIVE_INDUSTRY_A_CASE_STUDY.
- https://www.us-cert.gov/resources/assessments.
- Wei, D., & Ji, K. (۲۰۱۰). Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights. Paper presented at the Resilient Control Systems (ISRCS), ۲۰۱۰ ۳rd International Symposium on.