امنیت الکترونیک

فصل‌نامهٔ تخصصی، علمی، آموزشی و خبری صنعت امنیت الکترونیکی (e-security)

سال ششم | شمارهٔ ششم | بهار ۱۴۰۳ | ۲۵۰هزار تومان

در این شماره می‌خوانیم:


هزاربین
آتن
آزمایشگاه تجهیزات نظارت تصویری
سیمنا
سامانه یکپارچه مدیریت و نظارت ایکس-ری
Automation
IP
سامانه
میهن
سامانه مدیریت یکپارچه هشدار نفوذ
رخ پایش®
نگهبان هوشمند
امن پایش®
AmnPaayesh
هوبان
سامانه‌ی
اتوماسیون
پارکینگ
فرجا

امنیت الکترونیک

صاحب امتیاز و مدیرمسئول:
محمد قلم‌چی

سردبیر:
معصومه عباسیان

هیئت تحریریه (به‌ترتیب حروف الفبا):
حمید حاتمی
معصومه عباسیان
محمد قلم‌چی
نرگس نصیری

ویراستار:
معصومه عباسیان

صفحه‌آرایی و طراحی:
معصومه عباسیان

نشانی دبیرخانه: تهران- اقدسیه- بلوار ارتش- اراج- شانزده‌متری ولیعصر- نبش خیابان پروین- پلاک ۲- واحد ٤
تلفن: ۰۲۱-۲۲۹٦۷۷٦۳
نمابر: ۰۲۱-۲۲۹٦۷۷٦۹
نشانی اینترنتی: www.electronicsecurity.ir
پست الکترونیک: info@electronicsecurity.ir

فهرست

سرمقاله

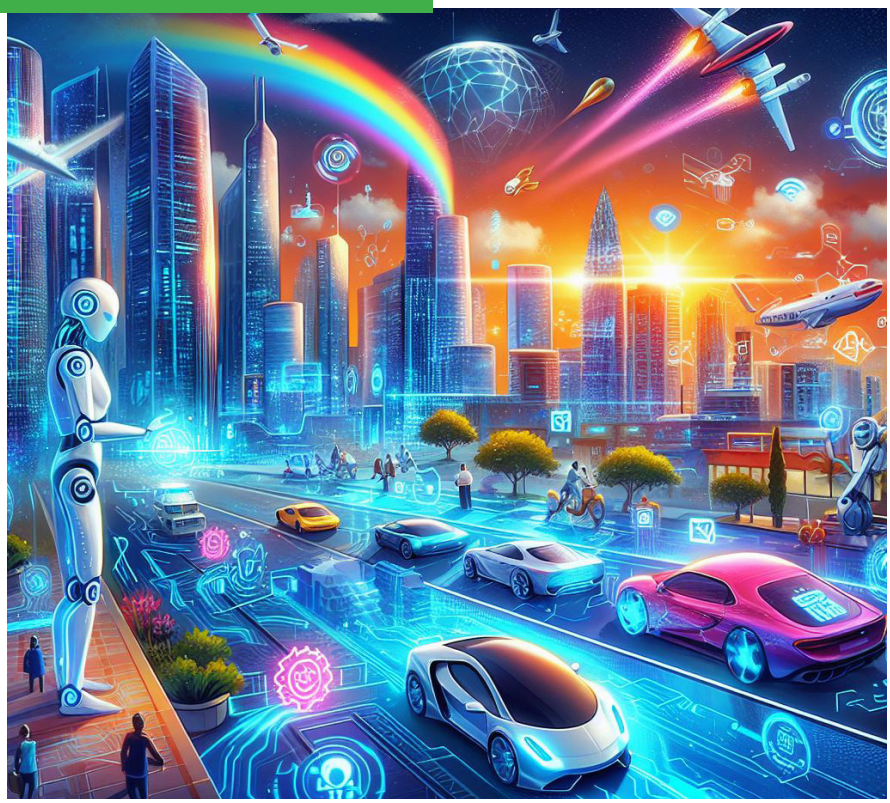
نویسنده:
محمد قلم‌چی

با پیشرفت‌های حاصل‌شده در فناوری آزمایشگاهی از یک‌سو و استانداردها و دستورالعمل‌هایی که در کشور درحال تصویب هستند یا ابلاغ شده‌اند، از سوی دیگر، انتظار می‌رود سطح امنیت الکترونیکی دستگاه‌ها و اماکن ارتقای قابل‌توجهی پیدا کند. پیاده‌سازی استاندارد موجب تأمین تجهیزات استانداردْ متناسب با سطوح امنیتی براساس نوع کاربری و نیاز متقاضی، نصب توسط متخصصان تأیید صلاحیت شده، آموزش بهره‌برداران، همچنین نگهداری منظم تجهیزات امنیت الکترونیکی خواهد بود. سرویس‌های ابری نیز در سال گذشته حضور قابل‌توجهی در حوزهٔ امنیت الکترونیکی داشته‌اند و خدمت‌های جدیدی نیز مبتنی بر این فناوری به بازار کشور افزوده شده است. با وجود این خدمات، دیگر تمامی مشتریان نیازمند خرید کامل تجهیزات نیستند و می‌توانند با هزینهٔ کمتر، تجهیزات را به‌صورت امانی تأمین کنند. از طرفی خدماتی همچون مشاهدهٔ برخط تصاویر دوربین‌های مداربسته که با هوش مصنوعی توانمندسازی شده‌اند نیز مزیت‌هایی ازجمله کاهش هزینه و افزایش بهره‌وری را به‌دنبال خواهد داشت. این نشریهٔ تخصصی در تلاش است با افزایش سطح دانش و تخصص فعالان و بهره‌برداران، در حد و توان خود گامی مؤثر در ارتقای این حوزه بردارد. به همین دلیل دست تمامی اساتید و متخصصان حوزهٔ امنیت را به‌منظور همکاری و ارائهٔ مقاله‌های تخصصی در این روند ارزشمند به‌گرمی می‌فشارد.

۷ جریان پرطرفدار در صنعت امنیت در ۲۰۲۴

به روایت خبرنگار هایک‌ویژن از چین در ژانویه‌ی ۲۰۲۴

مترجم:
معصومه عباسیان



جذابیت‌های صنعت امنیت در سال ۲۰۲۴ هیجان‌انگیز است. فناوری‌های پیشرفته‌ای همچون هوش مصنوعی (AI)، اینترنت اشیا (IoT) و کلان‌داده درحال هم‌گرایی هستند. این نوآوری‌ها راه را برای راه‌حل‌های امنیتی هوشمندتر، فعال‌تر و با قابلیت پیش‌بینی بیشتر هموار می‌کنند که نه‌تنها قدرتمندتر هستند، بلکه نیازهای کاربر را آسان‌تر برآورده می‌کنند.

سعی نویسنده در این مقاله بر آن است که هفت جریان برتر را که تأثیر قابل‌توجهی بر صنعت امنیت در سال ۲۰۲۴ دارند، معرفی کند.

هوش مصنوعی به افزایش ادراک در ماشین‌ها سرعت می‌بخشد

هوش مصنوعی با افزایش قابلیت‌های ادراکی ماشین‌ها، سیر تحول در صنعت امنیت را تسریع می‌کند. این کار به‌لطف ادغام فناوری‌های مربوط به نور مرئی، صدا، اشعهٔ ایکس، نور مادون قرمز، رادار و سایر فناوری‌ها امکان‌پذیر می‌شود. یکی از این نمونه‌ها، هوش مصنوعی با قابلیت پردازش تصویر است که تصویربرداری ویدئویی را متحول می‌کند و تصاویری با کیفیت بالا را از طریق کاهش هوشمند نویز ارائه می‌کند. بدین ترتیب تصاویری واضح‌تر با دامنهٔ دینامیکی[1] وسیع و جزئیات واضح حتی در محیط‌های کم‌نور حاصل می‌شود، در نتیجه اتکا به نورپردازی اضافی کاهش می‌یابد.

برنامه‌های کاربردی مبتنی بر هوش مصنوعی صنایع مختلف را متحول خواهند کرد

در سال ۲۰۲۳، پیشرفت‌های وسیع در مدل‌های هوش مصنوعی، توانایی تفسیر موقعیت‌های پیچیده را با استفاده از داده‌های متنوع بهبود بخشیده است. این پیشرفت امکانات ویژه‌ای برای راهکارهای مبتنی بر هوش مصنوعی ایجاد می‌کند که در بخش‌های مختلفی از جمله تولید، انرژی، مراقبت‌های بهداشتی و آموزش متناسب‌تر عمل کنند. پلتفرم‌های باز، الگوریتم‌های پیشرفته، معماری‌های کارآمدتر، پذیرش یکپارچهٔ هوش مصنوعی را در طیف وسیعی از کارها تسهیل می‌کند و اکوسیستمی نوآورانه برای پیشرفت فناوری به‌وجود می‌آورد.

1. dynamic range

هم‌گرایی رایانش ابری و لبه‌ای[2] رو به فزونی است

هم‌گرایی رایانش ابری و لبه‌ای باعث ظهور خدمت‌رسانی سریع‌تر و کارآمدتر می‌شود. بدین ترتیب راهکارهای بی‌درنگ و هوشمند مانند کنترل محیطی هوشمندتر و مدیریت راحت‌تر سیستم امنیتی مبتنی بر ابر فزونی می‌یابند. این موضوع امکان تجزیه‌وتحلیل آنی و تصمیم‌گیری‌های بهتر را فراهم می‌کند. همچنین، پلتفرم‌های مبتنی بر ابر سرمایه‌گذاری‌های سخت‌افزاری را به‌حداقل می‌رسانند و می‌توانند از مشاغل با اندازه و بودجهٔ مختلف پشتیبانی کنند و هزینه‌های اولیه و مداوم را کاهش دهند.

فناوری دوقلوی دیجیتال[3] انقلابی در مدیریت کسب‌وکار ایجاد خواهد کرد

دوقلوهای دیجیتال مدل‌های مجازی هستند که سناریوهای دنیای واقعی را در زمان واقعی شبیه‌سازی می‌کنند. آنها با ادغام با اینترنت اشیا مبتنی بر هوش مصنوعی، محاسبات ابری و سایر فناوری‌ها، بینش‌هایی راجع به معیارهای عملکرد نظیر امنیت، ترافیک و مصرف انرژی در اختیار ما قرار می‌دهند. بدین ترتیب کارایی فرایند تولید بهبود می‌یابد و امکان نگهداری پیشگیرانه مهیا می‌شود که منجر به صرفه‌جویی در هزینه‌ها و مدیریت بهتر کسب‌وکار می‌گردد.

فناوری‌های حوزهٔ نمایش، به‌ویژه LED، به‌سرعت در حال پیشرفت است

پذیرش سریع فناوری COB[4] باعث افزایش تقاضا برای LEDهای کوچک شده است. راه‌حل‌های ابتکاری نیز در این حوزه در حال ظهور هستند که هم مصرف انرژی کمتری دارند و هم وضوح بیشتر. مثلاً، دیوارهای ویدئویی یکپارچه در مراکز فرماندهی، در تصمیم‌گیری هوشمندانه‌تر کمک می‌کنند. همچنین، نمایشگرهای تعاملی و علایم دیجیتال به‌عنوان کاتالیزور برای تحول دیجیتال در بخش‌های آموزش، تجارت و گردشگری عمل می‌کنند.

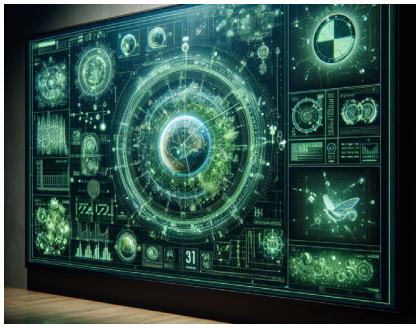
2. edge computing

3. digital twin

4. Chip On Board

اهمیت امنیت احراز هویت دیجیتال در امنیت سایبری رو به فزونی است

احراز هویت دیجیتال اقدامی اساسی در حوزهٔ امنیت سایبری است. مهاجمان از تکنیک‌هایی مانند فیشینگ، بدافزار و مهندسی اجتماعی برای سرقت اطلاعات و هویت شخصی استفاده می‌کنند. کاربران و سازمان‌ها برای محافظت از هویت دیجیتال باید از رمزهای عبور قوی و احراز هویت چندعاملی استفاده کنند، از شبکه‌های عمومی اجتناب کنند، نرم‌افزار را به‌موقع به‌روزرسانی نمایند.



فناوری‌های نوآورانه پایداری محیط‌زیستی و انعطاف‌پذیری در برابر تغییرات آب‌وهوایی ایجاد می کنند

صاحبان صنعت به‌طور فزاینده‌ای از شیوه‌های سبز برای کاهش انتشار کربن و استفاده از منابع استفاده می‌کنند. این رویه شامل حمل‌ونقل کارآمد محصول، بسته‌بندی مطمئن و استفادهٔ استاندارد از قطعات است. هایک‌ویژن همچنین انتظار دارد که شاهد استفاده از فناوری‌های نوآورانه برای افزایش انعطاف‌پذیری در برابر تغییرات آب‌وهوایی باشد. مثلاً، با ادغام حسگرهای محیطی و سیستم‌های امنیتی می‌توان در برابر بلایای طبیعی مانند سیل، آتش‌سوزی، رانش زمین و بهمن مجهز شد.

آزمایشگاه دانش‌بنیان آتن: اولین تجربه‌ی اندازه‌گیری تخصصی پارامترهای ویدئویی در جهان

نویسندگان:
معصومه عباسیان
محمد قلم‌چی

امروزه محصولات تجهیزات نظارت تصویری بسیار متنوع است و شرکت‌های فراوانی در این زمینه فعالیت می‌کنند. در حال حاضر، بیش از هزار برند تجهیزات نظارت تصویری در سراسر جهان ثبت شده‌اند که بسیاری از این تجهیزات به بازار کشور ما نیز وارد شده‌اند. بازار جهانی و همچنین کشورمان مملو از محصولاتی است که هرکدام ادعاهایی در خصوص کیفیت و کارایی محصولات خود دارند. به‌دلیل نبود ابزارهای اندازه‌گیری عملکردی، مشتریان حتی پس از خرید و بهره‌برداری از تجهیزات نظارت تصویری نیز از اصالت، صحت عملکرد، سطح کیفیت و سطح امنیت این تجهیزات اطمینان کامل ندارند. همچنین کارشناسان نیز ابزار قابل‌اتکایی نداشته‌اند تا بتوانند نظرات رسمی و کارشناسی درباره‌ی این تجهیزات ارائه نمایند. از این رو، نیاز به وجود ابزاری برای سنجش عملکرد حقیقی این تجهیزات برای مشتریان و متولیان بسیار احساس می‌شود.

مؤسسهٔ دانش‌بنیان خدمات مدیریت و فناوری رشد قلم‌چی، با شناسایی این نیاز در ابداع این‌چنین آزمایشگاهی پیش‌قدم شد. آزمایشگاه تجهیزات نظارت تصویری با نام تجاری آتن با هدف سنجش پارامترهای عملکردی تجهیزات نظارت‌تصویری ایجاد شد تا برای متخصصان این حوزه و مشتریان نقش مشاور را بازی کند. پارامترهایی که توسط این آزمایشگاه بررسی و اندازه‌گیری می‌شوند در حوزه‌های اصالت، کارآمدی، پایداری، کیفیت و امنیت فضای تبادل اطلاعات دسته‌بندی می‌شوند. توانمندی‌های آتن محدود به تجهیزات نظارت تصویری نیست و برای اندازه‌گیری پارامترهای فنی ویدئو ازجمله دوربین فیلم‌برداری نیز کاربرد دارد.

شایان ذکر است که هیچ رقیب داخلی و خارجی در زمینهٔ آزمون تجهیزات نظارت تصویری برای آتن، تا این زمان، وجود نداشته است.

سابقهٔ سنجش کیفیت ویدئو در جهان

سنجش کیفیت ویدئو تنها در تجهیزات نظارت تصویری کاربرد ندارد. برخی کشورها همچون انگلستان، مراجعی دارند که کیفیت فیلم‌ها را بررسی می‌کنند. QoE[1] یکی از پارامترهایی است که کیفیت فیلم‌برداری انجام‌شده، مثلاً در فیلم‌های سینمایی را معین می‌کند.

وقتی کیفیت یک روش فشرده‌سازی ویدئو یا روش رمزنگاری جدید با سایر روش‌ها مقایسه می‌شود، کارشناسان از روش‌هایی بهره‌برداری می‌کنند که تماماً براساس عکس پیاده‌سازی شده‌اند و در اصل هیچ‌گاه در این روش‌ها تحلیل روی ویدئو انجام نمی‌شود. به همین دلیل نتایج آنها برای عملکرد واقعی ویدئو قابل‌اتکا نیستند. در ادامه چند روش از این دست معرفی می‌شوند.

PSNR

روش PSNR[1] متداول‌ترین معیار سنجش کیفیت ویدئوست. این روش کمترین ارزش پیش‌بینی را دارد، بنابراین نتایج آن ناسازگار هستند. این روش توسط پلتفرم‌های بزرگی مانند نتفلیکس و فیس‌بوک برای مقایسهٔ کدک‌های مختلف و برای موارد مشابه استفاده می‌شود. استفاده از این معیار رو به کاهش است.

SSIM

SSIM[2] بیشتر توسط کارشناسان فنی مانند محققان کدک و مهندسان فشرده‌سازی استفاده می‌شود. استفاده از این روش نیز دائماً دارد کم می‌شود. با این حال، ارزش پیش‌بینی بالاتری نسبت به PSNR دارد.

SSIMPlus

SSIMPlus[3] نسبت به سه روش دیگر ارزش عملکردی بالاتری دارد و مورد توجه مهندسان و کاربران قرار گرفته است. با این حال، انحصاری است و به‌راحتی برای عموم در دسترس نیست.

VMAF

VMAF[4] این شیوه در آغاز توسط نتفلیکس معرفی شد اما سپس به‌صورت متن‌باز[2] ارائه شد. VMAF به‌راحتی در دسترس است و به‌طور گسترده استفاده می‌شود. این شیوه به‌ویژه برای ارزیابی کیفیت ویدئوی استریم‌های کدگذاری‌شده برای «گام‌های با وضوح چندگانه»[3] طراحی شده است.

چرا آتن تنها آزمایشگاه اندازه‌گیری مؤثر پارامترهای ویدئویی در جهان است؟

پیش از آتن هیچ‌گاه در آزمایشگاه‌ها عملکرد فیلم‌برداری صحنه‌واقعی در دوربین سنجش نشده و صرفاً خروجی عکس موردبررسی قرار گرفته است. به بیان دیگر، سایر آزمایشگاه‌های موجود در جهان، جز آتن، برای سنجش کیفیت تجهیزات نظارت تصویری در حوزهٔ ویدئو براساس عکس SFR عمل می‌کنند. ایراد بزرگ این روش آن است که در اصل فقط یک عکس، نه توالی فریم‌ها بررسی می‌شود.

ورودی آتن ویدئوست نه عکس. آتن با محاسبهٔ ماتریس برداری تفاضل فریم‌های ویدئویی ورودی (ویدئوی تست) با نتیجهٔ عملیاتی حاصل‌شده از خروجی دوربین (براساس Feedback) پارامترهای ویدئویی را محاسبه می‌کند و این یعنی آتن روی تصاویر فراوان در توالی‌های متعدد کار می‌کند و با حجم بسیار زیاد و پیچیده‌ای از محاسبات مواجه است.

در داخل ایران، آزمایشگاه‌هایی مدعی هستند که دوربین‌های نظارت تصویری را آزمون می‌کنند. این آزمون‌ها که صرفاً شرایط فیزیکی دوربین و

1. live quality of experienc

2. Open source

3 multiple-resolution rungs

تداخلات الکترومغناطیس را بررسی می‌کنند از قرار ادامه هستند:

- سازگاری الکترومغناطیسی[4] (EMC) یا توانایی عملکردی تجهیزات در میدان‌های مغناطیسی؛
- تداخل الکترومغناطیس[5] (EMI)؛
- IP – مقاومت در برابر گردوخاک و رطوبت؛
- IK – مقاومت در برابر ضربه.

برای اهل فن روشن است که آزمون‌های یادشده ارتباطی به کارآمدی دوربین ندارند.

سایر آزمایشگاه‌های تجهیزات نظارت تصویری در جهان

همان‌طور که پیش از این گفته شد، آزمایشگاه‌های دیگری که در جهان برای آزمون تجهیزات نظارت تصویری و همچنین دوربین‌های ویدئویی استفاده می‌شوند، همگی فقط آزمون‌هایی براساس عکس ثابت دارند و در اصل هیچ‌کدام پارامتر ویدئو را اندازه‌گیری نمی‌کنند؛ چون فقط یک تصویر ثابت را به‌عنوان ورودی به آزمایشگاه ارائه می‌کنند در نتیجه نمی‌توان فهمید که در دنیای واقعی و در مواجهه با صحنه‌ای متحرک این اندازه‌گیری‌ها تا چه حد با واقعیت تطابق دارد. در ادامه دو آزمایشگاه از این دست معرفی شده است.

Image Engineering GmbH & Co

همان‌طور که از نام این آزمایشگاه برمی‌آید، این آزمایشگاه بر اندازه‌گیری پارامترهای عکس تمرکز دارد (و در اصل این اندازه‌گیری‌ها برای ویدئو معتبر نیستند). این مرکز مدعی است که همهٔ تجهیزات و ادوات لازم برای آزمون تصاویر (نه ویدئو!) دوربین‌های دیجیتال حفاظتی یا عکاسی را در اختیار دارد و این آزمون‌ها را انجام می‌دهد.

Imatest

Imatest که دفتر مرکزی آن در بولدرِ ایالت کلرادو در امریکا واقع شده است، تقریباً ۲۰ سال است که در آزمون کیفیت تصویر ثابت (نه ویدئو) پیشرو بوده است. این شرکت، نرم‌افزاری به همین نام دارد (Imatest) که ارائهٔ نمودارهای آزمون تجهیزات ازجمله خدمات مشاوره‌ای این شرکت است. مشتریان این شرکت از همهٔ صنایع ازجمله شرکت‌های الکترونیکی گوشی همراه هستند. تجهیزات و خدمات این شرکت برای آزمون انواع دوربین، ماهواره یا دوربین‌های گوشی همراه، دوربین‌های نور مرئی یا فروسرخ استفاده می‌شوند. آزمون‌های این شرکت نیز صرفاً مبتنی بر عکس است و فاقد تجهیزاتی برای اندازه‌گیری پارامترهای ویدئوست.

اهداف کلان ایجاد آزمایشگاه نظارت تصویری آتن

- سنجش کیفیت، کارآمدی، اصالت و امنیت سایبری تجهیزات نظارت تصویری و دوربین‌های فیلم‌برداری به‌صورت عینی[6] به جای ذهنی[7]؛
- ایجاد امکان مقایسه برای خریداران سامانه‌های نظارت تصویری اعم از خریداران خرد و عمده؛
- افزایش سطح کیفی صنعت نظارت تصویری در کشور؛

4. Electromagnetic Compatibility
5. Electromagnetic Interference
6. Objective
7. Subjective

نمایی از اتاق تاریک

- افزایش امنیت صنعت نظارت تصویری در کشور؛
- کمک به افزایش سطح امنیت ملی و تقویت پدافند غیرعامل؛
- معیار علمی و کاربردی برای سنجش عملکرد تجهیزات نظارت تصویری.

دامنهٔ کاربرد

تجهیزاتی که می‌توان توسط دستگاه آتن آزمون کرد، عبارتند از:

- دوربین‌های مداربسته (شامل هر نوع فناوری و با هر شکل و اندازهٔ فیزیکی)؛
- دستگاه‌های ضبط تصاویر: NVR، DVR و XVR؛
- دستگاه‌های انکودر.

ضرورت آتن برای کشور

دلایلی که می‌توان برای اهمیت ویژهٔ آتن برشمرد، از قرار ادامه‌اند:

۱- جلوگیری از تقلب‌های صنفی و فروش تجهیزات با مشخصات فنی اعلامی مغایر با واقعیت؛

۲- انتخاب دوربین‌های مناسب برای تحلیل‌های مبتنی بر هوش مصنوعی (مانند پلاک‌خوان، کنترل سرعت و...)؛

۳- افزایش امنیت سامانه‌های نظارت تصویری در کشور؛

۴- بهبود کیفیت تجهیزات نظارت تصویری به‌منظور افزایش عملکرد آنها در پیشگیری از وقوع جرم؛

۵- افزایش استنادپذیری ویدئوهای دوربین‌های نظارت تصویری.

معرفی آتن

ویدئو در حال حاضر حجیم‌ترین نوع داده در جهان است که چه برای انتقال و چه برای ذخیره‌سازی، منابع ویژه‌ای می‌طلبد. این حجم از داده به‌دلیل جذابیت بسیار بالا، از تنوع بهره‌برداری نیز برخوردار است، در نتیجه توانایی فشرده‌سازی آن برای کاهش ظرفیت ذخیره‌سازی، کیفیت ویدئو، امنیت ارسال و دریافت آن و مواردی از این دست، مسائلی در لبهٔ فناوری به‌حساب می‌آیند. در حوزهٔ تعیین کیفیت تصویر، استانداردهایی به‌قرار ادامه وجود دارند:

- ISO ۱۲۲۳۳ (Resolution)
- UL ۲۸۰۲
- ISO ۱۹۲۶۲,۱۹۲۶۳,۱۹۲۶۴ (Image Quality)
- ISO ۱۸۸۴۴ (Flare)
- ISO ۱۹۰۹۳ (Low Light Performance)
- ISO ۱۹۵۶۷ (Texture)
- ISO ۲۰۴۹۰ (Auto Focus)
- ISO ۲۰۹۵۴ (Image Stabilization)
- IEC ۱-۶۱۱۴۶ (Minimum Illumination)
- ISO ۱۴۵۲۴ and ISO ۱۵۷۳۹ (Dynamic Range)
- ISO ۱۷۸۵۰ (Image Distortion)
- ISO ۱۵۷۸۱ (Maximum Frame Rate)

پارامترهای فنیِ معرفی‌شده در این استانداردها در بعضی موارد فاقد راهکار اندازه‌گیری هستند و در سایر موارد راهکارهای بسیار پیچیده‌ای دارند. این موضوع نشان می‌دهد که فضای پژوهش در حوزهٔ کیفیت ویدئو تا چه اندازه بکر است.

آتن نه‌تنها، پارامترهای از پیش تعریف‌شدهٔ جهانی را اندازه می‌گیرد، بلکه، خودْ پارامترهای مؤثر و کاربردی جدیدی به دنیای ویدئو معرفی کرده است. این پارامترها و روش‌های نوین، در دستورکار اختصاصی آزمون تألیف شده‌اند. این بخشی از دانش تولیدشده در فرایند تولید آتن به‌شمار می‌رود.

پس، به‌طور خلاصه، آتن راهکاری شامل اجزای سخت‌افزاری، نرم‌افزاری و دانش فنی است که امکان اندازه‌گیری پارامترهای کارآمد فنی را در اختیار متخصصان، مشتریان و تولیدکنندگان قرار می‌دهد.

سخت‌افزار آتن

سخت‌افزار آتن از دو بخش تشکیل می‌شود:

۱. تجهیزات عمومی مانند کامپیوتر و سوئیچ.

۲. جزء ویژه و نوآورانهٔ آن که اتاق تاریک با گواهی ثبت اختراع است.

وظیفهٔ بخش سخت‌افزاریِ آتن، ایجاد محیط مناسب برای آزمون است. آتن از یک اتاق تاریک به‌همراه مجموعه‌ای حسگر و عملگر از جمله صفحه‌نمایش آزمون‌های در حال انجام، نمایشگر وضعیت، حسگرهای سنجش میزان نور، توان، دما، رطوبت و صدا، عملگرهای نوری و صوتی و غیره تشکیل شده است. منبع تصویر در اتاق

تاریک نمایشگر شبیه‌ساز است. شبیه‌ساز قادر است تصاویر و ویدئوهای گوناگونی که ممکن است برای این تجهیزات در حین عملکرد واقعی به‌وجود بیاید، اعم از تغییرات در میزان نویز، نور، رنگ، حرکت، راه‌اندازی مجدد تجهیز و... را شبیه‌سازی کند. تجهیز نظارت تصویری در اتاق تاریک نصب می‌شود.

نرم‌افزار آتن

نرم‌افزار آتن که پیشرفته‌ترین و پرهزینه‌ترین بخش آن به‌شمار می‌رود، مسئولیت دریافت داده‌ها از سخت‌افزارها و تحلیل آنها طبق دستورکار آتن را بر عهده دارد. این نرم‌افزار بخش‌ها، سرویس‌ها و لایه‌های مختلفی دارد که هریک وظایف مشخصی دارند که روی بستر شبکه با یکدیگر در ارتباط هستند و به این واسطه مدیریت و کاربری راهکار را میسر می‌سازند.

مهم‌ترین ویژگی‌های بخش نرم‌افزار عبارتند از:

- معماری توزیع‌شده و منعطف آن که اجازهٔ گسترش افقی و عمودی را فراهم می‌کند؛
- در هیچ کجای راهکار از نرم‌افزارها، کتابخانه‌ها یا کدهای متن‌بسته، قفل‌شکسته یا بدون مجوز استفاده نشده؛
- جز بخش مرتبط با واحد DAQ که مبتنی بر میکروپروسسور توسعه داده شده، سایر بخش‌های نرم‌افزار به‌صورت cross platform هستند و روی انواع سیستم عامل معمول در کشور قابل‌اجرا و بهره‌برداری هستند؛
- بخش عمدهٔ کاربری و بهره‌برداری تنها توسط واسط کاربری وب قابل‌استفاده است؛
- در بخش backend، تحلیل و پردازشْ کاملاً مبتنی بر ۱۴/۱۷ c++ و ۱۱ c توسعه داده شده است. طراحی و پیاده‌سازی این بخش با دقت بسیار و با توجه به راندمان و سرعت عمل نرم‌افزار انجام شده است؛
- تمام سامانه روی سرویس وب پیاده‌سازی شده و هر بهره‌بردار یا شخص ثالث می‌تواند با استفاده از مستندات پروتکل‌های آتن به آن متصل شده و از خدمات آن بهره‌مند شود.

مسئولیت بخش نرم‌افزاری آتن دریافت اطلاعات اولیه، اجرای آزمون، داده‌برداری، تحلیل داده‌ها، ثبت اطلاعات و تولید گزارش عملکرد تجهیزات نظارت تصویری است.

حوزه‌های آزمون

حوزه‌های اصلی که توسط آتن بررسی می‌شوند به‌شرح زیر هستند:

- کیفیت استریم (ویدئو و صوت)؛
- کیفیت تصویر؛
- تصحیح تصویر در شرایط نوری خاص؛
- فشرده‌سازی؛
- کیفیت صدا؛
- منبع تغذیه؛
- امنیت تبادل داده؛
- سهولت نصب؛
- اصالت تجهیز.

کیفیت استریم (ویدئو و صوت)

کیفیت استریم با محاسبه و بررسی پهنای باند، وضوح، تحلیل فریم، بسته‌های ارسالی و بررسی استریم سنجیده می‌شود.

کیفیت تصویر

به‌منظور تعیین کیفیت تصویر، مواردی چون نور، وضوح تصویر، اختلال در تصویر، تباین[8]، صحت رنگ‌ها، اعوجاج، نویز، محدودهٔ دینامیک[9] در تصاویر ثابت و متحرک بررسی می‌شود.

تصحیح تصویر در شرایط نوری خاص

یکی از مهم‌ترین نیازهای مشتریان تشخیص محتوای تصویر در شرایط نوری متضاد (سایه‌روشن) است. سازندگانِ تجهیزات نظارت تصویری، در چنین شرایطی، از فناوری‌های مختلفی همچون WDR BLC و HLC استفاده می‌کنند.

مستقل از نام فناوری که در بسیاری از موارد صرفاً کاربرد تجاری و بازرگانی دارد، اطلاع مشتری از میزان عملکرد مناسب تجهیز در شرایط نوری خاص اهمیت ویژه‌ای دارد.

آتن خود را محدود به فناوری مورداستفادهٔ سازنده نمی‌کند و با بهره‌گیری از روش آزمون خودْ میزان تصحیح تصویر را در شرایط گفته‌شده اندازه می‌گیرد. به بیان دیگر، آزمون‌های آتن همچون همهٔ آزمون‌های مدرن و کارآمد کارکردگرا هستند.

8 Contrast

9. Dynamic Range

مبرهن است تصحیح تصویر در شرایط متفاوت نوری سبب تولید نویز در تصویر می‌شود. اندازه‌گیری نویز تولیدشده کارکرد دیگر آتن با رویهٔ منحصربه‌فرد خودش است.

فشرده‌سازی

فشرده‌سازی تأثیر قابل‌توجهی در کاهش و مدیریت پهنای باند مصرفی تجهیز دارد. آتن می‌تواند نشان دهد که فشرده‌سازی تصویر چقدر باعث افت کیفیت ویدئوی تولیدی می‌شود. همچنین عملکرد روش‌های فشرده‌سازی VBR و CBR توسط آتن بررسی شده و نرخ تغییرات در میزان فشرده‌سازی محاسبه می‌گردد.

صدا

در آتن صدای ورودی و خروجی تجهیزْ هم از جنبهٔ کیفیت، هم از جنبهٔ پهنای باند مصرفی سنجیده و بررسی می‌شود.

منبع تغذیه

یکی از مشکلات شایع در بهره‌برداری از سامانه‌های نظارت تصویری، مشکلاتی است که به‌واسطهٔ بروز مشکل در تأمین تغذیهٔ تجهیزات به‌وجود می‌آید. از شاخص‌های کیفی و عملکردی دوربین، کمینه، بیشینه و متوسط توان مصرفی آن است. مثلاً در دوربین‌های متحرک مهم است که بدانیم منبع تغذیهٔ در نظر گرفته شده پاسخگوی توان تمام بار مصرفی هست یا خیر.

در صورتی که دوربین دارای سیستم PoE باشد، آتن صحت عملکرد این سیستم و تأثیر آن روی ویدئو را بررسی می‌کند.

امنیت تبادل داده‌ها

متأسفانه، تجهیزات نظارت تصویری، نسبت به سایر تجهیزات ICT، پیشرفت کندتری در حوزهٔ امنیت تبادل اطلاعات داشته‌اند، اما مخاطرات امنیتی بسیار زیادی توسط تجهیزات نظارت تصویری در ایران و جهان گزارش شده و مشکلات متعددی از این ناحیه به دولت‌ها و کسب‌وکارها حادث شده است. بنابراین، بررسی سطح امنیت در تجهیزات نظارت تصویری اهمیت ویژه‌ای دارد. از آنجا که استانداردهای

موجود در حوزهٔ امنیت تبادل اطلاعات، بسیاری از مخاطرات امنیت سایبری تجهیزات نظارت تصویری را شامل نمی‌شوند و تجهیزات نظارت تصویری از پروتکل‌های اختصاصی همچون ONVIF و PSIA بهره‌برداری می‌کنند که در هیچ کجای دیگر دانشِ ICT وجود و کاربرد ندارند، موارد متعددی در حوزهٔ امنیت، موردنیاز یک سامانهٔ امن نظارت تصویری است که در سایر استانداردها موردتوجه قرار نگرفته است. راهکار آتن امنیت تبادل اطلاعات تجهیزات نظارت تصویری را با دستورالعمل داخلی خود و با ابزاری که خود پیاده‌سازی نموده، به‌صورت تخصصی بررسی می‌کند.

بررسی فناوری‌های امنیتی تجهیز، سطح امنیتی پیاده‌سازی‌شده، نوع و سطح پروتکل‌های امنیتی پیاده‌سازی‌شده، جزء آزمون‌های امنیتیِ راهکار آتن است.

سهولت نصب

قابلیت و سهولت نصب تجهیز، موجب تسریع در پیاده‌سازی پروژهٔ نظارت تصویری می‌شود. آتن قابلیت‌های تنظیم خودکار IP دوربین، تنظیمات گروهی یا تنظیمات انفرادی را نیز شناسایی می‌کند.

همچنین اگر تجهیز دارای پروتکل‌های یکپارچه‌ای از جمله ONVIF باشد، توسط آتن قابل‌تشخیص بوده و در نتیجه امکان سهولت توسعهٔ آتی، یکپارچگی با سایر سامانه‌های امنیت الکترونیکی و مواردی از این دست افزایش خواهد یافت. بنابراین بررسی‌های متنوعی در این حوزه در آتن پیش‌بینی شده است.

تشخیص اصالت تجهیز

بررسی اصالت کالا برای خریدار اهمیت بسزایی دارد. آتن با بررسی قطعات، از جمله مک‌آدرس تجهیز، اصالت آن را می‌آزماید. همچنین بررسی تطبیقی برد اصلی الکترونیکی تجهیز با نمونه‌های اصلی، از روش‌های دیگرِ بررسی اصالت تجهیز است.

نتیجهٔ آزمایش

بسته به نوع آزمایش‌های انجام‌شده در فرایند آزمون، گزارش نهایی تجهیز در قالب pdf تولید می‌شود. گزارش با تعریف مشخصات تجهیز آغاز و با اعلام نتایج نموداری و رقمی آزمون‌ها ادامه می‌یابد. اخرین بخش گزارش آتن نتایج تحلیل‌های تخصصی است.

بهره‌برداری از نتایج آتن

آتن در موارد گوناگونی از جمله موارد زیر کاربرد دارد:

- کنترل کیفیت (QC) در حوزهٔ تولید، نگهداری و...؛
- سطح‌بندی تجهیزات نظارت تصویری؛
- کمک به تحقیق‌وتوسعه در زمینهٔ تجهیزات نظارت تصویری؛
- انتخاب محصولات با کیفیت مطلوب؛
- پیشگیری از واردات محصولات بی‌کیفیت یا تولید آنها؛
- شناسایی کالاهای فاقد اصالت؛
- کمک به انتخاب تجهیزْ متناسب با نیاز مصرف‌کننده؛
- مقایسهٔ دو یا چند تجهیز نظارت تصویری با یکدیگر.

منابع

-https://www.ni.com/en/shop/data-acquisition-and-control/add-ons-for-data-acquisition-and-control/what-is-vision-development-module/peak-signal-to-noise-ratio-as-an-image-quality-metric.html

-https://www.ni.com/docs/en-US/bundle/ni-vision-concepts-help/page/structural_similarity_index.html

-https://ece.uwaterloo.ca/~z۷۰wang/research/ssimplus/

-https://en.wikipedia.org/wiki/Video_Multimethod_Assessment_Fusion

نمایی از اتاق آزمون شرکت Imatest

نویسندگان:
محمد قلم‌چی
نرگس نصیری

تعیین روشی برای اندازه‌گیری خطا در تشخیص چهره‌ی ویدئویی

تعاریف متفاوتی در استانداردهای مختلف در این خصوص ارائه شده است، اما هیچ‌کدام به‌تنهایی کاربردی نیستند. این پژوهش با بررسی تمامی استانداردهای موجود بین‌المللی، روشی تلفیقی برای محاسبه‌ی مهندسی خطای سامانه‌ی تشخیص چهره ارائه می‌نماید.

تعاریف

الگوی چهره: داده‌هایی که از نسبت ابعاد مؤلفه‌های چهرهٔ یک شخص توسط کامپیوتر استخراج شده و به‌صورت اطلاعات دیجیتالی ثبت شده باشد.

تشخیص چهره[1]: به معنی تعیین محدودهٔ چهره است. به بیان دیگر زمانی اتفاق می‌افتد که نرم‌افزار چهره را در تصویر دریافتی از دوربین مشخص می‌کند.

شناسایی چهره[2]: زمانی است که نرم‌افزار هویت فرد را شناسایی می‌کند.

روند شناسایی و تشخیص چهره: نرم افزار ابتدا چهره را در تصاویر دریافتی از دوربین تشخیص می‌دهد، سپس الگوی چهرهٔ شناسایی‌شده توسط نرم‌افزار تولید می‌شود. در گام بعدی با محاسبات ریاضی، الگوی چهرهٔ شناسایی‌شده با الگوهای موجود در بانک اطلاعاتی نرم‌افزار مقایسه می‌شود که به این کار تطابق[3] می‌گویند. بدین وسیله هویت چهره تعیین می‌شود.

افراد شناس: افرادی که اطلاعات هویتیِ آنها در سیستم ثبت شده است. به بیان دیگر، افرادی که دست‌کم یک الگوی چهره از آنها در بانک اطلاعاتی وجود دارد.

افراد ناشناس: افرادی که اطلاعات هویتی آنها در سیستم ثبت نشده است. به بیان دیگر افرادی که حتی یک الگوی چهره از آنها در بانک اطلاعاتی وجود ندارد.

چهرهٔ تشخیص داده‌نشده[4]: یعنی چهره در تصویر وجود داشته ولی به‌عنوان چهرهٔ شخص تشخیص داده نشده است.

چهرهٔ تشخیص داده‌شده شناسایی نشود[5]: چهرهٔ تشخیص داده شده، ولی شناسایی نشده است یعنی ناشناس باقی می‌ماند که به این وضعیت خطای منفی کاذب[6] گفته می‌شود.

چهرهٔ تشخیص داده‌شده به‌اشتباه شناسایی شود[7]: در این حالت چهره تشخیص داده شده و شناسایی نیز می‌شود، اما به‌عنوان فرد دیگری و به اشتباه شناسایی می‌شود که به این وضعیت، مثبت کاذب[8] گفته می‌شود.

چهره به‌درستی شناسایی شده[9]: چهره تشخیص داده شود و به‌درستی نیز شناسایی شود.

خطاهای نرم‌افزار تشخیص چهره

با توجه به شرایط فوق و تعاریف منابع موردبررسی در خصوص تعریف خطا در تشخیص چهره از یک سو و کارکرد سامانهٔ تشخیص چهرهٔ برخط از روی ویدئوی دریافتی از دوربین مداربسته، خطاهای زیر جهت تعیین صحت عملکرد راهکار تشخیص چهره تعریف می‌شوند:

1. Face Detection
2. Face Recognition
3. Matching
4. Not Detected Faces
5. Detected-Not Recognized Faces
6. False Negative
7. Detected – False Recognized Face
8. False Positive
9. Correctly Recognized Face

خطای عدم‌تشخیص چهره

این خطا زمانی رخ می‌دهد که چهرهٔ افراد شناس یا ناشناس در مقابل دوربین باشد و چهره‌ها با یکدیگر همپوشانی نداشته باشند، اما برخی مواقع یا مشخصاً در برخی از فریم‌های دریافت‌شده توسط نرم‌افزار تشخیص چهره برخی افراد تشخیص داده نشوند.

مقدار این خطا نرخ متوسط تعداد چهرهٔ تشخیص داده نشده در هر فریم به تعداد کل چهره‌های موجود در تصویر است.

$$NDFR = \sum_{Frame=1}^{Frame=n} \frac{\text{Number of not detected faces}}{n * \text{Count of people in the view}} \quad (1)$$

نحوهٔ اندازه‌گیری خطا	در کل زمان اندازه‌گیری، افراد مشخص و ثابتی در پرسپکتیو دوربین قرار می‌گیرند به‌گونه‌ای که تصویر یک نفر با تصویر دیگران همپوشانی نداشته باشد و در نهایت خطا با استفاده از رابطهٔ ۱ محاسبه می‌شود. درصورتی‌که n بیشتر از ۳۳ باشد، میزان خطای محاسبه‌شده نرمال خواهد بود.
پارامترهای لازم برای ثبت در مستندات	• تعداد افراد موجود در تصویر • شرایط پارامترهای آزمون
قابلیت‌های نرم‌افزاری لازم	نرم‌افزار تعداد افراد موجود در تصویر را از کاربر دریافت می‌نماید و با این تعداد طبق تعریف، خطا را محاسبه می‌کند. به بیان دیگر، نرم‌افزار صرفاً خروجی NDFR را با واحد درصد در پایان آزمون ارائه می‌کند.

عدم‌شناسایی چهره

این خطا زمانی رخ می‌دهد که چهرهٔ افراد آشنا برای سیستم در پرسپکتیو دوربین باشد و چهره‌ها با یکدیگر همپوشانی نداشته باشند، اما برخی مواقع یا مشخصاً در برخی از فریم‌های دریافت‌شده توسط نرم‌افزار، چهرهٔ برخی افراد شناسایی نشود. به بیان دیگر، این خطا در حالتی رخ خواهد داد که چهرهٔ شناسایی‌شده، کلاً تشخیص داده نشود.

مقدار این خطا نرخ متوسط تعداد چهره‌های شناسایی‌نشده در هر فریم به تعداد کل چهره‌های موجود در تصویر است. n تعداد فریم‌های دریافت‌شده توسط نرم‌افزار در طول مدت آزمون است.

شناسایی نادرست چهره

این خطا زمانی رخ می‌دهد که چهرهٔ افراد آشنا برای سیستم در پرسپکتیو دوربین باشد و چهره‌ها با یکدیگر همپوشانی نداشته باشند، اما برخی مواقع یا مشخصاً در برخی از فریم‌های دریافت‌شده توسط نرم‌افزار، چهرهٔ برخی افراد به‌اشتباه شناسایی شود، به این معنی که چهرهٔ یک شخص به‌عنوان چهرهٔ شخص دیگری شناسایی شود.

مقدار این خطا نرخ متوسط تعداد چهره‌های نادرست شناسایی‌شده در هر فریم به تعداد کل چهره‌های موجود در تصویر است. n تعداد فریم‌های دریافت‌شده توسط نرم‌افزار در طول مدت آزمون است.

کارایی در تشخیص و شناسایی چهره

سیستم برای شناسایی چهره به‌طور کلی سه مرحلهٔ مهم و اصلی را انجام می‌دهد که محاسبهٔ کارایی در این سه مرحله امکان‌پذیر و ضروری است:

۱. تشخیص: مرحله‌ای است که در آن نرم‌افزار محدودهٔ چهره را تشخیص داده و برای محاسبات بعدی در الگوریتم‌ها، از آن استفاده می‌کند.

$$NRFR = \sum_{Frame=1}^{Frame=n} \frac{\text{Number of not recognized faces}}{n * \text{Count of people in the view}} \quad (2)$$

نحوهٔ اندازه‌گیری خطا	برای محاسبهٔ این خطا به‌دلیل محدودیت در تعیین مکان چهرهٔ اشخاص، ناچار به استفاده از تنها یک شخص در طول زمان آزمون هستیم. در کل زمان اندازه‌گیری، یک نفر در پرسپکتیو دوربین قرار می‌گیرد، به‌گونه‌ای که چهرهٔ شخص در مقابل دوربین باشد.
پارامترهای لازم برای ثبت در مستندات	• هویت فرد موجود در پرسپکتیو دوربین • شرایط پارامترهای آزمون
قابلیت‌های نرم‌افزاری لازم	نرم‌افزار تعداد افراد موجود در تصویر را از کاربر دریافت می‌کند و با این تعداد طبق تعریف، خطا را محاسبه می‌کند. به بیان دیگر، نرم‌افزار صرفاً خروجی NDFR را با واحد درصد در پایان آزمون ارائه می‌کند.

۲. استخراج الگو[10]: مرحله‌ای است که نرم‌افزار نسبت ابعاد چهرهٔ فرد را در ماتریسی ذخیره می‌کند که به آن الگو می‌گویند.

۳. تطابق: مرحله‌ای است که در آن نرم‌افزار مشخصه‌های چهرهٔ تشخیص داده شده را با مشخصه‌های الگوهای موجود مقایسه می‌کند تا بهترین تطابق با آن را پیدا کند.

توضیح: یافتن ویژگی‌های چهره همچون تعیین جنیست، برآورد حدود سن، میزان بازبودن چشم یا دهان و مواردی از این

10. Pattern Extraction

دست که به تجزیه‌وتحلیل چهره نیز معروف است، بعد از استخراج الگو ممکن است برای کارکردهای جنبی سامانه انجام شود. هدف این مقاله تعیین خطا یا کارآمدی این تجزیه‌وتحلیل‌ها نیست.

در اینجا کارایی سیستم برای هرکدام از مرحله‌های بالا براساس عوامل زیر تعریف می‌شود:

۱. زمان محاسبات صورت‌گرفته در هر مرحله توسط الگوریتم (ترجیحاً با واحد ns)؛
۲. میزان توان مصرف‌شده از پردازندهٔ مرکزی سیستم (بار پردازشی کارایی ترجیحاً با واحد KHz)؛
۳. میزان حافظهٔ RAM مصرف‌شده (ترجیحاً با واحد KB).

کارایی تشخیص

زمان تشخیص

متوسط زمانی که سیستم برای رخداد تشخیص صرف می‌کند.

نحوهٔ اندازه‌گیری

میانگین زمان تشخیص: میانگین زمانی است که سیستم برای تشخیص یک چهره صرف نموده است.

متوسط میانگین زمان تشخیص در فریم‌ها: متوسط میانگین زمان تشخیص یک چهره در فریم‌هاست.

پردازش تشخیص

متوسط مقداری از توان پردازنده که سیستم برای رخداد تشخیص صرف می‌کند.

نحوهٔ اندازه‌گیری: میانگین متوسط تمامی توان‌هایی از پردازنده که سیستم برای رخدادهای تشخیص صرف می‌کند.

میزان حافظهٔ RAM اشغال‌شده در مرحلهٔ تشخیص

متوسط حافظهٔ RAM که سیستم برای رخداد تشخیص صرف می‌کند.

نحوهٔ اندازه‌گیری: میانگین متوسط تمامی مقادیر حافظهٔ RAM که سیستم برای رخدادهای تشخیص صرف نموده است.

$$WRFR = \sum_{Frame=1}^{Frame=n} \frac{\text{Number of wrong recognized faces}}{n * \text{Count of people in the view}} \quad (3)$$

نحوهٔ اندازه‌گیری خطا

برای محاسبهٔ این خطا به‌دلیل محدودیت در تعیین مکان چهرهٔ اشخاص، به‌ناچار تنها از یک شخص در طول زمان آزمون استفاده می‌شود. در کل زمان آزمون، یک نفر در پرسپکتیو دوربین قرار می‌گیرد به‌گونه‌ای که چهرهٔ شخص در مقابل دوربین باشد.

پارامترهای لازم برای ثبت در مستندات

- هویت فرد موجود در مقابل دوربین
- شرایط پارامترهای آزمون

قابلیت‌های نرم‌افزاری لازم

نرم‌افزار هویت شخص داخل تصویر را که از پیش در سیستم تعریف شده، از کاربر دریافت می‌کند و با توجه به اینکه تنها یک شخص در مقابل دوربین قرار گرفته، خطا را محاسبه می‌کند. به بیان دیگر، نرم‌افزار صرفاً خروجی FRFR را با واحد درصد در پایان آزمون ارائه می‌کند.

کارایی استخراج الگو

زمان استخراج الگو

متوسط زمانی که سیستم برای رخداد استخراج الگو صرف می‌کند.

نحوهٔ اندازه‌گیری: میانگین متوسط تمامی زمان‌هایی که سیستم برای رخدادهای استخراج الگو صرف نموده است.

پردازندهٔ مصرف‌شده در رخداد استخراج الگو

متوسط مقداری از توان پردازنده که سیستم برای رخداد استخراج الگو صرف می‌کند.

نحوهٔ اندازه‌گیری: میانگین متوسط تمامی توان‌هایی از پردازنده که سیستم برای رخدادهای استخراج الگو صرف نموده است.

میزان حافظهٔ RAM اشغال‌شده در مرحلهٔ استخراج الگو

متوسط حافظهٔ RAM که سیستم برای رخداد استخراج الگو صرف می‌کند.

نحوهٔ اندازه‌گیری: میانگین متوسط تمامی مقادیر حافظهٔ RAM که سیستم برای رخدادهای استخراج الگو صرف نموده است.

کارایی تطابق

زمان محاسبهٔ تطابق

متوسط زمانی که سیستم برای رخداد تطابق صرف می‌کند.

نحوهٔ اندازه‌گیری: میانگین متوسط تمامی زمان‌هایی که سیستم برای رخدادهای تطابق صرف نموده است.

پردازندهٔ مصرف‌شده برای رخداد تطابق

متوسط مقداری از توان پردازنده که سیستم برای رخداد تطابق صرف می‌کند.

نحوهٔ اندازه‌گیری: میانگین متوسط تمامی توان‌هایی از پردازنده که سیستم برای رخدادهای تطابق صرف نموده است.

میزان حافظهٔ RAM اشغال‌شده در مرحلهٔ تطابق

متوسط حافظهٔ RAM که سیستم برای رخداد تطابق صرف می‌کند.

نحوهٔ اندازه‌گیری: میانگین متوسط تمامی مقادیر حافظهٔ RAM که سیستم برای رخدادهای تطابق صرف نموده است.

قابلیت‌های نرم افزاری لازم	پارامترهای لازم برای ثبت در مستندات	رابطه
نرم‌افزارْ زمان مشخصی از کاربر گرفته و در آن دورهٔ زمانی، محاسبات مربوط به زمان صرف‌شده برای هر رخداد تشخیص را با استفاده از رابطهٔ ۴ انجام داده و در نهایت نتیجهٔ این محاسبه را به کاربر برمی‌گرداند.	• زمان صرف‌شده برای محاسبهٔ هر رخداد تشخیص • تعداد کل تشخیص‌های انجام‌شده • شرایط آزمون	$$DMT = \frac{\sum_{Frame=1}^{Frame=n} \text{Time spent on detection}}{\sum_{Frame=1}^{Frame=n} \text{Number of faces detected in this frame}} \quad (4)$$ $$DMFT = \frac{1}{n} \sum_{Frame=1}^{Frame=n} \frac{\text{Time spent on detection}}{\text{Number of faces detected in this frame}} \quad (5)$$
نرم‌افزار زمان مشخصی را از کاربر گرفته و در آن دورهٔ زمانی محاسبات مربوط به توان پردازنده که برای هر رخداد تشخیص صرف شده با استفاده از رابطهٔ ۶ محاسبه می‌شود و در نهایت نتیجهٔ این محاسبه به کاربر اعلام می‌شود.	• میزان توان صرف‌شده برای محاسبهٔ هر رخداد تشخیص • تعداد کل تشخیص‌های انجام‌شده • شرایط آزمون	$$DPU = \frac{\sum_{Frame=1}^{Frame=n} \text{Process used for detection}}{\sum_{Frame=1}^{Frame=n} \text{Number of faces detected in this frame}} \quad (6)$$
نرم‌افزارْ زمان مشخصی را از کاربر گرفته و در آن دورهٔ زمانی محاسبات مربوط به میزان حافظهٔ RAM صرف‌شده برای هر رخداد تشخیص را با استفاده از رابطهٔ ۷ محاسبه می‌کند و در نهایت نتیجهٔ این محاسبه را ارائه می‌کند.	• میزان حافظهٔ RAM صرف‌شده برای محاسبهٔ هر رخداد تشخیص • تعداد کل تشخیص‌های انجام‌شده • شرایط آزمون	$$DRAMU = \frac{\sum_{Frame=1}^{Frame=n} \text{RAM used for detection}}{\sum_{Frame=1}^{Frame=n} \text{Number of faces detected in this frame}} \quad (7)$$
نرم‌افزارْ زمان مشخصی را از کاربر گرفته و در آن دورهٔ زمانی محاسبات مربوط به زمان صرف‌شده برای هر رخداد استخراج الگو را با استفاده از رابطهٔ ۸ انجام داده و در نهایت نتیجهٔ این محاسبه را ارائه می‌کند.	• زمان صرف‌شده برای محاسبهٔ هر رخداد استخراج الگو • تعداد کل استخراج‌های الگوی انجام‌شده • شرایط آزمون	$$TET = \frac{\sum_{Frame=1}^{Frame=n} \text{Time spent on pattern exreaction}}{\sum_{Frame=1}^{Frame=n} \text{Number of faces detected in this frame}} \quad (8)$$
نرم‌افزارْ زمان مشخصی را از کاربر گرفته و در آن دورهٔ زمانی محاسبات مربوط به توان پردازندهٔ صرف‌شده برای هر رخداد استخراج الگو را با استفاده از رابطهٔ ۹ انجام داده و در نهایت نتیجهٔ این محاسبه را ارائه می‌کند.	• میزان توان صرف‌شده برای محاسبهٔ هر رخداد استخراج الگو • تعداد کل استخراج‌های الگوی انجام‌شده • شرایط آزمون	$$TEPU = \frac{\sum_{Frame=1}^{Frame=n} \text{Process used for detection}}{\sum_{Frame=1}^{Frame=n} \text{Number of faces detected in this frame}} \quad (9)$$
نرم‌افزار زمان مشخصی را از کاربر گرفته و در آن دورهٔ زمانی محاسبات مربوط به میزان حافظهٔ RAM صرف‌شده برای هر رخداد استخراج الگو را با استفاده از رابطهٔ ۱۰ انجام داده و در نهایت نتیجهٔ این محاسبه را ارائه می‌کند.	• میزان حافظهٔ RAM صرف‌شده برای محاسبهٔ هر رخداد استخراج الگو • تعداد کل استخراج‌های الگوی انجام‌شده • شرایط آزمون	$$TERAMU = \frac{\sum_{Frame=1}^{Frame=n} \text{RAM used for pattern extraction}}{\sum_{Frame=1}^{Frame=n} \text{Number of faces detected in this frame}} \quad (10)$$
نرم‌افزار زمان مشخصی را از کاربر گرفته و در آن دورهٔ زمانی محاسبات مربوط به زمان صرف‌شده برای هر رخداد تطابق را با استفاده از رابطهٔ ۱۱ انجام داده و در نهایت نتیجهٔ این محاسبه را ارائه می‌کند.	• زمان صرف‌شده برای محاسبهٔ هر رخداد تطابق • تعداد کل تطابق‌های انجام‌شده • شرایط آزمون	$$MT = \frac{\sum_{Frame=1}^{Frame=n} \text{Time spent on matching}}{\sum_{Frame=1}^{Frame=n} \text{Number of faces detected in this frame}} \quad (11)$$

قابلیت‌های نرم افزاری لازم	پارامترهای لازم برای ثبت در مستندات	رابطه
نرم‌افزار زمان مشخصی را از کاربر گرفته و در آن دورهٔ زمانی محاسبات مربوط به توان پردازندهٔ صرف‌شده برای هر رخداد تطابق را با استفاده از رابطهٔ ۱۲ انجام داده و در نهایت نتیجهٔ این محاسبه را ارائه می‌کند.	• میزان توان صرف‌شده برای محاسبهٔ هر رخداد تطابق • تعداد کل تطابق‌های انجام‌شده • شرایط آزمون	$$MPU = \frac{\sum_{Frame=1} \text{Process used for matching}}{\sum_{Frame=1}^{Frame=n} \text{Number of faces detected in this frame}} \quad (12)$$
نرم‌افزار زمان مشخصی را از کاربر گرفته و در آن دورهٔ زمانی محاسبات مربوط به میزان حافظهٔ RAM صرف‌شده برای هر رخداد تطابق را با استفاده از رابطهٔ ۱۳ انجام داده و در نهایت نتیجهٔ این محاسبه را ارائه می‌کند.	• میزان حافظهٔ RAM صرف‌شده برای محاسبهٔ هر رخداد تطابق • تعداد کل تطابق‌های انجام‌شده • شرایط آزمون	$$MRAMU = \frac{\sum_{Frame=1}^{Frame=n} \text{RAM used for matching}}{\sum_{Frame=1}^{Frame=n} \text{Number of faces detected in this frame}} \quad (13)$$

منابع

[۱] Singh, ShilpiPrasad, S. V.A.V. (۲۰۱۸), Techniques and challenges of face recognition: A critical review

[۲] https://www.nist.gov/speech-testimony/facial-recognition-technology-part-iii-ensuring-

[۳] Harakannanavar, Sunil S.R, Prashanth, Kanabur, VidyashreePuranikmath, Veena I.Raja, K. B. (۲۰۱۹), Technical Challenges, Performance Metrics and Advancements in Face Recognition System

[۴] Ramachandra, Raghavendra, Busch, Christoph (۲۰۱۷), Presentation attack detection methods for face recognition systems: A comprehensive survey

[۵] Hu, Shuowen, Hong, Tsai Hong, Maschal, Robert, Phillips, Jonathon P., Young, S. Susan (۲۰۱۰), Performance assessment of face recognition using super-resolution

انتخاب راهبند خودکار مناسب وسایل نقلیه

نویسنده:
حمید حاتمی

در سال‌های اخیر، حمله‌های با استفاده از وسایل نقلیه گسترش یافته، به همین دلیل مسئولان حفاظت و برقراری امنیت موظف هستند به‌طور کارآمد و دقیق میزان خطر را ارزیابی کرده و بهترین محافظت ممکن را برای جلوگیری یا کاهش حملات خودرو فراهم نمایند.

مقدمه

همانند بسیاری از موارد در زندگی ما، هیچ راه‌حل واحدی وجود ندارد که بتواند محافظت کلی از نفوذ همه‌نوع خودرو/ وسیلهٔ نقلیه را در هر شرایطی با توجه به این نکته، ASTM [1] یک روش آزمون استاندارد برای انتخاب و آزمون بهترین نوع موانع خودکار وسیلهٔ نقلیه منتشر کرده است. در این استاندارد روش مشخصی برای ارزیابی عملکرد موانع (راهبندها، بولاردها و ...) در طیف گسترده‌ای از شرایط، سناریوها، عملکردها و ریسک‌ها طراحی شده است تا براساس نیاز، مناسب‌ترین گزینه انتخاب شود. همچنین روش آزمون تجهیزات نیز در این استانداردها آمده است. شایان ذکر است استاندارد انگلیسی PAS[2] نیز در این حوزه کاربرد دارد که به استانداردهای ASTM شباهت زیادی دارد.

مقدور سازد. به‌ازای امکانات، محیط‌ها و رویدادهای مختلف، با منابع و ویژگی‌های تهدید متفاوتی روبه‌رو خواهیم شد. به همین دلیل، هر مکان نیاز به راه‌حلی خاص برای پاسخگویی به نیازهای خود دارد. بنابراین، شاید تنها مهم‌ترین عاملی که متخصصان امنیتی باید به‌خاطر بسپارند نیاز به راه‌حلی است که نیازهای خاص آنها را در رابطه با ارزیابی و سطح تهدیدها، نیازهای عملیاتی تأسیسات، تطبیق‌پذیری سیستم مانع و مقرون‌به‌صرفه بودن برآورده کند.

انواع راهبند

هرکدام از انواع راهبندها سازوکار و کارآیی خاصی دارند و برای مصارف و نیازهای متفاوتی در راستای مسدودکردن مسیر

---

۱. American Society for Testing and Materials؛ انجمن آزمون و مواد آمریکا

2. Publicly Available Specification

نمونه‌هایی از رتبه‌بندی مانع سقوط ASTM

نوع وسیلهٔ نقلیه	حداکثر وزن	درجهٔ نفوذ با سرعت خاص
ماشین مسافربری کوچک	۱۱۰۲ کیلوگرم	SC۳۰ (۵۰ کیلومتر در ساعت) SC۴۰ (۶۵ کیلومتر در ساعت) SC۵۰ (۸۰ کیلومتر در ساعت) SC۶۰ (۹۵ کیلومتر در ساعت)
سدان فول سایز	۲۱۰۰ کیلوگرم	FS۳۰; FS۴۰; FS۵۰; FS۶۰
وانت باربری	۲۳۰۰ کیلوگرم	PU۳۰; PU۴۰; PU۵۰; PU۶۰
وسیلهٔ نقلیهٔ متوسط	۶۸۰۰ کیلوگرم	M۳۰; M۴۰; M۵۰
وسیلهٔ نقلیهٔ سنگین	۲۶۵۰۰ کیلوگرم	H۳۰; H۴۰; H۵۰

عبور وسایل نقلیه استفاده می‌شوند. بنابراین، نمی‌توان آنها را به‌جای یکدیگر استفاده کرد. راهبندها به چهار خانوادهٔ اصلی به‌شرح زیر تقسیم می‌شوند که در هر خانواده زیرمجموعه‌هایی وجود دارد.

راهبند بازویی

راهبندهای خودکار بازویی متداول‌ترین و پرمصرف‌ترین نوع راهبندهای خودکار هستند. در راهبند بازویی، قدرت موتور محرک متناسب با طول بازوی راهبند متفاوت است. راهبندهای بازویی شامل میله‌ای متحرک و سیستم محرکه (مجموعهٔ موتور و فنر) است که عملکرد آن از طریق یک مدار الکترونیکی کنترل می‌شود. تفاوت اصلی میان مدل‌های مختلف راهبند میله‌ای در طول میله، سرعت حرکت میله و تعداد چرخهٔ کارکرد راهبند در هر ساعت است. طول بازوی این راهبندها بسته به مدل دستگاه معمولاً بین ۲ تا ۸ متر متغیر است. از مهم‌ترین عوامل تعیین‌کننده در انتخاب راهبند می‌توان به‌میزان تردد اشاره کرد. زیربنای راهبندهای الکترومکانیکی چرخدنده‌هایی است که به‌صورت نسبی بسته به مدل دستگاه بین ۱۰۰ تا ۵۰۰ مرتبه تردد را در روز پاسخگو هستند، ولی در راهبندهای الکتروهیدرولیکی این کار توسط پمپ‌های روغن و شیر هوا انجام می‌شود که اصطلاحاً به آنها راهبند تردد نامحدود می‌گویند. به بیان دیگر، راهبندهای بازویی به دو دستهٔ زیر تقسیم می‌شوند:

- الکترومکانیکی (تردد محدود)
- الکتروهیدرولیکی (تردد نامحدود)

راهبند ستونی

راهبند ستونی برای کنترل عبورومرور خودرو در ورودی مکان‌های با ضریب امنیتی بالا استفاده می‌شود. این نوع راهبند شامل یک استوانهٔ فولادی است که به کمک یک سیستم محرک خطی به‌سمت بالا و پایین حرکت

می‌کنـد. کل مجموعـهٔ اسـتوانهٔ متحـرک و سیسـتم محرکـه درون یـک گـودال در داخـل زمیـن قـرار داده می‌شـوند و عملکـرد سیسـتم محرکه ازطریـق مـدار فرمـان کـه در اتـاق کنتـرل نصـب شـده، هدایـت می‌شـود. وقتـی قصـد بسـتن محـل عبـور را داشـته باشـیم، بـا صـدور فرمـان، اسـتوانهٔ فـولادی بـولارد به‌سـمت بـالا حرکـت کـرده (بسـته بـه مـدل دسـتگاه از ۱/۵ ثانیـه تـا ۷ ثانیـه) و به‌صـورت یـک مانـع در برابـر تـردد خودروهـا عمـل خواهـد کـرد. راهبنـد سـتونی مقاومـت بالایـی در برابـر برخـورد داشـته و قـادر اسـت مانـع از عبـور خودروهـای غیرمجـاز شـود.

راهبند ضدتروریستی (بلاکر)

راهبنـد خودرویـی ضدتروریسـتی از ورقه‌هـای بـزرگ فـولادی و مسـتحکم سـاخته می‌شـود کـه در زمیـن دفـن می‌شـوند و ازلحـاظ عمـق بـه دو نـوع سـطحی و نیمه‌عمیـق تقسـیم می‌شـوند. مدل‌هایـی کـه در عمـق کمتـر از ۵۰ سـانتی‌متر دفـن می‌شـوند، مدل‌هـای سـطحی نـام دارنـد.

عـلاوه بـر اماکـن حیاتـی، حسـاس و مهـم، ایـن راهبنـد در مراکـزی ماننـد مجتمع‌هـای اداری و تجـاری بـزرگ عمومـی کـه ممکـن اسـت قربانـی حمله‌هـای مختلـف ماننـد حمله‌هـای تروریسـتی شـوند، کاربـرد دارد، چراکـه در بیـن راهبندهـای مختلـف، راهبنـد خودرویـی ضدانتحـار سـطحی و نیمه‌عمیـق بهتریـن کارآیـی ممکـن را بـرای جلوگیـری از نفـوذ ناخواسـتهٔ وسـایل نقلیـه دارد. ایـن راهبنـد بـا نام‌هـای راهبنـد کف‌خـواب، راهبنـد زرهـی و راهبنـد ضدانتحـاری نیـز شـناخته می‌شـود. در برخـی مدل‌هـای راهبندهـای ضدتروریسـتی، تعـدادی نیـزه نیـز در کـف قـرارداده شـده اسـت کـه بـا بالاآمـدن آنهـا، عبـور از یـک سـمت بـرای وسـایل نقلیـه غیرممکـن می‌شـود. در برخـی مدل‌هـای دیگـر، نیزه‌هایـی روی سـطح افقـی و همچنیـن بدنـه نیـز نصـب می‌شـود.

راهبند زنجیری

ایـن مـدل از راهبنـد بهتریـن پیشـنهاد بـرای مکان‌هایـی اسـت کـه نیازمنـد طـول دهنـهٔ پوشـش‌دهی زیـاد (تـا ۱۶ متـر) هسـتند یـا از لحـاظ ارتفـاع محدودیـت دارنـد. دو سـتون در دو طـرف بـه زمیـن متصـل می‌شـوند و بـا پایین‌آمـدن و بالارفتـن زنجیـر عمـل تـردد انجـام می‌شـود. ایـن مـدل دارای تـردد بالاسـت.

دسـته‌بندی راهبندهـای فعـال ازلحـاظ میـزان مقاومـت در برخوردهـا

موانع خودرو براساس سه حوزهٔ زیر دسته‌بندی می‌شوند:

- وزن تهدید موردانتظار (وسیلهٔ نقلیه)؛
- سرعت حرکت وسیلهٔ نقلیه؛

سطح نفوذ در ASTM

کد	میزان نفوذ
P۱	نفوذ حداکثر تا ۱ متر
P۲	نفوذ حداکثر تا ۷ متر
P۳	نفوذ حداکثر تا ۳۰ متر
P۴	نفوذ بیش از ۳۰ متر

- بیشینه فاصلهٔ قابل‌قبول از سد معبر که وسیلهٔ نقلیه باید طی کند.

رتبه‌بندی مانع سقوط ASTM براساس این سه پارامتر انجام می‌شود. مثلاً، یک درخواست کامل براساس استاندارد ASTM بدین شرح است: توانایی متوقف‌کردن یک کامیون متوسط (M) با وزن ۶۸۰۰ کیلوگرم با سرعت ۸۰ کیلومتر در ساعت با فاصلهٔ نفوذ کمتر از ۱ متر.

ذکـر ایـن نکتـه ضـروری اسـت کـه هرچـه فاصلـهٔ نفـوذ وسـیلهٔ نقلیـه کوتاه‌تـر باشـد، امتیـاز مانـع بالاتـر اسـت.

سطح‌بندی K یا سطح‌بندی M؟

سیسـتم درجه‌بنـدی K کـه قبـلاً در ASTM اسـتفاده شـده بـود، بـا سیسـتم رتبه‌بنـدی M جایگزیـن شـده اسـت. در سیسـتم جدیـد بـا رتبه‌بنـدی M، دامنـهٔ وسـیع‌تری از جهـت وزن، سـرعت و فواصـل نفـوذ خـودرو نسـبت بـه درجـهٔ قبلـی K در نظـر گرفتـه شـده اسـت.

شبیه‌سازی یا آزمون در فضای واقعی؟

اسـتاندارد ASTM بـه شـمارهٔ Active Standard ASTM F۲۶۵۶/ F۲۶۵۶M یـک روش بـرای ارزیابـی عملکـرد مانـع در برابـر برخـورد وسـیلهٔ نقلیـه ارائـه می‌دهـد. شـایان ذکـر اسـت کـه ایـن اسـتاندارد عـلاوه بـر راهبندهـای خـودکار، بـرای موانـع غیرفعـال نیـز کاربـرد دارد. روش‌هـای آزمـون ایـن اسـتاندارد شـامل روش‌هـای آزمـون در فضـای واقعـی و همچنیـن روش‌هـای مبتنـی بـر شبیه‌سـازی اسـت.

همان‌طـور کـه قبـلاً گفتیـم، هیـچ راهبنـدی وجـود نـدارد کـه مانعـی بـرای ورود خـودرو بـا سـطح حفاظتـی ۱۰۰٪ ایجـاد کنـد. بنابرایـن، اهمیـت حیاتـی فرایندهـای آزمایـش راه‌حـل ارزیابـی و حفاظـت از تهدید روشـن می‌شـود. بـه همیـن دلیـل، در حالـی کـه شبیه‌سـازی‌های رایانـه‌ای، ابـزاری بسـیار کارآمـد و مقرون‌به‌صرفـه بـرای شبیه‌سـازی تهدیدهـای مختلـف و پاسـخ‌های مناسـب هسـتند، امـا دامنـهٔ آنهـا هنـوز محـدود اسـت و توصیـه می‌شـود آزمایش‌هـای فیزیکـی بـرای ارزیابـی عملکـرد واقعـی نیـز عـلاوه بـر شبیه‌سـازی، انجـام شـود.

مدیریت امنیتی در کارخانهٔ فولاد

مترجم: محمد قلم‌چی

بهره‌برداری از کارخانه‌ی تولید فولاد مستلزم توجه دقیق به ایمنی، امنیت و پادمان است. هدف امنیت، جلوگیری از اقدامات عمدی است که ممکن است به کارخانه‌ی فولاد آسیب برساند یا منجر به سرقت مواد شود. کارکنان امنیتی نقش بسیار مهمی در کارخانه‌ی فولاد بازی می‌کنند و بخشی جدایی‌ناپذیر از تیم مدیریت هستند. برای تأمین امنیت کارخانه‌ی فولاد چند سطح متفاوت حفاظتی لازم است. این سطوح متناسب با شرایط تهدید انتخاب می‌شوند.

نظرات کارشناس برجستهٔ بین‌المللی در حوزهٔ مدیریت امنیت کارخانهٔ فولاد

این مقاله در وبسایت شخصی ساتیندرا کومار سارنا[1] نگاشته و منتشر شده است. ایشان از سال ۱۹۶۵ با صنعت فولاد در ارتباط بوده و سمت‌های متعددی از کارشناسی تا مدیریت ارشد بر عهده داشته است. از اقدامات او می‌توان به انتخاب مکان برای کارخانهٔ گرین‌فیلد[2]، ارائهٔ طرح‌های مفهومی و راه‌اندازی آنها، انجام پروژه‌های مختلف، انجام کنترل فرایند، نگهداری، تجزیه‌وتحلیل خرابی، تجربهٔ ادارهٔ شرکت در تمام سطوح مدیریتی، کنترل کیفیت، تحقیق‌وتوسعه، مدیریت ایمنی و محیط زیست، ممیزی فنی/ ارزیابی دستگاه و آموزش و غیره اشاره کرد. او امنیت کارخانهٔ فولاد را یکی از مهم‌ترین ارکان آن توصیف کرده. این مقاله را در سال ۲۰۱۵ به رشتهٔ تحریر درآورده است. با وجود گذشت مدت‌زمان زیادی از انتشار مقاله، این متن از لحاظ مفهومی و بررسی سامانه‌های مورد نیاز اهمیت ویژه‌ای دارد.

مفهوم ریسک مبنای امنیت است

ریسک تهدید یا مخاطره‌ای است که از نظر احتمال و تأثیر ارزیابی می‌شود. تهدید رویدادی با پیامدهای منفی است که از نیت سوء و مخرب انسانی ایجاد شده است. مخاطره رویدادی با پیامدهای منفی است که از طریق قصد انسان، محیط زیست یا محیط غیرمخرب ایجاد می‌شود.

سامانهٔ امنیتی کارخانهٔ فولاد براساس رویدادهایی که موجب کاهش امنیت کارخانه می‌شود طراحی می‌شود تا برای محافظت از انسان‌ها و دارایی‌های فیزیکی، در برابر ریسک‌های شناسایی‌شده مؤثر واقع شود. این اقدامات به‌منظور کاهش خطرات امنیتی به سطوح قابل‌قبول در نیروگاه با رعایت حداقل کنترل‌های تعیین‌شده توسط سطح تأثیر خطرات امنیتی است. کنترل‌های لازم به‌منظور عملکرد ایمن کارخانهٔ فولاد برای پوشش تهدیداتی است که هم در خارج و هم در داخل کارخانه وجود دارد.

چهار شکل از اقدامات حفاظتی در کارخانهٔ فولاد وجود دارد: پیش‌گیرانه، محافظت‌کننده، مجازات‌کننده و کارآگاهی. اقدامات امنیتی در کارخانهٔ فولاد از عملکردهای ایمنی به‌منظور محافظت در برابر خسارت‌ها و خطرات ناشی از آن متمایز است. همچون ایمنی، حفاظت از کارخانه اساساً عملکردی مدیریتی است که برای عملکرد صحیح کارخانهٔ فولاد اساسی است.

با پیشرفت فناوری، عملیات کارخانهٔ فولاد بسیار پیچیده شده است و عوامل متعددی وجود دارد که بر تولید تأثیر منفی می‌گذارد. برخی از این عوامل در ادامه آورده شده است:

- مسائل داخلی امنیتی؛
- تهدیدهای خارجی؛
- وضعیت قانون و نظم؛
- ناآرامی‌های صنفی و کارگری؛
- آشوب‌های اجتماعی؛
- فشارهای منطقه‌ای/ محلی؛
- تولید، ذخیره‌سازی و بازاریابی در شرایط دشوار؛
- بی‌صداقتی کارمندان.

تلفات و خسارات احتمالی کارخانهٔ فولاد برای بقای کارخانه تهدیدی واقعی است. این تهدیدها ناشی از زورگیری، ارتکاب جرم جنایی، سرقت، دله‌دزدی، آتش‌سوزی، اقدامات تخریبی، کلاهبرداری، خسارت شیطنت‌آمیز، جاسوسی صنعتی، براندازی، اعتصابات، تحریکات، آشوب‌های مدنی، شورش، سایر مشکلات مجرمانه و بلایای طبیعی است. درک صحیح از این خطرات واقعی و بالقوه از سوی مدیریت مسلماً منجر به درک بیشتر نیاز به امنیت مؤثر برای کارخانهٔ فولاد خواهد شد.

با توجه به تمام دلایلی که در بالا توضیح داده شد، ضروری است که یک گروه امنیتی قوی و مؤثر در کارخانهٔ فولاد ایجاد شده و پرورش یابد و با دقت بسیار از آن مراقبت شود تا شاهد تولیدی مصلحانه و یکنواخت در کارخانهٔ فولاد باشیم. در واقع در کارخانه‌های تولید فولاد، امنیت از همان ابتدا بخشی جدایی‌ناپذیر از مدیریت است و برنامه‌ریزی‌های امنیتی مناسب حتی در مرحلهٔ طراحی نیز انجام می‌شود.

امنیت در کارخانه‌های فولاد تابعی از موارد زیر است:

- درک تهدید و تجزیه‌وتحلیل ریسک؛
- کنترل دسترسی و محافظت از محیط؛
- کاربری صحیح از سامانه‌های حفاظتی؛
- کنترل دسترسی و جلوگیری از نفوذ؛
- جلوگیری از ورود افراد غیرمجاز به مناطق حیاتی که در آنها تجهیزات حساس نصب و راه‌اندازی شده‌اند؛
- امنیت دارایی‌ها، اماکن و انبارها و محافظت در برابر خرابکاری‌ها، جاسوسی و آتش‌سوزی؛
- امنیت مواد (مواد اولیه، مواد فرآوری‌شده، محصولات نهایی، لوازم یدکی و غیره) و تجهیزات؛
- امنیت در برابر دله‌دزدی، سرقت مواد و محصولات و سایر جرایم صنعتی؛
- گشت‌زنی در جاده‌های حاشیه‌ای و مناطقی که ترافیک انسانی کمتری در آنها وجود دارد؛
- مشارکت در مدیریت بحران و مدیریت اضطراری؛
- امنیت کارکنان و حمایت از مدیریت؛

1. Satyendra Kumar Sarna
2. Greenfield

- هوش داخلی و محافظت از اطلاعات طبقه‌بندی‌شده و حساس؛
- بازرسی امنیتی؛
- جلوگیری از بدترشدن وضعیت نظم و قانون در کارخانه به‌منظور کنترل جمعیت؛
- آموزش کارکنان در امور امنیتی.

اقدامات احتیاطی امنیتی در کارخانهٔ فولاد

- اطمینان از ورود افراد/ وسایل نقلیهٔ مجاز به محل کارخانهٔ فولاد؛
- تمرین منظم استراتژی و برنامهٔ حفاظتی برای مواجهه با موارد احتمالی؛
- تعامل با دستگاه‌های اطلاعاتی دولتی برای آمادگی عملیاتی؛
- کنترل امنیت کلیهٔ مکان‌های حساس داخل مناطق گیاهی.

کارخانهٔ فولاد هزاران نفر را استخدام می‌کند. به‌علاوه تعداد زیادی از آژانس‌های پیمانکاری و کارگران پیمانکاری در این کارخانه کار می‌کنند. از این رو، سازوکار امنیتی در کارخانهٔ تولید فولاد باید نه‌تنها از وسایل فیزیکی مانند نرده‌ها، دیوارها، دروازه‌ها و موانع دیگر استفاده کند، بلکه باید از ابزارهایی برای غربالگری همهٔ افرادی که به دروازه‌ها وارد می‌شوند، بهره‌برداری نماید. میزان نیاز به این بازرسی و غربالگری شخصی به میزان امنیتی بستگی دارد که برای جلوگیری از تلاش افراد غیرمجاز برای سرقت، آسیب‌رساندن، قطع یا به‌خطرانداختن فرایندهای تولید ضروری است. یک کارت مجاز یا نشان حاوی نام، عکس، شمارهٔ اشتغال، چاپ اثر انگشت شست، امضای مقام کارخانه و سایر داده‌های شناسایی بازدیدکنندگان، فروشندگان و پیمانکاران صادر شده است تا از این طریق به کارمندان عادی که بدون تأخیر بی‌دلیل وارد محل شوند توسط دستگاهی که معمولاً در دروازه کار می‌کند، اجازهٔ ورود داده شود. سایر افرادی که مایل هستند به‌منظور انجام کاری وارد کارخانه شوند، ابتدا باید قبل از گرفتن مجوز موقت، به‌صورت کامل احراز هویت شوند.

ابزارهای امنیتی که معمولاً توسط کارکنان امنیتی کارخانه استفاده می‌شوند

- دوربین مداربسته و سامانهٔ حفاظت پیرامونی که از دوربین مداربسته نیز برای توانمندسازی خود بهره می‌برد؛
- شبکهٔ Walkie-Talkies و VHF (بی‌سیم برای ارتباط صوتی)؛
- آشکارسازهای فلزی دستی و گیت‌های فلزیاب؛
- راهبندهای نیزه‌ای/ گیت‌های ضدتروریستی/ شناساگرهای زیر وسایل نقلیه؛
- جلیقه‌های ضدگلوله با کلاه ایمنی؛
- گیت‌های نفررو مجهز به اسکنر اثر انگشت؛
- نورافکن‌های دستی/ دستگاه‌های دید در شب؛
- دستگاه‌های ایکس ری چمدانی؛
- آشکارساز مواد منفجره/ پتو بمب/ جوخهٔ سگ.

برخی از اقدامات استاندارد امنیت فیزیکی در کارخانه‌های فولاد

- ارتفاع استاندارد دیوار محیط ۳ متر بوده و سیم‌پیچ حلقوی روی آن به ارتفاع ۶۰ سانتی‌متر نصب می‌شود؛
- گیاهان باید در فواصل منظم زمانی هرس شوند؛
- روشنایی مناسب در داخل و اطراف دیوارهٔ محیط، به‌خصوص در شب، لازم است؛
- ورودوخروج کارمندان/ پیمانکاران/ کارگران/ بازدیدکنندگان/ وسایل نقلیه باید ازطریق دروازه‌ها انجام شود، یعنی دروازه‌ای جداگانه برای افراد، دروازه‌ای جداگانه برای وسایل نقلیه و دروازه‌ای جداگانه برای مواد وجود داشته باشد. همهٔ وسایل نقلیه باید

از نظر حمل‌ونقل بررسی شوند؛
- برای جلوگیری از هرگونه ورود اجباری وسایل نقلیه، باید از موانع آهنی در دروازه استفاده شود؛
- گشت منظم توسط تیم واکنش سریع به‌صورت شبانه‌روزی صورت پذیرد؛
- اتاق کنترل یکپارچه با امکانات ارتباطی مناسب و اتاق دوربین مداربسته وجود داشته باشد؛
- سامانهٔ کنترل تردد هوشمند برای پیمانکار/ کارگر و مواد - تشخیص هویت و بررسی تاریخچه - جلوگیری از تردد هرگونه عنصر غیرمجاز به کارخانهٔ فولاد ضروری است؛
- سامانه‌ای رایانه‌ای برای کنترل تردد وجود داشته باشد.

عملکرد مدیریت امنیت به تمام قسمت‌های کارخانهٔ فولاد کشیده شده و باید در تمام سطوح کارخانه نفوذ کند. امنیت کارخانهٔ فولاد به جای تحمیل اجباری از بالا از طریق بخشنامه‌ها و دستورالعمل‌های اداری باید به‌گونه‌ای از داخل رشد کند و به تمام حوزه‌ها و بخش‌های کارخانه گسترش یابد. حراست نمی‌تواند جداگانه فعالیت کند و باید با همهٔ بخش‌ها و کارمندان صرف‌نظر از سطح مدیریتی آنها، عضویت در اتحادیه‌های صنفی یا وابستگی‌های سیاسی‌شان همکاری کند. در عین حال، باید اطمینان حاصل شود که کنترل‌های امنیتی مانع از فعالیت کارخانهٔ فولاد نمی‌شوند. از طرف دیگر، این کنترل‌ها باید به‌گونه‌ای طراحی شوند که به حداکثر کارایی ماشین‌آلات تولید و عملیات کارخانه کمک کنند. اقدامات امنیتی باید از کنترل شدید و سختگیرانه، جز در موارد اضطراری شدید، جلوگیری کند. افزون بر این، این موارد باید با گسترش آگاهی امنیتی میان کارکنان، از جمله سطوح مختلف مدیریتی، اجرا شود. همهٔ کارکنان امنیتی به‌جای اعتماد زیاد به کنترل‌های سختگیرانه، به ایجاد انضباط شخصی میان کارمندان تلاش کنند. هر کارمند باید احساس کند که جزئی از مدیریت امنیت است اما تفاوت او با کارمندان امنیتی در این است که آنان تمام‌وقت در این حوزه کار می‌کنند و متخصص در این حوزه هستند.

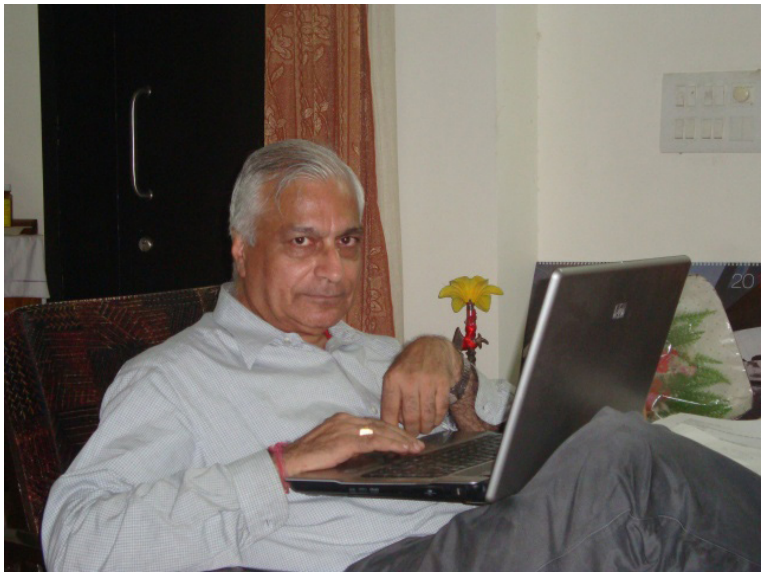
رهبری در امور امنیتی باید در بالاترین سطح مدیریت در کارخانهٔ فولاد نشان داده شود و باید با استفاده از یک سیستم مدیریت مؤثر حاصل شود.

در زمینهٔ امنیت در کارخانهٔ تولید فولاد، به‌منظور جلوگیری از دسترسی مهاجمان به اطلاعات حساس مربوط به اقدامات محافظتی یا ضعف‌های ایمنی، دسترسی اطلاعات معمولاً باید به گروه کوچک و منتخبی از افراد محدود شود. افزون بر این، مهم است که با انجام اقدامات لازم اطمینان حاصل شود که دانش اقدامات مخرب باعث رویدادهای مشابه نمی‌شود.

روش فعالیت‌های امنیتی در کارخانهٔ فولاد

از آنجا که مساحت کارخانهٔ فولاد بسیار بزرگ است، کارخانه به چندین منطقهٔ امنیتی تقسیم می‌شود. مناطق امنیتی براساس ارزیابی خطر امنیتی، روشی را برای کاهش امنیت فیزیکی ارائه می‌دهند. ریسک مترتب بر این اماکن متفاوت خواهد بود و برنامهٔ امنیت فیزیکی باید براساس مطالعات ریسک رقم بخورد. سایر روش‌های اتخاذشده برای مدیریت امنیت در کارخانهٔ فولاد در ادامه شرح داده شده است:

- درک تهدید و تجزیه‌وتحلیل ریسک با در نظر گرفتن پیشینهٔ محل کارخانه و قانون محلی انجام می‌شود. تهدیدهای خارجی و داخلی به‌منظور تحلیل در نظر گرفته می‌شوند. در صورت لزوم، از پلیس محلی و سایر مقامات محلی کمک گرفته می‌شود؛
- ممیزی‌های امنیتی منظم در ارتباط با روش‌ها، رویه‌های امنیتی در کارخانهٔ فولاد انجام می‌شود. کفایت سیستم در طی ممیزی امنیتی ارزیابی می‌شود و نقاط ضعف برای انجام اقدامات اصلاحی مؤثر شناسایی می‌شود؛
- نیروی انسانی و تجهیزات امنیتی مرتباً به‌روز می‌شود و در صورت ناکافی‌بودن تجهیزات موجود، اقداماتی برای خرید ابزارها انجام می‌شود. بدون چشم‌پوشی



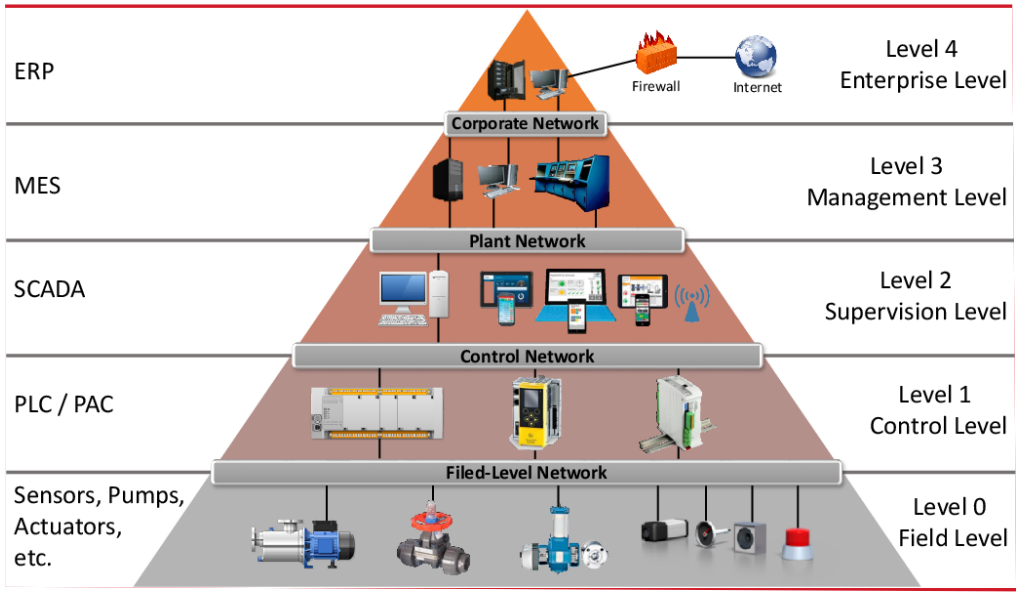
ساتیندرا کومار سارنا؛ کارشناس برجستهٔ بین‌المللی در حوزهٔ مدیریت امنیت کارخانهٔ فولاد

از پیامدهای مالی باید ترکیبی بهینه از مأموران و تجهیزات وجود داشته باشد؛

- تمام ابزارهای موجود موردارزیابی قرار می‌گیرند و پیشرفت‌های لازم همراه با ابزارهای جدید و ادغام آنها شناسایی می‌شوند؛
- رویه‌های از پیش نگاشته شده برای تعیین وظایف و مسئولیت‌های کارکنان امنیتی تهیه شده است؛
- طرح‌های مدیریت بحران براساس نیاز و تعمیقی که باید هنگام تهیهٔ پیش‌نویس دنبال شود، طراحی می شوند؛
- درک تهدید با توجه به سرقت داخلی مواد و همچنین کارخانه و تجهیزاتموردتوجهقرارگرفتهاست؛
- تمام اقدامات لازم برای تقویت سیستم موجود باید مشخص شود. که نه‌تنها شامل اقدامات حفاظت فیزیکی بلکه امنیت اسناد، جلوگیری از نشت اطلاعات باارزش را نیز شامل می‌شود؛
- روش‌های جابه‌جایی مواد ورودی و خروجی و جابه‌جایی محصول نهایی ساده است. جنبه‌های امنیتی موجود شامل مواد اولیه و حرکات محصول نهایی به طور منظم ارزیابی می‌شود و اصلاحات مناسب در رویه‌های تقویت سیستم ایجاد می شود؛
- الگوی استقرار نیروی انسانی به‌همراه وظایف و مسئولیت‌های آنها تدوین شده است. طرح نظارت بر مأموران امنیتی نیز بخشی از این سند است. روش‌های عملیاتی برای نقاط مختلف کار در هر کجا که لازم باشد انجام می شود؛
- روش ممیزی داخلی برای ارزیابی سیستم‌های امنیتی شامل چک‌لیست‌های کامل و قالب‌های تحلیلی تدوین شده است؛
- پس از ارزیابی سیستم‌های موجود و فعالیت‌های گروه‌های مختلفی که در محل فعالیت می‌کنند، در هرکجا که نیاز باشد، یک سیستم جمع‌آوری اطلاعات داخلی ساخته می‌شود.

سایر جنبه‌های امنیتی که باید موردتأکید قرار گیرند، به درک تهدید و تجزیه‌وتحلیل ریسک بستگی دارد. جنبهٔ مهم دیگر برای امنیت کارخانهٔ فولاد این است که اقدامات امنیتی باید متناسب با ریسک‌های واقعی و بالقوه باشد. اقتصاد در برنامه‌ریزی‌های امنیتی، کلید مدیریت امنیت است. نه از نظر اقتصادی امکان‌پذیر است و نه از نظر اداری ضروری است که همواره سختگیرانه‌ترین پوشش امنیتی ایجاد شود، بلکه با بررسی فرصت‌ها، تهدیدها و ریسک‌ها، نظر به سطح امنیتی ناحیه، باید راهکارهای مناسب استفاده شود. تهدید بالقوه و واقعی برای کارخانهٔ فولاد باید شناسایی و ارزیابی شود تا میزان حفاظت لازم تعیین شود و تدابیر امنیتی که در واقع لازم است تدوین شود. در حالی که تدابیر امنیتی باید رعایت شود ، هر دو اصل «امنیت مبتنی بر نیاز» و «عمق امنیت» باید در نظر گرفته شوند.

یک سیستم امنیتی یکپارچه برای کارخانهٔ فولاد شامل مجموعه‌ای از طرح‌های حفاظتی، استراتژی‌های امنیتی، دستگاه‌ها و کنترل‌هایی است که از طرح کارخانه، مناطق حساس کارخانه، توپوگرافی، شرایط محیطی، عامل جمعیتی و سایر مسائل اقتصادی-اجتماعی نیز مراقبت می‌کنند. بهعنوان جنبه‌های ژئوپلیتیک، مدیریت و کارمندان باید به سیستم امنیتی اعتماد کنند. سامانهٔ امنیتی باید به‌طور دوره‌ای مورد بهبود قرار گیرد تا از عملکرد مؤثر آن اطمینان حاصل شود.



دستگاه‌های X-RAY

نویسنده:
محمد قلم‌چی

این مقاله به‌منظور آشنایی مقدماتی با کارکردهای اصلی و فناوری‌های مبنایی به‌کاررفته در بیشتر دستگاه‌های بازرسی ایکس‌ری به رشته‌ی تألیف در آمده است.

بازرسی ایکس‌ری، نوعی از بازرسی بدون مزاحمت[1] (NII) است.

منظور از دستگاه در این مقاله، تجهیزاتی هستند که برای تصویربرداری داخل احجام با فناوری ایکس‌ری کاربرد دارند. مخاطب این مقاله، مشتریان این دستگاه‌ها، علاقه‌مندان و همچنین کارشناسان فروش و بازاریابی این نوع دستگاه هستند.

دسته‌بندی دستگاه‌های بازرسی بدون مزاحمت براساس نوع ورودی

زمان زیادی از استفاده از فناوری ایکس‌ری برای بازرسی در جهان نمی‌گذرد. جذابیت ایکس‌ری امکان نمایش تمامی محتویات ازخلال حصارهای فیزیکی و بدون بازکردن آنهاست. بعضاً افرادی این موضوع را خلاف حقوق بشر قلمداد کرده‌اند، خصوصاً وقتی قرار باشد بدن انسان با ایکس‌ری به‌منظور بازرسی اسکن شود. انواع دستگاه‌های ایکس‌ری از نظر نوع ورودی به دسته‌های زیر تقسیم می‌شوند:

- دستگاه بازرسی ایکس‌ری کیف و بسته؛
- دستگاه بازرسی ایکس‌ری خودرویی؛
  - دستگاه‌های بازرسی ایکس‌ری خودروهای بزرگ ازجمله کانتینر و اتوبوس،
  - دستگاه‌های بازرسی ایکس‌ری خودروهای شخصی و وانت‌بار.
- دستگاه‌های بازرسی ایکس‌ری بدن انسان.

اجزای سخت‌افزاری دستگاه اسکن ایکس‌ری

دستگاه‌های ایکس‌ری، از قسمت‌های سخت‌افزاری مختلفی چون تونل تصویربرداری، نوار نقاله، ژنراتور و پنل کاربری تشکیل می‌شوند. همچنین معمولاً کامپیوتری در کنار این تجهیزات وجود دارد که نرم‌افزار ویژهٔ مدیریت تصاویر دستگاه روی آن نصب می‌شود. در این بخش به بررسی اجزای سخت‌افزاری یک دستگاه ایکس‌ری می‌پردازیم. مطالعهٔ موردی این بخش بر روی دستگاه اسکن کالا صورت گرفته است.

تونل تصویربرداری

سطح‌مقطعی است که کالا یا وسیلهٔ نقلیه از داخل آن عبور کرده و تصویربرداری از آن انجام می‌شود. در دستگاه‌های ثابت، این سطح کاملاً توسط پرده‌ها و پنل‌های سربی برای جلوگیری از تابش اشعهٔ ایکس به بیرون از دستگاه محافظت می‌شود. اندازهٔ تونل تصویربرداری یا بازرسی براساس ابعاد و اندازهٔ وسایل و بارهایی که تصویربرداری از آنها انجام می‌شود، طبقه‌بندی می‌شود. در دستگاه‌های ثابت اسکن کیف و بسته (کالا)، این ابعاد از ۵۵cm × ۳۵cm تا حداکثر ۱۸۰cm × ۱۸۰cm افزایش می‌یابد. نوع ورودی دستگاه براساس طول و عرض دهانه مشخص می‌شود. به‌منظور تصویربرداری از اندازه‌های بزرگ‌تر همچون تصویربرداری از کامیون یا تریلرها از دستگاه‌های ویژه استفاده می‌شود که براساس نیاز خریدار طراحی و ساخته می‌شوند.

نوار نقاله

سطحی است که کالا یا بار روی آن قرار گرفته و برای تصویربرداری از داخل ایکس‌ری عبور داده

1. Non-Intrusive Inspection

می‌شود. در دستگاه‌های بزرگ که برای تصویربرداری از بارهای بزرگ و پالت به‌کار گرفته می‌شوند، به‌جای نوار نقاله از غلتک‌های مخصوص استفاده می‌شود.

ژنراتور ایکس‌ری

معمولاً، ژنراتورهای ایکس‌ری اشعهٔ تابشی را به‌سمت بالا و با زاویهٔ ۹۰ درجه در داخل تونل بازرسی می‌تابانند. اکثر ژنراتورهایی که در دستگاه‌های ایکس‌ری استفاده می‌شوند، از لامپ‌های ایکس‌ری با قدرت تابشی ۱۴۰، ۱۶۰ یا ۱۸۰ کیلوولت استفاده می‌کنند. البته در سیستم‌های بزرگ‌تر این لامپ‌ها تا ۲۰۰ یا حتی ۳۲۰ کیلوولت نیز می‌رسد.

حسگرهای آشکارساز

مجموعهٔ حسگرهای آشکارساز از تعدادی دیود حسگر برای اندازه‌گیری سطوح بالا و پایین انرژی تشکیل می‌شوند. این مجموعهٔ دیودها که به‌شکل ال هستند برای محاسبهٔ انرژی عبوری از کالا یا شیء داخل تونل استفاده می‌شوند.

واسط کاربری

اپراتور توسط این پنل تنظیمات را اعمال و عملیات مربوط به دستگاه ایکس‌ری را هدایت می‌کند. در حقیقت توسط این پنل اپراتور می‌تواند شروع یا خاتمهٔ بازرسی را کنترل کند، همچنین از تمام امکاناتی که نرم‌افزار برای شناساییِ بهتر کالا در اختیار او قرار می‌دهد، استفاده نماید.

مشخصات سخت‌افزاری تعیین‌کننده در کارکرد دستگاه‌های اسکن ایکس‌ری

ولتاژ ژنراتور

میزان ولتاژ لامپ ایکس‌ری تابعی از میزان چگالی جسم و دهانهٔ تونل دستگاه است. به عبارت دیگر، هر چه ابعاد تونل ایکس‌ری بزرگ‌تر باشد، برای بازبینی دقیق‌ترْ ژنراتور قوی‌تری موردنیاز است. البته این رابطه خطی نیست و ملاحظاتی در این خصوص وجود دارد. اگر توان ژنراتور خیلی بالا باشد، به‌دلیل نفوذ بسیار بالا امکان تشخیص کامل تصویر از بین می‌رود.

به‌طور کلی، در دستگاه‌های ایکس‌ری از ژنراتورهای با ولتاژ ۱۴۰ کیلوولت در دستگاه‌های کوچک، ۱۶۰ تا ۱۸۰ کیلوولت در دستگاه‌های متوسط و بزرگ و ۳۲۰ تا ۴۵۰ کیلوولت برای دستگاه‌هایی که چگالی بسیار بالایی دارند، استفاده می‌شود.

موقعیت قرارگرفتن ژنراتور

طراحی محل قرارگرفتن ژنراتور ایکس‌ری معمولاً در بخش پایینی دستگاه است، طوری که جهت آن رو به بالا باشد. البته، در برخی از دستگاه‌ها، بنا به مصالحی ژنراتور در بالای دستگاه یا در پاره‌ای از موارد در سمت راست یا چپ دستگاه قرارمی‌گیرد. البته، در دستگاه‌هایی که از دو دستگاه ژنراتور استفاده می‌شود، موقعیت قرارگرفتن ژنراتورها یکی در پایین و دیگری در سمت چپ یا راست یا تلفیقی از این موارد می‌باشد.

رو به بالا[2]: در این دستگاه‌ها، ژنراتور ایکس‌ری در بخش پایینی تونل و به‌سمت بالا قرار گرفته که شامل بیشتر دستگاه‌های ایکس‌ری می‌شود.

«**تصویربرداری از پهلو**»[3]: در دستگاه‌هایی که تصویربرداری به‌صورت جانبی انجام می‌شود، ژنراتور ایکس‌ری در قسمت راست یا چپ تسمه نقاله قرار می‌گیرد. در مواردی که تصویربرداری از اجسام سنگین انجام می‌شود، معمولاً تصویربرداری به‌صورت افقی انجام می‌شود.

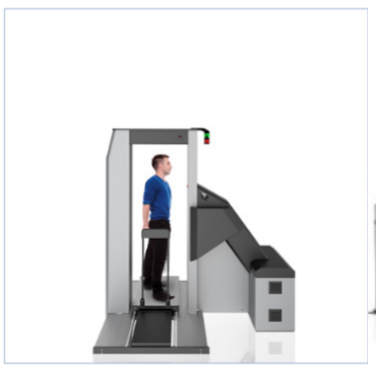
تصویربرداری از بالا به پایین[4]: در مقابل، در دستگاه‌های تصویربرداری از بالا، ژنراتور در بخش بالایی دستگاه سوار شده و به‌صورت عمودی و رو به پایین تصویربرداری انجام می‌شود.

به‌دلیل ساختار فیزیکی این دستگاه‌ها برای دریافت تصویر مناسب لازم است تا سرعت حرکت جسم بسیار کمتر از موارد دیگر باشد و عمدتاً برای تصویربرداری از بارهای بزرگ و پالت‌ها از این روش استفاده می‌شود. بیشترین کاربرد این روش در بازرسی بار Cargo است.

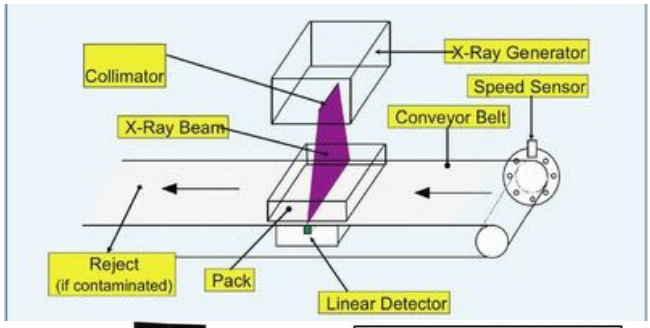
تصویربرداری دوجهته[5]: در این دستگاه‌ها دو ژنراتور نصب شده است که هم‌زمان از دو جهت مختلف از بار تصویربرداری نموده و دو تصویر هم‌زمان را روی دو مانیتور در اختیار اپراتور قرار می‌دهند. این دستگاه‌ها در مکان‌های بسیار حساس و برای تصویربرداری بسیار دقیق استفاده می‌شوند.

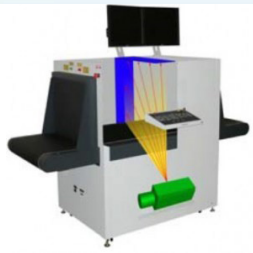
«ضریب نفوذ در فولاد»[6] و «تشخیص سیم»[7]

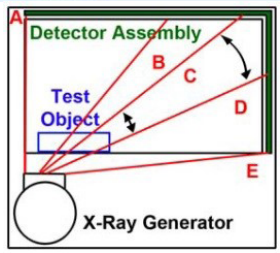
در دستگاه ایکس‌ری، میزان نفوذ در فولاد یا به عبارتی تشخیص نوع موادی که پوشش فلزی دارند، بسیار مهم است. همچنین آشکارسازی یا تشخیص سیم‌های بسیار نازک که ممکن است در ساخت هرگونه بمب به‌کار گرفته



2. Up-Shooting
3. Side-Shooting
4. Down-Shooting
5. Dual View
6. Steel Penetration
7. Wire Resolution







شود، از اهمیت ویژه‌ای برخوردار است. در حقیقت این دو پارامتر می‌توانند در شناسایی هرچه بیشتر کالاهای تصویربرداری‌شده، مخصوصاً با کارکردهای حفاظتی مؤثر باشند.

قابلیت تشخیص مواد و نوع آن، در حالتی که توسط یک حفاظ فلزی به‌صورت کامل پوشیده شده باشد، اصطلاحاً شیلد شده باشد، با عبارت ضریب نفوذ در فولاد معرفی می‌شود. این میزان معمولاً برحسب میلی‌متر اندازه‌گیری می‌شود و می‌تواند از ۲۹ میلی‌متر تا ۳۹ میلی‌متر و حتی تا بیش از ۴۰ میلی‌متر باشد.

مقایسهٔ فناوری‌های بازرسی بدون مزاحمت

در حال حاضر ۴ فناوری ایکس‌ری برای بازرسی محموله و افرادْ تحت استاندارد تک‌انرژی، انرژی دوگانه، پس‌پراکنده[8] و توموگرافی کامپیوتری (CT) وجود دارد.

شناخت فناوری‌های ایکس‌ری به‌منظور اجرای قانون، امنیت، بازرسی گمرک و کنترل مرز ارزش افزوده دارد. تفاوت‌های اساسی میان فناوری‌های ایکس‌ری در جدول ۱ به‌طور خلاصه آمده است.

استاندارد تک‌نما

اشعهٔ ایکس ازخلال جسم منتقل می‌شود و آشکارسازهایی که در مقابل پرتو قرار دارند، میزان جذب اشعهٔ ایکس را اندازه‌گیری می‌کنند. تصویر حاصل عمدتاً خاکستری است.

انرژی دوگانه/ نمای تک یا دوگانه

در این حالت اشعهٔ ایکس با دو انرژی متفاوت تولید می‌شود. پرتوهای پرانرژی جذب کمتری دارند، پرتوهای کم‌انرژی عناصر روشن را تیره‌تر نشان می‌دهد. تصاویر حاصل از انرژی‌های مختلف با یکدیگر مقایسه می‌شوند و عناصر سنگین در مقابل سبک مشخص می‌گردند. بدین ترتیب مواد آلی، معدنی و غیرشفاف (فلز) از یکدیگر متمایز می‌شوند.

8 Backscatter

نمای دوگانه

این نوع دستگاه شامل دو منبع اشعهٔ ایکس است و نمای عمودی و افقی را به‌طور هم‌زمان برای چمدان و محموله‌های غربال‌شده نمایش می‌دهد. نماهای دوگانه شناسایی کارآمدتری را برای اپراتور فراهم می‌کنند.

پس‌پراکنده

در این حالت اشعهٔ ایکس سراسر شیء را اسکن می‌کند تا دو تصویر ایجاد کند: تصویر انتقال عادی و تصویر پس‌پراکنده.

۳D /CT

در این حالت آشکارسازهای اشعهٔ ایکس متعدد در اطراف جسم می‌چرخند و تصویر دوبعدی ایجاد می‌کنند، اما چون جسم روی نوار نقاله به‌سمت جلو حرکت می‌کند، حاصل تصویر سه‌بعدی است. این اسکن را می‌توان با استفاده از تکنیک‌های نمایش کامپیوتری در همهٔ زوایا، به‌صورت سه‌بعدی، مشاهده کرد.

قابلیت‌های نرم‌افزار مدیریت تصاویر اسکن ایکس‌ری

مهم‌ترین پارامتر در کارکرد سامانهٔ ایکس‌ری نرم‌افزار آن می‌باشد که به اپراتور توانایی تشخیص هرچه بهترِ نوع کالا و محتویات آن را می‌دهد. به همین دلیل در شرکت‌های شاخصِ تولیدکنندهٔ این دستگاه، نرم‌افزارْ جزء پارامترهای بسیار منحصربه‌فرد دستگاه به‌حساب می‌آید. بیشتر فناوری دستگاه اسکن ایکس‌ری در همین حوزه متبلور می‌شود و با شناخت نرم‌افزار و بررسی این موضوع که نرم‌افزار توسط خود شرکت تولید شده یا از جای دیگری خریداری شده، می‌توان به اصالت تولیدکنندهٔ دستگاه ایکس‌ری پی برد.

نرم‌افزار دستگاه ایکس‌ری به دو بخش نرم‌افزار محلی و نرم‌افزار مرکزی تقسیم می‌شود. نرم‌افزار محلی، نرم‌افزاری است که روی کامپیوتر نصب شده و در کنار دستگاه ایکس‌ری قرار می‌گیرد و کارکرد آن نگهداری و تجزیه‌وتحلیل تصاویر اسکن‌های دریافتی است. تعداد رنگ‌های قابل‌تفکیک و قابلیت اندازه‌گیری عدد اتمی[9] که مشخص‌کنندهٔ جنس کالاست، از پارامترهای مهم در نرم‌افزار محلی است.

نرم‌افزار مرکزی ایکس‌ری، نرم‌افزاری است که برای سازمان‌های متوسط و بزرگ که بیش از یک دستگاه ایکس‌ری در اختیار دارند کاربرد دارد و دارای قابلیت‌های بسیار بیشتری است.

رنگ‌ها در اسکن ایکس‌ری

رنگ تصویر نمایش داده شده در تصاویر رنگی اسکن ایکس‌ری، بستگی به چگالی مواد و نوع ماده دارد. مواد آلی مانند کاغذ، لباس و بسیاری از مواد منفجره به رنگ نارنجی، مواد مخلوط مانند آلومینیوم به رنگ سبز، مواد معدنی مانند مس به رنگ آبی و مواد غیرقابل‌نفوذ به رنگ سیاه‌وسفید نمایش داده می شوند؛ در برخی از دستگاه‌ها، این نوع مواد به رنگ سبز مایل به زرد یا به رنگ قرمز نمایش داده می‌شوند. شدت رنگ بستگی به چگالی و ضخامت ماده دارد.

تعیین چگالی موارد توسط آشکارساز دوسطحی صورت می‌پذیرد. لایه‌های

9. Atomic Z- Number

جدول ۱	معمولی	انرژی دوگانه	Backscatter	CT
	تک‌نما	تک‌نما/دونما	تک‌نما	سه‌بعدی
تشخیص نوع ماده	✗	✓	✓	✓
تهدید قابل‌شناسایی				
دقت	✓	✓✓	✓	✓✓✓
سرعت	سریع	سریع	متغیر	کند
مزایا	– هزینهٔ پایین	– تمیزدادن جنس اجسام و اختصاص کد رنگ برای اپراتورها – توانایی تشخیص مواد منفجره که در پشت کالای دیگری پنهان شده باشند	– تمیزدادن اجناس با پارامتر Z پایین	– بالاترین وضوح اسکن حتی در حد میلی‌متر – توانایی تشخیص پس و پیش و اطراف، حتی در اشیای بزرگ یا با چگالی بالا
محدودیت‌ها	– ضعف در تمیزدادن جنس اجسام – خطای زیاد	– ضعف در تمیزدادن اجناس با چگالی بالا	– ضعف در نفوذ خصوصاً در چگالی‌های بالا	– سرعت پایین
قیمت	$	$$	$$$	$$$$

پیکسل آشکارساز با یک نوار فلزی جدا شده است. فلز اشعهٔ نرم را جذب نموده و به طول موج کوتاه‌تر اجازهٔ نفوذ بیشتر به لایه‌های پایین‌تر می‌دهد که باعث آشکارسازی طیف‌سنج دوباند می‌شود.

در دستگاه‌هایی که قابلیت تصویربرداری ۶ رنگ دارند، افزون بر رنگ‌های نارنجی، سبز، آبی، از رنگ‌های قهوه‌ای، زرد و بنفش نیز استفاده می‌شود. این تفکیک رنگی اپراتور را قادر می‌سازد بسیاری از مواد و کالاها را تشخیص دهد. مثلاً در دستگاه‌های ایکس‌ری با قدرت تفکیک ۳ رنگ، مواد منفجره از نوع C4، Semtex، TNT، همچنین هروئین و کوکائین به رنگ نارنجی نشان داده می‌شوند، ولی در دستگاه‌های با تفکیک ۶ رنگ، مواد منفجرهٔ C4، Semtex، TNT، با رنگ قهوه‌ای و مواد مخدر مثل هروئین و کوکائین و الکل با رنگ نارنجی نشان داده می‌شوند، همچنین مواد شیمیایی جامد و باروت در دستگاه‌های با تفکیک ۶ رنگ، به رنگ سبز نمایش داده می‌شوند. بنابراین، دستگاه‌های ۶ رنگ مواد شیمیایی جامد را به رنگ زرد و مواد منفجره چون باروت را به رنگ سبز نشان می‌دهند. دستگاه‌های ۳ رنگ فلزات را به رنگ آبی نشان می‌دهند، در حالی که، دستگاه‌های ۶ رنگ اپراتور را قادر می‌سازند که فلزاتی چون طلا و نقره را از سایر فلزات کم‌ارزش‌تر تشخیص دهد؛ این دستگاه‌ها طلا و نقره را به رنگ بنفش و آهن و فولاد را به رنگ آبی نشان می‌دهند.

اندازه‌گیری عدد اتمی

با استفاده از جدول ۲ به‌راحتی می‌توان از طریق رنگ و عدد اتمی، نوع مواد به‌کاررفته در کالا را تشخیص داد.

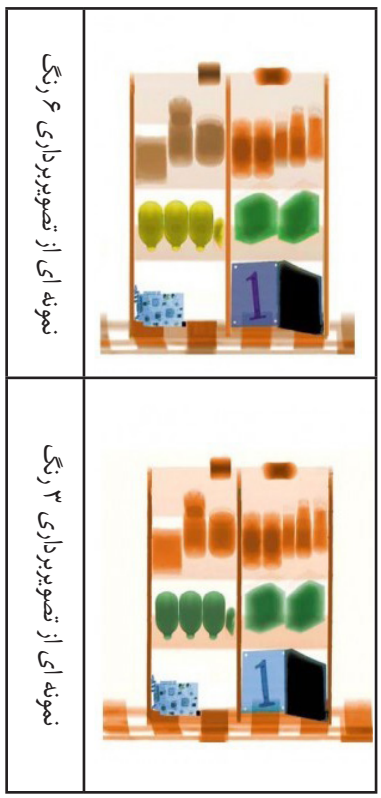
نرم‌افزار مدیریت جامع ایکس‌ری

وقتی بیش از یک دستگاه ایکس‌ری در اختیار سازمانی قرار گیرد، نظارت دقیق بر عملکرد این تجهیزات در مرکز، هرچه بیشتر اهمیت می‌یابد. کارکردهای اصلی سامانهٔ جامع مدیریت ایکس‌ری به شرح زیر است:

۱. جمع‌آوری و انتقال امن تصاویر ایکس‌ری به‌همراه فراداده‌های مرتبط با آنها در مرکز
۲. ایجاد مرکز دادهٔ پشتیبان از تصاویر ایکس‌ری به‌همراه داده‌های هویتی مرتبط با آنها
۳. ارائهٔ داده‌های موردنیاز به سایر سامانه‌های کنترلی با کارکردهای:

- افزایش سرعت ورود اطلاعات به سامانه

مقایسهٔ تصویربرداری ۶ رنگ با ۳ رنگ



- جلوگیری از خطای انسانی در ورود اطلاعات
- امکان کنترل متقاطع بر صحت داده‌های واردشده به سامانه

۴. نظارت بر نتایج عملکرد دستگاه‌های ایکس‌ری

۵. مدیریت کاربران: تعیین سطوح دسترسی کاربران در چندین ردهٔ سازمانی

۶. امکان جست‌وجوی به‌هنگام با کمترین زمان تأخیر

۷. امکان مقایسهٔ خودکار بسته یا بار ورودی با خروجی (برای تشخیص تغییرات و غیره)

۸. تولید گزارش‌های متنوع و قابل شخصی‌سازی، با سرعت و کیفیت قابل‌قبول

۹. نظارت خودکار بر صحت عملکرد دستگاه‌های ایکس‌ری (سامانهٔ نظارت بر سلامت سامانهٔ ایکس‌ری) بازرسی و نظارت بر روند ایکس‌ری و جلوگیری از سوءاستفاده‌های احتمالی

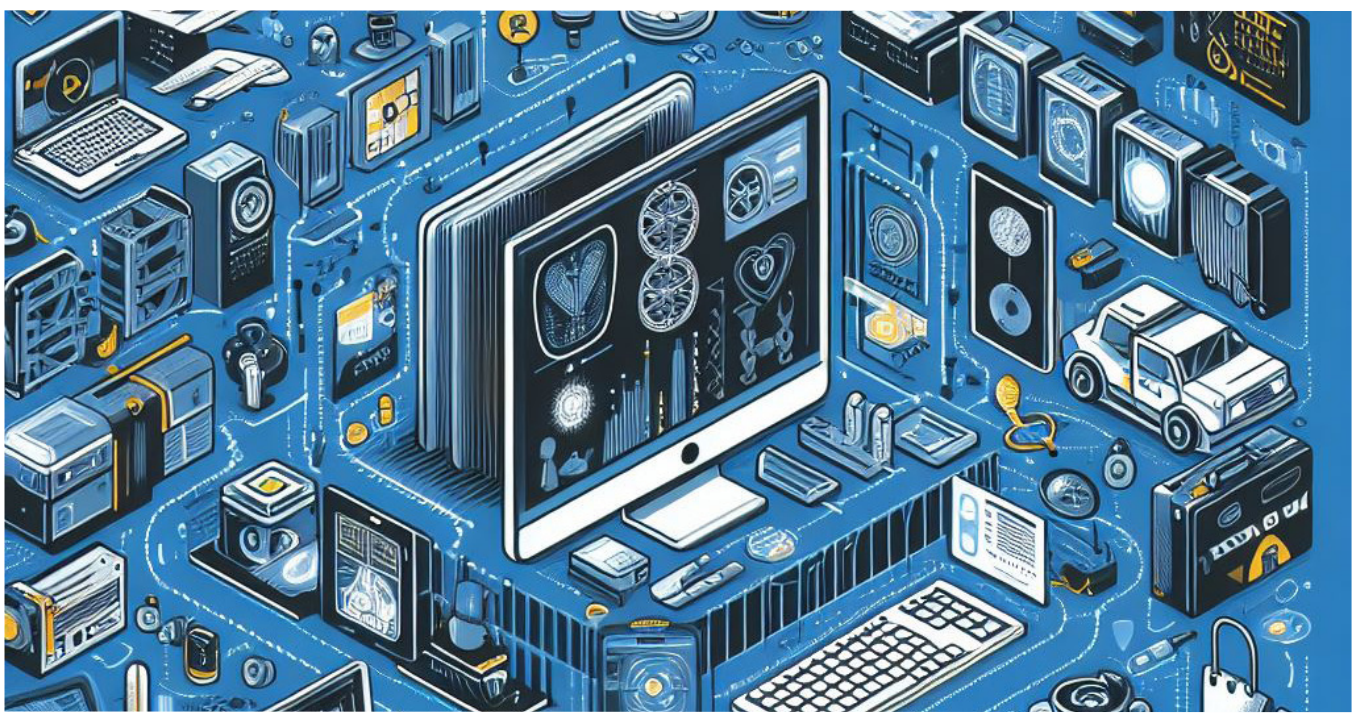
۱۰. ورود فرادادهٔ ایکس‌ری بدون دخالت عامل انسانی از طریق:

- تشخیص چهرهٔ صاحبان کیف دستی یا بار برای درج در سامانه با امکان مقایسهٔ بعدی
- ورود خودکار شمارهٔ پلاک خودرو یا تریلر
- ورود خودکار شمارهٔ کانیتنر
- ورود خودکار داده‌های قبوض مرتبط از جمله قبض باسکول از طریق بارکدخوان

نوع کالای خطرناک	مثال	رنگ جسم در تصویربرداری ٦ رنگ	رنگ جسم در تصویربرداری ۳ رنگ	نوع ماده	عدد اتمی (Z-Number)
مواد منفجره	C۴، TNT و Semtex			ارگانیک	۸–۰
مواد مخدر	هروئین، کوکائین			غیرارگانیک یا سطح کم	۱۰–۸
مواد خنثی	شیشه			کالاهای کاملاً غیرارگانیک	۱۰ – ۱۲
آلومینیوم سیلیکن	باروت، چاشنی‌های انفجاری			فلزات سبک	۱۲ – ۱۷
آهن، فولاد	اسلحه، گلوله، چاقو			فلزات سنگین	۱۷ – ۲۸
طلا، نقره	شیء باستانی زرین، سکهٔ طلا			فلزات با چگالی بالا	بیشتر از ۲۸
سرب	استفاده برای پوشش کالایی خطرناک			غیرقابل‌نفوذ	–

جدول ۲

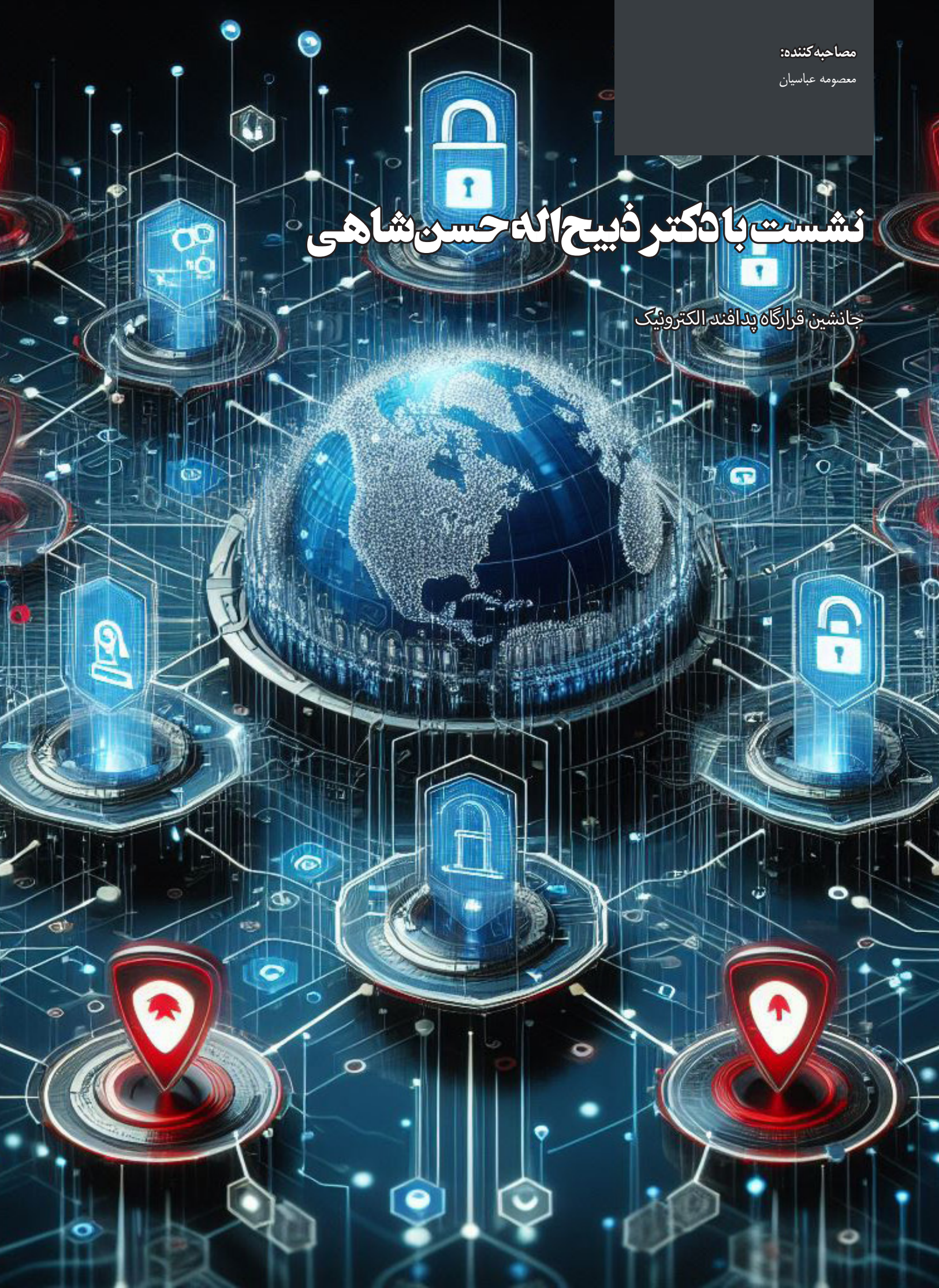
شماتیک سامانهٔ جامع مدیریت ایکس‌ری



مصاحبه کننده:
معصومه عباسیان

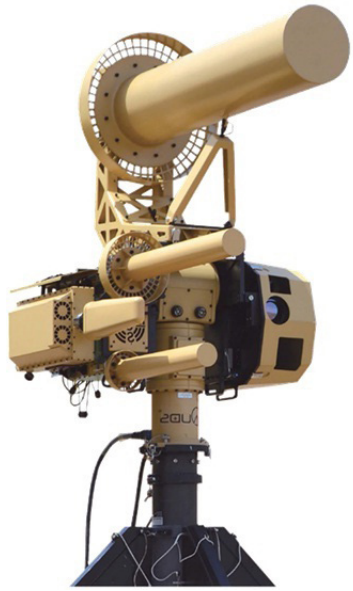
نشست با دکتر ذبیح‌اله حسن‌شاهی

جانشین قرارگاه پدافند الکترونیک



«نبیح‌اله حسن‌شاهی هستم. دکترای مجموعهٔ مهندسی برق الکترونیک از دانشگاه امام حسین(ع) که مدت ۳ سال است جانشین قرارگاه پدافند الکترونیک کشور هستم. فرماندهی این قرارگاه بر عهدهٔ سردار دکتر جلالی رئیس محترم سازمان پدافند غیرعامل کشور است. تخصص بنده در حوزهٔ مخابرات-گرایش سیستمی- بخش پردازش سیگنال، حوزهٔ الکترونیک گرایش دیجیتال- بخش تراشه‌های الکترونیک، گرایش جنگ الکترونیک-بخش‌های ES و EP حوزه‌های مخابراتی و راداری است.

هدف از تشکیل سازمان پدافند غیرعامل احصای تهدیدهای تخصصی انسان‌ساخت و مقابله با آنهاست. در یک کلام پدافند غیرعامل، دفاع بی‌سلاح است که با پدافند عامل یک اکوسیستم دفاعی برای کل کشور ایجاد می کند.»



فرصت‌ها و تهدیدهای سامانه‌های نظارت تصویری از نظر شما چیست؟

«قبل از اینکه به فرصت‌ها و تهدیدهای سامانه‌های نظارت تصویری بپردازم، لازم است اشاره کنم که حوزهٔ تخصصی این قرارگاه صرفاً در حوزهٔ اپتیک نیست. بلکه حوزه‌هایی را مانند ژئوالکترومغناطیس و موضوع اثر طیف الکترومغناطیس بر باران‌زایی یا باران‌زدایی، بیوالکترومغناطیس و موضوع اثر طیف الکترومغناطیس بر بدن و سلامت جامعه، سایبرالکترونیک و تروجان‌های سخت‌افزاری، میکروالکترونیک و سخت‌افزارهای امن، سایبرالکترومغناطیس و آلودگی صنعتی ناشی از سیگنال الکترومغناطیسی توان‌بالا، بمب‌های الکترومغناطیس و EMP، مکاترونیک و بخش ریزپرنده‌ها، ماهواره‌ها و بخش الکترونیک حوزهٔ فضایی، اپتیک، لیزر و مادون قرمز و دوربین‌های تصویربرداری و همچنین حوزهٔ آکوستیک و صوت در بر می گیرد.

درحوزهٔ امنیت الکترونیکی، سامانه‌های نظارت تصویری نقش بسیار مهمی در حفاظت پیرامونی ایفا می کنند. بنابراین در یک سامانهٔ حفاظتی و امنیتی در یک زیرساخت، علاوه بر وجود سامانه‌های ES (سامانه‌های جمع‌آوری اطلاعات سیگنالی) سامانهٔ اپتیکی نقش مهمی دارد که با اضافه‌کردن ماژول‌های هوش مصنوعی و DSS (سامانه‌های تصمیم‌یاری) فرصت بسیار خوبی برای ارتقای سامانه‌های امنیتی به‌وجود می‌آورد. اما از سوی دیگر، بهره‌گیری دشمن از آسیب‌پذیری‌های سامانه‌های نظارت تصویری ازطریق حملات سایبری (در صورت اتصال به اینترنت) و از طرفی

استفاده از حملات سایبرالکترومغناطیس و آلوده‌سازی دوربین‌ها از طریق سیگنال و همچنین آلوده‌سازی کل سامانه یا دوربین‌ها ازطریق تهدیدهای درون‌زا و نیروی انسانی مخرب تهدیدزا به‌شمار می‌آید.»

اقدامات سازمانِ شما در حوزهٔ امنیت فیزیکی خصوصاً پدافند الکترونیک و نظارت تصویری چه بوده است؟

«باتوجه به رسالت این قرارگاه، مقابله با تهدیدهای اشاره‌شده در لایهٔ راهبردی بر عهدهٔ این قرارگاه است. اما برای دفاع جامع و مؤثر، صرفاً لایهٔ راهبردی کفایت نمی‌کند، بلکه تمامی بازیگران حوزهٔ دفاعی و امنیتی، باید در اکوسیستم دفاعی، نقش خود را در لایه‌های عملیاتی، فنی و تاکتیکی به‌خوبی ایفا نمایند.

در لایهٔ عملیاتی، وظیفهٔ بهره‌برداری از سامانه‌های نظارت الکترونیکی (رادار) و تصویری (دوربین) بر عهدهٔ حراست‌های زیرساخت‌های حیاتی و حساس کشور است. همچنین در لایهٔ فنی، شرکت‌های دانش‌بنیان و تولیدکنندگان یا تأمین‌کنندگان تجهیزات الکترونیک، باید ملاحظات امنیتی و پدافندی را در قبال تجهیزات خود رعایت نمایند تا از امنیت و آسیب‌پذیرنبودن تجهیزات خود اطمینان حاصل کنند.»

اصول کلیدی زیربنای اقدامات امنیت سایبرالکترونیکی پدافند غیرعامل چیست و چرا در حفاظت از زیرساخت‌های دیجیتال مهم است؟

«تمام اقدامات پدافند غیرعامل، مبتنی بر سه پارامتر مهم است: ۱. احصای آسیب‌پذیری‌ها، ۲. شناخت تهدیدها، ۳. تعیین، ارزش‌گذاری و سطح‌بندی دارایی‌های سایبری، الکترونیک، شیمیایی، هسته‌ای، زیستی. با شناخت این سه پارامتر است که می‌توان میزان ریسک یک زیرساخت را مشخص کرد و با شناخت ریسک و تحلیل پیامدهای آن و میزان مخاطرات ناشی از آن، دارایی‌ها را مطابق اولویت‌بندی تعیین‌شده مصون نمود.

شاید از نظر عموم، طلا و پول، دارایی به‌حساب بیاید، اما همان‌طور که اشاره شد، دارایی‌های سایبرالکترونیکی اهمیت‌بسیار زیادی دارند؛ چراکه اختلال در مرکز کنترل پالایشگاه یا پتروشیمی، دیسپاچینگ گاز یا برق کشور، می‌تواند علاوه بر خسارت‌های مالی، خسارت‌های جبران‌ناپذیر امنیتی در سطح ملی و بین‌المللی ایجاد نماید.»

تفاوت استراتژی‌های پدافند غیرعامل با پدافند فعال در امنیت سایبرالکترونیکی چیست و مزایا و محدودیت‌های هر رویکرد چیست؟

«همان‌طور که قبلاً اشاره شد، استراتژی پدافند غیرعامل، دفاع بدون سلاح است. البته، نه به این معنا که درپدافند غیرعامل باید با دست خالی دفاع کرد.

در پدافند غیرعامل می‌توان با ابزارهای مختلفی آسیب‌پذیری‌های یک زیرساخت را در حوزهٔ سایبری و الکترونیکی احصا کرد و نسبت به کاهش یا ازبین‌بردن آن اقدام نمود. همچنین می‌توان پس از شناخت تهدیدها، از ابزارهای مقابله با آنها استفاده کرد. اقدامات پدافند غیرعامل، پیش از وقوع رخداد، باید انجام شود، چراکه در آستانهٔ رخداد یا در حین رخداد، دیگر زمان کافی برای دفاع وجود

ندارد. متأسفانه به‌دلیل ضعف در رعایت پدافند غیرعامل در زیرساخت‌های کشور، سازمان‌ها پس از آنکه موردحمله قرار گرفتند، تازه متوجه می‌شوند، پدافند غیرعاملی هم هست و در آن زمان اقدامات پساخدادی انجام می‌شود که این گونه اقدامات صرفاً تجربه ای برای بعد خواهد بود و در نهایت می‌توان زیرساخت را با روش‌های دیگری به‌صورت موقت وارد مدار کرد

برخی از سامانه‌های استفاده‌شده در پدافند غیرعامل به‌خصوص در حوزهٔ پدافند الکترونیک، اقدامات آفندی است که برخی از آن تعبیر به پدافند عامل می کنند. ازجمله سامانهٔ مختل کنندهٔ ارتباطات رادیویی یا سامانه‌های فریب ناوبری GNSS.»

الزامات ضروری برای پیاده‌سازی سازوکارهای پدافند غیرعامل مؤثر در زیرساخت‌های حیاتی مانند شبکه‌های برق، سیستم‌های مالی و شبکهٔ مراقبت‌های بهداشتی چیست؟

«درسازمان پدافند غیرعامل کشور، قرارگاه‌های مختلفی همچون قرارگاه پدافند الکترونیک، سایبری، زیستی، شیمیایی و پرتوی وجود دارند که متناسب با هر تخصص، سازوکارهای پدافندی خود را در حوزه‌های تخصصی مربوط به خود ارائه می کنند. مثلاً سازوکارهای پدافند غیرعامل سایبری در قالب نظام عملیاتی پدافند سایبری کشور، که لازم است زیرساخت‌های حیاتی کشور در شبکه‌های برق، گاز، سامانه‌های مالی و شبکهٔ سلامت کشور و حوزه‌های دیگر از این نظام استفاد نمایند، توسط قرارگاه پدافند سایبری سازمان تهیه و ابلاغ شده است و مشابه همین رویداد نیز برای بقیهٔ قرارگاه‌ها نیز انجام شده یا در حال انجام است.»

چهارچوب‌ها و استانداردهای نظارتی چگونه بر اتخاذ اقدامات امنیت سایبری پدافند غیرعامل در صنایع مختلف تأثیر می‌گذارند و سازمان‌ها در رعایت آن با چه چالش‌هایی مواجه هستند؟

«با توجه به اینکه اولویت تهدیدهای حوزهٔ سایبرالکترونیکی در تمام کشورها یکسان نیست

و از طرفی لزوماً استانداردها و چهارچوب‌های جهانی در حوزهٔ امنیت، نیازمندی همهٔ کشورها را برطرف نمی کند، بنابراین لازم است در حوزهٔ امنیتی و پدافندی، استانداردهای بومی‌شده‌ای وجود داشته باشد تا مطابق با آن الزامات و ملاحظات پدافندی و امنیتی رعایت شود. مضاف بر اینکه برای امن‌سازی یک زیرساخت نمی‌توان به استانداردها و چهارچوب‌های یک کشور خارجی که خود در مظان اتهام حمله است، اعتماد نمود.»

با دیجیتالی‌شدن روزافزون جامعه، استراتژی‌های پدافند غیرعامل چگونه می‌توانند با فناوری‌های نوظهور مانند اینترنت اشیا، هوش مصنوعی و رایانش ابری سازگار شوند تا از محافظت جامع در برابر تهدیدهای سایبری در حال تکامل اطمینان حاصل شود؟

«شاید در زمانی نه‌چندان دور، تصور مردم و حتی دست‌اندرکاران زیرساخت‌های کشور از پدافند غیرعامل تنها به مفاهیمی همچون اختفا، استتار و مقاوم‌سازی استحکامات محدود می‌شد. اما امروزه پدافند غیرعامل در کشور، با ایجاد قرارگاه‌های تخصصی که قبلاً به آنها اشاره شد، تا حد ممکن سعی کرده است که تمام موضوعات تخصصی را در حوزهٔ پدافندی وارد کند و مسائل پدافندی را با فرمول علمی و تخصصی حل نماید.

فناوری‌هایی مانند اینترنت اشیا، هوش مصنوعی، رایانش ابری، پردازش‌های کوانتومی، رادارهای کوانتومی و رمزهای کوانتومی ازجمله مباحثی است که در کارگروه‌های مختلفی مورد بحث و بررسی قرار می گیرد.

موضوعاتی مانند اختفا، استتار و مقاوم‌سازی استحکامات و حوزه‌های کالبدی، همچنان در سازمان مطرح است و با اضافه‌شدن مباحث جدید فنی و استفاده از نوآوری‌ها در حوزهٔ علم و فناوری در قرارگاه پدافند کالبدی سازمان درحال انجام است.»

همکاری و به‌اشتراک‌گذاری اطلاعات چه نقشی در افزایش انعطاف‌پذیری امنیت سایبری پدافند غیرعامل، به‌ویژه در زمینهٔ به‌اشتراک‌گذاری

اطلاعات راجع به تهدید در میان نهادهای بخش دولتی و خصوصی دارد؟

«حفظ محرمانگی اطلاعات همواره اصلی مهم در امنیت اطلاعات است. یکی از اهداف حمله و نفوذ به سامانه‌های صنعتی و اداری در کشورها سرقت اطلاعات است. اگر فرد یا سازمانی، محرمانگی داده را رعایت نکند، در واقع کار را برای مهاجم در دستیابی به اطلاعات ساده‌تر کرده است. اما این امر به معنای عدم‌اشتراک‌گذاری اطلاعات نیست، بلکه اشتراک‌گذاری اطلاعات باید در چهارچوب‌های امنیتی و رعایت سطح‌بندی صورت گیرد تا بتوان هم‌افزایی مطلوبی برای نیل به اهداف و مأموریت‌های تبیین‌شده ایجاد کرد.»

چگونه از مدل‌سازی تهدید و ارزیابی ریسک برای شناسایی آسیب‌پذیری‌ها و اولویت‌بندی سرمایه‌گذاری‌ها در سازوکارهای پدافند غیرعامل استفاده می‌شود و سازمان‌ها چگونه می‌توانند از رویکرد فعالانه به وضعیت امنیت سایبرالکترونیکی اطمینان حاصل کنند؟

«مدل‌سازی تهدید برای سازمان یا زیرساخت به شناسایی و مستندسازی تهدیدهای امنیتی کمک می‌کند. مدل‌سازی هر تهدید، در قالب یک سامانهٔ شبیه‌سازی، به‌صورت آزمایشی اجرا می‌شود. مدل‌سازی تهدیدها تیم پدافندی را در درک ماهیت هر تهدید و میزان تأثیر و تأثر آن بر شبکه توانا می‌کند تا در مصون‌سازی بتواند ضمن رفع آسیب‌پذیری‌های احصاشده، بالاترین میزان آمادگی را در برابر تهدیدهای سایبرالکترونیکی داشته باشد.»

گرایش‌ها و نوآوری‌های نوظهور در راه‌حل‌های امنیت سایبرالکترونیکی پدافند غیرعامل چیست و چگونه سازمان‌ها می‌توانند با استفاده از فناوری‌های پیشرفته و بهترین شیوه‌ها از دشمنان سایبری پیشی بگیرند؟

«برای تعیین گرایش‌ها و راهبردها برای حل یک موضوع، مثلاً امنیت سایبرالکترونیکی، باید از مدل‌های مختلف برنامه‌ریزی استراتژیک استفاده کرد. مثل مدل SWOT که یک مدیر راهبردی باید ضمن احصای نقاط ضعف، قوت، فرصت‌ها و تهدیدها را احصا کند با در نظر گرفتن نقاط ضعف و تهدیدها دسته‌ای از چالش‌ها تعیین می‌شوند و از طرفی با در نظر گرفتن نقاط قوت و فرصت‌ها، دسته‌ای از پیشران‌ها مشخص می‌گردند. در برنامه‌ریزی استراتژیک، باید بتوان از طریق پیشران‌ها، چالش‌ها را رفع نمود. خروجی از خلال برنامه‌ریزی، گرایش‌ها و راهبردها مشخص می‌شود.

در بخش فرصت‌ها، فناوری‌های پیشرفته می‌تواند مدنظر قرار گیرد. یقیناً در صورتی که در برنامه‌ریزی استراتژیک، همهٔ موارد به‌صورت جامع در نظر گرفته شود، بهترین شیوه برای حل مسئله و تعیین افق که همان پیشی گرفتن از دشمنان

در حوزهٔ سایبری و الکترونیک است، محقق می‌شود.»

مشارکت بین دانشگاه، صنعت و دولت چگونه می‌تواند به تحقیق‌وتوسعهٔ استراتژی‌ها و فناوری‌های پدافند غیرعامل پیشرفته برای رسیدگی به چالش‌های امنیت سایبری در یک چشم‌انداز تهدیدآمیزِ به‌سرعت در حال تحول کمک کند؟

«برای رسیدن به اهداف و اجرای مأموریت‌ها که در واقع همان رسیدگی به چالش‌های امنیت سایبری و الکترونیک است، لازم است که راهبردها به‌درستی تعیین شود.

ایجاد و افزایش مشارکت بین دانشگاه و صنعت می‌تواند نقطهٔ قوتی در ایجاد اکوسیستم دفاعی در حوزهٔ الکترونیک و سایبری باشد چراکه دانشگاه مولد نیروی فرهیخته برای به‌کارگیری در حوزهٔ صنعت و صنعت نیز مولد نیروی متخصص و کارآمد برای ارائهٔ خدمات اساسی به ملت و دولت کشور هستند.»

ملاحظات و پیامدهای اخلاقی اجرای اقدامات پدافند غیرعامل، به‌ویژه از نظر حریم خصوصی، حفاظت از داده‌ها و اثرات بالقوهٔ آن بر تجربهٔ کاربر در اکوسیستم دیجیتال چیست؟

«اقدامات پدافند غیرعامل و اجرای الزامات و ملاحظات آن، که بخشی از آن مصون‌سازی است، باعث حفاظت از داده‌ها می‌شود و در یک کلام پدافند غیرعامل باعث کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، افزایش تاب‌آوری، تسهیل در مدیریت بحران و در نهایت ارتقای پایداری ملی در همهٔ حوزه‌ها از جمله حوزهٔ سایبری و الکترونیکی می‌شود.»

چه صاحب خانه باشید چه صاحب یک کسب و کار یا مدیر یک سازمان بزرگ، بی‌تردید دارایی‌های مشهود ارزشمندی دارید که همواره در معرض تهدیدها و آسیب‌های گوناگون از جانب بزه‌کاران، سارقین و یا حتی وقایع مخرب هستند. مراقبت از دارایی‌های اینچنینی نیازمند تمهیدات و تدابیر مراقبتی و حفاظتی مناسب است که اغلب به درستی انجام نمی‌شوند و از همین رو مطمئن و اثربخش نیز نیستند.

روش‌های سنتی به کارگیری نگهبان انسانی برای پایش رخدادها و اقدام واکنشی مناسب که در بسیاری از مکان‌ها مورد استفاده قرار می‌گیرد علاوه بر کارایی پایین، هزینه بالایی نیز دارد و جمع این معایب می‌تواند یک محرک جدی برای صاحبان دارایی باشد تا در جستجوی راهکاری موثرتر و البته مقرون به صرفه‌تر باشند.

نصب و استقرار دوربین‌های مدار بسته در محل ممکن است بهترین راه‌حل به نظر آید اما تجربه نشان داده است که میزان خطای بالای متصدی پایشگری دوربین‌ها، عدم طراحی تخصصی سامانه و مکان‌یابی نادرست دوربین‌ها، نبود فرآیند دوره‌ای نگهداری و رفع خرابی‌ها، عدم امکان واکنش به رخدادها و همچنین آگاه‌سازی بهنگام نیروی انتظامی، کارآیی این روش را نیز با سوال جدی روبرو کرده است ضمن اینکه در این حالت به دلیل استقرار سامانه ضبط تصاویر در محل تحت نظارت، احتمال تخریب یا سرقت تجهیزات و عدم دسترسی به تصاویر پس از وقوع حادثه وجود دارد.

نگهبان هوشمند راهکاری نوین، پیشرفته، هوشمند و خودکار است که می‌تواند تمامی ویژگی‌های مفید هر دو راهکار پیشین را به همراه امکانات جدید در اختیار بگذارد. با نگهبان هوشمند، یک پایشگر پیرامونی ئ تمام وقت و هوشمند، مراقبت از دارایی شما را به عهده می‌گیرد. تهدیدها را رصد و در مواقع لزوم با تفاهم و همکاری نیروی انتظامی برای دفع خطر و رسیدگی به رخدادها اقدام می‌نماید. تمامی فرآیندهای حفاظتی مراقبتی در نگهبان هوشمند متناسب با موقعیت و مکان شما برپایهٔ الزامات ابلاغی توسط پلیس و چارچوب‌های استاندارد بومی امنیت اماکن و با استفاده از پیشرفته‌ترین سامانه بومی و تایید شده پایش، حفاظت و هشدار پیاده‌سازی می‌شوند. نگهبان هوشمند بسته به سناریوهای مختلف مجهز به هوش‌مصنوعی، تحلیل بیومتریک تصاویر، سنسورهای گوناگون و امکانات ارتباطی و پیام‌رسانی متنوع است.

چرا پایش و پویش هوشمند تصاویر از راه دور؟

۱. هزینه نگهبانان مستقر در محل تقریباً ده برابر بیشتر از خدمات نظارت پایش و پویش نگهبان هوشمند است.
۲. متخصصان نظارت بر پایش و پویش نگهبان هوشمند می‌توانند چندین دوربین را به طور همزمان مشاهده کنند، که امکان پوشش و نظارت بیشتری را نسبت به نگهبان در محل فراهم می کند.
۳. استفاده از به روزترین و تنها نرم افزار هوش مصنوعی بومی برای تشخیص حرکت انسان و اشیا
٤. رویدادها در چند ثانیه شناسایی، تجزیه و تحلیل و مورد بررسی قرار خواهد گرفت.
۵. نگهبان هوشمند معمولاً دارای یک سیستم رادیویی دو طرفه هست تا اطمینان حاصل شود که مجرمان می‌دانند که توسط یک شخص واقعی نظارت می‌شوند.
٦. نگهبان هوشمند برای کمک به کاهش هزینه‌ها بدون به خطر انداختن امنیت تأسیسات و امکان شما طراحی شده است.
۷. تهیه تصاویر و مستندات محکمه پسند.
۸. هماهنگی برای حضور همزمان پلیس با ورود متجاوزین به حریم خصوصی طرف قرارداد
۹. حفاظت از تصاویر به دور از محل مورد مشاهده .
۱۰. رعایت حقوق شهروندی از طریق فعال یا غیرفعال نمودن دوربین توسط مشتری طرف قرارداد .
۱۱. بهره گیری از توانایی و ظرفیت پلیس در مواقع مورد نیاز مندرج در قرارداد .
۱۲. جلوگیری یا کاهش ضریب خطا و یا تبانی نگهبان حاضر در محل .
۱۳. کاهش هزینه ها و دعوای احتمالی نگهبان حاضر از نظر بیمه ، پاداش ، سنوات و .... در مبادی مانند بیمه و مراجع قضایی و ....
١٤ . اجرای سناریوهای مناسب با محل قرارداد مانند تطبیق چهره ، حساسیت به ابزار های نامتعارف
۱۵. عقد قرارداد در سه حالت وضعیت موجود ، مطلوب و ایده آل متناسب با تجهیزات موجود یا مورد نیاز در محل قرارداد .
١٦ . ایجاد احساس امنیت و بازدارندگی در برابر مجرمین

ویژگی کارکردی نگهبان هوشمند
شرح
پایش متمرکز در پایگاه مانیتورینگ مجهز توسط پایشگر آموزش دیده
امکان مشاهده تصاویر و هشدارها به طورمستقل برای هر کاربر مجاز دیگر بدون هزینهٔ افزونه
عدم امکان سرقت یا از میان بردن تصاویر ضبط شده به دلیل ذخیره‌سازی متمرکز
ثبت و آرشیو کامل اقدامات و رویدادها به همراه امکان ارایه گزارش به مبادی ذیربط
کنترل صحت عملکرد تصاویر دوربین‌ها و هشدار فوری در صورت هرگونه خرابی به مرکز مانیتورینگ
امکان ارایه شواهد دیجیتال به مراجع قضایی در صورت بروز حادثه
حداقل هزینه ممکن پهنای باند اینترنت و اینترانت مورد نیاز انتقال تصاویر
امکان بهره‌برداری مدیریتی و بهبود عملکرد پرسنل با پایش از راه‌دور برای شرکت‌ها و سازمان‌ها
کاهش احتمال خطای انسانی پایشگر به وسیلهٔ هوش مصنوعی

ویژگی کارکردی نگهبان هوشمند		
موضوع	انسانی	هوشمند
هزینه ماهیانه (برای ۱۲ ساعت نگهبانی بدون وقفه)	۳۵ میلیون تومان	۳/۵ میلیون تومان
امکان خلع سلاح یا بیهوش کردن نگهبان	آسیب‌پذیر	مطمئن
نظارت بر عملکرد نگهبان	فاقد نظارت مداوم	نظارت همیشگی
اطلاع از عدم عملکرد یا اختلال در سامانه نظارتی	خیر	آری
مشکلات بیمه، مالیات، مرخصی، شکایت نگهبان و ...	مشکلات متعدد	فاقد مشکل
میان رفتن تصاویر ضبط شده (سرقت یا انهدام توسط مهاجم و ...)	آری	خیر
میزان پایداری و بیداری نگهبان در ۲٤ ساعت	حداکثر ٪۷۰	٪۱۰۰

تهران ■ اقدسیه ■ بلوار ارتش ■ شانزده‌متری ولیعصر ■
نبش خیابان پروین ■ پلاک ۲ ■ واحد ۴
تلفن: ۲۲۹۶۷۷۶۳، ۲۲۹۶۴۳۹۲، ۲۲۹۶۴۳۹۶ (۰۲۱) نمابر: ۲۲۹۶۷۷۶۹ (۰۲۱)

www.nhpk.ir

نگهبان هوشمند
پارس خاورمیانه

نگهبان هوشمند

مراقب هوشیار دارایی شما

سامانه مطمئن و کارآمد
با ابزاری پیشرفته، هوشمند و امن در
صحنه هوشیاریم

کارکنان آموزش دیده
ما پایشگران باتجربه را برای نظارت به کار
گرفته‌ایم

خدمات حرفه‌ای
با ابزاری پیشرفته، هوشمند و امن در
صحنه هوشیاریم۷

پایبندی به تعهد
قرارمان حفاظت از دارایی شماست، پای
آن ایستاده‌ایم

پشتیبانی شبانه‌روزی
۲۴ ساعته، ۷ روز هفته
پشتیبان شما هستیم

هستیم تا
امنیت را دوباره تعریف کنیم

تهران ■ اقدسیه ■ بلوار ارتش ■ شانزده‌متری ولیعصر ■
نبش خیابان پروین ■ پلاک ۲ ■ واحد ۴
تلفن: ۲۲۹۶۷۷۶۳، ۲۲۹۶۴۳۹۲، ۲۲۹۶۴۳۹۶ (۰۲۱) نمابر: ۲۲۹۶۷۷۶۹ (۰۲۱)

+۹۸ ۲۱-۲۲۹۴۸۸۶۸
+۹۸ ۲۱-۲۲۹۶۷۷۶۹
www.electronicsecurity.ir
info@electronicsecurity.ir