ارائه‌ی الگویی جهت ارزیابی آسیب‌پذیری امنیتی در صنعت نفت

مطالعه‌ی موردی: تأسیسات نفتی دریایی

علی جمشیدی* -کارشناس ارشد مدیریت سوانح، دانشگاه تهران، دانشکده محیط زیست، Ali.jam663@gmail.com
علی علیدوستی -کارشناس ارشد مهندسی مکانیک، دانشگاه صنعتی مالک اشتر
سعید گیوه‌چی -استادیار مدیریت سوانح، دانشگاه تهران
روزبه رجبی -دانشجوی دکتری مهندسی برق، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس

تاریخ دریافت:۱۳۹۱/۲/۲۲ | تاریخ پذیرش: ۱۳۹۱/۶/۱۵

چکیده

پس از حادثه‌ی ۱۱ سپتامبر ۲۰۰۱ میلادی در ایالات متحده، بار دیگر محافل علمی به اهمیت توجه به مخاطرات ناشی از مواد شیمیایی تأکید کردند. اگرچه در این حادثه، صنعت نفت مورد هدف قرار نگرفت، اما با این وجود، این صنعت به روشنی به‌دلیل توانایی بالقوه در ایجاد خسارات و تلفات سنگین، همواره، در معرض بحران‌های مختلف است. این تحقیق به ارزیابی آسیب‌پذیری امنیتی ناشی از سوانح انسان‌ساخت در جزایر نفتی می‌پردازد. تحقیق پیش رو، با معرفی سامانه‌ی ارزیابی آسیب‌پذیری امنیتی (سامانه‌ی جوشن) در صدد تغییر نگرش رایج درخصوص شیوه‌های ارزیابی ریسک ناشی از حملات نظامی، تروریستی و خرابکاری است. از این رو، هدف از ارزیابی ریسک امنیتی دارایی‌های جزیره، بر دو بخش: ۱. شناسایی مخاطرات امنیتی، تهدیدها و آسیب‌پذیری‌های محتمل در مواجهه با دارایی‌های هدف و ۲. اقدامات متقابل در برابر تهدیدها در جهت حفاظت از عرصه‌ی عمومی، کارگران، سرمایه‌های ملی، محیط زیست و شرکت نفت فلات قاره تقسیم می‌شود. مراحل پنج‌گانه‌ی مدل ارزیابی آسیب‌پذیری امنیتی عبارتند از: مشخصات دارایی‌ها، ارزیابی تهدید، تحلیل آسیب‌پذیری، ارزیابی ریسک و اقدامات متقابل. از سویی، در این تحقیق از نرم‌افزار بومی ارزیابی آسیب‌پذیری امنیتی (جوشن پرو) بدین منظور استفاده شده است.

واژه‌های کلیدی: جوشن، ارزیابی آسیب‌پذیری امنیتی، نرم افزار جوشن پرو، تأسیسات نفتی دریایی

A model for Security Vulnerability Assessment in the oil industry

Case study: Marine Oil Industry

Ali Jamshidi [1], Ali Alidoosti [2], Saeed Givehchi [3], Roozbeh Rajabi [4]

Abstract

After the 9.11 disaster in New York, we have become more aware of the catastrophic threats in our communities. While the 9.11 disaster was not directed toward the oil industry, oil production facilities may pose an attractive target for terrorism. This study focuses on assessing the security risk of man–made disasters for critical assets in the oil industry. This research modifies conventional risk assessment methods for including terrorism and sabotage scenarios by Joshan model. The objective of this risk assessment is to identify possible security hazards, threats and vulnerabilities facing each target asset, and to find the adequate countermeasures to protect the public, workers, national interest, environment, and companies. This model includes five steps: asset characterization, threat assessment, vulnerability analysis, risk assessment and new countermeasures. Joshan–Pro, an in–house software, is introduced for security vulnerability assessment in critical asset protection.

Keywords: Joshan, Security Risk Assessment, Joshan–Pro, Marine Oil Industry.

1 MSc in Disaster Management, Faculty of Environment, Tehran University
2 MSc in Mechanical Engineering, Malek Ashtar University of Technology
3 Assistant Professor of Disaster Management, Tehran University
4 PhD Candidate of Electrical Engineering, Faculty of Electrical Engineering, Tarbiat Modares University

مقدمه

در قرن بیست و یک میلادی، شکل جدیدی از تهدیدهای مرتبط با دارایی‌های حیاتی پدیدار گشته است. پس از حادثه‌ی ۱۱ سپتامبر سال ۲۰۰۱ میلادی در ایالات متحده، محافل علمی بار دیگر به اهمیت توجه به مخاطرات تهدیدکننده‌ی دارایی‌های حیاتی تأکید کردند. اگرچه در این حادثه، صنایع پتروشیمی و صنعت نفت مورد هدف قرار نگرفتند، اما با این وجود، این صنایع به‌دلیل توانایی بالقوه در ایجاد خسارات و تلفات سنگین و همچنین، اثرات قابل ملاحظه‌ی زیست‌محیطی، همواره در معرض بحران‌های مختلف هستند. نظر به اهمیت فراوان صنایع نفت در ایران، و احتمال تأثیرات اساسی سوانح و حوادث، به‌ویژه سوانح انسان‌ساخت، لزوم استقرار رویکرد سیستماتیکی در راستای کاهش درست‌نمایی مخاطرات محیطی در دارایی‌های واقع در واحدهای صنعتی بیش از پیش احساس می‌گردد. با توجه به سانحه‌خیزی کشور و همچنین تهدیدهای قابل ملاحظه‌ی طبیعی و غیرطبیعی، لازم است که مدیریت ریسک در برابر بحران‌ها و استراتژی‌های مدیریتی مناسب جهت کاهش آسیب‌پذیری دارایی‌ها و تأسیسات، بیشتر مورد توجه قرار گیرد.

ارزیابی ریسک امنیتی، از مباحث نوین در حیطه‌ی مدیریت ریسک است که متأسفانه تاکنون در داخل کشور مورد توجه جدی قرار نگرفته است. البته لازم به ذکر است که در خارج از کشور نیز مطالعات چندانی در زمینه‌ی ارزیابی ریسک امنیتی انجام نشده و تعداد مطالعات انجام گرفته انگشت‌شمار است. هلستروم (۲۰۰۷) یک رویکرد سیستماتیک برای تعیین آسیب‌پذیری سیستمی زیرساخت‌های حیاتی ارائه نموده است. [۱] کراگر (۲۰۰۸) به بررسی زیرساخت‌های حیاتی در معرض ریسک پرداخته و رویکردی برای انتخاب نقاط ضعف سیستم پرداخته و تعدادی از گزینه‌های سیاسی که برای بررسی‌های آینده تعیین می‌شوند را ارائه نموده است. [۲] کروتر (۲۰۰۸) با استفاده از تجزیه‌ی مدل ورودی - خروجی غیرعملی، به مدیریت ریسک انفصالی برای استراتژی‌های آماده‌ی اجرای زیرساخت‌های حیاتی پرداخته است. [۳] بایردی و دیگران (۲۰۰۹) مطالعات سلسله‌مراتبی را به‌صورت مدیریت ریسک بر پایه‌ی مدل، برای زیرساخت‌های حیاتی توسعه دادند. [۴] مارتز و جانسون مدلی را با به‌کارگیری تحلیل درخت خطا با تأکید بر ارزیابی ریسک سرقت مهمات توسط مهاجمان مسلح و میزان موفقیت سرقت‌های احتمالی، ایجاد نمودند. [۵] دیسنت مدل مشابهی را برای سامانه‌ی امنیتی زندان‌ها به‌منظور جلوگیری از فرار زندانیان طراحی کرد. با این وجود، به‌دلیل نواقص و محدودیت‌هایی که در این مدل‌ها وجود دارد، هیچ یک از مدل‌های مشابه، قابلیت تخمین خسارات در پی تهدیدهای بالقوه را به‌صورت دقیق ندارند. به‌علاوه چون مشخصات کامل تهدیدها از پیش تعیین شده است، هیچ یک از مدل‌های مذکور، توانایی پاسخ به تهدیدهای جدید را نخواهند داشت. [۶] گویکما مدلی نسبتاً کاراتر در قیاس با مدل‌های دیگر معرفی می‌نماید. این مدل به‌منظور تخمین ریسک تهدیدهای احتمالی در برابر تروریسم ایجاد گردیده است. مطابق با این مدل، ممکن است اهمیت یک سناریو با گذشت زمان تغییر نموده و میزان جذابیت آن برای مخاطرات و تهدیدهای احتمالی افزایش و یا کاهش یابد. لذا به‌نظر می‌رسد که این مدل توانایی واکنش مناسب در مواجهه با تهدیدهای تروریستی را داشته باشد. با این وجود، چون در این مدل اطلاعات و مشخصات تهدید در طراحی سناریو مدنظر قرار می‌گیرد، در صورت نبود اطلاعات کافی امکان بهره‌گیری از سناریوها میسر نخواهد بود. [۷] کیم و همکاران سامانه‌ی نرم‌افزاری را مبتنی بر روش ارزیابی آسیب‌پذیری امنیتی ارائه شده توسط مؤسسه‌ی نفت ایالات متحده‌ی آمریکا تولید نموده‌اند. [۸] باجپای و گوپتا نیز در یک مجموعه پژوهش، مدلی نوین به‌منظور ارزیابی ریسک امنیتی ارائه داده‌اند که مشتمل بر دو ایده‌ی جدول فاکتور ریسک امنیتی "SRFT" و روش ماتریس گام به گام "SMP" است. در این شیوه، متخصصان پیش از ارزیابی دقیق ریسک امنیتی در یک منطقه، اقدام به تحلیل وضعیت امنیتی محل با استفاده از فاکتورهای استاندارد و از پیش تعیین‌شده می‌نمایند و بر پایه‌ی نمرات کسب‌شده از فاکتورها، مشخص می‌گردد که آیا محل به ارزیابی با جزئیات ریسک امنیتی نیاز دارد یا خیر. سپس با بهره‌گیری از شیوه‌ی (SMP) اقدامات مناسب در برابر تهدیدها تعیین می‌گردند. [۹، ۱۰، ۱۱، ۱۲]

فاکتور ریسک	دامنه‌ی نمرات ریسک				نمرات واقعی
موقعیت	تراکم بالا ۵	شهری ۲،۳،۴	روستایی ۱		.....
توانایی دید	بالا ۵	متوسط ۳،۴	پایین ۱،۲	عدم دید ۰	.....
موجودی	بسیار بالا ۵	بالا ۳،۴	متوسط ۲	پایین ۱	.....
مالکیت	دولتی ۴،۵	عمومی ۲،۳	خصوصی ۱		.....
پیشینه تروریسم در منطقه	زیاد ۴،۵	به ندرت ۱،۲،۳	عدم وجود ۰		.....
اقدامات امنیتی موجود	ضعیف ۴،۵	معمولی ۲،۳	سطح بالا ۱		.....
کنترل دسترسی	ضعیف ۴،۵	معمولی ۲،۳	سطح بالا ۱		.....
پشتیبانی محیطی	ضعیف ۴،۵	معمولی ۲،۳	سطح بالا ۱		.....
کاهش اثر مخاطرات	ضعیف ۴،۵	معمولی ۲،۳	سطح بالا ۱		.....
روشنایی مطلوب	ضعیف ۴،۵	معمولی ۲،۳	سطح بالا ۱		.....
آموزش و آمادگی شخصی	ضعیف ۴،۵	آمادگی متوسط ۲،۳	آمادگی خوب ۱		.....
مجموع (نمره‌ی ریسک واقعی)					

جدول شماره‌ی ۱: فاکتور ریسک امنیتی

در مقاله‌ی پیش رو الگوی بومی ارزیابی آسیب‌پذیری امنیتی (جوشن) و نرم‌افزاری که بدین منظور طراحی و تهیه شده، تحت عنوان جوشن پرو، ارائه شده است. لذا در این مطالعه در بخش نخست به لزوم پیش غربال‌گری امنیتی پرداخته شده، سپس الگوی جوشن معرفی می‌شود. همچنین، در بخش بعدی، جزیره‌ی مورد مطالعه به‌عنوان مطالعه‌ی موردی بررسی شده و در انتها، با استفاده از نرم‌افزار جوشن اقدام به ارزیابی آسیب‌پذیری امنیتی می‌شود.

پیش غربال‌گری با استفاده از جدول فاکتور ریسک امنیتی (SRFT)

وضعیت موجود ریسک امنیتی یک سایت صنعتی را می‌توان با استفاده از جدول فاکتور ریسک امنیتی (SRFT) ارزیابی نمود. این جدول ابزاری به‌منظور سنجش این مهم است که آیا دارایی مورد نظر نیاز به تحلیل آسیب‌پذیری و ارزیابی تهدید دارد و یا خیر. بدین منظور، تمامی فاکتورهای ریسکی که بر دارایی‌های حیاتی تأثیر می‌گذارند، از صفر (پایین‌ترین ریسک) تا پنج (بالاترین ریسک) رتبه‌بندی می‌شوند. این رتبه‌بندی بنا بر قضاوت خبرگان انجام می‌شود. مجموع امتیازهای کسب‌شده از SRFT در ارزیابی ریسک امنیتی دارایی‌ها که در جدول شماره ۱ تشریح گشته است، استفاده می‌گردد. مطابق با جدول شماره‌ی ۲، چنانچه مجموع نمرات کسب‌شده بیشتر از نمره‌ی ۳۰ گردد، تحلیل تفصیلی آسیب‌پذیری و تهدید ضروری است. [۱۳]

وضعیت ریسک امنیتی موجود	نمره ریسک واقعی
پایین	<۱۵
متوسط	۱۶-۳۰
بالا	۳۱-۴۵
خیلی بالا	۴۵>

جدول شماره‌ی ۲: فاکتور ریسک امنیتی

سامانه‌ی جوشن

سامانه‌ی جوشن، الگویی جامع است که به‌منظور پیاده‌سازی و اجرای ارزیابی ریسک امنیتی برای زیرساخت‌ها و دارایی‌های حیاتی بسط یافته است. مبنای این الگو، روش‌شناسی (SVA) است، که در سال ۲۰۰۳ توسط مؤسسه‌ی نفت ایالات متحده (API) ارائه شده است. سامانه‌ی جوشن دارای رویکردی سیستماتیک است که از قابلیت ترکیب دانش‌ها و مهارت‌های چندگانه به‌منظور تحلیل آسیب‌پذیری جامعِ تأسیسات و دارایی‌ها برخوردار است. همچنین این مدل، ابزاری مدیریتی در دست مدیران بحران در جهت تصمیم‌گیری برای بررسی شیوه‌های اقدام متقابل در مواجهه با تهدیدها و آسیب‌پذیری‌های احتمالی است. در این روش، ارزیابی ریسک دارایی‌ها در صنایع براساس تحلیل آسیب‌پذیری تأسیسات و دارایی‌های منطقه مورد مطالعه انجام می‌گیرد. بنابراین، از این روش می‌توان به‌منظور تخمین میزان آسیب‌پذیری دارایی‌های حیاتی و همچنین بررسی سناریوهای ریسک استفاده نمود. علاوه بر این، پیامدهای سناریوها نیز در این روش در نظر گرفته می‌شوند و سطوح ریسک با استفاده از معیارهایی به‌صورت کمی ارائه می‌گردند. ارزیابی آسیب‌پذیری امنیتی مبتنی بر سامانه‌ی جوشن، شامل مراحل زیر است:

- دارایی‌شناسی: هدف از این مرحله، شناسایی دارایی‌های حساس است. منظور از دارایی‌های حساس، آن دسته از دارایی‌ها است که نیاز به مقاوم‌سازی امنیتی در برابر تهدیدهای بالقوه دارند.
- ارزیابی تهدید: شناسایی و تعیین تهدیدهای بالقوه و ارزیابی دارایی‌ها برحسب میزان جذابیت آن‌ها و همچنین سنجش پیامد احتمالی در صورت موفقیت‌آمیز بودن تهدیدها در این مرحله صورت می‌پذیرد.
- ارزیابی آسیب‌پذیری: شناسایی آسیب‌پذیری‌های امنیتی بالقوه که دارایی‌های حیاتی را تهدید می‌نماید.
- ارزیابی ریسک امنیتی: در این مرحله، ریسک مربوط به هر تهدید بنا بر درست‌نمایی تحقق آن‌ها و پیامد ناشی از رویدادشان تعیین می‌گردد. پس از تعیین ریسک مربوط به هر تهدید، ریسک‌ها رتبه‌بندی شده و چنانچه مقدار ریسک محاسبه شده بالا باشد، توصیه‌هایی به‌منظور پایین آوردن ریسک ارائه می‌گردد.
- ارائه‌ی پیشنهادها: پس از محاسبه و رتبه‌بندی ریسک، گزینه‌های موجود به‌منظور شناسایی و ارزش‌یابی شیوه‌های کاهش اثر ریسک اتخاذ می‌شود. همچنین در صورت نیاز، در اقدامات متقابل نیز تجدیدنظر می‌گردد.

رویکرد کلی سامانهٔ جوشن، استفاده از ارزیابی ریسک و نهایتاً اعمال اقدامات امنیتی ویژه بر پایه‌ی نتایج حاصل از بررسی‌ها و ارزیابی پیامدها است. در این روش تجهیزات هم از نظر کلی و هم از نقطه‌نظر رویژه مورد ملاحظه قرار می‌گیرند.

در سطح عمومی مواردی همچون تعیین اثرات و پیامدهای کلی خسارات، زیرساخت‌ها و وابستگی‌های متقابل آن‌ها و در سطح خود دارایی و محیط پیرامون، امنیت فیزیکی عمومی و کنترل دسترسی‌ها مورد ملاحظه قرار می‌گیرد. به‌عنوان مثال برای همه‌ی تجهیزات یک سطح حداقل امنیتی با اقدامات کلی مثل روش‌های کنترل دسترسی به تجهیزات و کنترل‌های اداری وجود دارد؛ اما در مورد دارایی‌های ویژه باید اقدامات امنیتی بیشتری همانند اعمال نظارت یا موانع بیشتر که براساس ارزش‌ها و سطح اهمیت آن برای دشمن تعیین شده است، در نظر گرفت. فایدهٔ ارزیابی ویژه‌ی دارایی‌ها این است که یک درجه‌ی ریسک خاص و منحصر به فرد برای هر دارایی به دست می‌آید و با توجه به عدد ریسک، اقداماتی علاوه بر اقدامات موجود برای آن در نظر گرفته می‌شود. [۱۵]

اعضای کارگروه تخصصی سامانه‌ی جوشن باید از مواردی همچون کلیت تجهیزات، اجزای هر کدام از تجهیزات، عملکردهای حیاتی هر کدام از تجهیزات، خطرات و پیامدهایی که در صورت به خطر افتادن دارایی‌ها یا عملکردهای حیاتی تجهیزات به وجود می‌آید، اطلاع داشته باشند.

حیاتی بودن تجهیزات و دارایی‌ها هم به میزان تأثیر بالقوه‌ی آن روی افراد سازمان، جامعه و محیط زیست و هم به اهمیت عملکرد آن برای سازمان یا صنایع بستگی دارد. به‌عنوان نمونه یک تانکر ذخیره‌سازی مواد شیمیایی یا یک انبار نگهداری مواد منفجره ممکن است حیاتی‌ترین بخش فرآیند عملیاتی را تشکیل ندهد اما اگر مورد حمله واقع شود، می‌تواند پیامدهای مختلفی را به همراه داشته باشد. لذا ممکن است از اولویت بالایی برای انجام تحلیل‌های بیشتر و اقدامات امنیتی ویژه برخوردار شوند. بنابراین لازم است دارایی‌های موجود در سازمان یا صنعت از نقطه‌نظر میزان اهمیت مورد بررسی قرار گیرند تا حیاتی‌ترین آن‌ها از نظر تهدیدات، شناخته شود. دشمنان ممکن است اهداف مختلفی داشته باشند، لذا سرمایه‌های حیاتی از دید هر دشمن به‌صورت مجزا مورد بررسی قرار گرفته و درجه‌ی جذابیت هر سرمایه به‌دست می‌آید. این روند در واقع یک مقیاس مناسب جهت تشخیص این موضوع است که آیا این دارایی‌ها از نظر دشمن ارزش کشف شدن، ویران شدن یا به سرقت رفتن را دارا هستند یا خیر.

اگر یک سرمایه هم حیاتی بوده (از نظر ارزش و پیامد) و هم برای دشمن جذاب باشد به‌عنوان یک هدف در سامانه‌ی جوشن مورد تحلیل‌های امنیتی بیشتری قرار گرفته و سناریوهای وسیع‌تری به‌منظور شناسایی آسیب‌پذیری‌های آن بررسی می‌شوند. در سامانه‌ی جوشن، همه‌ی دارایی‌ها حداقل یک‌بار مورد بررسی کلی قرار می‌گیرند. این عمل از طریق ملاحظات امنیتی که از قبل در چک‌لیست‌هایی متناسب با ساختمان، تجهیزات زیربنایی و امنیتی، نوع فعالیت‌ها، تهدیدات و موارد دیگر گردآوری شده است، انجام می‌شود.

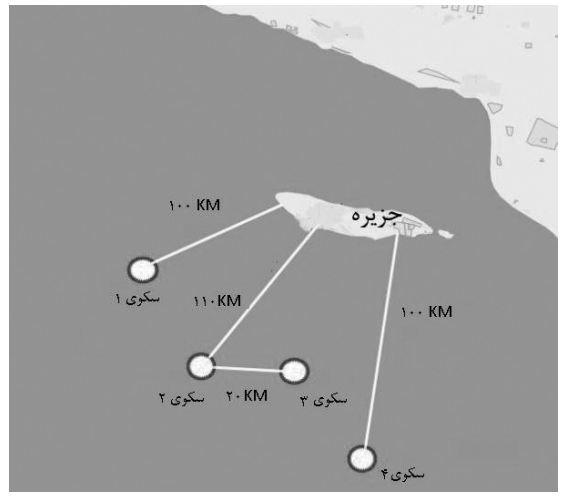
نکته‌ی حائز اهمیت در این میان آن است که باید بین مدیریت ریسک امنیتی و ارزیابی ریسک امنیتی، تفاوت قائل بود. به بیان دیگر، می‌توان گفت مدیریت ریسک امنیتی چارچوبی مدیریتی شامل سامانه‌ی ارزیابی آسیب‌پذیری امنیتی در جهت توسعه و اجرای طرح‌های امنیتی و درخواست اقدامات مورد نیاز جهت بهبود سطح امنیتی است. اما سامانه‌ی جوشن شامل برآورد ریسک امنیتی هر کدام از تجهیزات با هدف تصمیم‌گیری و مدیریت ریسک است. از این رو، سامانه‌ی ارزیابی آسیب‌پذیری امنیتی (جوشن) دارای ویژگی‌های زیر است: [۱۴، ۱۵]

- قابلیت بازخورد: سامانه‌ی جوشن یک فرآیند تکرار شونده است. تمرین‌ها، بازرسی‌ها و جمع‌آوری داده‌ها از منابع داخلی و خارجی در جهت تأیید یا رد فرضیات، استفاده می‌شود.
- ریسک‌محور: در این روش باید بیشترین توجه روی نقاط امنیتی مشخصی باشد که پایه‌ی ارزیابی ریسک هستند. ریسک همچنین می‌تواند جهت بررسی کفایت اقدامات موجود استفاده گردد.
- نظام‌مند: اساس و ساختار این روش به گونه‌ای است که در آن یک ارزیابی دقیق صورت می‌گیرد ضمن اینکه این روش از انعطاف‌پذیری خوبی برخوردار است و از آنجا که استفاده از ساختارهای انعطاف‌پذیر آسان‌تر است، باید بیشتر از اطلاعات مربوط به تخصص و تجربهٔ افراد کار گروه تخصصی استفاده کرد. اما در همهٔ روش‌ها از اعداد و ارقام جهت تعیین ریسک که تحت تأثیر احتمال و پیامد است استفاده می‌شود.
- متکی بر منابع کافی: افراد شایسته، زمان کافی و منابع مالی با توجه به سطح ارزیابی پروژه باید اختصاص داده شود.
- تجربه‌محور: تکرار و شدت حوادث امنیتی گذشته و امکان وقوع آن‌ها در آینده، مورد توجه قرار می‌گیرد. در این روش اطلاعات به‌دست آمده توسط مهندسین، تجربه عملیاتی و کارشناسان خبره‌ی بیرون از سازمان، مورد توجه است.
- پیش‌گویانه: در سامانهٔ جوشن، با بررسی و تحقیق، تهدیدات شناخته شده و شناخته نشده‌ای که تجهیزات با آن‌ها روبه‌رو هستند، شناسایی می‌شوند و بدین منظور باید از حوادث گذشته استفاده کرد. اما تمرکز اصلی روی امکان وقوع حوادث در آینده است. از جمله احتمال وقوع سناریوهایی که ممکن است هرگز قبلاً رخ نداده باشند.
- مبتنی بر اطلاعات کارآمد: از آنجا که بسیاری از تصمیم‌های این روش، بر مبنای خرد جمعی هستند، باید داده‌های مربوط به تجهیزات تحت بررسی، مورد اطمینان باشند.

مطالعه‌ی موردی

تأسیسات نفتی مورد نظر در اطراف یک جزیره که از خشکی فاصله دارد قرار گرفته است. این جزیره با طول تقریبی ۲۰ کیلومتر و عرض حداکثر ۱۵ کیلومتر دارای مساحتی بالغ بر ۸۰۰ کیلومتر مربع است که در حدود ۶۰ کیلومتر مربع از قسمت غیرمسکونی و نیمه‌سنگی جزیره در تصرف شرکت‌های نفتی است. این منطقه از تولیدی به میزان ۱۵۰ هزار بشکه در روز برخوردار است. این منطقه به‌عنوان یک منطقه‌ی نفتی و گازی با شتاب خوبی در حال افزایش تولید است. بالغ بر ۵ میلیون بشکه نفت ذخیره در این میدان وجود دارد که توسط شناور به مقاصد تعیین شده حمل می‌شود. بخشی از نفت خام تولیدی این میدان نیز برای تأمین خوراک پالایشگاه به میزان ۳۵ هزار بشکه در روز ارسال می‌شود. به‌منظور توسعه‌ی میادین نفتی و گازی این منطقه، سه دکل حفاری مستقر شده‌اند. [۱۶]

این منطقه‌ی نفتی شامل سکوهای مجتمع گازی یک الی چهار است. در شرقی‌ترین بخش جزیره، اسکله‌ی خاکی متعلق به شرکت نفت و انبارهای آن قرار دارد و بعد از آن، منطقه‌ی مسکونی آلفا، منطقه‌ی صنعتی آلفا، منطقه‌ی صنعتی بتا و منطقه‌ی مسکونی بتا تا غرب جزیره کشیده شده‌اند. میدان‌های نفتی ۳ و ۴ با حداکثر ظرفیت (۱۵ هزار بشکه نفت در روز) مشغول تولید نفت خام هستند و نفت تولیدی آن‌ها به وسیله‌ی خط لوله‌ی ۱۸ اینچی به طول ۹۸ کیلومتر برای فرآورش به جزیره منتقل می‌شود. تصویر شماره‌ی ۱ نمایی از منطقه به همراه میادین نفتی را نشان می‌دهد. [۱۷]



تصویر شماره‌ی ۱: منطقه‌ی نفتی مورد نظر

اجرای الگو در جزیره

ارزیابی ریسک تهدیدهای بالقوه در جزیره، این نیاز که آیا دارایی‌های موجود در سایت‌ها نیاز به تجدیدنظر درخصوص افزایش توان مقابله با این تهدیدها را دارند یا نه مرتفع می‌سازد. از سویی، با توجه به دامنه‌ی مطالعات و فعالیت‌های منطقه‌ی نفتی مورد نظر، استخراج و فرآوری، لزوم محدود ساختن مورد مطالعاتی به‌منظور ارزیابی کارآمد ریسک امنیتی، از اهمیت فراوانی برخوردار است. بنابراین پژوهش حاضر، حوزه‌ی مطالعات خود را به جزیره محدود نموده و مشخصاً از ملاحظه‌ی سکوهای نفتی و گازی منطقه در تحقیق، خودداری نموده است. با استفاده از نظر خبرگان، فاکتورهای ریسک در نرم‌افزار جوشن پرو امتیازدهی شده‌اند. مطابق با محاسبات نرم‌افزار جوشن، عدد ۳۴ به‌عنوان فاکتور کلی ریسک امنیتی جزیره به‌دست می‌آید. لذا براساس استاندارد تبیین شده در جدول شماره‌ی ۲، ارزیابی آسیب‌پذیری امنیتی در جزیره، از اهمیت "بالا" برخوردار است. در این بخش ارزیابی ریسک دارایی‌های حیاتی جزیره مورد نظر است. این جزیره با توجه به امتیاز فاکتورهای ایجاد در مدل "SRFT" نیاز به ارزیابی دقیق ریسک دارایی‌ها دارد. از این رو، فرم‌های چهارگانه‌ای توسط نرم‌افزار جوشن اجرا شده تا آسیب‌پذیری هر کدام از دارایی‌ها سنجیده شود. این فرم‌ها عبارتند از:

- فرم تعیین دارایی‌های حیاتی
- فرم ارزیابی تهدید
- فرم تعیین جذابیت هدف

فرم انتهایی که به‌منزله‌ی فرم نتایج است، شامل نتایج تحلیل آسیب‌پذیری/ اقدامات مقابله است. نخست فرم دارایی‌های حیاتی توسط نرم‌افزار تولید می‌شود، سپس تهدیدهای بالقوه‌ی جزیره تعیین و رتبه‌بندی می‌شوند.

براساس دارایی‌ها و تهدیدهای تعیین‌شده در فرم‌های پیشین، آسیب‌پذیری امنیتی در هر یک از دارایی‌ها/ تأسیسات همانند تصویر شماره‌ی ۲ آنالیز می‌شود.

به‌منظور محاسبه‌ی ریسک در الگوی جوشن، از رابطه‌ی ۱ استفاده می‌گردد:

$$R = T \times V \times C$$

که در آن به ترتیب T به رتبه‌ی تهدید، V آسیب‌پذیری و C پیامد ناشی از هر سناریوی تهدید قلمداد می‌شود. لازم به ذکر است که محاسبه‌ی آسیب‌پذیری به دو بخش سازه‌ای و فرآیندی دسته‌بندی می‌شود. آسیب‌پذیری فرآیندی با استفاده از ابزار چک‌لیست و آسیب‌پذیری سازه‌ای با استفاده از شبیه‌سازی به‌دست می‌آید.

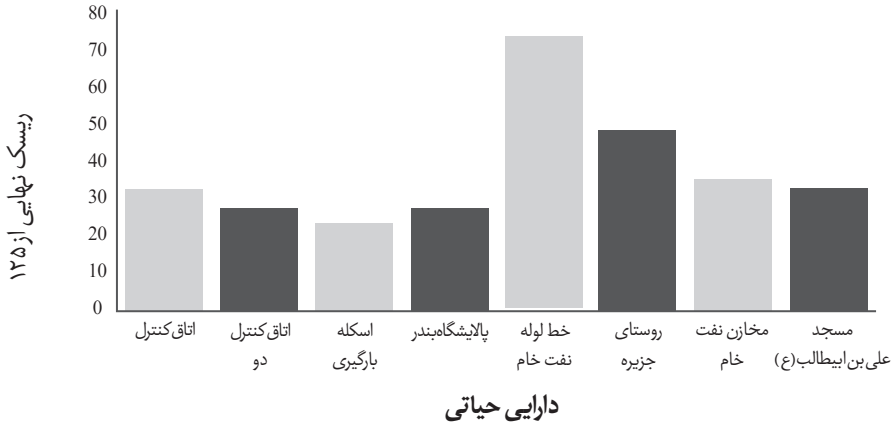
براساس میزان ریسک امنیتی به‌دست آمده در فرم آنالیز آسیب پذیری، اقدامات پیشنهادی و مدیریت اجرای هر کدام در فرمی بدین نام، تهیه می‌شود. همچنین نرم‌افزار جوشن پرو علاوه بر ترسیم نمودار ریسک پدافندی همانند آنچه در تصویر شماره‌ی ۲ آمده، به تفکیک دارایی‌های بحرانی، قادر است با استفاده از فرآیند تحلیل سود و هزینه، اقدام به بررسی هزینه‌های هر یک از اقدامات در دارایی‌های بحرانی نماید.

نتیجه‌گیری

این تاسیسات دریایی با کسب امتیاز ۳۴ دارای آسیب‌پذیری امنیتی بالا در برابر تهدیدهای محتمل است. لذا استقرار سامانه‌ی ارزیابی ریسک تهدیدها با ملاحظه‌ی دارایی‌های حیاتی و ارائه برنامه‌ی از پیش تعیین‌شده برای دارایی‌های مورد مطالعه الزامی است.

با توجه به اینکه خروجی الگوی ارائه‌شده در این تحقیق مشتمل بر شناسایی آسیب‌پذیری‌های امنیتی هر کدام از دارایی‌ها و ارائه‌ی شیوه‌های مقابله به مثل است، با استفاده از ماتریس ریسک، سطح ریسک هر یک از حوادث امنیتی مفروض و شیوه‌های پیشنهادی مقابله با تهدیدها ایجاد گشته‌اند. شایان ذکر است که طبق سامانه، ماکزیمم مقادیر پیامدهای انسانی، زیست‌محیطی، فیزیکی و اقتصادی به‌عنوان اندازه‌ی پیامد بیان می‌شود. نتایج حاصل شده در فرم‌های موسوم به " فرم نتایج تحلیل آسیب‌پذیری/ اقدامات مقابله" قابل مشاهده است. همان‌طور که در فرم نیز نمایان است، چنانچه سناریوی مورد بررسی بر پایه‌ی حادثه‌ی امنیتی خسارت به تأسیسات آلفا پی‌ریزی گردد، مخازن یک میلیون و پانصد هزار بشکه‌ای نفت خام با ریسک نهایی ۴ مواجه خواهند شد. این ریسک بنابر ماتریس ریسک در ریسک بالا دسته‌بندی شده است. اقدامات متقابل پیشنهادی در این سناریو، شامل به‌کارگیری شیوه‌های استتار و اختفا به‌ویژه در تأسیسات آلفا، استفاده از دیتکتورهای حملات هوایی، افزایش استحکام بدنه‌ی مخازن در برابر حملات موشکی، تغییر در برنامه‌ی زمانی فعالیت تأسیسات آلفا (در صورت امکان) است.

اگر سناریوی مورد بررسی مبتنی بر حادثه‌ی امنیتی خسارت به دارایی‌های مجاور تبیین شود، اسکله‌ی بارگیری واجد ریسک ۳ شده و دارای ریسک متوسط است. در این صورت، محققان این مقاله اقدامات بهبود یافته‌ی افزایش تجهیزات حفاظت دریایی (قایق‌های تندرو، گشت‌های شبانه و ...)، بازنگری در سیستم‌های رادیویی و دیسپچینگ، ایجاد سیستم هشدار اولیه متصل به شبکه‌ی ارتباطی و گسترش شبکه‌ی اطلاعاتی بین حراست محل با حراست منطقه را پیشنهاد می‌نمایند. خطوط نفت خام نیز



تصویر شماره‌ی ۲: ریسک نهایی هر یک از دارایی‌ها

براساس سناریوی خسارت و افت عملکرد دارایی‌ها، دارایی ریسک ۳ (ریسک متوسط) را تجربه می‌نماید. اقدامات پیشنهادی مشتمل بر استقرار کنترل امنیت کارکنان، ارتقای استانداردهای تضمین امنیت اطلاعات، افزایش دیتکتورهای حریم فیزیکی، پایش توسط دوربین‌های CCTV، استقرار شیوه‌های نوین "حفاظت در عمق" همانند بازرسی تصادفی وسایل نقلیه‌ی ورودی به حریم لوله‌ها و بهبود سیستم روشنایی در شب در مسیر است. در انتها نیز، پالایشگاه بنا بر نظر خبرگان، با بیشترین ریسک ممکن مواجه شده و امتیاز ۵ را دریافت می‌نماید. ارائه‌ی اقدامات پیشنهادی درخصوص پالایشگاه قابل گسترش بوده و به توسعه‌ی زیرساخت‌های پدافندی در منطقه وابسته است. لذا نگارندگان مهم‌ترین اقدام‌ها را بهبود سیستم‌های نورپردازی، کنترل دسترسی، پایش به‌وسیلهٔ دوربین‌های مداربسته، استقرار سامانه‌ی موشکی پیشرفته در برابر حملات غافلگیرکننده‌ی شبانه، ایجاد سامانه‌ی استتار و اختفا به‌ویژه پیرامون مخازن، اتاق کنترل و برج تقطیر و ارتقای سامانه‌های امنیت اطلاعات در پالایشگاه می‌دانند.

پیشنهادها و جهت‌گیری‌های آینده

روش‌های مورد استفاده در کشور به‌منظور ارزیابی ریسک صنایع، بر پایه‌ی اصول ایمنی دارایی‌ها، تأسیسات و زیرساخت‌ها طراحی شده است. اساس این اصول مبتنی بر دو معیار: ۱: خطای سیستم (طبیعت) و ۲: خطای انسانی است. این در حالی است که همواره هوش انسانی در رفتارشناسی مخاطرات محیطی در این روش‌ها نادیده گرفته شده است. با توجه به شرایط استراتژیک کشور و ژئوپولیتیک منطقه، گسترش حوزه‌ی پدافند غیرعامل و نیاز مبرم به بررسی سوانح انسان‌ساخت در دارایی‌ها و زیرساخت‌ها، ملاحظه‌ی الگوها و مدل‌های ارائه‌شده در این زمینه بیش از پیش احساس می‌شود.

الگوی ارائه شده در این مقاله در صدد بررسی تهدیدها و آسیب‌پذیری‌های محتمل در صنعت نفت بر پایه‌ی ارزیابی ریسک دارایی‌های حیاتی جزیره است. محقق در این تحقیق از شیوه‌ی کیفی در محاسبه‌ی ریسک امنیتی بهره جسته است اما با این وجود امکان استفاده از روش‌های کمی در محاسبه‌ی ریسک وجود داشته است. استفاده از شیوه‌های کمی در تهدیدهای انسان‌ساخت با دشواری‌های بیشتری در قیاس با سوانح طبیعی و تکنولوژیک همراه است چرا که بررسی رفتار انسانی در ملاحظات محاسبه‌ی ریسک نه چندان ساده به نظر می‌رسد. با این حال، به‌کارگیری الگوهای کمی به میانجی مدل‌های احتمالاتی (در قیاس با مدل‌های تعینی و الگوریتم‌های تصادفی) به‌ویژه در این تحقیق که بدترین حالت سناریو (Worst scenario) دارای احتمال ناچیزی است و کارایی برنامه در حالت متوسط (Average case) سنجیده می‌شود از اهمیت زیادی برخوردار است.

از این رو، به دلیل پیچیدگی و عدم شناخت کامل از رفتار تهدیدها، پیشنهاد می‌گردد مدل‌سازی تهدیدها همواره با فرضیاتی واقعی از تجارب سوانح گذشته همراه باشد تا فرآیند محاسبه‌ی ریسک و تحلیل آسیب‌پذیری با دقت بیشتری همراه شود. همچنین استفاده از روش‌های تحلیل سود- هزینه (CBA) در اتخاذ بهترین اقدام متقابل از بین اقدامات پیشنهادی را می‌توان یکی از مهم‌ترین فعالیت‌های تحقیقاتی آینده در این راستا دانست.

منابع و مآخذ

1. Hellstrom, T., "Critical infrastructure and systemic vulnerability: Towards a planning framework", Safety Science, 2007, 45(3), 415-430.

2. Kroger, W., "Critical infrastructures at risk: A need for a new conceptualapproach and extended analytical tools", Reliability Engineering and System Safety, 2008, 93(12), 1781-1787.

3. Crowther, K.G., "Decentralized risk management for strategic preparedness of critical infrastructure through decomposition of the inoperability input-output model", International Journal of Critical Infrastructure Protection, 2008, 1, 53-67.

4.Baiardi, F., Telmon, C., and Sgandurra, D., Modeling and Managing Risk in Billing Infrastructures, 3nd International Conference on Critical Infrastructure Protection, Boston, USA, 2009.

5.Matalucci, R. V., Risk assessment methodology for dams (RAM-D, Proceedings of the 6th International Conference on Probabilistic Safety Assessment and Management, San Juan,), USA, 2002.

6.Hoffman, B., Inside Terrorism, Columbia University Press, New York, 1998.

7.Grabo, M., Anticipating Surprise: Analysis for Strategic Warning, Washington, DC, Joint Military Intelligence College, 2002.
8.Kim, J., Lee, Y. and Kim, J., "Development of a risk assessment program for chemical terrorism", Korean J. Chem. Eng , 2010, 27(2), 399-408.
9.Bajpai, S., Gupta, J.P., "Securing oil and gas infrastructure", J. Pet. Sci. Eng. 2007, 55,174-186.
10.Bajpai, S., Gupta, J.P., Protecting chemical plants from terrorist attacks, 2005, Chem.Weekly L34.
11.Bajpai, S., Gupta, J.P., Site security for chemical process industries, J. Loss Prev.Process. 2005, Ind. 18.
12.Bajpai, S., Sachdeva, A. and Gupta, J.P., Security risk assessment: Applying the concepts of fuzzy logic, Journal of Hazardous Materials 173, 2010, 258-264.
13.Bajpai, S., Gupta, J. P., "Terror-Proofing chemical process industries", Process Safety and Environmental Protection, 2007, 85 (B6), 559-565.
14.Moore, D., Fuller, B., Hazzan, M., Jones, W., "Development of a security vulnerability assessment process for the RAMCAP chemical sector", Journal of Hazardous Materials, 2007,142, 689-694.
15.American Petroleum Institute, Security vulnerability assessment Methodology for the pertroleum and petrochemicael industries, API Publishing Services, 2nd, Washington, USA, 2004.
16. www.iooc.co.ir.
17. www.salmancomplex.blogfa.com.