نشریه علمی پدافند غیرعامل

سال سیزدهم، شماره ۳، پاییز ۱۴۰۱، (پیاپی ۵۱): صص ۴۴-۳۷

علمی- پژوهشی

ارزیابی ریسک در پست‌های برق در برابر عملیات خرابکارانه از منظر پدافند غیرعامل و ارائه راهکارهای مقابله با آن (مطالعه موردی پست فشارقوی ۴۰۰ کیلوولت)

یاسر مرتضائی*[۱]

تاریخ دریافت: ۱۴۰۰/۱۰/۱۰
تاریخ پذیرش: ۱۴۰۱/۰۵/۲۲

چکیده

یکی از زیر ساخت‌های ملی و حیاتی هر کشوری شبکه برق آن کشور می‌باشد. آسیب‌پذیری در پست‌های برق که به‌عنوان شاهرگ اصلی در چرخه تولید، انتقال و توزیع برق می‌باشند صدمات جبران ناپذیری را به دنبال خواهد داشت. یکی از منافذ ایجاد بحران، عملیات خرابکارانه بر روی پست‌های برق می‌باشد که در این صورت موجب نارضایتی عمومی، بروز بحران‌های اقتصادی و اجتماعی و حتی سیاسی و... در سطح وسیعی خواهد شد. یکی از اهداف استراتژیک پدافند غیرعامل، کاهش آسیب‌پذیری و استمرار فعالیت مراکز حیاتی و حساس کشور در مقابل اقدامات دشمن می‌باشد. در این میان دفاع غیرعامل به‌عنوان یکی از مؤثرترین و پایدارترین روش‌های دفاع در مقابل تهدیدات شناخته شده است. هدف از این تحقیق ارزیابی ریسک در پست‌های برق در برابر عملیات خرابکارانه از منظر پدافند غیرعامل و ارائه راهکارهای مقابله با آن می‌باشد. پست برق ۴۰۰ کیلوولت با قرارگیری در رده پست‌های مهم و حساس یکی از مطلوب‌ترین اهداف جهت نیل به این هدف می‌باشد. بدین منظور در این مقاله به بررسی تعدادی از تهدیدات محتمل برای پست پرداخته و تجهیزات از این نظر ارزیابی شده‌اند. در ارزیابی انجام شده ریسک نهایی تهدید خرابکارانه به ترتیب، اتوترانسفورماتور درجه ریسک بالا و ترانسفورماتور، ریسک متوسط و بریکر، اتاق فرمان درجه ریسک متوسط رو به بالا را به خود اختصاص داده‌اند. در این تحقیق از متدولوژی RAMCAP (رمکپ) به‌عنوان چهارچوب تحقیق در ارزیابی ریسک استفاده شده است. با توجه به ماهیت شبکه‌ای زیرساخت مورد مطالعه، از ساختارهای شبکه‌ای جهت تجزیه و تحلیل اطلاعات استفاده شده و از روش تصمیم‌گیری چند معیاره به روش ANP و نرم‌افزار Super Decisions جهت تحلیل بهره گرفته شده است.

کلید واژه‌ها: ارزیابی ریسک، پست برق، عملیات خرابکارانه، ANP

[۱] کارشناسی ارشد مدیریت بحران، دانشگاه صنعتی مالک اشتر، تهران، ایران- mrz893020@gmail.com

۱- مقدمه

صنعت برق، هر لحظه با زندگی همه شهروندان سروکار دارد، حتی چند لحظه قطعی برق ممکن است سلامت و امنیت شهروندان را به خطر اندازد و یا خسارت سنگینی به زندگی آن‌ها وارد کند. در جوامع کنونی، قطع برق زودتر از هر مشکل دیگری احساس می‌شود و بیشتر از هر کمبود دیگری می‌تواند خطر آفرین باشد. چرا که علاوه بر متوقف شدن بیشتر فعالیت‌های روزمره از جمله فعالیت‌های صنعتی، تجاری و اقتصادی و وارد کردن خسارت سنگین در این حوزه‌ها، می‌تواند امنیت اجتماعی جامعه را نیز به مخاطره بیاندازد [۱]. خاموشی برق می‌تواند در بخش‌های مختلف مانند بهداشت و درمان، حمل و نقل زندگی روزمره، خطرات قطع برق وسایل برقی، صنایع، ادارات، مراکز خدماتی و تجاری، کشاورزی، سامانه‌های مخابراتی، تخریب وسایل منزل اختلال ایجاد کرده و حتی به‌صورت زنجیره‌ای منجر به قطع آب و گاز شهری شود [۲]. بنابراین می‌توان اظهار داشت از آنجایی که شبکه برق از زیرساخت‌های حیاتی کشور می‌باشد، بنابراین با هرگونه خلل در این زیرساخت سایر زیرساخت‌های کشور تحت تأثیر قرار می‌گیرند که خود باعث بروز مشکلات عدیده‌ای در جامعه گردیده و می‌تواند بر بخش‌های مختلف آن تأثیرات قابل توجهی بگذارد و اداره کشور را با چالش‌های جدی مواجه سازد [۳]. تجارب حاصل از جنگ‌های نوین نشان دهنده مورد هدف قرار گرفتن این زیرساخت حیاتی می‌باشد. در این شرایط مشخص نمودن الزامات پدافند غیرعامل در زیرساخت برق و عمل به آن‌ها از اهمیت به سزایی برخوردار است [۱].

پست‌های برق به‌عنوان یک دارایی حیاتی در یک سامانه در صورت آسیب دیدگی، بیشترین اختلال عملکرد را به وجود آورده و باعث قطع خدمات در سطح وسیعی می‌گردند و ممکن است کل شبکه سراسری به حالت ناپایدار رفته و شبکه blackout شود. متأسفانه تا به امروز پست‌های برق با اصول پدافند غیرعامل سازگار نبوده و حتی در نگاه اولیه نیز می‌توان تشخیص داد که در برابر طیف وسیعی از تهدیدات آسیب‌پذیر هستند. رعایت اصول پدافند غیرعامل در پست‌های برق ۴۰۰ کیلوولت به‌عنوان یکی از اجزای مهم واسط در سامانه برق از اهمیت به سزایی برخوردار است و موجب کاهش آسیب‌پذیری این دارایی‌ها و درنهایت کاهش ریسک آن‌ها خواهد شد. پدافند غیرعامل در زیرساخت‌ها شامل تأسیسات و شبکه برق، شبکه‌های آب، گاز، پتروشیمی، تأسیسات زیرزمینی مثل مترو و تأسیسات هوایی مثل فرودگاه در مقالات مختلف مورد بررسی قرار گرفته است. با توجه به اهمیت شبکه‌های الکتریکی، بررسی ریسک آسیب‌پذیری تأسیسات الکتریکی و پست‌های برق یکی از مباحث بروز تحقیقات در حوزه پدافند غیرعامل می‌باشد. در همین راستا مرجع [۴] به دنبال ارائه چارچوبی جهت ارزیابی صحیح و دقیق تهدیدات، آسیب‌پذیری وخطرپذیری زیرساخت‌های حیاتی کشور با ملاحظات پدافند غیرعامل می‌باشد چرا که بر اساس راهبردهای دشمنان خارجی، زیرساخت‌های اساسی یک کشور به‌عنوان اولین اهداف در تهاجم احتمالی مدنظر قرار می‌گیرند. مرجع [۵] بعد از معرفی شریان‌های آب و برق با استفاده از دو مدل تئوری گراف و مدل لئونتیف ۲۴۰ سناریو برای ارزیابی آسیب‌پذیری و ریسک این شریان‌ها احصاء شده که در بین سناریوهای تک متغیره سناریو انفجار در تصفیه‌خانه و در بین سناریوهای ترکیبی انفجار دو تصفیه‌خانه و یک پست برق بیشترین احتمال وقوع را دارد. مرجع [۶] روشی را برای ارزیابی ریسک سامانه قدرت ارائه کرده‌اند. در این روش احتمال وقوع حمله موفقیت آمیز به همراه خسارت ناشی از حمله، ریسک سامانه قدرت را تشکیل می‌دهند. در روش مذکور نویسندگان برای تعیین احتمال حمله به تجهیزات سامانه قدرت مجموعه‌ای از مشخصات حمله کننده مانند انگیزه حمله، میزان فعالیت، منابع، ساختار سازمانی حمله کننده، روش حمله و غیره توجه کرده‌اند. تعیین احتمال حمله موفقیت آمیز بر اساس پارامترهای متعدد حمله کننده، منجر به سناریوهای بسیار زیاد خواهد شد. مدافع از اطلاعات، انگیزه‌ها، تاکتیک‌ها و روش‌های مهاجم، اطلاعات روشنی در دست ندارد و یا ممکن است فریب بخورد. بنابراین غالباً در این نوع مسائل، بهتر است مدافع بر روی داشته‌ها و دانسته‌های خود تمرکز کند. مرجع [۷] برای تعیین مدل احتمال حمله موفقیت آمیز تروریستی، بر وضعیت موجود پدافندی اجزای سامانه تمرکز می‌کند. در این روش، سامانه قدرت به زیرسامانه‌ها و زیرسامانه‌ها خود به اجزائی تقسیم می‌شوند، برای هر جز از سامانه سه تابع جلوگیری، شناسایی و واکنش تعریف می‌شود. جلوگیری به معنای اقداماتی است که طرف خرابکار را از نفوذ و دسترسی به اجزای سامانه بازمی‌دارد مانند پست نگهبانی، کشیدن حصار، موقعیت جغرافیایی منطقه و غیره. شناسایی به معنی فهمیدن و آگاه کردن دیگران از وقوع اعمال خرابکارانه است دوربین‌های مدار بسته و آژیر خطر نمونه‌هایی از اقدامات شناسایی است واکنش به معنی اقداماتی است که از زمان به صدا درآمدن آژیر تا حضور سریع نیروهای امنیتی برای واکنش و ممانعت از انجام خرابکاری انجام می‌پذیرد.

از آنجایی‌که ارزیابی ریسک در پست‌های برق در برابر عملیات خرابکارانه از منظر پدافند غیرعامل با ارائه ریسک هر یک از دارایی‌های هدف، به تفکیک به‌طور جامع در مقالات و مراجع مورد بررسی قرار نگرفته است، در این مقاله به ارزیابی ریسک در پست‌های برق در برابر عملیات خرابکارانه از منظر پدافند غیرعامل و ارائه راهکارهای مقابله با آن پرداخته شده است. بدین منظور از متدولوژی RAMCAP[1] به‌عنوان استراکچر تحقیق در

[1] RAMCAP: Risk Analysis and Management for Critical Asset Protection

ارزیابی ریسک استفاده گردیده است و معیارها و تجهیزات هدف مشخص شده و پرسشنامه‌های تدوین شده بین جامعه خبرگان توزیع گردید و با استفاده از روش تصمیم‌گیری چند معیاره به روش ANP و نرم‌افزار Super Decisions تجهیزات از نظر ارزش، آسیب‌پذیری، تهدیدات و ریسک اولویت بندی شده و نتایج حاصل از ارزیابی ریسک جهت بهره‌گیری از اقدامات پدافند غیرعامل برای کاهش آسیب‌پذیری ارائه شده است.

۲- پست انتقال و تجهیزات آن

پست انتقال به‌عنوان محل استقرار تجهیزات در حال بهره‌برداری برای تبدیل ولتاژهای ۴۰۰ و ۲۳۰ کیلوولت به ولتاژهای ۶۳ یا ۲۰ کیلوولت یکی از زیرساخت‌های اصلی فرآیند تولید، انتقال و توزیع انرژی الکتریکی می‌باشند. تعداد پست‌های انتقال بر اساس آمار ۱۳۹۸ به شرح جدول (۱) می‌باشد [۸].

جدول (۱): تعداد پست‌های انتقال [۸]

تعداد	غیر نیروگاهی	نیروگاهی
۴۰۰ کیلوولت	۱۴۵	۳۸
۲۳۰ کیلوولت	۳۲۱	۵۷

پدافند غیرعامل در پست‌های انتقال به‌عنوان سپر اصلی حفاظتی در تأمین انرژی پایدار الکتریکی از اهمیت ویژه‌ای برخوردار است. از این منظر تجهیزات حساس پست انتقال را می‌توان در موارد زیر خلاصه نمود:

اتوترانسفورماتور و ترانسفورماتور: ترانسفورماتورهای قدرت یکی از عناصر مهم و حیاتی سامانه‌های قدرت به شمار می‌روند با توجه به اینکه توان با حاصل‌ضرب ولتاژ در جریان متناسب است بنابراین برای توان معینی می‌توان با افزودن ولتاژ جریان را کم نمود و یا برعکس. بنابراین باید وسیله‌ای طراحی گردد که به‌طور قابل اطمینانی ولتاژ و جریان را با راندمان قابل ملاحظه‌ای تغییر دهد و این نقش را ترانسفورماتور به خوبی انجام می‌دهد.

بریکرهای قدرت: بریکرهای قدرت یکی از مهم‌ترین عناصر در تأسیسات فشارقوی می‌باشند. کلیدهای قدرت نقش اصلی در قطع و وصل خطوط و ترانسفورماتورها و سایر تجهیزات را برعهده دارند. کلیدهای قدرت باید دارای مشخصاتی همچون اینکه جریان نامی را به‌طور دائم تحمل کند و این جریان را بدون هیچ مشکلی قطع نماید و دیگر آنکه در زمان اتصال کوتاه در اسرع وقت جریان را قطع نماید و قسمت معیوب را از شبکه جدا نماید، برخوردار باشد.

ترانسفورماتور ولتاژ: ترانسفورماتور ولتاژ، ترانسفورماتوری است که در آن ولتاژ ثانویه متناسب و هم‌فاز با ولتاژ اولیه بوده و برای تبدیل ولتاژ یک سامانه به ولتاژی مناسب جهت تجهیزات اندازه‌گیری و تجهیزات حفاظتی به‌کار می‌رود. ترانسفورماتور ولتاژ به‌طور موازی در مدار نصب می‌گردد.

ترانسفورماتور جریان: ترانسفورماتور جریان جهت تبدیل جریان‌های بالا به جریان‌های کم معمولاً (۵ آمپر) برای تجهیزات اندازه‌گیری و تجهیزات حفاظتی طراحی گردیده است. ترانسفورماتور جریان به‌صورت سری در مدار قرار می‌گیرد.

لاین تراپ: در شبکه انتقال نیرو از خطوط انتقال نیرو به‌منظور انتقال سیگنال‌های مختلف نظیر سیگنال اندازه‌گیری، مکالمات تلفنی و ... نیز استفاده می‌گردد. جهت ورود امواج فرکانس بالا از موج‌گیر استفاده می‌گردد. موج‌گیر در انتهای خطوط انتقال نیرو به‌صورت سری نصب می‌گردد.

اتاق فرمان: اتاق فرمان به‌عنوان مرکز فرمان و مغز یک پست کلیه رله‌ها و حسگرهای تجیزات را در خود جای داده است و وظیفه دریافت سیگنال‌ها و اعمال آن برروی تجهیزات را برعهده دارد.

مقره‌ها: مقره‌ها نگهدارنده قسمت‌هایی از تأسیسات الکتریکی هستند که نسبت به زمین دارای اختلاف ولتاژ می‌باشند بنابراین مقره‌ها باید از یک استقامت مکانیکی و الکتریکی خاص برخوردار باشند تا بتوانند علاوه بر نیروهای مختلف مکانیکی و الکترودینامیکی که به آن‌ها وارد می‌گردد در نامناسب‌ترین شرایط(مه، باران و یخ) مقاومت الکتریکی لازم را دارا باشند [۹].

۳- روش ارزیابی ریسک RAMCAP

روش رمکپ، یکی از روش‌های ارزیابی ریسک می‌باشد که توسط یک مؤسسه وابسته به وزارت دفاع آمریکا ارائه گردید. این روش مبتنی بر تعیین دارایی‌های کلیدی یک زیرساخت می‌باشد که ضمن تأکید بر تحلیل ریسک به‌صورت عدد به دنبال کشف آسیب‌های احتمالی در یک سامانه خواهد بود. این واژه مخفف تحلیل ریسک و مدیریت آن برای حفاظت از دارایی‌های حیاتی است. در این روش سناریو پیش رو تهدید انسان ساخت می‌باشد. با توجه به انتخاب زیرساخت برق و سابقه بالای عملیات خرابکارانه بر روی این زیرساخت، رخداد این تهدید با توجه به شرایط کشور و منطقه از احتمال بالایی برخوردار است و با توجه به جذابیت بالای دارایی و همچنین ضعف بالا در رویارویی و توانمندی بالای دشمن در ایجاد تهدیدات و آسیب‌پذیری زیرساخت اعمال استراتژی‌های کاهش خطر امری ضروری به نظر می‌رسد که در شکل (۱) روند کلی نشان داده شده است [۱۰ و ۱۱].

شکل (۱) از سه قسمت تشکیل شده است در طیف اول دارایی شناسایی انجام می‌گردد به‌طوری که پس از شناسایی زیرساخت، هر کدام از تجهیزات حساس تفکیک شده و پس از اعمال شاخص‌های مربوط ارزش هر یک از دارایی‌ها استخراج

می‌گردد. در طیف دوم که تهدید شناسی می‌باشد، از مجموع تهدیدات متصور برای پست برق، تهدیدات مردم محور (خرابکارانه) و تهدیدات فناوری پایه (گرافیتی و الکترومغناطیسی) مورد بررسی قرار می‌گیرد. در این قسمت بر روی دارایی‌های تفکیک شده، تهدیدات در سه دسته خرابکارانه، گرافیتی و الکترومغناطیسی اعمال گردیده است و پس از اعمال شاخص‌های مربوط نمرات تهدیدات هر یک از دارایی‌ها استخراج می‌گردد. در طیف سوم آسیب‌پذیری دارایی‌ها در سه دسته خرابکارانه، گرافیتی و الکترومغناطیسی با اعمال شاخص‌های مربوطه استخراج می‌گردد و نمرات حاصل از هر بخش جهت به‌دست آوردن ریسک در رابطه (۱) قرار خواهد گرفت.

$$R = A * V * T \qquad (۱)$$

که در آن، R، A، V و T به ترتیب بیانگر ریسک، ارزش دارایی، آسیب‌پذیری و تهدید می‌باشد. جهت وزن‌دهی و رتبه‌بندی هر کدام از تجهیزات در سه طیف دارایی شناسی، تهدید شناسی و آسیب‌پذیری، جهت تحلیل داده‌های آماری حاصل از پرسشنامه از روش ANP و نرم‌افزار Super Decisions استفاده خواهد شد.

۳-۱- روش تحلیل داده‌ها به روش ANP

واژه ANP مخفف عبارت Analytical Network Process به معنی فرآیند تحلیل شبکه است. فرآیند تحلیل شبکه روش جامع و قدرتمندی را برای تصمیم‌گیری دقیق با استفاده از اطلاعات تجربی و یا قضاوت‌های شخصی هر تصمیم گیرنده در اختیار و با فراهم کردن ساختاری برای سازماندهی معیارهای متفاوت و ارزیابی اهمیت و ارجحیت هر یک از آن‌ها نسبت به گزینه‌ها، فرآیند تصمیم‌گیری را آسان می‌کند. این روش قابلیت پیاده‌سازی در نرم‌افزار Super Decisions دارد.

جهت پیاده‌سازی روش ANP گام‌های زیر به ترتیب باید انجام شوند:

۱- ساختن نمودار شبکه‌ای پژوهش: در این گام باید مسئله را به سطوح معیار و در صورت وجود زیرمعیار و گزینه تقسیم کرد و روابط بین آن‌ها را تعیین نمود.

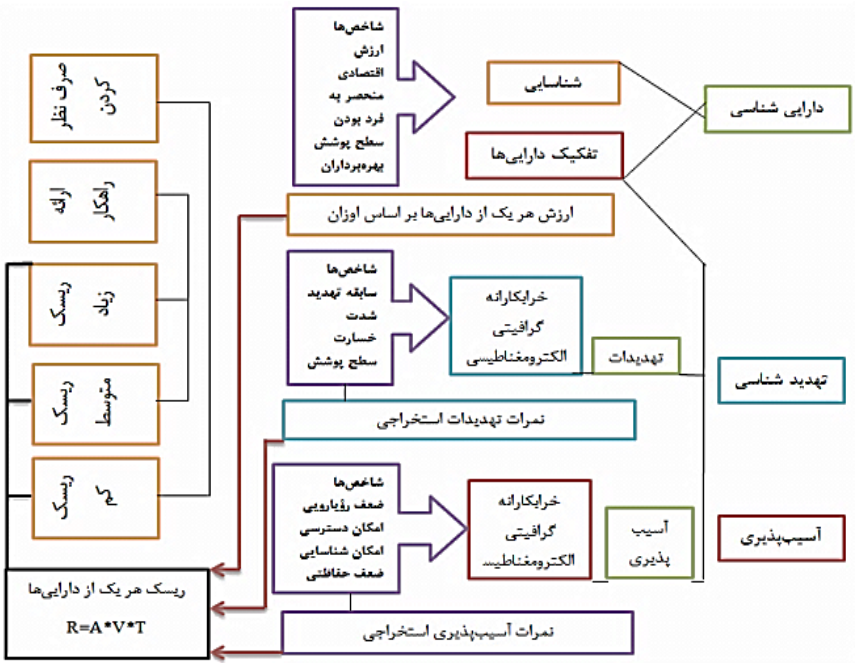
۲- تشکیل ماتریس مقایسات زوجی: در این مرحله عناصر هر سطح نسبت به سایر عناصر مربوط خود در سطح بالاتر به‌صورت زوجی مقایسه شده و ماتریس‌های زوجی تشکیل می‌شوند.

۳- محاسبه نرخ ناسازگاری: در این گام نرخ ناسازگاری ANP با روش‌های موجود محاسبه می‌شود. چنانچه این نرخ از ۰/۱ کمتر باشد، نشان از سازگاری ماتریس است.

۴- تشکیل سوپر ماتریس اولیه: با استفاده از وزن مقایسات زوجی به‌دست آمده، سوپر ماتریس اولیه تشکیل می‌گردد. سوپر ماتریس اولیه، همان وزن‌هایی است که در مرحله دوم از مقایسات زوجی حاصل شده است.

۵- ایجاد سوپر ماتریس موزون: بعد از ایجاد سوپر ماتریس اولیه، باید آن را از روش‌های چون مجمع سطری، مجموع ستونی و ... نرمالیزه کرد تا سوپر ماتریس موزون ایجاد شود.

۶- تشکیل سوپر ماتریس حدی: سوپر ماتریس وزن دار را باید به توان بی‌نهایت رساند تا هر سطر آن به عددی همگرا شود که آن عدد همان وزن آن معیار یا زیرمعیار یا شاخص خواهد بود [۱۱].



شکل(۱): روند کلی [۱۱]

۴- مطالعه موردی برای ارزیابی ریسک تجهیزات پست انتقال

به‌منظور ارزیابی ریسک تجهیزات پست برق فشارقوی، پست برق ۴۰۰ کیلوولت به‌عنوان مطالعه موردی انتخاب شده است اطلاعات مربوط به تجهیزات پست برق در جدول (۲) ارائه گردیده است.

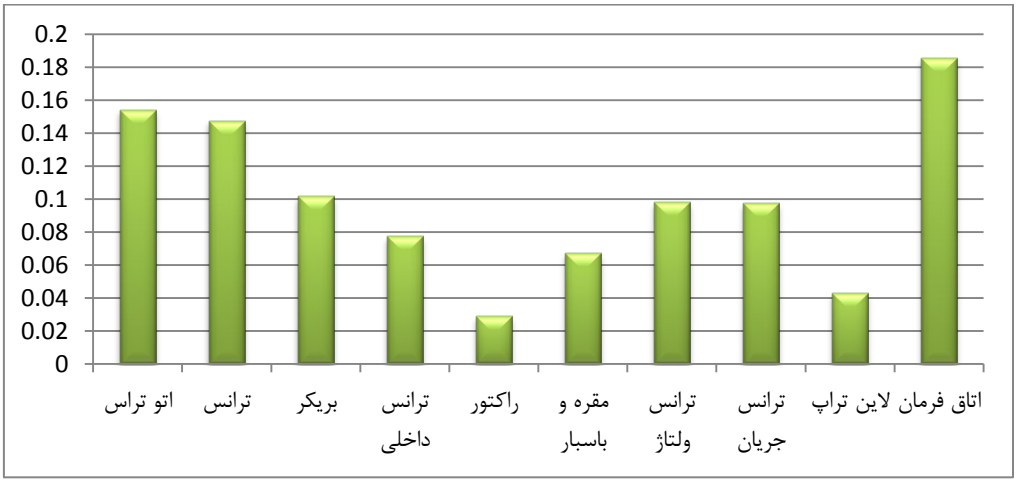
جدول (۲): تجهیزات پست

تعداد	تجهیزات	مشخصات
۳	اتوترانسفورماتور	YNO AUTO.D11-400/230KV-500MVA
۲	ترانسفورماتور	YNd11-230/63KV-180MVA
۳	بریکر	SF6-2000A-50KA-420KV
۲	ترانس مصرف داخلی	DYN11-500KVA

برای پژوهش حاضر با توجه به اهمیت موضوع، از نخبگان حوزه برق قدرت، پدافند غیرعامل و مدیریت بحران مطابق جدول (۳) استفاده گردیده است. نتایج کسب شده از پرسشنامه با استفاده از نرم‌افزار Super Decisions به روش ANP برای هر سه طیف دارایی شناسی، تهدید شناسی و آسیب‌پذیری در شکل‌های (۲ تا ۸) آورده شده است. شکل (۲) نتایج نهایی دارایی شناسی می‌باشد. همان‌طور که از شکل مشخص است در بین دارایی‌ها اتاق فرمان دارای بیشترین وزن می‌باشد و بعد از آن اتوترانس و ترانس به ترتیب بیشترین وزن را به خود اختصاص داده‌اند.

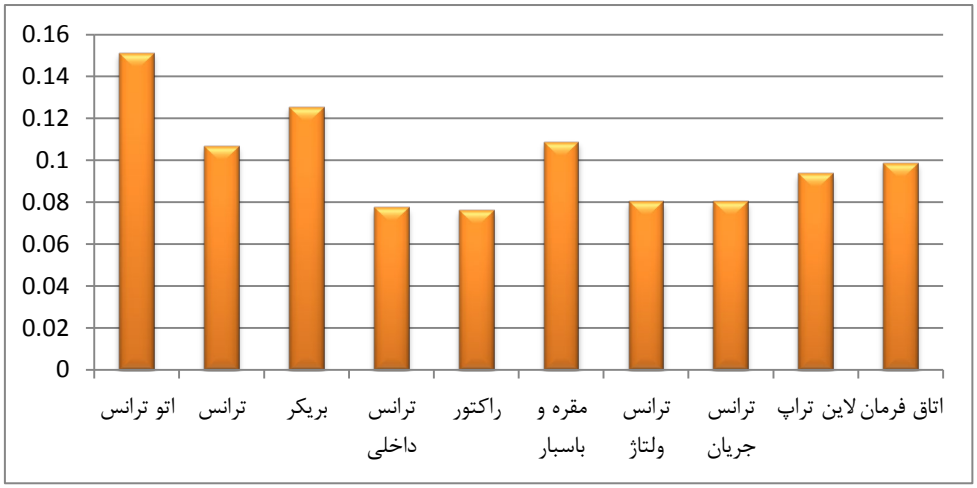
جدول (۳): جامعه آماری

تخصص	تعداد نفرات
مهندسین برق قدرت	۱۵
کارشناسان پدافند غیرعامل	۸
کارشناسان مدیریت بحران	۷



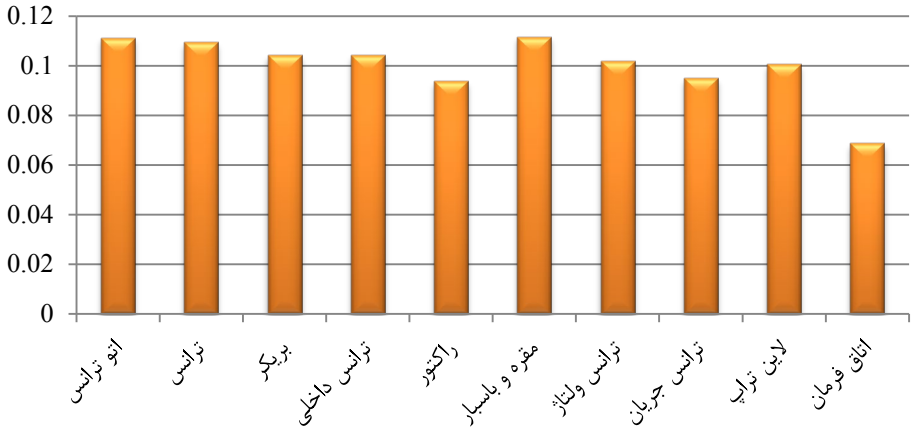
شکل (۲): نتایج نهایی دارایی شناسی

شکل (۳) نتایج نهایی تهدید خرابکارانه بر روی دارایی‌ها را نشان می‌دهد. همان‌طور که از شکل مشخص است در تهدید خرایکارانه اتوترانس بیشترین وزن را به خود اختصاص داده است.



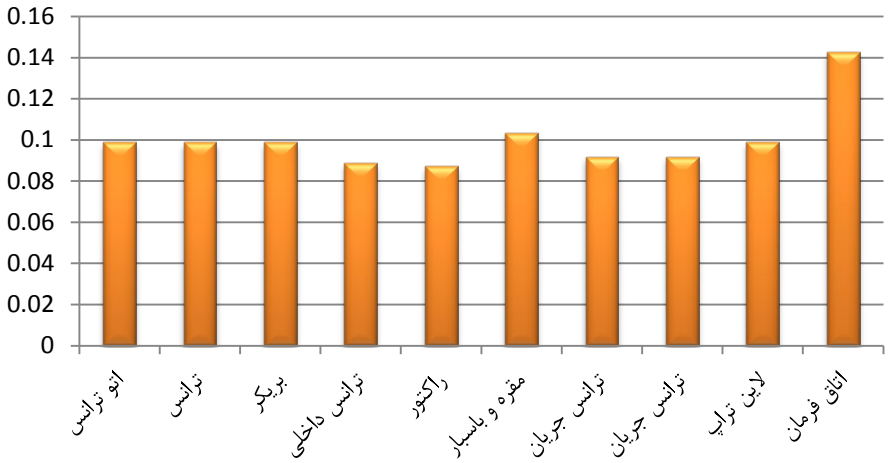
شکل (۳): نتایج نهایی تهدید خرابکارنه

شکل (۴) نتایج نهایی تهدید گرافیتی بر روی دارایی‌ها را نشان می‌دهد. شکل (۴) مشخص می‌کند که در تهدید گرافیتی مقره‌ها و باسبار بیشترین وزن را به خود اختصاص داده است.



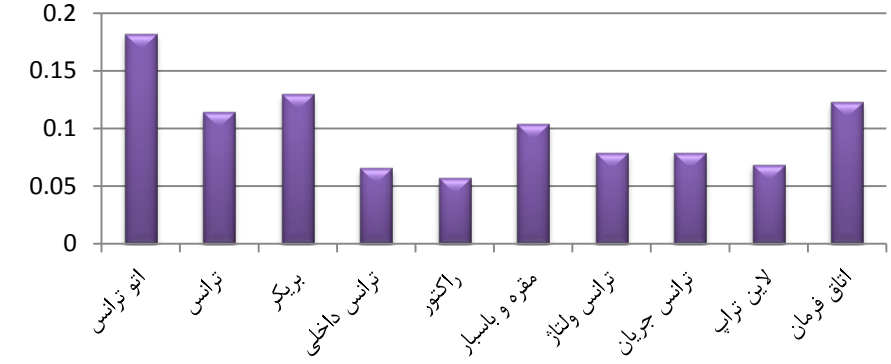
شکل (۴): نتایج نهایی تهدید گرافیتی

شکل (۵) نتایج نهایی تهدید الکترومغناطیسی بر روی دارایی‌ها را نشان می‌دهد. همان‌طور که از شکل مشخص است در تهدید الکترومغناطیسی اتاق فرمان بیشترین وزن را به خود اختصاص داده است.



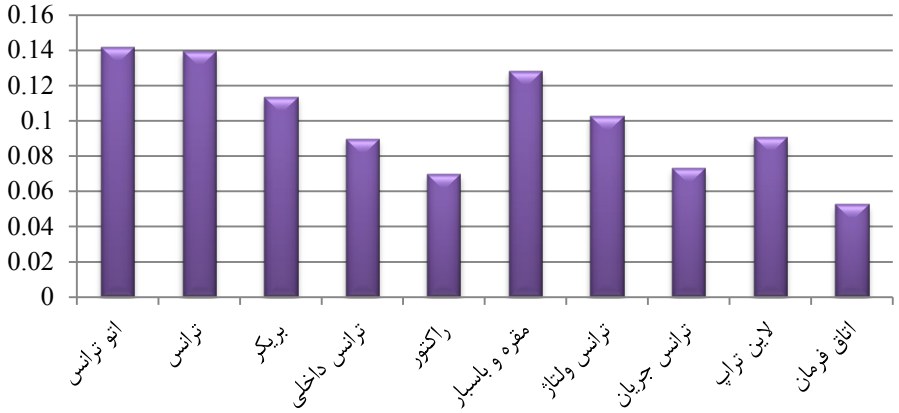
شکل (۵): نتایج نهایی تهدید الکترومغناطیسی

شکل (۶) نتایج نهایی آسیب‌پذیری خرابکارانه دارایی‌ها را نشان می‌دهد و نتایج حاصل بیانگر آن است که آسیب‌پذیرترین تجهیز از نظر آسیب‌پذیری خرابکارانه اتوترانس می‌باشد



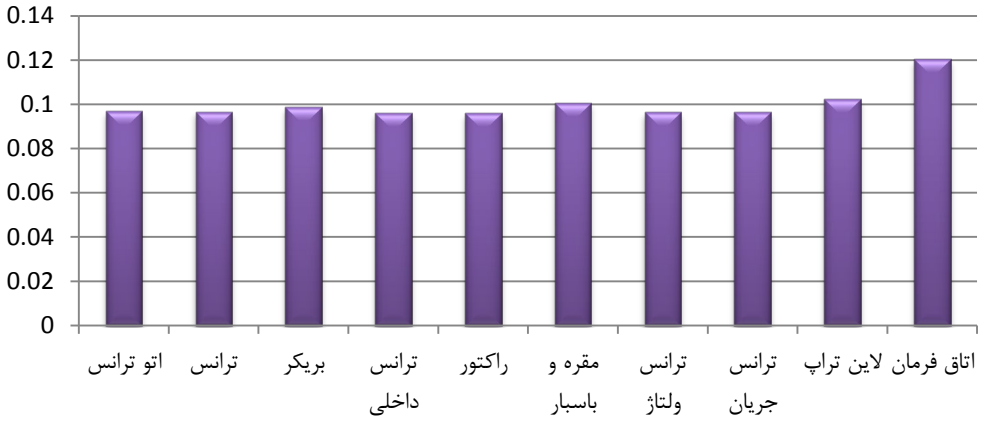
شکل (۶): نتایج نهایی آسیب‌پذیری خرابکارانه

شکل (۷) نتایج نهایی آسیب‌پذیری گرافیتی دارایی‌ها را نشان می‌دهد و نتایج حاصل بیانگر آن است که آسیب‌پذیرترین تجهیز از نظر تهدید گرافیتی اتوترانس و ترانس می‌باشد.



شکل (۷): نتایج نهایی آسیب‌پذیری گرافیتی

شکل (۸) نتایج نهایی آسیب‌پذیری الکترومغناطیسی دارایی‌ها را نشان می‌دهد و نتایج حاصل بیانگر آن است که آسیب‌پذیرترین تجهیز از این نظر اتاق فرمان می‌باشد.



شکل (۸): نتایج نهایی آسیب‌پذیری الکترومغناطیسی

پس از محاسبه ریسک هر یک از دارایی‌ها طبق رابطه (۱) نتیجه کلی را می‌توان به‌صورت جدول (۴) بیان نمود.

جدول (۳): ریسک دارایی‌ها

تهدید / دارایی	خرابکارانه	گرافیتی	الکترومغناطیسی
اتو ترانس	ریسک بالا	ریسک متوسط رو به بالا	ریسک متوسط
ترانس	ریسک متوسط	ریسک متوسط رو به بالا	ریسک متوسط
بریکر	ریسک متوسط رو به بالا	ریسک متوسط	ریسک کم
ترانس داخلی	ریسک کم	ریسک کم	ریسک کم
راکتور	ریسک کم	ریسک کم	ریسک کم
مقره و باسبار	ریسک کم	ریسک متوسط	ریسک کم
ترانس ولتاژ	ریسک کم	ریسک متوسط	ریسک کم
ترانس جریان	ریسک کم	ریسک کم	ریسک کم
لاین تراپ	ریسک کم	ریسک کم	ریسک کم
اتاق فرمان	ریسک متوسط رو به بالا	ریسک کم	ریسک بالا

۵- نتیجه‌گیری

کشور ایران با وجود قرار گرفتن در منطقه‌ای حساس از دنیا همواره در معرض انواع تهدیدات از جمله تهدیدات تروریستی و خرابکارانه می‌باشد. با توجه به وقایع اخیر سپری شده در کشور با وجود دشمنان خارجی انجام عملیات خرابکارانه احتمال بیشتری پیدا نموده است. یکی از تهدیدات مهم جهت ایجاد ناامنی و مشکلات، حمله به پست‌های برق و ایجاد خاموشی گسترده می‌باشد. پست برق ۴۰۰ کیلوولت با قرارگیری در رده پست‌های مهم و حساس یکی از مطلوب‌ترین اهداف جهت نیل به این هدف می‌باشد. بدین منظور در این مقاله به بررسی تعدادی از تهدیدات محتمل برای پست پرداخته و تجهیزات از این نظر ارزیابی شده‌اند. در ارزیابی انجام شده ریسک نهایی تهدید خرابکارانه به ترتیب، اتوترانسفورماتور درجه ریسک بالا و ترانسفورماتور، ریسک متوسط و بریکر، اتاق فرمان درجه ریسک متوسط رو به بالا را به خود اختصاص داده‌اند. قابل ذکر است کاهش ریسک اتوترانسفورماتور موجب کاهش ریسک ترانس و بریکر و اتاق فرمان نیز خواهد شد. یکی از دلایل ریسک بالای اتوترانسفورماتور امکان دسترسی بالا و ضعف حفاظتی بالا می‌باشد. با توجه به درجه ریسک بالای اتوترانسفورماتور برای عملیات خرابکارانه جهت کاهش ریسک این دارایی باید آسیب‌پذیری کالبدی این دارایی را کاهش داد. کاهش امکان دسترسی به این دارایی، استقرار ۲۴ ساعته نگهبان و افزایش روشنایی پست، استفاده از دوربین‌های مداربسته مشرف به کلیه محدوده‌های پست، عدم صدور مجوز ساختمانی بیش از یک طبقه در اطراف پست و ایجاد الزام به کاهش طبقات ساختمان‌های بیش از دو طبقه می‌تواند به‌عنوان اقدامات پدافند غیرعامل پیشنهاد گردد.

تهدید بمب گرافیتی یکی از تهدیدات بالقوه و یکی از کارآمدترین تهدیدات برای پست برق می‌باشد. با توجه به ریسک متوسط رو به بالا برای اتوترانس، ترانس و ریسک متوسط برای بریکر، ترانس ولتاژ، و باسبار، جهت کاهش ریسک، استفاده از روش‌هایی چون کابل کشی زیرزمینی، سقف‌های محافظ، توری‌های پلاستیکی در جمع‌آوری الیاف، استفاده از چترهای جمع کننده الیاف، بی‌برق کردن تجهیزات در لحظه حمله گرافیتی با تعبیه پوش باتن Emergency stop، آموزش نیرو انسانی متخصص برای مقابله و رفع بحران و جمع‌آوری الیاف و پاک‌سازی منطقه، استفاده از فناوری GIS برای پست‌های جدید تأسیس شده، مقاوم سازی با استفاده از نوارهای روکش عایق جهت حفاظت باسبارها، عایق‌بندی پایه نگهدارنده و زمین کردن تجهیزات با نوار عایق و مقاوم سازی با استفاده از چترک افزارها به‌منظور تغییر شکل پروفیل مقره‌ها پیشنهاد می‌گردد. تهدید الکترومغناطیسی برای از کار انداختن سامانه‌های کنترل و فرماندهی، ارتباطات و مخابرات، بدون ایجاد خسارت ناشی از انفجار می‌باشد. در پست برق اتاق فرمان آسیب‌پذیرترین قسمت در برابر تهدید الکترومغناطیسی است. اقدامات حفاظتی در برابر پالس الکترومغناطیسی بر پایه جلوگیری از ورود انتشار امواج استوار می‌باشد. جهت کاهش ریسک و کاهش آسیب‌پذیری استفاده از روش‌های پیشرفته برای حفاظت از سامانه‌های الکتریکی مانند ساخت قفس فارادی و قرار دادن تجهیزات حساس در آن، ارتباط دادن زیرسامانه‌ها به وسیله فیبر نوری، شیلد کردن کابل‌ها، ارت نمودن تجهیزات، ایزولاسیون اتاق فرمان و رعایت پوشش تجهیزات و استفاده از Surge arrester می‌تواند اقدامات مؤثری باشند.

۶- منابع

[1] H. Nemati, M. A. Latify, and G. R. Yousefi, "Coordinated Generation and Transmission Expansion Planning for a Power System under Physical Deliberate Attacks," International Journal of Electrical Power & Energy Systems vol. 96, no. 1, pp. 208-221, 2017.

[2] M. T. Tahooneh, R. Dashti, R. Ghaffarpour, and Gh. Jalali," New Critical Infrastructure Protection Strategies," Passive Defense Quarterly, vol. 11, no. 4, pp. 1-6, 2021 (In Persian).

[3] M. Mehrabi, H. Zakidizaji, S. Ghahremani, M. Lotfabadi, "An Enquiry into Blackouts and the Presentation of Solutions to Deal with Threats and Vulnerabilities of the Power Network Through the Passive Defense Approach," Passive Defense Quarterly, vol. 12, no. 4, pp. 65-79, 2022. (In Persian)

[4] G. Chen, Z. Y. Dong, and D. L. Hil, "Exploring Reliable Strategies for Defending Power System against Targeted Attacks," IEEE Trans. Power Syst. 2011.

[5] H. Dadashpoor and A. Jalali Fath, "Analysis of the Patterns of Regional Specialization and Spatial Concentration of Industries in Iran", journal of Regional Planning, vol. 3, no. 11, pp. 1-18, 2013.

[6] R. Ghaffarpour and A. A. Pourmoosa, "Risk Assessment Modeling and Ranking for Power Network Facilities Regarding to Sabotage" International Journal of Scientific and Technology Research, vol. 6, no. 2, pp. 127-144, 2015.

[7] H. Mashhadi and S. Amini Verki, "The Development and Provision of Threat Assessment Vulnerability and Risk Analysis Critical Infrastructures with an Emphasis on Passive Defense," The First National Conf. on Risk Management in Infrastructure, 2015.

[8] R. Shabaninezhad, A. Balilashak, I. Soltany, and H. Fayazi, "The Principles of Passive Defense Against Electromagnetic Threats for the Power Systems," Passive Defense Quarterly, vol. 12, no. 2, pp. 65-88, 2021 (In Persian).

[9] M. Soltani, "Power Plant Equipment", UTP, 2014 (In Persian).

[10] M. Palizvan and R. Dashti, "Reinforcing Power Network Infrastructures by Employing Passive Defense Applications," Passive Defense Quarterly, vol. 9, no. 4, pp. 57-67, 2019 (In Persian).

[11] M. Ataei, "Fuzzy Multi- Criteria Decision Making", SUTP, 2011 (In Persian).

Risk Assessment of Power Substations Against Subversive Operations and the Provision of Solutions from the Passive Defence Perspective

(The Case Study of a 400KV Power Substation)

Y. Mortezaei*

Abstract

One of the national and vital infrastructures of any country is the electricity network of that country. Vulnerability in power stations, which are the main artery in the cycle of electricity production, transmission and distribution, would result in irreparable damage. One of the ways to create a crisis is vandalism on electric substations, which causes public dissatisfaction, economic, social and even political crises on a large scale. One of the strategic goals of passive defense is to reduce this vulnerability and ensure the continuous functionality of vital and sensitive centers of the country against the actions of the enemy. Meanwhile, passive defense is known as one of the most effective and stable methods of defense against threats. The purpose of this research is to assess the risk of vandalism in substations from the passive defense point of view and provide solutions to deal with it. A 400 KV substation, being in the category of important and sensitive substations, is one of the most desirable goals to achieve this objective. For this purpose, in this article, a number of possible threats to the post were examined and the equipment was evaluated. In the evaluation of the final risk of sabotage threat, the auto-transformer, transformer and breaker were ranked at high, medium and low risk levels respectively, while the control room had the risk of medium upwards. In this research, the RAMCAP methodology was used as a research framework in risk assessment. Considering the network nature of the studied infrastructure, the network structures were used for information analysis and the multi-criteria decision-making method using the ANP method and Super Decisions software was used for the analysis.

Key Words: *Risk Assessment, Electrical Substation, Sabotage Operation, ANP*

*Master of Crisis Management, Malik Ashtar University of Technology, Tehran, Iran (mrz393020@gmail.com)- Writer-in-Charge