فصلنامه علمی-ترویجی پدافند غیرعامل
سال نهم، شماره ۳، پاییز ۱۳۹۷، (پیاپی ۳۵): صص ۱۹-۱۱

افزایش امنیت سامانه‌های انتقال شبکه برق در برابر حملات مخرب در حوزه پدافند غیرعامل

محمد پالیزوان[1*]، رضا دشتی[2]

تاریخ دریافت: ۱۳۹۶/۰۴/۱۵
تاریخ پذیرش: ۱۳۹۶/۱۱/۲۳

چکیده

خرابکاری تروریست‌ها و حمله دشمنان به زیرساخت‌های حوزه انرژی، علی‌الخصوص سیستم‌های انتقال برق که واسط مابین مراکز تولید و مصرف انرژی الکتریکی هستند، یک خطر بالقوه امنیتی به حساب می‌آید. با توجه به اهمیت و جایگاه انرژی الکتریکی در هنگام مقابله با بحران و لزوم آمادگی برای کاهش آسیب‌پذیری و بازیابی تأسیسات برقی، ضرورت تقویت پدافند غیرعامل در این حوزه بیش از پیش احساس می‌شود. در این مقاله ابتدا به شناسایی تهدیدات خرابکارانه در شبکه‌های انتقال انرژی الکتریکی در سیستم قدرت (اعم از خطوط انتقال و پست‌های فشار قوی) پرداخته شده، سپس راهبردها و ایده‌های موثری در جهت کاهش میزان آسیب‌پذیری این مراکز ارائه گردیده که در مجموع به افزایش پایداری و امنیت شبکه تحت شرایط بحرانی و غیرطبیعی کمک خواهد کرد. همچنین، یک ارزیابی کلی جهت تعیین میزان اثرگذاری سیستم‌های انتقال انرژی الکتریکی بر امنیت سیستم قدرت انجام شده که در پی آن، با انجام شبیه‌سازی‌های آنالیز حوادث در یک شبکه نمونه، تاثیر خروج سیستم‌های انتقال برق در اثر حملات مخرب مورد ارزیابی قرار گرفته است. بدین منظور، ملاحظه گردیده که خروج ترانسفورماتورهای قدرت بیشترین تاثیر را در امنیت اضافه بار، و خروج خطوط انتقال بیشترین تاثیر را در امنیت ولتاژ داشته، و اختلال در عملکرد این عناصر باعث ایجاد تغییراتی در امنیت دینامیکی شبکه نمونه شده است.

کلیدواژه‌ها: پدافند غیرعامل، سیستم‌های انتقال شبکه برق، حملات مخرب، امنیت سیستم قدرت.

۱- دکتری هوافضا، معاونت انرژی سازمان پدافند غیرعامل کشور (palizvan_1363@yahoo.com) - نویسنده مسئول
۲- استادیار، دانشکده فناوری‌های نوین دانشگاه علم و صنعت

۱- مقدمه

توسعه روزافزون کشورها، وقوع حوادث و بلایای طبیعی، جنگ و حمله نظامی کشورهای مهاجم از یک سو و لزوم تأمین مداوم انرژی الکتریکی از سوی دیگر، استفاده از فناوری‌های جدید جهت تولید، انتقال و توزیع انرژی الکتریکی و اجرای اقدامات پدافند غیرعامل را به‌منظور تأمین امنیت در حوزه‌های مختلف این صنعت را اجتناب ناپذیر نموده است. عملیات سایبری، روانی، تهاجم سخت، نفوذ و خرابکاری جزو مهم‌ترین تهدیدات حوزه صنعت برق در جنگ است. با توجه به این که حفظ و تأمین انرژی برق جهت برقراری فعالیت در تمام مراکز مهم امری بسیار ضروری است، لذا حفظ و نگهداری نیروگاه‌ها و شبکه برق در هنگام وقوع حملات جنگی موضوعی غیرقابل انکار می‌باشد. سیستم قدرت همواره در معرض اغتشاش‌های مختلفی قرار دارد که درحین مواجهه با آن‌ها باید تصمیمات مناسب در اسرع وقت توسط بهره‌بردار اتخاذ گردد، تا از ناپایدار شدن سیستم جلوگیری گردد. بنابراین، وجود مدیریت در سیستم قدرت در برابر وقوع چنین حملاتی برای امنیت زیرساخت‌ها، امر حیاتی خواهد بود؛ زیرا پیامدهای چنین حملاتی از جنبه‌های عملیاتی مختلف (اعم از اقتصادی و اجتماعی) بر جامعه تحمیل می‌گردد.

نیروگاه‌ها و خطوط انتقال برق، معمولا از جمله اهداف جذابی هستند که در ساعات اولیه جنگ مورد اصابت قرار می‌گیرند. از آنجا که تمام وسایل الکتریکی و الکترونیکی، ساختمان‌ها و برخی سایت‌ها (تلویزیون، رادیو، رایانه، شبکه‌ی مخابرات، فرودگاه‌ها، بیمارستان‌ها، سایت‌های نظامی) با نیروی برق تغذیه می‌شوند، بنابراین، با از کار افتادن آن‌ها در اثر قطع برق، دشمن به بسیاری از موارد مورد نظر خود دست می‌یابد. زیرساخت‌ها اعم از شبکه آب و برق، علاوه بر تأثیرپذیری در رخدادهای طبیعی، بر اثر سوانح انسانی (همچون حملات هدفمند موشکی و تروریستی) نیز دچار خسارت و قطع سرویس‌دهی و استمرار فعالیت خود شده‌اند. دارایی‌های زیرساختی، اهداف بسیار نرم‌تری نسبت به تأسیسات دولتی هستند و جذابیت بیشتری برای تروریست‌ها دارند. علاوه بر این، پیامدهای اقتصادی و روانی ناشی از ضربه به هریک از بخش‌های زیرساختی، مخرب‌تر و وسیع‌تر از تخریب یکی از تأسیسات نظامی است. بیش از دو- سوم حملات تروریستی معطوف به اهداف اقتصادی است و به غیر از مواردی است که جنبه انتقام‌جویانه و خاص دارد. گروه‌های تروریستی، امروز توجه خود را به اهداف آسیب‌پذیر و حیاتی‌تری از جمله پل‌ها و تونل‌ها، شبکه‌های ارتباطی و رایانه‌ای، شبکه‌های ملی برق، سوخت و گاز، حمل و نقل و آب آشامیدنی معطوف کرده‌اند [۱].

در جدول (۱) نتایج مرور کلی وقایع تاریخی حملات انسانی بر شبکه برق نشان داده شده است [۲].

جدول ۱- مروری بر وقایع تاریخی حملات انسانی بر شبکه برق [۲]

ردیف	تاریخ	شرح حادثه	میزان خسارت
۱	۲ ژوئن ۲۰۰۴، آماریلو[۷]، آمریکا	بدون یافتن دلیلی خاص، برق در تأسیسات مهمات هسته‌ای آماریلو به مدت یک ساعت قطع گردید.	خاموشی تمام مرکز؛ گرچه برق پشتیبان خیلی زود فعال شد.
۲	۱۷ ژوئن ۲۰۰۴، ویسکانسین[۸]، آمریکا	فردی به نام کونپکا[۹] معروف به دکتر آشفتگی، خرابکاری‌های زیادی از جمله خطوط انتقال برق و آسیب به رایانه‌ها وارد کرد.	قطع برق بیش از ۳۰۰۰ مصرف‌کننده، خسارت بالغ بر ۸۰۰ هزار دلار
۳	۴ اوت، ۲۰۰۴، آتن یونان	انفجار بمب دست‌ساز در نزدیکی مرکز برقی در آتن	وارد کردن خرابی‌های بدون آسیب جانی، ایجاد رعب و وحشت با توجه به نزدیکی به المپیک آتن
۴	۱۵ سپتامبر ۲۰۰۴، ایرون[۱۰]، اسپانیا	انفجار ۴ قطعه بر روی دکل برق	آسیب به پی دکل
۵	۷ دسامبر ۲۰۰۴، کانادا	کار گذاشتن مواد منفجره در یک برج برق فشار قوی	این اتفاق همزمان با بازدید رئیس جمهور آمریکا (بوش) از کانادا بود. قطع سراسری برق مهار شد.
۶	۲۸ دسامبر ۲۰۰۴، نوادا، آمریکا	خرابکاری بر ۴ خط انتقال فشار قوی برق به ناحیه‌ی رنو[۱۱]	سقوط هر یک از دکل‌ها، سبب خرابی زنجیره‌ای سایر دکل‌ها می‌شود.
۷	۲۰ مه ۲۰۰۶، ویزی[۱۲]، آمریکا	افرادی وارد نیروگاه هیدروالکتریک بانگور[۱۳] شدند و سیم‌های مسی را دزدیدند.	قطع برق برای حدود ۶ ساعت
۸	۲۰ مه ۲۰۰۶، کلمبیا	حمله‌ی شورشی‌ها با نارنجک به شهر بوناونتورا[۱۴]	جراحت ۲۴ نفر و قطع کامل برق شهر

با توجه به داده‌های به‌دست‌آمده از موسسه WITS، از مجموع ۵۴۹۳۲ حمله تروریستی بین سال‌های (۲۰۰۸-۲۰۰۴)، تعداد ۹۴۱ حمله تروریستی مربوط به زیرساخت‌های انتقال انرژی (یعنی ۱/۷٪) و ۹۰ حمله تروریستی مربوط به زیرساخت‌های توزیع انرژی و ۹۶ حمله تروریستی مربوط به زیرساخت‌های تولید انرژی بوده است. همان‌طور که مشاهده می‌شود، به‌دلیل در دسترس بودن خطوط انتقال، بیشترین حملات تروریستی در حوزه انرژی، مربوط به بخش انتقال انرژی بوده است [۳].

نظر به تحقیقات صورت‌گرفته، مشخص شده که تاکنون تحقیقات

و کارگاه‌های آموزشی قابل توجهی در کشورهای مختلف انجام شده و نتایج مفیدی از آن‌ها حاصل شده است. در این مقاله از تجربیات کسب‌شده از تحقیقات سایر کشورها و همچنین تحقیقات انجام‌شده توسط محققان داخلی نیز استفاده خواهد شد. از جمله تحقیقات مهم و بین‌المللی انجام‌شده در این حوزه می‌توان به [۱۰-۴] اشاره کرد. از این‌رو، باید تمهیدات لازم برای مواجهه با تهدیدات مذکور اندیشیده شود که در این مقاله با انجام بررسی‌های لازم، راه‌کارهای موثری در جهت افزایش قدرت دفاعی سیستم قدرت در بخش انتقال، بیان خواهد شد.

۲- راهبردهای مدیریت بحران و پدافند غیرعامل در وزارت نیرو

در این بخش به راهبردهای مدیریت بحران و پدافند غیرعامل وزارت نیرو در صنعت آب و برق پرداخته می‌شود که مهم‌ترین آنها عبارتند از [۱]:

- نهادینه‌سازی و اجرای اصول و ضوابط مدیریت بحران و پدافند غیرعامل در صنعت آب و برق به‌منظور افزایش بازدارندگی، تداوم ارائه خدمات در شرایط اضطراری، کاهش آسیب‌پذیری و ارتقای پایداری در کلیه تاسیسات و فرآیندهای صنعت؛
- شناسایی و طبقه‌بندی تاسیسات و فرآیندهای حیاتی، حساس و مهم و آسیب‌پذیر و تدوین و اجرای برنامه‌های کوتاه‌مدت و بلندمدت؛
- تدوین، بازنگری و اجرای استانداردها و ضوابط مدیریتی و فنی در سیستم‌ها، فرآیندها و تاسیسات موجود و طرح‌های توسعه؛
- تدوین، آموزش، فرهنگ‌سازی و تمرین دستورالعمل‌ها و شرح وظایف کلیه واحدها، مدیران و کارکنان برای شرایط اضطراری و اطلاع‌رسانی مؤثر به مردم؛
- انجام پژوهش‌های مورد نیاز در جهت دستیابی به راهکارهای جدید کم هزینه، مؤثر و عملیاتی در عرصه پدافند غیرعامل؛
- بهره‌گیری از فناوری‌های نوین جهت مقابله با تهدیدات نرم‌افزاری و الکترونیکی و سایر تهدیدات جدید.

۳- تهدیدات عمده و موثر در سیستم‌های انتقال برق

یک اقدام تروریستی موفق در شبکه برق می‌تواند آثار ویرانگری بر امنیت ملی، اقتصاد و زندگی هر شهروند داشته باشد. با این‌حال، سیستم قدرت جنبه‌های مختلفی دارد که هیچ‌گاه نمی‌تواند در برابر یک حمله از پیش تعیین‌شده، کاملا محافظت شود. به‌دلیل ارتباط نزدیک سیستم قدرت و زیرساخت‌های سایر جوامع، می‌توان سه نوع تهدید مختلف را در نظر گرفت [۴]:

الف) حمله بر سیستم قدرت: در این حالت، حمله به زیر ساخت‌های برقی و تحمیل بی‌برقی به مردم هدف اولیه می‌باشد. هدف حمله می‌تواند تک‌قسمتی باشد (مانند حمله به یک برج انتقال یا یک پست حساس) و یا یک حمله چندجانبه هم‌زمان به‌منظور براندازی کامل یک شبکه منطقه‌ای باشد. همچنین، هدف حمله می‌تواند بازارهای برق باشد، که به‌دلیل اوضاع متغیرشان بسیار آسیب‌پذیر هستند.

ب) حمله به‌وسیله سیستم قدرت: در اینجا، با استفاده از قسمت‌هایی از زیرساخت‌های سیستم قدرت به‌عنوان یک سلاح، مردم هدف نهایی حمله هستند. در این راستا، دشمنان می‌توانند از برج‌های خنک‌کننده نیروگاه جهت پراکنده کردن عوامل شیمیایی یا زیست‌محیطی استفاده کنند.

ج) حمله از طریق سیستم قدرت: در این مورد، هدف زیرساخت‌های شهری می‌باشد. بدین منظور، شبکه‌ها شامل چندین مجرا برای حمله می‌باشند که خطوط انتقال انرژی الکتریکی، خط لوله‌های سوخت، کابل‌های زیرزمینی، تونل‌ها و مجراهای فاضلاب از جمله این موارد می‌باشند. برای مثال، تروریست‌ها می‌توانند یک پالس الکترومغناطیسی را از طریق شبکه برای آسیب رساندن به زیرساخت‌های کامپیوتری یا مخابراتی اعمال کنند.

سیستم‌های انتقال انرژی الکتریکی (اعم از خطوط انتقال و پست‌های فشار قوی) به‌دلیل وسعت ساختمان و حجم تجهیزات و همچنین به‌دلیل در دسترس بودن، یکی از مهم‌ترین اهداف کشورهای مهاجم در جنگ‌های نوین می‌باشند. عمده تهدیدات محتمل برای تأسیسات را می‌توان به شرح ذیل دسته‌بندی نمود [۱۱]:

- حمله مستقیم دشمن با استفاده ار انواع سلاح‌های متعارف (از جمله: بمباران هوائی، حملات موشکی، توپخانه‌ای و خمپاره‌ای و خرابکاری در خطوط در خطوط انتقال تأسیسات و تجهیزات الکتریکی و الکترونیکی).
- حمله مستقیم دشمن با استفاده از انواع سلاح‌های غیر متعارف (از قبیل: شیمیایی، میکروبی، هسته‌ای، نوترونی).
- قطع یا ایجاد نقصان در ارائه خدمات ناشی از قطع جریان برق و آب به‌دلیل از کار افتادن سامانه وزارت نیرو توسط

دشمن (مانند حمله با بمب‌های گرافیتی).

- بروز خرابکاری و آلودگی توسط عوامل نفوذی یا جاسوسان دشمن.
- بروز اختلال در سامانه‌های کامپیوتری و شبکه‌های مخابراتی توسط عوامل انسانی یا اثرات بمب‌های الکترومغناطیسی.
- بروز زلزله و تخریب تأسیسات انتقال، تصفیه و توزیع.
- آسیب دیدن تأسیسات ناشی از اصابت صاعقه و قطع جریان برق یا آسیب‌های کلی‌تر به تأسیسات. از آن‌جایی که آسیب‌های ناشی از حوادث طبیعی و برخی اشتباهات انسانی به لحاظ نتیجه نهایی، تفاوتی با حوادث غیر طبیعی نداشته و در هر حال قطع یا کمبود شدید انرژی الکتریکی یا نقصان و مشکل در خدمات نیروگاه را موجب می‌شوند، لذا هر ساختاری که برای اعمال مدیریت در زمان آسیب‌دیدگی ناشی از حمله دشمن به تأسیسات ایجاد گردد، باید توانایی مدیریت بر مشکلات ناشی از حوادث طبیعی را نیز داشته باشد.

۴- کاربردهای پدافند غیرعامل در سیستم‌های انتقال الکتریکی

از نقطه نظر مدیریتی، اقدامات مورد نظر برای اجرای اصول پدافند غیرعامل، عمدتا قبل از حادثه انجام می‌شود؛ هرچند ممکن است برخی اقدامات آن، حین و پس از حادثه نیز صورت گیرد. بنابراین، با توجه به اهمیت سیستم قدرت در حفظ و تداوم فعالیت‌های جامعه لازم است تا تدابیر امنیتی کافی برای کم‌اثر نمودن تهدیدات و کاهش آسیب‌پذیری‌ها اتخاذ گردد. در این حالت پدافند غیرعامل می‌تواند نقش مهمی در استمرار فعالیت چرخه تولید تا مصرف انرژی الکتریکی ایفا نماید. به‌طور کلی، قسمت‌های اصلی دستورالعمل‌های امنیتی به قرار زیر می‌باشد [۱۲]:

- ارزیابی میزان ریسک و آسیب‌پذیری
- قابلیت واکنش به تهدیدات
- مدیریت بحران
- تداوم فرآیندهای اقتصادی
- ارتباطات
- امنیت فیزیکی
- فناوری اطلاعات/ امنیت سایبری
- حفاظت از اطلاعات حساس

۴-۱- اعمال پدافند غیرعامل در حوزه پست‌های انتقال و فوق توزیع برق

در این بخش به بررسی اصول پدافند غیرعامل در رابطه با پست‌های انتقال و فوق توزیع پرداخته می‌شود. به‌طور کلی، در خصوص مقاوم‌سازی و افزایش امنیت پست‌های برق در برابر حملات تروریستی و مخرب، نکات زیر پیشنهاد می‌گردد که هرچه سطح ولتاژ پست افزایش یابد، رعایت آن‌ها نیز حیاتی‌تر می‌شود (زیرا از لحاظ مباحث امنیت و پایداری در شبکه قدرت، اهمیت پست‌های فوق توزیع از پست‌های توزیع بیشتر است و همچنین اهمیت پست‌های انتقال از پست‌ها فوق توزیع نیز بیشتر می‌باشد). این نکات شامل موارد زیر می‌شوند:

- رعایت اصول مربوطه در زمینه‌های اختفاء، پراکندگی و استحکامات در زمان احداث پست‌های برق که از اصول مهم پدافند غیرعامل محسوب می‌شوند.
- در شناسایی محل احداث پست‌های جدید، علاوه بر مباحث فنی و اقتصادی، نکات مربوطه در زمینه بررسی پتانسیل حفاظت فیزیکی در برابر حملات مخرب باید مورد توجه قرار گیرد که در این راستا از تجربیات متخصصان نظامی می‌توان استفاده کرد.
- مراکز تولید، پست‌ها، و همچنین مراکز کنترل در شبکه برق از اهمیت بالایی برخوردار هستند. برای این مراکز نیاز به توسعه تجهیزات امنیتی فیزیکی خاص مانند دوربین‌ها، حسگرها، دستگاه‌های تشخیص نفوذ، کنترل دسترسی، روشنایی پیشرفته، دیوارها و نرده‌های امنیتی محیطی، و نیز افزایش تعداد نیروهای انسانی حاضر در محل به‌همراه ارائه آموزش‌های لازم به آن‌ها، وجود دارد، که همه این موارد منجر به کاهش آسیب‌پذیری و افزایش امنیت این اماکن (به‌خصوص در شب‌ها)، خواهد شد.
- با توجه به این‌که مهم‌ترین تجهیز پست‌های برق ترانسفورماتورها هستند (از لحاظ فنی و اقتصادی)، لذا باید تهیه ترانسفورماتورها به شرکت سازنده تاکید شود که بدنه آن‌ها مجهز به پوشش فلزی مقاوم در برابر گلوله باشد.
- استفاده از ابزارهای سیستم که می‌توانند محل حادثه راشناسایی و سیستم را کنترل نمایند و همچنین حوادث احتمالی را پیش‌بینی نمایند.
- احداث و جایگزینی پست‌های داخلی (indoor) در مقابل پست‌های فضای باز باید افزایش یابد که پست‌های گازی (GIS) نمونه مناسبی از این پست‌ها هستند و در آن تجهیزات سوئیچ‌گیر و ترانسفورماتورها با استفاده از عایق گازی (SF6) از یکدیگر ایزوله

می‌شوند و این روش تاثیر بسیار مثبتی بر کوچک‌سازی فضای پست و اختفای آن (بیشتر در پست‌های فوق توزیع و توزیع) می‌گذارد.

با توجه به هزینه سرمایه‌گذاری، بهره‌برداری و نگهداری بالا، مزایای عمده GIS را می‌توان به صورت زیر برشمرد:

- ✓ فضای لازم بسیار کم (۱۰٪ فضای پست AIS)
- ✓ عدم حساسیت به تأثیرات خارجی
- ✓ سازگاری با محیط
- ✓ ایمنی افراد و تجهیزات

۲-۴- اعمال پدافند غیرعامل در حوزه خطوط انتقال الکتریکی

در این قسمت به بررسی اعمال اصولی پدافند غیرعامل در رابطه با خطوط انتقال انرژی الکتریکی پرداخته می‌شود. در خصوص افزایش امنیت خطوط انتقال برق در برابر حملات تروریستی و مخرب، نکات زیر پیشنهاد می‌گردد (بدیهی است که در این‌جا نیز هرچه سطح ولتاژ خط افزایش یابد، رعایت این موارد نیز حیاتی‌تر می‌شود):

- رعایت اصول مربوطه در زمینه‌های اختفاء، پوشش و استحکامات که از اصول مهم پدافند غیرعامل محسوب می‌شوند.
- هنگام تعیین محل عبور یک خط انتقال برق علاوه بر مسائل فنی و اقتصادی، دسترسی آن جهت انجام حملات تروریستی نیز باید در نظر گرفته شود و مسیر مربوطه باید تا جایی که ممکن است از محل‌هایی عبور کند که در معرض دید عموم باشد.
- برای خطوطی که در مناطق دور افتاده و کم تردد احداث می‌شوند و کمتر قابل مشاهده عموم هستند، باید اقدامات حفاظتی اضافی در طراحی دکل‌ها در نظر گرفته شود و مقاومت بیشتری برای آن‌ها در نظر گرفته شود.
- استفاده از دوربین‌های مادون قرمز، حسگرهای ارزان‌قیمت، و سیستم‌های ماهواره‌ای جهت ارائه اطلاعات از وضعیت الکتریکی و فیزیکی خط انتقال در زمان‌های مختلف که کمک زیادی به پایش امنیت خطوط توسط مراکز کنترل می‌نماید.
- استفاده بیشتر از دکل‌های خود- نگهدار (self-supporting tower) برای سیستم‌های انتقال انرژی الکتریکی و همچنین سیستم‌های ارتباطی که در برابر سقوط‌های متوالی دکل‌ها در شرایط حادثه، مقاوم هستند.
- توسعه استفاده استفاده از مقره‌های کامپوزیت جدید به جای مقره‌های سنتی سرامیکی و شیشه‌ای که مقره‌های جدید دارای مقاومت الکتریکی، حرارتی، و مکانیکی بیشتری نسبت به انواع مقره‌های طرح سنتی هستند.
- جایگزینی و احداث خطوط کابلی و زیرزمینی به جای خطوط هوایی قبلی باید افزایش یابد که خطوط با عایق گازی (GIL) نمونه مناسبی از این موارد هستند و در آن خطوط حامل انرژی با استفاده از عایق گازی (SF6) از یکدیگر ایزوله می‌شوند و این روش تاثیر بسیار مثبتی بر کاهش فاصله بین خطوط و اختفای آن می‌گذارد (بیشتر در خطوط فشار متوسط و فشار ضعیف).

ویژگی‌های متعدد GIL سبب می‌شود که دامنه کاربردهای آن در خطوط انتقال افزایش یابد. به‌عنوان مثال می‌توان به موارد ذیل اشاره نمود [۱۳-۱]:

- ✓ استفاده در مسیرهای بلند و صعب العبور؛
- ✓ امکان نصب در تونل مشترک تاسیسات شهری؛
- ✓ ارتباط میان پست‌های اصلی و فرعی شبکه؛
- ✓ حذف حریم‌ها و زیباسازی فضای شهری؛
- ✓ امکان نصب در نزدیکی خطوط راه آهن و فرودگاه‌ها؛
- ✓ ارتباطات درون نیروگاهی و ایستگاهی.

۵- ارزیابی نتایج شبیه‌سازی

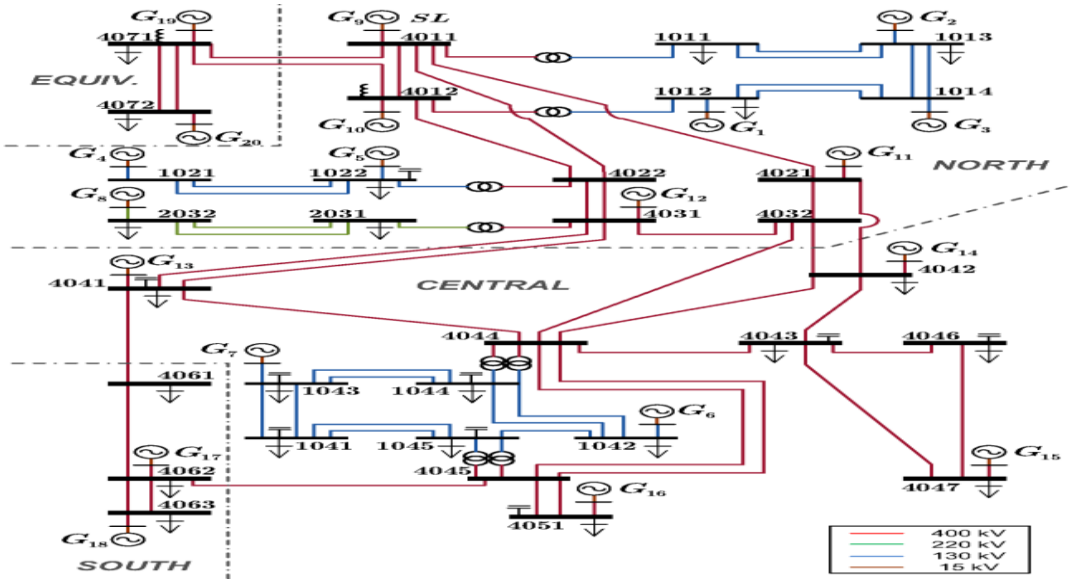
سیستم قدرت مورد مطالعه در این مقاله، شبکه برق Nordic32 است که یک سیستم قدرت با مقیاس وسیع محسوب گشته و گزینه مناسبی جهت انجام مطالعات استاتیکی و دینامیکی می‌باشد که در نرم‌افزار DIgSILENT پیاده‌سازی شده است [۱۴].

در این شبکه، کلیه پارامترهای دینامیکی ژنراتورها، کنترل‌کننده‌های خودکار ولتاژ ژنراتورها، گاورنرها، PSS ها، محدودکننده جریان ژنراتورها و کنترل‌کننده خودکار ترانسفورماتورهای OLTC لحاظ شده‌اند. این شبکه دارای سه سطح ولتاژ ۴۰۰، ۲۲۰ و ۱۳۰ کیلوولت در سطح انتقال و سطح ولتاژ ۱۵ کیلوولت در شین‌های ژنراتوری است. همچنین در شبکه مذکور، ۲۲ ژنراتور، ۹ بانک خازنی، ۲ راکتور شنت، ۵۲ خط انتقال، و ۳۷ ترانسفورماتور است که همگی آن‌ها مجهز به تپ‌چنجر هستند. همچنین ۲۲ بار از نوع وابسته به فرکانس و ولتاژ وجود دارد که به‌صورت زیر نشان داده می‌شوند [۱۵]:

$$\begin{cases} P_{load} = P_0 \left(\frac{V}{V_0}\right)\left(\frac{f}{f_0}\right)^{0.75} \\ Q_{load} = Q_0 \left(\frac{V}{V_0}\right)^2 \end{cases} \quad (۱)$$

که در رابطه ذکرشده، V_0 و f_0 ولتاژ و فرکانس نامی بار هستند.

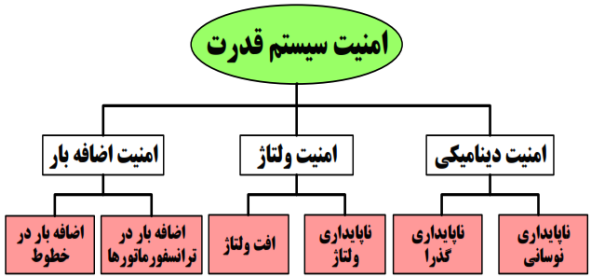
همچنین، شبکه نمونه دارای ۴۱ باس غیر ژنراتوری و ۲۰ باس ژنراتوری است؛ که فرض شده در همه باس‌های غیر ژنراتوری، دستگاه PMU نصب گردیده است که به این ترتیب ۴۱ دستگاه PMU در این شبکه قدرت نصب شده؛ تا رویت‌پذیری سیستم قدرت را به‌همراه داشته باشند. براساس اطلاعات اجمالی فوق، دیاگرام تک‌خط سیستم قدرت Nordic32 در شکل (۱) نشان داده شده است.



شکل ۱- دیاگرام تک‌خط شبکه قدرت Nordic32

در این بخش، با انجام شبیه‌سازی‌های مربوط به آنالیز پیشامد (Contingency Analysis) ، به ارزیابی امنیت سیستم قدرت در اثر خروج سیستم‌های انتقال برق پرداخته می‌شود. ارزیابی امنیت یک مفهوم گسترده است و هر روز بر وسعت آن اضافه می‌گردد. چنان‌که امروزه برخی از مفاهیم که قبلا به‌طور مستقل شناخته می‌شدند (مانند مبحث کیفیت توان) را در بر می‌گیرد. بنابراین، تعیین وضعیت امنیت یک سیستم منوط به انجام ارزیابی‌های متعددی می‌باشد. در شکل (۲)، آنالیزهای متفاوتی که در ارزیابی امنیت استفاده می‌شوند، نشان داده شده است [۱۶].

همان‌طور که در شکل (۲) مشاهده می‌گردد، امنیت سیستم قدرت شامل سه بخش کلی امنیت اضافه‌بار، امنیت ولتاژ، و امنیت دینامیک شبکه می‌گردد که در ادامه، با انجام آنالیز پیشامد بر روی شبکه مربوطه، هر یک از موارد مذکور به‌ازای خروج سیستم‌های انتقال برق مورد ارزیابی قرار می‌گیرند [۱۷].



شکل ۲- دسته‌بندی عملیات ارزیابی امنیت [۱۶]

۵-۱- ارزیابی امنیت اضافه بار

در این قسمت به‌منظور ارزیابی امنیت اضافه بار شبکه، یک آنالیز پیشامد بر روی شبکه انجام شده و نتایج مربوط به بارگذاری تجهیزات در اثر خروج خطوط انتقال و ترانسفورماتورها مطابق جدول (۲) به‌دست آمده است.

به‌ازای ارزیابی امنیت اضافه‌بار شبکه، با قید بارگذاری ۹۰٪ برای تجهیزات مربوطه، ۱۵ عدد از تجهیزات مختلف به‌ازای حالت‌های مختلف خروج خطوط انتقال و ترانسفورماتورها (جمعا ۸۹ حالت به‌تعداد خطوط و ترانسفورماتورها) از این قید تخطی می‌کنند و دچار اضافه‌بار می‌گردند. به‌عنوان مثال، در ردیف اول و دوم که بیشترین اضافه بار رویت می‌شود (افزایش بارگذاری از ۵۸/۴٪ به ۱۱۶/۳٪)، مربوط به دو ترانسفورماتور موازی با عنوان ۴۰۴۴-۱۰۴۴ و سطح ولتاژ ۴۰۰/۱۳۰ کیلو ولت است، که این اتفاق برای هریک از این دو ترانسفورماتور، در اثر خروج ترانسفورماتور موازی آن‌ها از شبکه، رخ داده است.

این ارزیابی نشان می‌دهد که ترانسفورماتورها بسیار بیشتر از خطوط انتقال در معرض اضافه‌بار در اثر اغتشاش‌های مختلف، قرار دارند؛ به‌طوری‌که در این شبکه، تمامی حالت‌های اضافه بار مربوط به ترانسفورماتورها بوده است. بنابراین، ترانسفورماتورها از این حیث در معرض آسیب‌پذیری بیشتری قرار دارند. همچنین با بررسی علل حوادث نیز مشاهده می‌گردد که این نسبت بین ترانسفورماتورها و

خطوط مجددا تکرار شده و خروج ترانسفورماتورها از شبکه، مهم‌ترین عامل اضافه‌بارها بوده است. در نتیجه، خروج ترانسفورماتورها از شبکه برق، جدی‌ترین مشکل اضافه‌بار در بحث امنیت شبکه است و از طرفی هم خود ترانسفورماتورها در معرض بیشترین آسیب‌پذیری ناشی از اضافه‌بار قرار دارند.

بنابراین، با استفاده از این آنالیز می‌توان نقاط ضعیف شبکه را از نظر اضافه بار ناشی از خروج ترانسفورماتورها و خطوط انتقال (و یا سایر تجهیزات مانند ژنراتورها) شناسایی کرده و اقدامات لازم را جهت تقویت آن‌ها به‌کار برد.

۵-۲- ارزیابی امنیت ولتاژ

در این قسمت به‌منظور ارزیابی امنیت ولتاژ شبکه، یک آنالیز پیشامد بر روی شبکه انجام شده و نتایج مربوط به افت ولتاژ نقاط مختلف (باس‌بارهای شبکه) در اثر خروج ژنراتورها، مطابق جدول (۳) به‌دست آمده است.

به‌ازای ارزیابی امنیت ولتاژ شبکه، با قید افت ولتاژ ۰/۹۵ پریونیت برای باس‌بارهای مربوطه، ۱۲ عدد از نقاط مختلف به‌ازای حالت‌های مختلف خروج خطوط انتقال و ترانسفورماتورها از این قید تخطی می‌کنند و دچار افت ولتاژ می‌گردند. به‌عنوان مثال، در ردیف اول که بیشترین افت ولتاژ رویت می‌شود (کاهش ولتاژ از ۱/۰۱۵ به ۰/۸۹۷ پریونیت)، مربوط به باس‌بار ۴۰۶۱ که با سطح ولتاژ ۴۰۰ کیلو ولت است، که این اتفاق در اثر خروج خط انتقال ۴۰۶۲-۴۰۶۱ (که آن‌هم یک خط انتقال ۴۰۰ کیلو ولت است)، از شبکه رخ داده است. این ارزیابی نشان می‌دهد که در اثر خروج تجهیزات مختلف، تعداد قابل توجهی از نقاط شبکه دچار افت ولتاژ می‌گردند. با بررسی علل حوادث، مشاهده می‌گردد که خروج خطوط از شبکه، بیشترین عامل افت ولتاژها بوده است، به‌طوری که در این شبکه، تمامی حالت‌های افت ولتاژ مربوطه ناشی از خروج خطوط از شبکه بوده است. در نتیجه، خروج خطوط از شبکه برق، جدی‌ترین مشکل افت ولتاژ در بحث امنیت شبکه است و منجر به ایجاد افت ولتاژهایی در نقاط مختلف شبکه می‌گردند.

بنابراین، با استفاده از این آنالیز می‌توان نقاط ضعیف شبکه را از نظر افت ولتاژ ناشی از خروج ترانسفورماتورها و خطوط انتقال (و یا سایر تجهیزات مانند ژنراتورها) شناسایی کرده و اقدامات لازم را جهت تقویت آن‌ها به‌کار برد.

جدول ۲- نتایج حاصل از ارزیابی امنیت اضافه بار (در اثر خروج سیستم‌های انتقال) بر روی شبکه برق Nordic32

Contingency Analysis Report: Maximum Loadings

Study Case: Study Case
Result File: Contingency Analysis DC
Loading Limit: 90
Overloading Limit: 90

	Component	Branch, Substation or Site	Loading Continuous [%]	Loading Short-Term [%]	Loading Base Case [%]	Contingency Number	Contingency Name	Base Case and Continuous Loading [0 % - 116 %]
1	tr1044-4044(p1)		116.3	116.3	58.4	57	tr1044-4044(p2)	
2	tr1044-4044(p2)		116.3	116.3	58.4	56	tr1044-4044(p1)	
3	trG1042		105.1	105.1	86.6	89	trG4072	
4	trG1043		105.1	105.1	86.6	89	trG4072	
5	trG4042		105.1	105.1	86.6	89	trG4072	
6	trG4047		105.1	105.1	86.6	89	trG4072	
7	trG4031		103.4	103.4	85.2	89	trG4072	
8	trG4063		103.2	103.2	85.0	89	trG4072	
9	trG2032		103.0	103.0	84.9	89	trG4072	
10	trG4051		100.1	100.1	82.5	89	trG4072	
11	trG4021		97.3	97.3	80.2	89	trG4072	
12	tr1045-4045(p1)		93.8	93.8	47.1	59	tr1045-4045(p2)	
13	tr1045-4045(p2)		93.8	93.8	47.1	58	tr1045-4045(p1)	
14	trG1022		93.4	93.4	77.0	89	trG4072	
15	trG1014		91.8	91.8	75.6	89	trG4072	

جدول ۳- نتایج حاصل از ارزیابی امنیت افت ولتاژ (در اثر خروج سیستم‌های انتقال) بر روی شبکه برق Nordic32

Contingency Analysis Report: Minimum Voltages

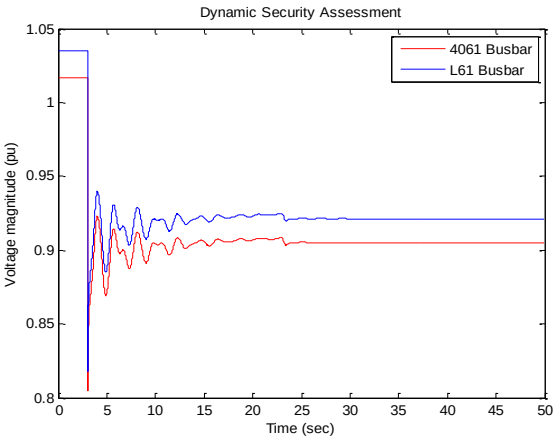
Study Case: Study Case
Result File: Contingency Analysis AC
Min. Voltage 0.95
Min.Voltage Limit: 0.95

	Component	Branch, Substation or Site	Voltage Min. [p.u.]	Voltage Step [p.u.]	Voltage Base [p.u.]	Contingency Number	Contingency Name	Base Case and Post Voltage [0.897 p.u. - 1.033 p.u.]
1	4061	Station4061	0.897	-0.118	1.015	48	Lne4061-4062	
2	L61	Station61	0.913	-0.120	1.033	48	Lne4061-4062	
3	4046	Station4046	0.917	-0.058	0.976	47	Lne4046-4047	
4	L46	Station46	0.933	-0.060	0.993	47	Lne4046-4047	
5	4043	Station4043	0.944	-0.026	0.970	47	Lne4046-4047	
6	4044	Station4044	0.945	-0.024	0.969	27	Lne4021-4042	
7	1041	Station1041	0.945	-0.016	0.961	9	Lne1041-1043(p1)	
8	L41	Station41	0.945	-0.053	0.998	30	Lne4031-4032	
9	4041	Station4041	0.946	-0.053	0.999	30	Lne4031-4032	
10	G4041	StationG4041	0.947	-0.053	1.000	30	Lne4031-4032	
11	4032	Station4032	0.948	-0.054	1.002	27	Lne4021-4042	
12	4022	Station4022	0.948	-0.036	0.984	28	Lne4022-4031(p1)	

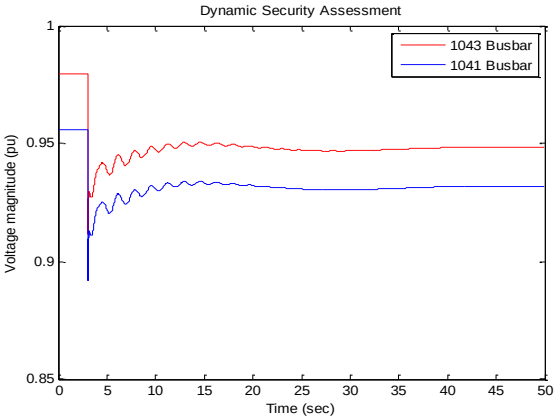
۵-۳- ارزیابی امنیت دینامیکی

در این قسمت به‌منظور ارزیابی امنیت پایداری شبکه، یک سری شبیه‌سازی‌های دینامیکی بر روی شبکه انجام شده و نتایج مربوط به خروج سیستم‌های انتقال گوناگون و تاثیر آن‌ها بر پایداری ولتاژ باس‌بارهای مختلف، مورد بررسی قرار گرفته است. نتایج حاصل از دو مورد این شبیه‌سازی‌ها در شکل‌های (۳) و (۴) آورده شده است. با توجه به نتایج حاصل از شبیه‌سازی‌های دینامیکی ملاحظه می‌گردد که خروج سیستم‌های انتقال انرژی الکتریکی در شبکه برق (اعم از خطوط انتقال و پست‌های فشار قوی) منجر به تغییرات دامنه ولتاژ و معمولا بروز افت ولتاژ در برخی نقاط می‌گردد.

از این‌رو، باید تهمیدات لازم در شرایط خروج سیستم‌های انتقال برق و تاثیرات آن‌ها بر شرایط دینامیکی شبکه قدرت، از قبل اندیشیده شود (لازم به ذکر است که خروج واحدهای تولیدی و به تبع ماشین‌های سنکرون، تاثیر بیشتری بر دینامیک شبکه می‌گذارد و تاثیر آن‌ها بر امنیت دینامیکی سیستم، به‌علت وجود پارامترها و ادوات تاثیرگذار بر دینامیک، محسوس‌تر است).



شکل ۳- خروج خط انتقال ۴۰۶۱-۴۰۶۲ از شبکه نمونه



شکل ۴- خروج ترانسفورماتور ۱۰۴۳ از شبکه نمونه

۶- نتیجه‌گیری

امروزه سیستم‌های تولید و انتقال انرژی الکتریسیته به‌عنوان یکی از اهداف راهبردی در جنگ‌های مدرن شناخته می‌شوند و خطرات گوناگونی آن‌ها را تهدید می‌نماید که می‌بایست جهت مقابله با آن‌ها تمهیداتی در نظر گرفته شود. در این مقاله پس از بررسی تهدیدات خصمانه در سیستم‌های انتقال انرژی الکتریکی (اعم از خطوط انتقال و پست‌های فشار قوی)، راهبردها و ایده‌های موثری در جهت کاهش میزان آسیب‌پذیری این مراکز ارائه گردیده که در مجموع به افزایش پایداری و امنیت سیستم قدرت تحت شرایط بحرانی و غیرطبیعی کمک می‌کنند. همچنین، با انجام یک ارزیابی کلی، میزان اثرگذاری سیستم‌های انتقال انرژی الکتریکی بر امنیت سیستم قدرت با انجام شبیه‌سازی‌های آنالیز حوادث در یک شبکه نمونه، مورد بررسی و تحلیل قرار گرفته است. نتایج حاصل از شبیه‌سازی‌ها برای ارزیابی امنیت اضافه بار در شبکه نمونه نشان می‌دهد که ترانسفورماتورها بسیار بیشتر از خطوط انتقال در معرض اضافه‌بار قرار دارند. همچنین با بررسی علل حوادث نیز مشاهده می‌گردد که این نسبت بین ترانسفورماتورها و خطوط مجددا تکرار شده و خروج ترانسفورماتورها از شبکه، مهم‌ترین عامل اضافه‌بارها بوده است. در حوزه ارزیابی امنیت ولتاژ نیز ملاحظه گردید که در اثر خروج تجهیزات مختلف در شبکه نمونه، تعداد قابل توجهی از نقاط شبکه دچار افت ولتاژ می‌گردند. با بررسی علل حوادث مشاهده می‌گردد که خروج خطوط از شبکه، بیشترین عامل افت ولتاژها بوده است. نهایتا در حوزه امنیت دینامیکی ملاحظه گردید که خروج سیستم‌های انتقال انرژی الکتریکی در شبکه برق (اعم از خطوط انتقال و پست‌های فشار قوی) منجر به تغییرات دامنه ولتاژ و معمولا بروز افت ولتاژ در برخی نقاط می‌گردد. لازم به ذکر است که خروج واحدهای تولیدی و به تبع ماشین‌های سنکرون به‌علت وجود اینرسی بالا، تاثیر بیشتری بر دینامیک سیستم می‌گذارد و تغییرات ناشی از فقدان آن‌ها در امنیت دینامیکی شبکه قدرت محسوس‌تر است.

۷- مراجع

۱. شرکت مهندسین مشاور مونتکو، مرکز مطالعات سیستم و انرژی: کاربرد پدافند غیرعامل در صنعت برق، ۱۳۹۳.

۲. اسکندری، محمد، امیدوار، بابک، توکلی ثانی، محمدصادق، تحلیل خسارت شریان‌های حیاتی با درنظرگرفتن اثرات وابستگی در اثر حملات هدفمند مطالعه موردی شبکه آب و برق در یک منطقه شهری؛ نشریه مدیریت بحران، ویژه‌نامه هفته پدافند غیر عامل، شماره ۲، صص ۳۰-۱۹، ۱۳۹۱.

۳. حق‌مرام، رضا، رحمانی، هادی، شناسایی تهدیدات تروریستی در یک شبکه برق و بهره‌گیری از منابع تجدیدپذیر به‌همراه خازن‌گذاری به‌منظور تقویت سطح پدافند غیرعامل، نشریه پدافند غیرعامل، دانشگاه امام حسین (ع)، سال ششم، شماره ۳، صص ۸۶-۷۹، ۱۳۹۴.

4. M. Amin, "Security challenges for the electricity infrastructure," IEEE, Supplement to computer, vol. 35, no. 4, pp. 8-10, 2002.

5. A. Abel, P. W. Parfomak, and A. D. Shea, "Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism," Congressional Research Service Reports, UNT Libraries Government Documents Department, 2004.

6. S. Hirschberg, C. Bauer, P. Burgherr, et al., "Health effects of technologies for power generation: Contributions from normal operation, severe accidents and terrorist threat," Reliability Engineering and System Safety, vol. 145, pp. 373-387, 2015.

7. D. Watts, "Security & Vulnerability in Electric Power Systems," 35th North American Power Symposium, University of Missouri-Rolla in Rolla, Missouri, pp. 559-566, 2003.

8. J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," IEEE Transactions on Power Systems, vol. 19, no. 2, pp. 905-912, 2004.

9. National Research Council, "Terrorism and the Electric Power Delivery System," Washington DC: The National Academies Press, 2012.

10. National Research Council, "The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters," Summary of a Workshop, Washington DC: The National Academies Press, 2013.

۱۱. میثمی، حسین، موسوی، پدرام، مبانی مهندسی و روش‌های اجرایی سازه‌ای پدافند غیرعامل شریان حیاتی وزارت نیرو، نشریه پدافند غیرعامل، دانشگاه امام حسین (ع)، شماره ۱، صص ۷۰- ۶۱، ۱۳۸۸.

۱۲. آزاده‌دل، رمضانعلی، منصف، حسن، دهقانی، حمید، مدل‌سازی و شبیه‌سازی سیستم قدرت با رویکرد پدافند غیرعامل در مقابل حملات الکترومغناطیسی، نشریه پدافند غیرعامل، دانشگاه امام حسین (ع)، سال پنجم، شماره ۴، صص ۴۰-۲۹، ۱۳۹۳.

۱۳. گندمکار، مجید، دادفر، سجاد، عزتی، سیدمیثم، مبانی پدافند غیرعامل و مصادیق آن در صنعت برق با نگاه به مدیریت استراتژیک، چهاردهمین کنفرانس دانشجویی مهندسی برق ایران، دانشگاه کرمانشاه، ۱۳۹۰.

14. D. Peppas, "Development and Analysis of Nordic32 Power System Model in PowerFactory," KTH Electrical Engineering, Stockholm, Master Thesis, 2008.

15. Th. Van Cutsem, M. Glavic, and W. Rosehart, "Test Systems for Voltage Stability Analysis and Security Assessment," IEEE PES Task Force on Test Systems for Voltage Stability Analysis and Security Assessment, 2015.

16. A. Dissanayaka, U. D. Annakkage, B. Jayasekara, and B. Bagen, "Risk-Based Dynamic Security Assessment," IEEE Transactions on Power Systems, vol. 26, no. 3, pp. 1302-1308, 2011.

17. G. Longatt, R. Francisco, and J. Luis, "Power Factory Applications for Power System Analysis," Springer International Publishing, 2014.

Enhancing Security of Power Transmission Systems Against Destructive Attacks in the Field of the Passive Defense

M. Palizvan[*], R. Dashti

Abstract

In recent years, concerns over hostile attacks against various infrastructures, especially the power system, have been increased. According to importance and the role of electrical energy in confronting with crisis, the need to rebuild the power grid, provide security conditions, and reduce the vulnerability of electrical installations, and the need to strengthen the passive defense have arisen more and more. In this paper, first, the threats and the vulnerability of the electrical energy transmission systems in the power grid (including transmission lines and high voltage substations) will be identified, then the strategies and Effective ideas will be provided to decrease the vulnerability of these centers, which, in general, will help to increase the stability and security of the power system under abnormal conditions. Also, by performing simulations of contingency analysis in a typical grid, the impact of outage of power transmission systems will be analyzed. Then, it will be observed that the outage of power transformers have the greatest impact on the overload security, and the outage of the transmission lines have the greatest impact on the voltage security, and any disturbance for them may cause changes in the dynamic security of the case study network.

Key Words: *Passive Defense, Power Transmission Systems, Destructive Attacks, Network Security.*

[*] Passive Defense Organization of Iran - (palizvan_1363@yahoo.com) - Writer-in-Charge