فصلنامه علمی-ترویجی پدافند غیرعامل
سال ششم، شماره ۱، بهار ۱۳۹۴، (پیاپی ۲۱): صص ۸۶-۷۹

شناسایی تهدیدات تروریستی در یک شبکه برق و بهره‌گیری از منابع تجدیدپذیر به همراه خازن‌گذاری به‌منظور تقویت سطح پدافند غیرعامل

رضا حق‌مرام[۱]، هادی رحمانی[۲]

تاریخ دریافت: ۹۳/۰۷/۰۷
تاریخ پذیرش: ۹۴/۰۴/۲۴

چکیده

خطرات امنیتی برای زیرساخت‌ها و منابع انرژی الکتریسیته به کرات به عنوان یکی از منابع ایجاد نگرانی در مباحث بین‌الملل ذکر شده است. بنابراین، شناسایی تهدیدات تروریستی در این حوزه اهمیت زیادی دارد. این مقاله با شبیه‌سازی یک سامانه تولید انرژی متشکل از دو شبکه متصل به هم، بر روی تهدیدات بالقوه در بخش امنیت انرژی مانند حملات تروریستی به زیرساخت‌های انرژی الکتریسیته از جمله نیروگاه‌ها تمرکز دارد و با بهره‌گیری از منابع تجدیدپذیر و خازن‌گذاری مناسب، سعی در تقویت سطح پدافند غیرعامل در حوزه انرژی الکتریسیته دارد. در این سامانه حالات مختلف حمله به ژنراتورها و استفاده از منابع تجدیدپذیر و خازن مورد بررسی قرار گرفته است. لازم به ذکر است که خازن‌گذاری باعث کاهش تلفات و افت ولتاژ و در نتیجه، مخارج کمتر انرژی و افزایش قابلیت اطمینان می‌گردد.

کلیدواژه‌ها: تهدیدات تروریستی، پدافند غیرعامل، منابع تجدیدپذیر، خازن‌گذاری.

۱- استادیار و عضو هیئت علمی دانشگاه جامع امام حسین (ع)
۲- کارشناس ارشد مهندسی برق-قدرت و پژوهشگر دانشگاه جامع امام حسین (ع)- hadi_rahmani65@yahoo.com- نویسنده مسئول

۱- مقدمه

در سال‌های اخیر، کشورهای پیشرو در صنعت، مطالعه بر روی شناسایی تهدیدات تروریستی و امنیت انرژی در حوزه الکتریسیته را در دستور کار امنیت ملی خود قرار داده‌اند و بلوک‌های منطقه‌ای، مانند اتحادیه اروپا و یا سازمان‌های بین‌المللی مانند ناتو توجه بی‌سابقه‌ای به مسائل امنیت انرژی الکتریسیته کرده‌اند. چه بسا که قطعی برق یک کشور در زمان جنگ می‌تواند اولین اولویت برای هدف قرار دادن امنیت آن کشور در تمام عرصه‌ها باشد و قطعی برق حتی برای یک مدت محدود، ممکن است پیامدهای جبران‌ناپذیری به دنبال داشته باشد. طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح برای تهیه چنین طرح هایی فراهم می‌گردد ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ گردند. با این حال، بزرگ‌ترین چالش در شبکه برق، جدا از دیگر جنبه‌های عمده در تولید برق، ثبات و ترمیم شبکه‌های قدرت و برگشت‌پذیری شبکه قدرت در زمان بروز یک مشکل می‌باشد. در مطالعات و یافته‌ها، به ادغام و تأثیر نفوذ منابع تجدیدپذیر، میکروشبکه، جزیره‌ای شدن شبکه و ذخیره‌سازی انرژی، اهمیت بیشتری داده شده است [۱۱].

۲- تهدیدات عمده و موثر در صنعت برق

نیروگاه برق به دلیل وسعت ساختمان و حجم تجهیزات و همچنین شبکه‌های انتقال و توزیع برق به دلیل در دسترس بودن، یکی از مهم‌ترین اهداف کشورهای مهاجم در جنگ‌های نوین می‌باشند [۱]. عمده تهدیدات موثر در صنعت برق عبارت‌اند از:

- تهدیدات ناشی از شناسایی توسط سامانه سنجش از راه دور دشمن
- تهدیدات ناشی از تهاجم هوایی (بمب، موشک)
- تهدیدات ناشی از اقدامات تروریستی
- تهدیدات ناشی از بمب‌های گرافیتی
- تهدیدات ناشی از تهاجم سایبری
- تهدیدات ناشی از سلاح‌های الکترومغناطیس
- تهدیدات ناشی از القای ولتاژ بالا

به‌طور کلی، خطر را می‌توان به این چهار دسته طبقه‌بندی نمود:

تهدیدات طبیعی، تهدید اتفاقی، تهدیدهای مخرب و تهدید در حال ظهور

۲-۱- تهدیدات طبیعی

علت بروز یک تهدید طبیعی، به قرار گرفتن سامانه قدرت در مکان جغرافیایی که قرار گرفته، مرتبط است. حادثه ناشی از تهدید طبیعی عمدتاً به دلیل پدیده‌های طبیعی، مانند تخلیه جوی، نور، باد، و نه یک عامل انسانی هست. یک سری از خاموشی‌های برق بزرگ و کوچک ناشی از تهدیدات طبیعی در سراسر جهان وجود دارد. در ۲۸ سپتامبر سال ۲۰۰۳، یک صاعقه بین یک کابل هادی و یک درخت توسط طوفان ایجاد شد که با تصمیم گیری های نادرست انسانی، در نهایت باعث قطع برق جدی شد که تمام ایتالیا را تحت تأثیر قرار داد. قطع برق به مدت ۱۲ ساعت به طول انجامید و در مجموع، ۵۶ میلیون نفر در خاموشی قرار گرفتند [۳]. در تاریخ ۸ ژانویه ۲۰۰۵، برق ارائه‌شده به بیش از ۴۰۰۰۰۰ خوابگاه محلی در جنوب سوئد به علت ضربه ناشی از طوفان قطع شد. قطع برق منجر به از دست دادن اقتصادی صدها میلیون کرون در سوئد شد [۴]. علاوه‌براین، در سال ۲۰۰۸، باران تگرگ باعث ایجاد ضربه به ارائه برق در جنوب چین شد. آب و هوای بد باعث شد تعداد زیادی از خطوط انتقال و برج‌ها با آسیب فیزیکی جدی روبرو شوند، به‌طوری‌که ۱۳ استان تحت تأثیر واقع‌شده و حدود ۱۶۹ شهرستان در خاموشی قرار گرفتند. خسارات اقتصادی مستقیم ناشی از این قطع برق، بیش از ۱۰۰ میلیارد یوان برآورد شده است [۵].

۲-۲- تهدیدات تصادفی

علل تهدیدات تصادفی می‌تواند خرابی تجهیزات، از جمله بریکرها، خرابی مقره‌ها، اضافه‌بار یک ترانسفورماتور، و یا خطاهای عملیاتی، از جمله به عنوان مثال، یک خطای انسانی و یا اشتباه در برنامه‌ریزی سامانه، عملیات، و یا تعمیر و نگهداری باشد. در ۸-۹ سپتامبر ۲۰۱۱، خرابی تجهیزات مانیتورینگ به علت مشکلات ناشی در یک پست برق در جنوب غربی آریزونا، در نهایت به قطعی برق گسترده منجر شد که بخش‌هایی از جنوب کالیفرنیا و آریزونا، و همچنین بخش‌هایی از شمال غربی مکزیک را تحت تأثیر قرار داد [۶]. یک خط قدرت با ولتاژ بالا به علت یک عملیات اشتباه توسط اپراتور خط انتقال از مدار خارج شد و سپس نتیجه آن به صورت آبشاری سراسر جنوب شرقی کانادا و شمال شرقی ایالات

متحده آمریکا را نحت تأثیر قرار داد [۷].

۲-۳- تهدیدات مخرب

سامانه قدرت در حال تبدیل شدن به یک هدف محبوب به‌منظور حمله‌های مخرب به دلایل مختلف، از جمله اهداف جنایی، نظامی و یا سیاسی که ناتوانی و یا تخریب آن اثرات ناتوان‌کننده بر روی اقتصاد ملی و امنیت ملی خواهد گذاشت، می‌باشد. سامانه‌های قدرت را می‌توان به سه لایه زیر تقسیم نمود: لایه فیزیکی، لایه انسانی، و لایه اینترنتی. لایه فیزیکی اشاره به خواص ملموس مرتبط با برق، مانند نیروگاه‌های برق، خطوط انتقال و ترانسفورماتورها دارد. لایه انسانی اشاره به افرادی دارد که دسترسی به سامانه‌های قدرت داشته باشند؛ و لایه اینترنتی شامل اطلاعات سخت‌افزاری، نرم‌افزاری، داده‌ها، و شبکه‌های ارتباطی است که از عملکرد سامانه انرژی الکتریکی حمایت می‌کند. یک تهدید، زمانی مخرب است که از طریق سه لایه، مانند تخریب ترانسفورماتور در لایه فیزیکی، خسارات ناشی از خودی های مخرب در لایه تصمیم‌گیری انسان و حملات از طریق بدافزارها و هکرها در لایه‌های اینترنتی پیاده‌سازی شود. از سال ۱۹۹۹ تا سال ۲۰۰۲، بیش از ۱۵۰ حمله عمدی در سامانه انرژی الکتریکی در سراسر جهان پیاده‌سازی شده است [۸].

۲-۴- تهدیدات در حال ظهور

ارائه تمام تهدیدات در حال ظهور که برخی از آن‌ها هنوز مشاهده نشده غیرممکن است. به تهدیدات پدیدآمده با تکامل سامانه‌های قدرت مانند ادغام انرژی‌های تجدیدپذیر و وابستگی متقابل بین سامانه برق و سایر زیرساخت‌ها، تهدیدات در حال ظهور گفته می‌شود.

۳- اجزای تهدیدپذیر شبکه برق از تروریسم

خرابکاری تروریست‌ها در زیرساخت‌های انرژی الکتریسیته خطر سیاسی بالقوه برای امنیت عرضه انرژی می‌باشد. درحالی‌که تأمین انرژی بدون وقفه، یک عامل حیاتی در عملکرد مناسب جوامع مدرن می‌باشد. حفاظت از زیرساخت‌های انرژی مانند نیروگاه‌ها، دکل‌ها و پست‌های برق برای تمام زمان‌ها تقریباً غیرممکن است و با توجه به آسیب‌پذیری فیزیکی مشهود و اهمیت زیرساخت‌های انرژی، انتظار می‌رود که به اهداف راهبردی جذابی برای حمله بالقوه تبدیل شوند. با توجه به داده‌های به‌دست‌آمده از موسسه GTD، از ۱۵۲۵۴ حمله تروریستی که در سراسر جهان بین سال‌های (۱۹۹۸ - ۲۰۰۷) انجام گرفته است چیزی نزدیک به ۲۳۲ حمله تروریستی مربوط به زیرساخت‌های انتقال انرژی بوده که تقریباً حدود ۱/۵٪ تروریسم جهانی است و ۱۶ حمله تروریستی مربوط به زیرساخت‌های توزیع انرژی و ۳۲ حمله تروریستی مربوط به زیرساخت‌های تولید انرژی می‌باشد. با توجه به داده های به‌دست‌آمده از موسسه WITS، از مجموع ۵۴۹۳۲ حمله تروریستی بین سال‌های (۲۰۰۴- ۲۰۰۸)، ۹۴۱ حمله تروریستی مربوط به زیرساخت‌های انتقال انرژی (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 می‌کنید به دلیل در دسترس بودن خطوط انتقال بیشترین حملات تروریستی در حوزه انرژی، مربوط به بخش انتقال انرژی بوده ولی کاراترین و موثرترین روش به‌منظور قطع سراسری برق و تحت تأثیر قرار دادن نقاط حساس، حمله به نیروگاه‌های تولید انرژی الکتریسیته می‌باشد. چون که برگرداندن یک نیروگاه به‌مراتب پرهزینه‌تر و زمان‌برتر از برگرداندن خطوط انتقال انرژی است و قابلیت اطمینان سامانه قدرت را به شدت پایین می‌آورد [۱۰-۹].

۴- اعمال پدافند غیرعامل به اجزاء تهدیدپذیر شبکه قدرت

مدیریت بهینه‌سازی شبکه، تأمین و توزیع نیروی برق مطمئن و پایدار، تأمین برق و روشنایی معابر و مراکز حساس و حیاتی در اولویت قرار دارد. با توجه به مورد هدف بودن نقاط حساس و حیاتی توسط دشمنان جمهوری اسلامی ایران، وظیفه بسیار مهم و سنگین این بخش بر عهده شرکت مدیریت تولید، انتقال و توزیع نیروی برق ایران (توانیر) است. صنعت برق از سه عنصر تولید، انتقال و توزیع تشکیل شده است که هر کدام وظایف بسیار مهم و حساسی دارند، از این‌رو با توجه به اهمیت نقش انرژی الکتریکی در هنگام مقابله با بحران و لزوم آمادگی برای احیای شبکه برق‌رسانی و تأمین شرایط امنیتی و کاهش آسیب‌پذیری تأسیسات برق، ضرورت تقویت پدافند غیرعامل بیش از پیش احساس می‌شود. یکی از موارد تهدید شبکه برق، بمب‌های الکترومغناطیسی (عملکرد بر اساس فرکانس‌های رادیویی) و گرافیتی (ذرات گرافیت به صورت مارپیچ) است که تجارب مختلفی از کاربرد آن‌ها در دنیا وجود دارد [۲]. در این بخش به تعمیم

پدافند غیرعامل در حوزه‌های ذیل خواهیم پرداخت:

- تولید انرژی الکتریکی
- خطوط انتقال انرژی الکتریکی
- پست‌های انتقال و فوق توزیع انرژی الکتریکی

۳-۱- اعمال پدافند غیرعامل در تولید انرژی الکتریکی

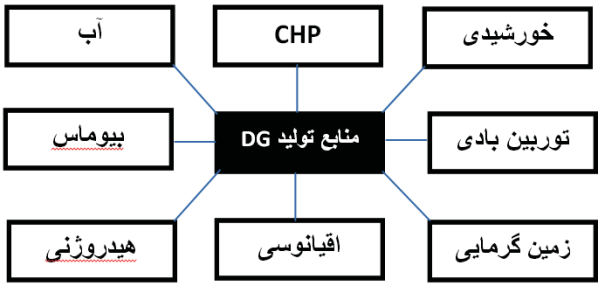
این اصول شامل سه اصل ذیل می‌باشد:

الف- استتار و اختفا: برای نیروگاه‌های تولید عمده انرژی الکتریکی، این اصل امکان‌پذیر نمی‌باشد، اما راهکارهای دیگری جهت اجرای این اصل وجود دارد که در ادامه به آن‌ها خواهیم پرداخت.

ب- پراکندگی: با توجه به آنکه سهم عمده‌ای از انرژی الکتریکی در نیروگاه‌های کشور به صورت متمرکز تولید می‌گردد و این نیروگاه‌ها از لحاظ راهبردی بدون حفاظ در مقابل هرگونه حمله نظامی کشورهای مهاجم طراحی گردیده‌اند، با توسعه نیروگاه‌های تولید پراکنده می‌توان این موضوع را تا حدی مرتفع نمود.

ج- مقاوم‌سازی و استحکام: برای اعمال پدافند غیرعامل در تولید انرژی الکتریکی در برابر حوادث طبیعی (سیل، زلزله و ...) پیش از ساخت نیروگاه‌ها، ابتدا مکان‌یابی با توجه به تمامی پارامترهای زیر صورت می‌گیرد و حتی‌الامکان مکانی انتخاب می‌گردد که:

- سیل‌گیر نباشد
- دارای زمین سست نباشد
- بر روی گسل‌های شناخته‌شده قرار نگرفته باشد



شکل ۱- منابع تولید پراکنده

۳-۲- اعمال پدافند غیرعامل به پست‌های الکتریکی برق

اصول پدافند غیرعامل در پست عبارت‌اند از:

الف- استتار و اختفا در پست‌ها: برای رسیدن به این منظور پست‌های GISکه می‌توان آن‌ها را در زیرزمین و دور از تیررس دشمن و نیز دور از بلایای طبیعی از قبیل سیل و طوفان و ... بنا نمود.

ب- پراکندگی پست‌ها: پراکندگی پست‌های برق امری است که به خودی خود انجام گرفته است و همه پست‌ها در یک منطقه خاص جمع‌آوری نمی‌شوند و در هر جایی که نیاز باشد، بنا می‌شوند و این اصل از اصول پدافند غیرعامل در پست‌ها به صورت ذاتی قرار دارد.

ج- مقاوم‌سازی و استحکام :پدافند غیرعامل در برابر حوادثی از قبیل زلزله و طوفان و ... در پروژه ساخت پست‌ها در نظر گرفته می‌شود و آن‌ها را در مقابل زلزله و طوفان مقاوم می‌سازند. با توجه به هزینه سرمایه‌گذاری، بهره‌برداری و نگهداری بالا، مزایای عمده GIS را می‌توان به‌صورت زیر برشمرد [۱۲]:

- فضای لازم بسیار کم
- عدم حساسیت به تأثیرات خارجی
- سازگاری با محیط
- ایمنی افراد و تجهیزات

این نوع پست‌ها جهت مناطق مسکونی و صنعتی، کوهستانی، دریایی، زیرزمینی و سیار، مناسب می‌باشند.

۳-۳- اعمال پدافند غیرعامل به خطوط انتقال انرژی الکتریکی

اصول پدافند غیرعامل در خطوط انتقال انرژی الکتریکی عبارت‌اند از:

الف- استتار و اختفا: به لحاظ امنیت ملی هرچه خطوط انرژی در دسترس‌تر نباشند، مطلوب‌تر است. چرا که بایستی ساماندهی کالبدی شهر بر اساس اصول پدافند غیرعامل و جهت حفاظت از منافع شهروندان و دارایی همگانی در برابر بحران‌های طبیعی و غیرطبیعی باشد و افزایش ایمنی اماکن حیاتی و شریان‌های مهم و حساس مانند خطوط انتقال انرژی برق موجب ارتقاء قابلیت‌های

شبکه در شرایط تهدید می‌گردد که با گسترش زیرساخت‌ها و سازه‌های ایمن و مقاوم امکان‌پذیر است.

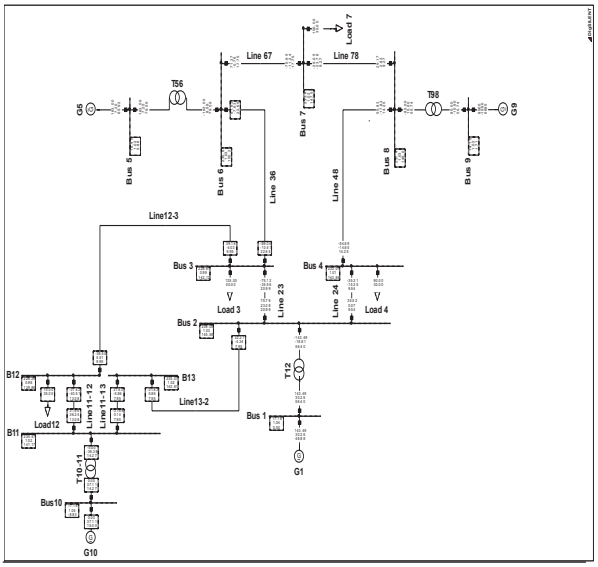
ب- پوشش: پنهان‌سازی و حفاظت تأسیسات و تجهیزات در برابر عوامل طبیعی و غیرطبیعی (صاعقه و...)

ج- مقاوم‌سازی و استحکامات: لحاظ کردن ضوابط اجرایی سازه‌های امن و استحکامات لازم در زیرزمین و تونل‌ها یکی از راهکارهای مناسب که هر سه آیتم فوق در آن لحاظ شده باشد خطوط انتقال GIL است که در داخل تونل زیرزمینی مشترک تأسیساتی و یا اختصاصی و در زیرزمین احداث می‌گردد [۲].

۵- شبیه‌سازی و بررسی آثار حمله تروریستی به اجزای یک سامانه تولید انرژی الکتریسیته متشکل از دو شبکه متصل به هم و بهره‌گیری از توربین بادی و انرژی خورشیدی به‌منظور تقویت سطح پدافند غیرعامل:

بعد از شبیه‌سازی شبکه ۹ باس IEEE و شبکه ۶ باس متصل به آن توسط نرم‌افزار Power Factory Digsilent و محاسبه پخش بار، همان‌طور که در شکل (۲) مشاهده می‌کنید چون شبکه در حالت نرمال خود بوده و اجزای شبکه با هیچ‌گونه تهدید تروریستی روبرو نیستند؛ در شبکه هیچ‌گونه اضافه‌بار، افت ولتاژ و یا اضافه ولتاژی مشاهده نمی‌شود و عمل پخش بار بین بارها به‌درستی و با موفقیت انجام می‌پذیرد. در تنظیمات شبکه شبیه‌سازی‌شده، رنگ آبی نشان‌دهنده افت ولتاژ، رنگ سبز نشان‌دهنده اضافه ولتاژ و رنگ قرمز نشان‌دهنده اضافه‌بار می‌باشد.

با تغییر ساختار جدیدی که در سال‌های اخیر در سامانه های قدرت پدید آمده و باعث شده است که واحدهای تولیدی، توان الکتریکی هرچه بیشتری را از خطوط انتقال عبور دهند، بدین ترتیب انتظار می‌رود شاهد فروپاشی ولتاژ گسترده‌تر و بیشتر سامانه‌های قدرت باشیم. برای مثال، عبور توان بیش از حد از یک خط انتقال باعث افت ولتاژ بیش از حد و کاهش ظرفیت انتقال توان الکتریکی به بخش مشخصی از سامانه قدرت گردد. تعریف IEEE از پایداری ولتاژ عبارت است از توانایی یک سامانه قدرت در نگهداری ولتاژ دائمی در همه شین‌های سامانه بعد از بروز اغتشاش در شرایط مشخصی از بهره‌برداری. اغتشاش ممکن است به‌دلیل خروج ناگهانی یکی از تجهیزات در اثر حملات تروریستی به یکی از

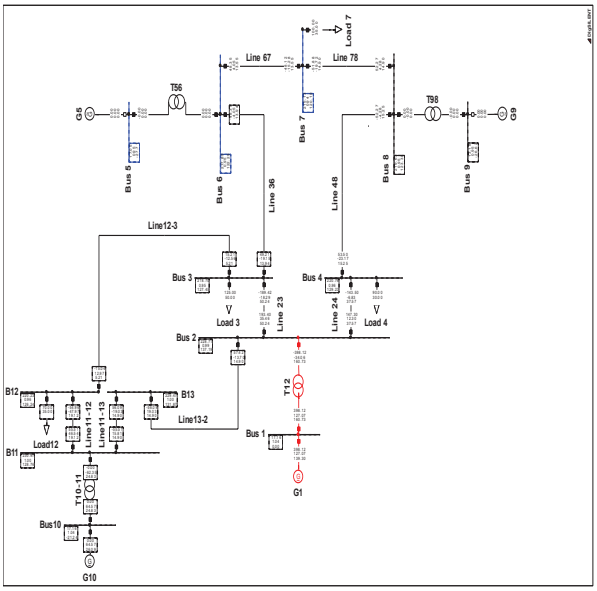


شکل ۲- شبیه‌سازی سامانه قدرت در حالت نرمال

اجزاء شبکه یا افزایش تدریجی بار باشد. فروپاشی ولتاژ هنگامی رخ می‌دهد که افزایش بار باعث غیرقابل‌کنترل شدن ولتاژ در ناحیه مشخصی از سامانه قدرت گردد. بنابراین ناپایداری ولتاژ در طبیعت، خود یک پدیده ناحیه‌ای است، که می‌تواند به صورت فروپاشی ولتاژ کلی بدون هیچ پاسخ سریعی بدل گردد [۱۳].

چنانچه ژنراتور g5 و g9 به‌طور هم‌زمان تحت حملات تروریستی قرار گیرند و از مدار خارج شوند، همان‌طور که در شکل (۳) مشاهده می‌کنید شبکه از حالت نرمال خود خارج شده و یک‌سری از باس‌بارها دچار افت ولتاژ و یکسری از ترانسفورماتورها و ژنراتورها دچار اضافه‌بار می‌شوند که این مسئله برای شبکه خوب نمی‌باشد. اگر در یک گوشه از شبکه، بنا به دلایلی ولتاژ شبکه افت کند و این افت را ژنراتورهای دیگر و یا سامانه‌های جبران کننده توان واکنشی جبران کنند ولتاژ به حالت عادی برمی‌گردد. در غیر این صورت چنانچه در این شرایط مشکل دیگری به سامانه وارد شود ممکن است مقدار افت ولتاژ به حد غیر قابل قبول برسد و رله‌های زیرولتاژ بعضی واحدهای تولیدی دیگر را از مدار خارج کنند و این عمل به نوبه خود باعث افت ولتاژ بیشتر شده و شبکه به چندین جزیره تبدیل می‌شود.

چنانچه در شکل (۳) علاوه بر ژنراتورهای g5 و g9، خطوط اتصال‌دهنده دو شبکه (line13-2 و line12-3) مورد حمله قرار گیرند، علاوه بر شین‌های ۵، ۶ و ۷، شین‌های ۳، ۴، ۸ و ۹ نیز دچار افت ولتاژ می‌شود که در این‌صورت، فشار وارده بر سامانه مذکور زیادتر می‌شود و باید هرچه سریع‌تر تمهیدات لازم صورت پذیرد.



شکل ۳– شبیه‌سازی سامانه قدرت با اعمال حمله فرضی به ژنراتورهای g5 و g9

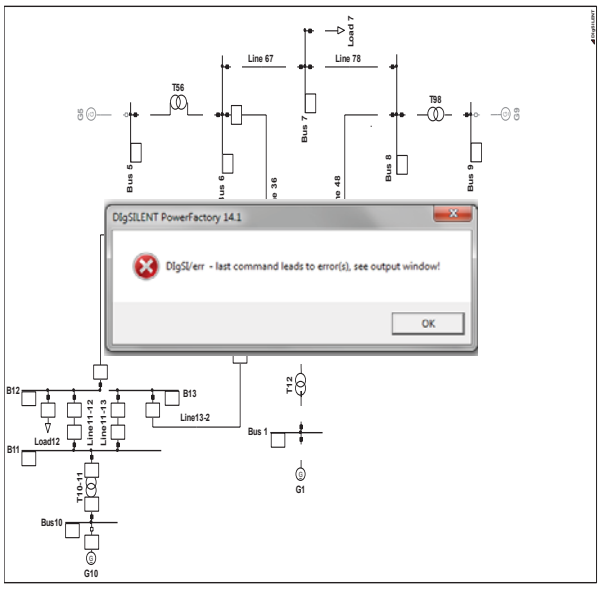
چنانچه در شکل فوق، علاوه بر ژنراتورهای g5 و g9، خطوط اتصال‌دهنده دو شبکه (line13-2 و line12-3) مورد حمله قرار گیرند علاوه‌بر باس‌بارهای ۵، ۶ و ۷، باس‌های ۳، ۴، ۸ و ۹ نیز دچار افت ولتاژ می‌شود که در این‌صورت، فشار وارده بر سامانه مذکور زیادتر می‌شود و باید هرچه سریع‌تر تمهیدات لازم صورت پذیرد.

حال چنانچه خطوط line13-2 و line12-3 وصل باشند، مقداری از فشار وارده به کل سامانه با تزریق توان از شبکه متصل به شبکه ۹ باسه، کاسته شده و همچنین با توجه به شکل (۴) از تعداد باس‌های زیر افت ولتاژ، کاسته می‌شود.

تمرکززدایی و پراکنده‌سازی، یکی از اصول مهم پدافند غیرعامل می‌باشد. بر همین اساس، می‌توان منابع تولید انرژی الکتریکی را نیز به‌صورت گسترده و پراکنده ایجاد نمود. امروزه منابع تولید پراکنده به‌دلیل اثرات چشمگیری که در روند خصوصی‌سازی داشته و همچنین به دلیل مزایایی که در بهبود پارامترهای شبکه دارند، به‌طور گسترده در سطح جهان مورد بهره‌برداری قرار می‌گیرند. همچنین امروزه بهره‌گیری از انرژی‌های تجدیدپذیر در جهان به‌دلیل مسائل زیست‌محیطی و کاهش ذخایر منابع سوخت‌های فسیلی رشد چشمگیری کرده است [۱۰]. کشور ایران نیز با توجه به وضعیت اقلیمی و آب و هوایی، منابع بالقوه بسیار زیادی به‌خصوص در زمینه انرژی خورشیدی و بادی دارد. از دیدگاه پدافند غیرعامل، منابع انرژی‌های تجدیدپذیر، منابع راهبردی به حساب می‌روند زیرا این منابع پایدار بوده و در صورت وقوع جنگ و یا تحریم‌های گوناگون، می‌توانند جایگزین مناسبی برای سوخت‌های فسیلی باشند.

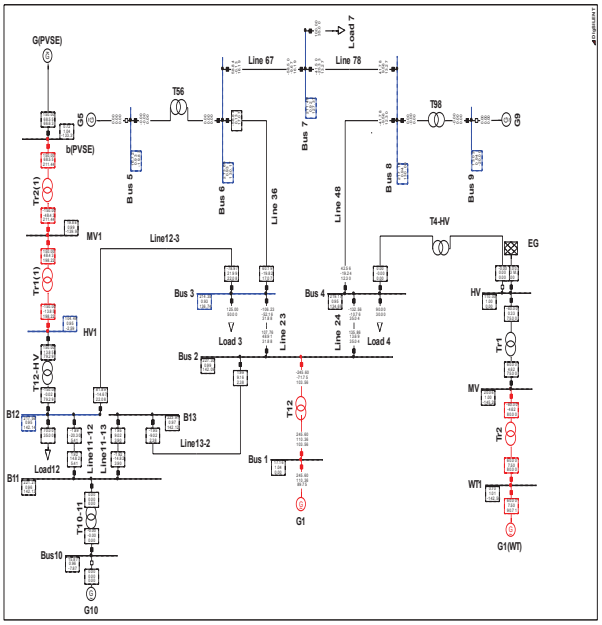
در صورتی که از دیدگاه پدافند غیرعامل نیز به این مسئله توجه شود، تولیدات پراکنده، اثرات قابل توجهی در بهبود سطح پدافند غیرعامل در حوزه انرژی خواهد داشت. در صورتی که شبکه‌های الکتریکی قابلیت عملکرد جزیره‌ای داشته باشند، این اثر بسیار چشمگیر خواهد بود. پراکنده‌سازی باعث تعدد اهداف شده و به‌عنوان مثال، درصورتی‌که برای قطع کامل برق در استان تهران، به تعداد نیروگاه‌های موجود در این استان، نیاز به بمب گرافیتی باشد، با رشد و گسترش بهره‌گیری از منابع تولید پراکنده، این عدد به چند ده برابر می‌رسد و به نوعی کشور متخاصم نمی‌تواند از این حربه بهره‌ای ببرد. اما چنانچه علاوه‌بر ژنراتورهای G5 و G9 از شبکه (۱) و ژنراتور G10 از شبکه (۲) به‌صورت هم‌زمان مورد حمله فرضی تروریستی قرار بگیرند، همان‌طور که در شکل (۴) مشاهده می‌شود عمل پخش بار در کل سامانه با مشکل مواجه می‌شود و شبکه قادر به پاسخگویی به بارها نمی‌باشد و با error روبرو خواهد شد.

بنابراین، بهترین حالت استفاده از انرژی‌های تجدیدپذیر مانند مزارع بادی و مزارع خورشیدی به‌عنوان نیروگاه‌های جایگزین هست تا درصورتی‌که نیروگاه‌های اصلی در شبکه برق به هر دلیلی از شبکه خارج شدند این منابع جایگزین وارد مدار شده تا برق‌رسانی به بارها در شبکه قطع نگردد.

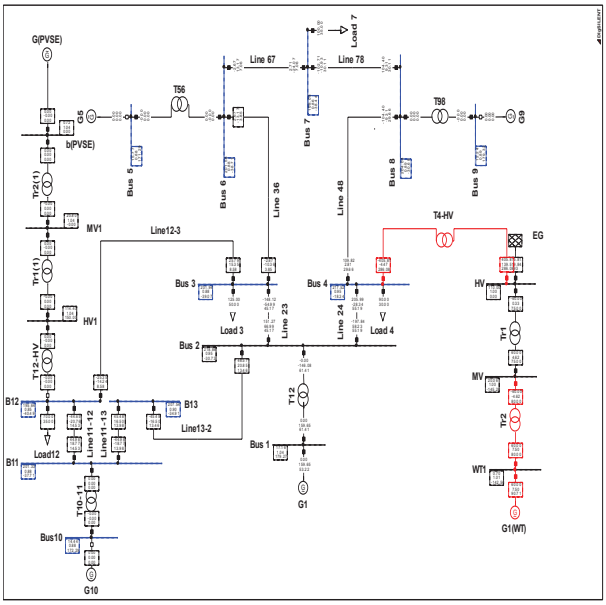


شکل ۴– حمله فرضی به ژنراتورهای g9 و g5 و g10 در یک سامانه تولید انرژی الکتریسیته متشکل از دو شبکه متصل به هم

در این سامانه توربین بادی متصل به شبکه (۱) و مزرعه خورشیدی متصل به شبکه (۲) هستند. در شکل‌های (۵) الی (۸) حالات مختلف اتصال توربین بادی و نیروگاه خورشیدی به شبکه نشان داده شده است که در هر سه حالت، شبکه قادر به توان‌رسانی به بارها می‌باشد.

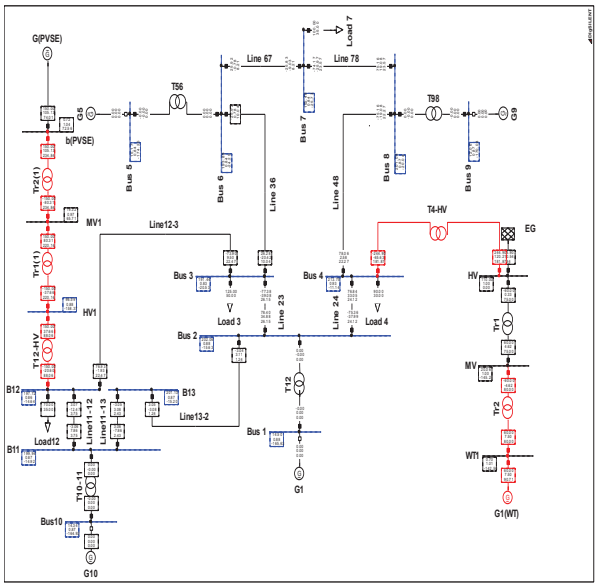


شکل ۵– توربین بادی خارج از مدار و مزرعه خورشیدی متصل به شبکه (۲)



شکل ۶– توربین بادی متصل به شبکه (۱) و مزرعه خورشیدی خارج از مدار

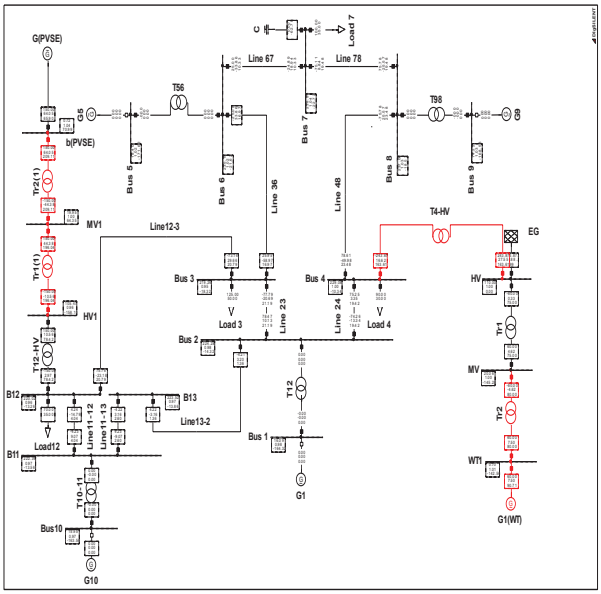
همان‌طور که در شکل (۸) مشاهده می‌کنید حتی اگر تمام ژنراتورها تحت حمله تروریستی قرار گیرند و از مدار خارج شوند، باز هم سامانه تولید انرژی قادر به پاسخگویی بخشی از بارها می‌باشد که در این حالت، بسیاری از باس‌بارها دچار افت ولتاژ شده و باید در اسرع وقت اقدامات لازم انجام پذیرد و یکسری از بارهایی را که ضروری نیستند از مدار خارج کرد و یا با خازن‌گذاری مناسب در سامانه قدرت، افت ولتاژ باس‌ها بر طرف گردد؛ چه بسا که ممکن است کل سامانه با مشکل جدی روبرو شود.



شکل ۸– توربین بادی و مزرعه خورشیدی متصل به شبکه و ژنراتورهای هر دو شبکه خارج از مدار

استفاده از خازن به‌عنوان تولیدکننده بار راکتیو به‌منظور تنظیم، کنترل ولتاژ، جلوگیری از نوسانات قدرت در شبکه‌ها و اصلاح ضریب توان در مصرف کننده ها به‌علت ارزانی و سادگی سامانه آن بسیار متداول است. استفاده از خازن‌ها به‌صورت شنت و سری در شبکه امکان‌پذیر است. اثرات خازن‌گذاری را به‌صورت ذیل می‌توان دسته‌بندی نمود: کاهش تلفات و افت ولتاژ و در نتیجه، مخارج کمتر انرژی و افزایش ضریب قدرت که نهایتًا به کاهش سرمایه‌گذاری جهت استفاده از قدرت حقیقی می‌انجامد استفاده اقتصادی از ژنراتورها، ترانس‌ها، سیم‌ها، کابل‌ها و کلیدها، همه این موارد به علت کاهش جریان راکتیو در تمام سامانه قدرت، از تولیدکننده تا مصرف کننده است. کاهش جریان و افزایش ضریب قدرت، سبب کاهش افت ولتاژ می‌گردد که این هم از مزایای خازن‌گذاری است. در شکل (۹) با توجه به این‌که افت ولتاژ باس ۷ از سایر باس‌بارهای دیگر کمتر

می‌باشد؛ به‌همین منظور خازن را روی باس ۷ قرار می‌دهیم که با خازن‌گذاری روی باس ۷ از شبکه (۱)، افت ولتاژ کل سامانه قدرت برطرف می‌گردد و نیازی به خارج کردن هیچ‌کدام از بارها از مدار نمی‌باشد.



شکل ۹- توربین بادی و مزرعه خورشیدی متصل به شبکه، ژنراتورهای هر دو شبکه خارج از مدار و خازن گذاری روی باسبار ۷

۶- نتیجه‌گیری

امروزه سامانه‌های تولید و انتقال انرژی الکتریسیته به‌عنوان یکی از اهداف راهبردی در جنگ‌های مدرن می‌باشند و خطرات گوناگونی آن‌ها را تهدید می‌نماید که بایستی جهت مقابله با آن‌ها تمهیداتی در نظر گرفته شود. بهره‌گیری از منابع انرژی تجدیدپذیر، می‌تواند راه‌حلی مناسب جهت بهبود پدافند غیرعامل در حوزه انرژی الکتریسیته باشد. البته چنانچه در یک سامانه قدرت، تولیدکننده‌ها به طور همزمان مورد حمله تروریستی قرار گیرند، اکثر باسبارها دچار افت ولتاژ می‌شوند؛ در این مقاله با خازن‌گذاری روی باس ۷ به‌دلیل بیشترین افت ولتاژ، مشکل افت ولتاژ سامانه قدرت، بدون این‌که باری از شبکه خارج شود، برطرف می‌شود که این امر قابلیت اطمینان شبکه را بالا می‌برد.

۷- مراجع

۱. مسکنی، حامد، علیشاهی، ذبیحی، سعیدمحسن، ارائه روشی جدید در کشور جهت ایجاد یک ریز شبکه در مراکز حساس باهدف ارتقای سطح پدافند غیرعامل در حوزه انرژی، نخستین کنگره اتوماسیون صنعت برق، دانشگاه فردوسی مشهد،۱۳۹۱.

۲. گندمکار، مجید، دادفر، سجاد، عزتی، سید میثم، مبانی پدافندغیرعامل و مصادیق آن در صنعت برق با نگاه به مدیریت استراتژیک، شانزدهمین کنفرانس ملی دانشجویی مهندسی برق ایران، شهریور ماه ۱۳۹۰.

3. Swiss Federal Office of Energy, “Report on the blackout in Italy on 28 September 2003,” Nov. 2003.

4. . Landstedt, Holmst, and M. Petter, “Electric power systems blackouts and the rescue services: the case of Finland, CIVPRO working paper 2007, vol. 1, 2007.

5. South China Bureau of State Electricity Regulatory Commission, “Power system operation condition report during 2008 snow disaster,” Guangzhou, China, Tech. Rep., Feb. 2008.

6. J. Watson editors, “Power failure leaves 5 million in the dark [Internet],” San Diego: The San Francisco Chronicle, 2011. <http://www.sfgate.com/cgi-bin/ article. cgi?f=/c/a/2011/09/08/ MND01L 2A1P.DTL> [cited 09.07.12].

7. US–Canada Power System Outage Task Force, “Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommendations,” April. 2004.

8. R. Zimmerman and C. E. Restrepo, “Simonoff JS,” Lave L. Risk and economic costs of a terrorist attack on the electric system [Internet]. Presentation for the CREATE economics of terrorism symp; 2005. <http://create.usc.edu/assets/pdf/ 51818.pdf> [cited 09.07.12].

9. Start, “2010 Global Terrorism Database,” Retrieved January 2010 /http://www.start.umd.edu / gtd/S.

10. National Counter terrorism Center, “World wide Incidents Tracking System Retrieved,” January 2010. /http://wits.nctc.gov/S, 2010.

11. K. V . Rupchand, “Importance of Reversible Hydro for Smart Grid,” IEEE PES ISGT Asia2014, KualaLumpur, May 2014.

12. http://www.hicoamerica.com/Files/

13. HICO.GIS.pdf

14. http://mohandesi-bargh.blogfa.com/post-191.aspx

Identifing Terrorist Threats on Electricity Grid and the Utilization of Renewable Resources and Capacitor Placement in Order to Strengthen the Passive Defense Surface

R. Haghmaram[1]

H. Rahmani[2]

Abstract

Security dangers to infrastructure and resources of electricity energy frequently as a source of concern on international issues listed so identify terrorist threats on this area is important. This paper with simulates a power generation system consisting of two interconnected networks focused onto potential threats in the field of security like terrorist attacks to electricity energy infrastructure such as plants and benefiting from renewable resources and capacitor appropriate placement try in passive defense surface promotion on the field of electricity. In this system different scenarios attack to generators and using of renewable sources and capacitor have been investigated. Capacitor placement reduces losses and voltage drop and therefore causes lower energy costs and increased reliability becomes.

Key Words: *Terrorist Threats, Passive Defense, Renewable Resources, Capacitor Placement.*

1- Assistant Professor and Academic Member of Imam Hussein Comprehensive University
2- Researcher of Imam Hossein University (hadi_rahmani65@yahoo.com)- Writer-in-Charge