فصلنامه علمی-ترویجی پدافند غیرعامل
سال هشتم، شماره ۲، تابستان ۱۳۹۶، (پیاپی ۳۰): صص ۵۳-۴۳

ارائه راه‌کارهای پدافند غیرعامل جهت جلوگیری از ایجاد خاموشی سراسری در ایران

سید پوریا مدنی[۱]، رضا دشتی[۲*]

تاریخ دریافت: ۱۳۹۵/۰۸/۰۵
تاریخ پذیرش: ۱۳۹۵/۱۱/۲۴

چکیده

امروزه انرژی برق به‌عنوان یکی از نیازهای حیاتی و اساسی هر جامعه‌ای محسوب می‌شود و تداوم آن دارای اهمیت بسیار زیادی است به‌طوری‌که در صورت قطع آن علاوه بر این‌که خسارت‌هایی به بخش‌های خانگی، صنعتی و کشاورزی وارد می‌کند، می‌تواند به‌عنوان یک تهدید جدی فراروی امنیت ملی به‌حساب آید. از سوی دیگر انرژی برق به‌عنوان در دسترس ترین و آسان‌ترین انرژی به شمار می‌رود و قطع آن می‌تواند به‌عنوان اقدام و هدفی بااهمیت از سوی گروه‌های تروریستی و دولت‌های متخاصم برای ضربه زدن و فلج کردن جوامع مورداستفاده قرار گیرد؛ بنابراین تحلیل و شناسایی نقاط ضعف سیستم در هریک از بخش‌های تولید، انتقال و توزیع و اقدامات مؤثر در جهت حل عیوب شبکه و اتخاذ راهکارهای مناسب در برخورد با تهدیدات دشمن امری مهم و ضروری است. با توجه به اهداف و مطالب بیان‌شده، اهمیت شبکه انرژی برق از نگاه پدافند غیرعامل به‌منظور حفظ، تداوم و تأمین این انرژی مهم در مواقع بحران و موردتوجه بودن این شبکه‌های زیرساختی برای کشور متخاصم و گروه‌های تروریستی انکارناپذیر است لذا هدف از نوشتن این مقاله تحلیل و بررسی ۳۰ خاموشی سراسری جهان و ایران و بیان علل ایجاد آن و ارائه راهکارهای پدافند غیرعامل جهت جلوگیری از ایجاد خاموشی سراسری و برخورد سریع و مناسب جهت مقابله با اقدامات تروریستی و بالا بردن سطح قابلیت اطمینان شبکه سراسری برق ایران است.

کلیدواژه‌ها: **امنیت ملی، خاموشی سراسری، پدافند غیرعامل، قابلیت اطمینان**

۱- کارشناسی، دانشگاه صنعتی قم
۲- استادیار، دانشگاه علم و صنعت، Email: drrezadashti@yahoo.com- نویسنده مسئول

۱- مقدمه

انرژی برق دارای مصارف متنوعی است و نیازهای متعددی از جامعه را پاسخ می‌دهد. ازجمله این مصارف می‌توان به مصارف خانگی و تجاری، صنعتی و کشاورزی، نظامی و عمومی اشاره کرد. در بسیاری از این موارد تداوم انرژی برق دارای اهمیت کلیدی است. به‌طوری‌که با قطع برق بیمارستان‌ها، مراکز کنترل و مدیریت متمرکز شبکه برق (اتاق کنترل) و مراکز حیاتی و حساس دیگر، نظم اجتماعی به‌هم‌ریخته و بدین ترتیب با ادامه یافتن وقفه در استمرار خدمات‌رسانی به مردم و جامعه، آستانه مقاومت ملی کاهش می‌یابد و اداره کردن کشور با چالش‌های جدی مواجه می‌شود. قطع نیازهای حیاتی جامعه در زمان جنگ و یا محاصره از روش‌های مرسوم در تمامی اعصار بوده است. با توجه به این‌که انرژی برق اکنون از یک خدمت یا کالای رفاهی به یک نیاز حیاتی تبدیل‌شده و کلیه نیازهای حیاتی چون تأمین آب، نان، گرما و... در جامعه امروزی به برق وابسته شده‌اند، ازاین‌رو برق به‌عنوان آسان‌ترین و در دسترس‌ترین روش جهت وارد آوردن آسیب به شمار می‌رود.

جهت تأمین کلیه مصارف، صنعت برق در سه وجه تولید، انتقال و توزیع گسترش‌یافته است. توجه مدیران صنعت برق همواره به توسعه تولید و احداث نیروگاه‌ها در مرحله اول و توسعه و بهره‌برداری بهینه از شبکه‌های انتقال در مرحله دوم بوده است. این امر باعث شده که شبکه‌های توزیع در طول عمر صنعت برق کمتر موردتوجه قرار گیرند و اکنون تبدیل به یکی از معضل‌های اصلی در صنعت برق گردند. شبکه‌های انتقال و همچنین نیروگاه‌ها به‌عنوان دارایی‌های حساس شمرده می‌شوند به‌طوری‌که با قطع و اختلال در آن‌ها حجم زیادی از شبکه‌ها و حوزه‌های جغرافیایی در خاموشی برق فرو می‌رود. باید توجه داشت انجام تدابیری در شبکه‌های توزیع می‌توانند تأثیر بسزایی بر کاهش اثر تهدیدها و یا سطح آسیب داشته باشد. اهداف پدافند غیرعامل در شبکه‌های انرژی برق را می‌توان به شرح زیر بیان داشت:

- حفاظت از سرمایه‌ها
- افزایش قابلیت اطمینان برق‌رسانی به‌ویژه برای مصارف حیاتی، حساس و مهم
- افزایش کیفیت توان به‌ویژه برای مصارف حیاتی، حساس و مهم

با توجه به اهداف و مطالب بیان‌شده، اهمیت شبکه انرژی برق از نگاه پدافند غیرعامل به‌منظور حفظ تداوم تأمین این انرژی مهم در مواقع بحران و موردتوجه بودن این شبکه‌های زیرساختی برای کشور متخاصم و گروه‌های تروریست انکارناپذیر است.

تاکنون در ایران تحقیقاتی در زمینه خاموشی سراسری و بررسی علل ایجاد آن تنها به‌صورت موردی (خاموشی سراسری در یک حادثه‌ای خاص) [۱۰ و ۱۳] و یا خاموشی‌های سراسری در سطح کل کشور مورد تحلیل و بررسی قرارگرفته است [۸ و ۱۵] همچنین در جهان نیز تحقیقاتی پیرامون خاموشی‌های سراسری انجام‌شده است که گستردگی آن در بخشی از آن‌ها در حد چند کشور [۱۴و ۱۸] و در بخشی دیگر از آن‌ها در سطح کل کشور [۶ و ۹] و یا در منطقه وسیعی از یک کشور [۵] اتفاق افتاده است.

در همه منابع مذکور دلایل خاموشی سراسری فقط از دید فنی مطرح‌شده و نسبت به بیان ارائه راهکار جهت جلوگیری از ایجاد خاموشی سراسری و بیان راهکارهای پدافند غیرعامل مطلبی بیان‌نشده است.

در این مقاله، تمامی خاموشی‌های سراسری جهان از سال ۱۹۶۵ میلادی (۱۳۴۴ شمسی) بیان می‌شود و زمان، مقدار انرژی ازدست‌رفته و دلایل ایجاد خاموشی سراسری موردبررسی و تحلیل قرار می‌گیرد، همچنین با بررسی و تحلیل آماری نمودارها و جداول راهکارهایی جهت جلوگیری از ایجاد خاموشی سراسری و مقابله با تهدیدات تروریستی دشمن ارائه می‌شود.

۲- شرح مسئله

با توجه به مطالب بیان‌شده، می‌توان به اهمیت و جایگاه کلیدی انرژی برق در فعالیت‌های حیاتی یک کشور پی برد. به‌طوری‌که با قطع این انرژی مهم فعالیت‌های حیاتی جامعه با اختلال جدی مواجه می‌شود. تاکنون چندین خاموشی سراسری در جهان اتفاق افتاده است که مطالعه هر یک می‌تواند در ارائه راهکارهای پدافندی و جلوگیری از تکرار آن تجارب ارزشمندی را ارائه دهد. بدین منظور در ادامه به تشریح بزرگ‌ترین خاموشی‌های سراسری جهان و خاموشی‌های سراسری ایران پرداخته‌شده است و علل آن را مورد تحلیل قرار می‌گیرد.

۲-۱- خاموشی سراسری در جهان

در این قسمت ۳۰ مورد از بزرگ‌ترین خاموشی‌های سراسری جهان و علل وقوع آن را به‌صورت جدول معرفی شده است [۴].

جدول ۱- علل ۳۰ خاموشی سراسری جهان

شماره	کشور یا شهر و سال وقوع	علل
۱	شمال شرق آمریکا و شمال کانادا (۱۹۶۵)	قطع شدن خطوط انتقال
۲	نیویورک (۱۹۷۷)	قطع شدن خطوط انتقال
۳	توکیو (۱۹۸۷)	رشد بار و ناپایداری ولتاژ [۷]
۴	رژیم صهیونیستی (۱۹۹۵)	قطع شدن خطوط انتقال [۱۷]
۵	غرب ایالات‌متحده (۱۹۹۶)	رشد بار و ناپایداری ولتاژ
۶	سواحل غربی ایالات‌متحده (۱۹۹۶)	قطع شدن خطوط انتقال
۷	تایوان (۱۹۹۹)	قطع شدن خطوط انتقال
۸	ایالات‌متحده و کانادا (۲۰۰۳)	عیب در نیروگاه
۹	لندن (۲۰۰۳)	عیب در پست برق
۱۰	سوئد (۲۰۰۳)	قطع شدن خطوط انتقال
۱۱	ایتالیا (۲۰۰۳)	قطع شدن خطوط انتقال [۱۱]
۱۲	لیبی (۲۰۰۳)	عیب در پست برق [۱۲]
۱۳	ایالات‌متحده، سانفرانسیسکو (۲۰۰۳)	عیب در پست برق
۱۴	آتن (۲۰۰۴)	رشد بار و ناپایداری ولتاژ
۱۵	اسپانیا (۲۰۰۴)	عیب در پست برق
۱۶	ویتنام (۲۰۰۵)	عیب در پست برق
۱۷	مسکو (۲۰۰۵)	رشد بار و ناپایداری ولتاژ
۱۸	اندونزی (۲۰۰۵)	عیب در نیروگاه
۱۹	لس‌آنجلس (۲۰۰۵)	رشد بار و ناپایداری ولتاژ
۲۰	هاینان چین (۲۰۰۵)	قطع شدن خطوط انتقال
۲۱	توکیو (۲۰۰۶)	قطع شدن خطوط انتقال
۲۲	پاکستان (۲۰۰۶)	عیب در پست برق
۲۳	آلمان، فرانسه، ایتالیا، اسپانیا (۲۰۰۶)	رشد بار و ناپایداری ولتاژ
۲۴	کلمبیا (۲۰۰۷)	عیب در نیروگاه
۲۵	چین (۲۰۰۸)	قطع شدن خطوط انتقال
۲۶	برزیل و پاراگوئه (۲۰۰۹)	عیب در پست برق
۲۷	برزیل (۲۰۱۱)	عیب در پست برق
۲۸	ایالات‌متحده و مکزیک (۲۰۱۱)	رشد بار و ناپایداری ولتاژ
۲۹	هند (۲۰۱۲)	رشد بار و ناپایداری ولتاژ [۱۸]
۳۰	کوبا (۲۰۱۲)	عیب در نیروگاه

۲-۲- خاموشی‌های سراسری در ایران

در ایران تاکنون ۳ خاموشی سراسری اتفاق افتاده است که در زیر زمان وقوع به همراه علل آن آورده شده است.

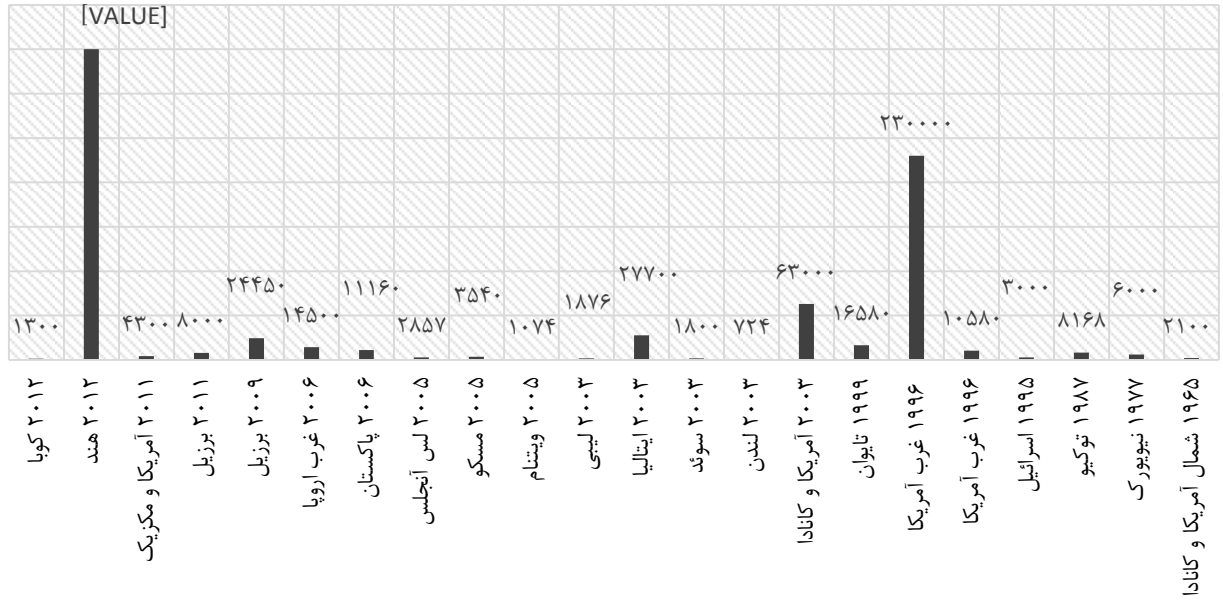
جدول ۲- علل ۳ خاموشی سراسری در ایران [۲، ۳، ۱۶]

شماره	تاریخ وقوع	علل
۱	۱۳۶۹/۵/۷	عملکرد بی‌دلیل رله بوخهلتس، خروج راکتورهای ثابت خطوط
۲	۱۳۸۰/۲/۳۰	توانایی نامناسب سامانه در پاسخ به اغتشاش، برنامه‌ریزی نامناسب تعمیر و نگهداری، خروج غیرضروری برخی خطوط انتقال، بار زدایی نامناسب
۳	۱۳۸۲/۱۱/۱۲	عملکرد ناموفق کلید، گسترش خطابه خطوط ۴۰۰ کیلوولت انتقال

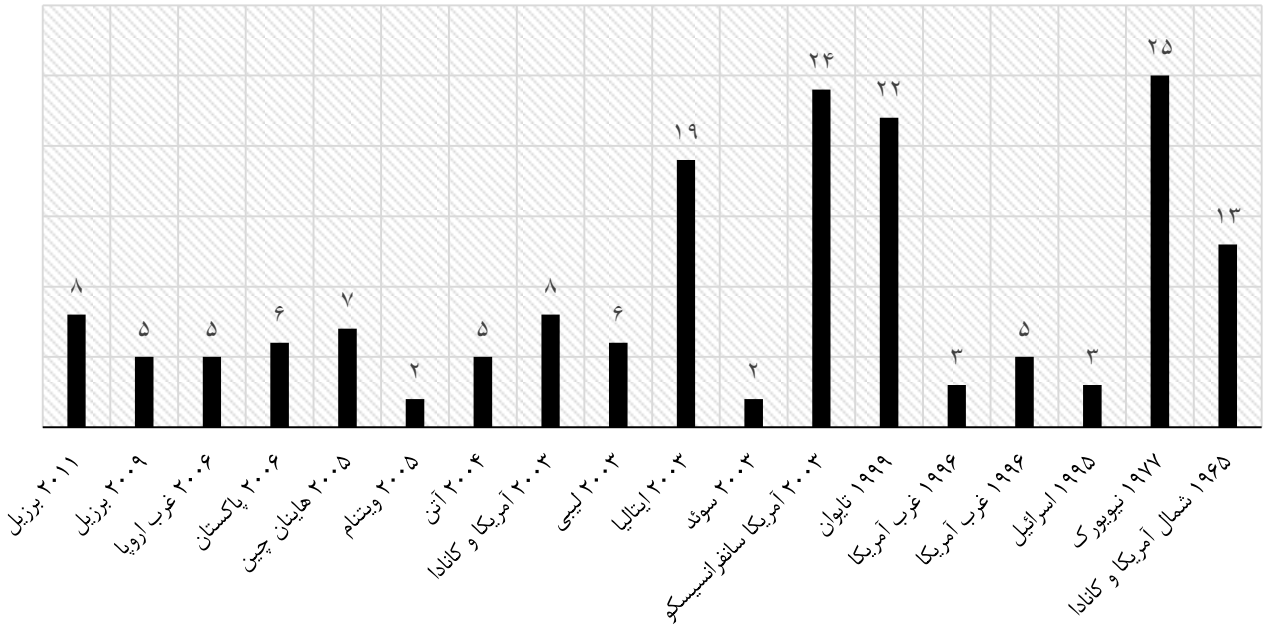
۲-۳- تحلیل آماری خاموشی‌های سراسری در جهان

شاخص‌های کلیدی ارزیابی خاموشی‌های سراسری اتفاق افتاده عبارتنداز: بار ازدست‌رفته، مدت‌زمان خاموشی و تعداد مشترکین و مصرف‌کنندگان خاموش شده. بزرگی هر یک از خاموشی‌ها از دید شبکه، فعالان صنعت برق و مصرف‌کنندگان به کمک یکی از سه شاخص فوق قابل ارزیابی خواهد بود.

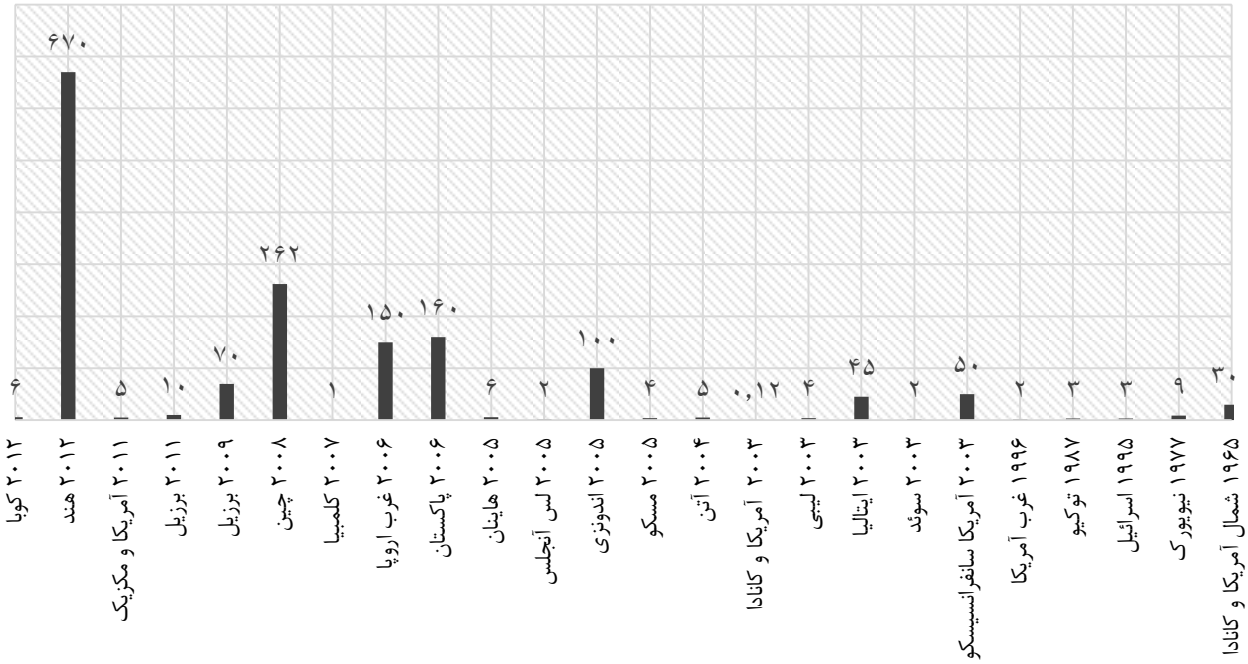
بدین منظور نمودارهای بار ازدست‌رفته، مدت‌زمان بازیابی سامانه و تعداد مصرف‌کنندگان تحت تأثیر خاموشی در شکل (۱ تا ۴) آمده است. همان‌طور که از نمودارها مشهود است، خاموشی سال ۲۰۱۲ در هند بزرگ‌ترین و گسترده‌ترین خاموشی است که حدود ۶۷۰ میلیون نفر تحت تأثیر این خاموشی بوده‌اند. همچنین از دید مدت‌زمان خاموشی (بازیابی سامانه) نیز خاموشی سراسری هند (نزدیک به ۴۸ ساعت) و همچنین ۱۹۹۷ نیویورک (۲۵ ساعت) بیشترین زمان را به خود اختصاص داده است.



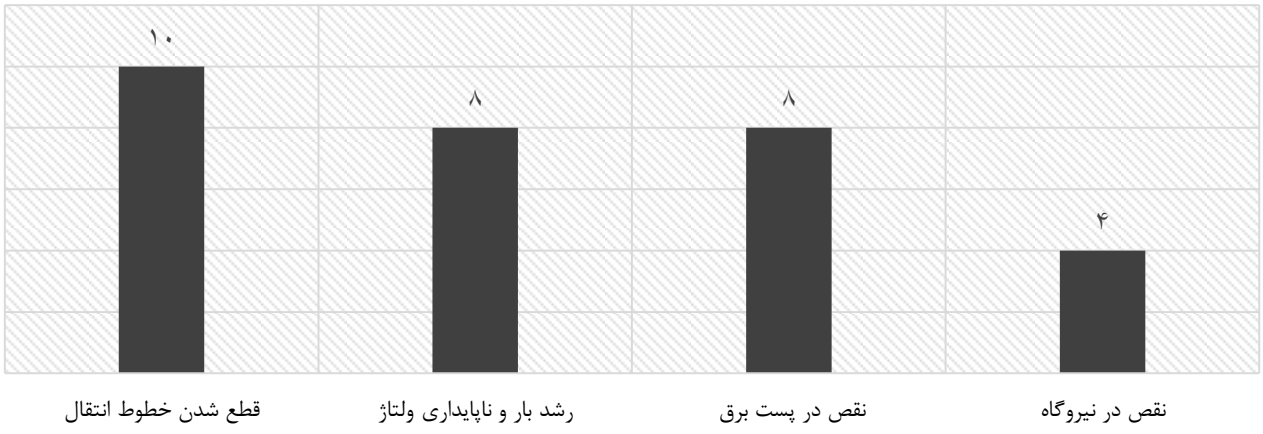
شکل ۱- نمودار بار از دست رفته (مگاوات)



شکل ۲- نمودار بازیابی سامانه (ساعت)



شکل ۳- نمودار تعداد مصرف کنندگان تحت تاثیر خاموشی (میلیون نفر)



شکل ۴- علل اصلی خاموشی از دید شبکه

۳- ریشه‌یابی و بررسی علل در خاموشی سراسری

۳-۱- علل اصلی خاموشی از دید شبکه

با توجه به نمودارها و مطالعات انجام‌شده علل اصلی خاموشی از دید شبکه به ۴ عامل قطع شدن خطوط انتقال، رشد بار و ناپایداری ولتاژ، نقص در پست برق و نقص در نیروگاه جدول (۱) تقسیم‌شده است. در شکل (۴) صرف‌نظر از علت اصلی عیب عامل شبکه‌ای هر خاموشی آورده شده است.

همان‌طور که از جدول (۱) و شکل (۴) ملاحظه می‌شود اختلالاتی که موجب خاموشی سراسری گردیده‌اند با ایجاد عیب در خطوط، پست‌ها و مراکز تولید شروع‌شده و گسترش‌یافته‌اند و یا این‌که تغییر غیرمنتظره و ناگهانی بار موجب خاموشی سراسری شده است.

۳-۲- ریشه‌یابی علل در خاموشی‌های سراسری

در این بخش علت اصلی قطع خطوط، پست‌ها و نیروگاه‌ها که از این به بعد دارایی‌های شبکه خوانده می‌شود، پرداخته می‌شود. بدین منظور عوامل اصلی به ۴ دسته اصلی عوامل خارجی، مسائل فنی،

مدیریت شبکه و سرمایه‌گذاری و بازار تقسیم می‌شود و به تشریح هر یک در خاموشی‌های سراسری می‌پردازد. با تقریب خوبی می‌توان گفت تاکنون در هر یک از خاموشی‌های سراسری اتفاق افتاده در کشورها، همه عوامل بیان‌شده نقش داشته‌اند.[۲۰]

عوامل خارجی: به مجموع عوامل غیر سامانه‌ای چون طوفان، سیل، آتش‌سوزی و ... اطلاق می‌شود که باعث ازکارافتادن دارایی‌های شبکه و یا تغییر شدید بار و مصرف می‌شود.

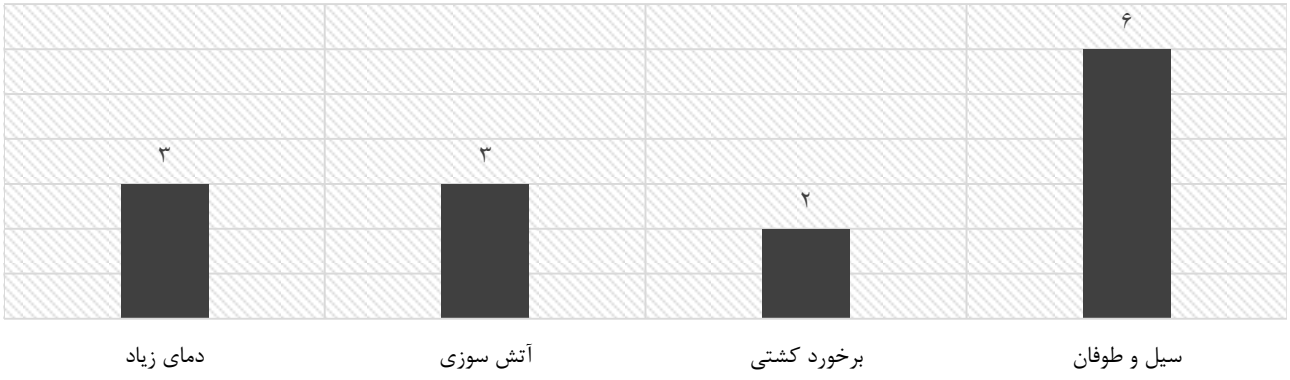
عوامل فنی: به نحوه ایجاد اختلال و گسترش خطا در شبکه اشاره دارد و علت‌های فنی اعم از هماهنگی‌های حفاظتی، اضافه‌بار خطوط، ساختار شبکه و... را بیان می‌کند.

عوامل مدیریت شبکه: عمدتاً شامل مدیریت شبکه در زمان وقوع حادثه و همچنین زیرساخت‌های سامانه جهت مواجهه با حادثه می‌شود. بدین ترتیب جریان صحیح و دقیق اطلاعات، اپراتوری صحیح و توازن تولید و مصرف ازجمله این عوامل هستند.

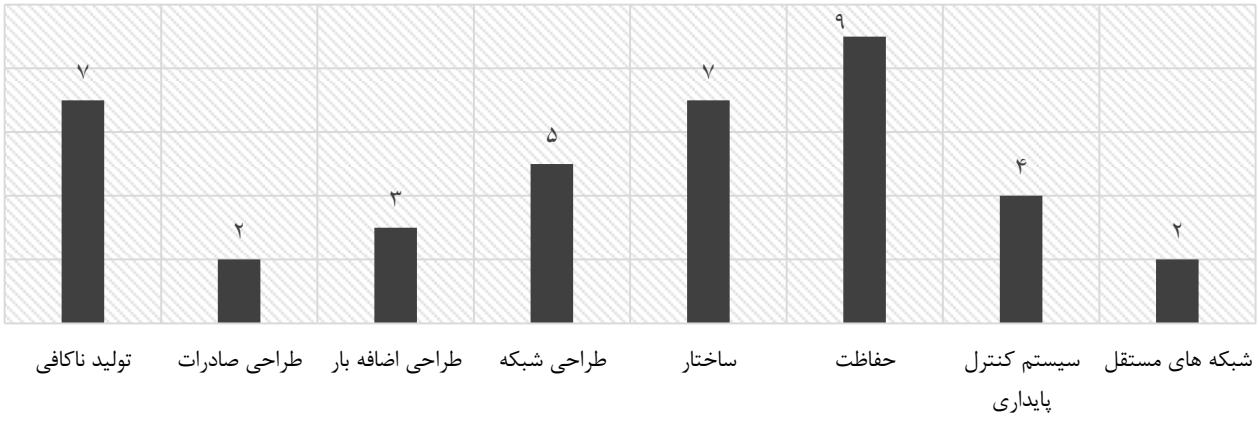
عوامل سرمایه‌گذاری و بازار: به مجموعه رویه‌های بازار برق و سرمایه‌گذاری مناسب و کافی اشاره دارد تا نقش آن‌ها را در خاموشی سراسری بیان نماید.

هر یک از عوامل چهارگانه خود به دسته‌های متنوعی قابل تقسیم‌بندی هستند. تحلیل هر یک از دسته‌بندی‌های ذکرشده می‌تواند راهکارهای پیشگیرانه‌ای را ارائه دهد.

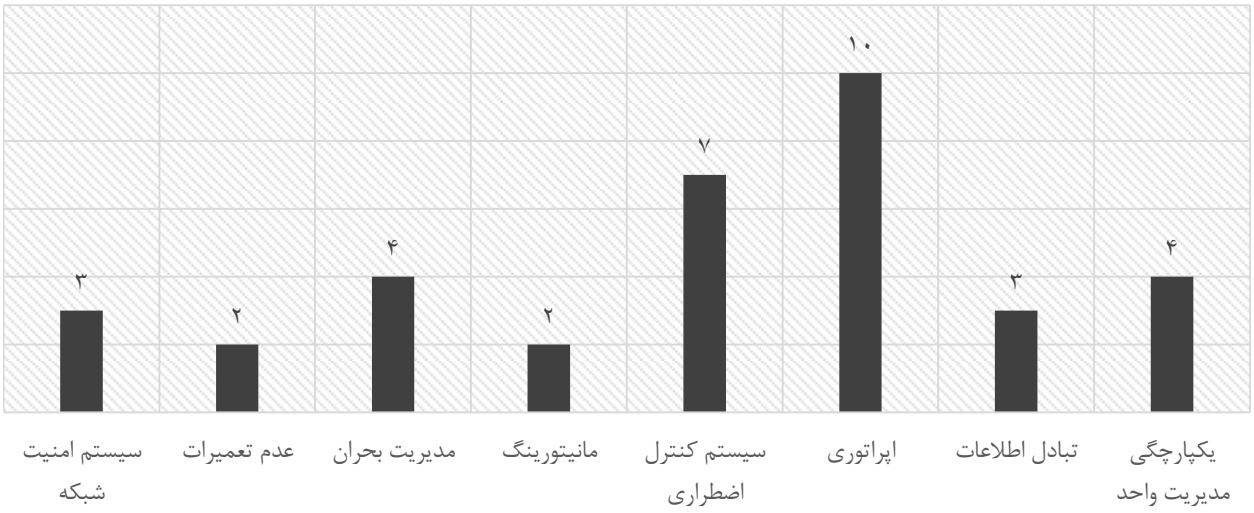
عوامل خارجی به ۴ دسته سیل و طوفان، برخورد کشتی، آتش‌سوزی و دمای زیاد هوا قابل‌تقسیم است. دمای زیاد به دلیل افزایش بار ناشی از به کار افتادن مصارف تهویه مطبوع، منجر به ناپایداری ولتاژ و اضافه‌بار دارایی‌های شبکه می‌گردد.



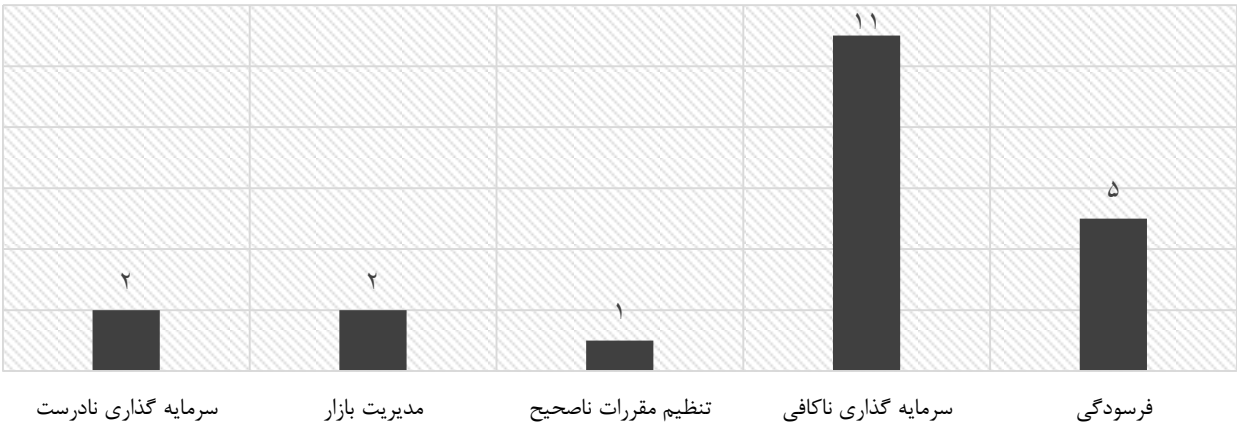
شکل ۵- دسته بندی خاموشی های سراسری ناشی از عوامل خارجی



شکل ۶- دسته بندی خاموشی های ناشی از مسائل فنی



شکل ۷- دسته بندی خاموشی های ناشی از مدیریت شبکه



شکل ۸- دسته بندی خاموشی های ناشی از سرمایه گذاری و بازار

عوامل فنی که در ایجاد خاموشی‌های سراسری دخیل بوده‌اند به دسته‌های مختلفی تقسیم می‌شوند. دسته‌بندی عوامل فنی را می‌توان به شرح زیر انجام داد:

وجود شبکه‌های مستقل متعدد با سطوح ولتاژ مختلف، حفاظت را با پیچیدگی و مشکلات متعددی مواجه می‌کند، عدم تعبیه و اشکال در سامانه کنترل پایداری، در صورت ایجاد خطا در این سامانه، خطا به‌سرعت گسترش‌یافته و منجر به خاموشی سراسری می‌شود، عدم عملکرد صحیح حفاظت [۱]، تولید ناکافی برق و طراحی نامناسب شبکه (تحقق شرط N-1 و پیش‌بینی اضافه‌بار، در نظر گرفتن ملاحظات صادرات و واردات برق و توپولوژی).

همان‌طور که پیش‌ازاین ذکر شد، یکی دیگر از عوامل مؤثر در خاموشی‌های سراسری، مدیریت شبکه است. عوامل مدیریت شبکه خود قابل تقسیم‌بندی به‌صورت زیر می‌باشند:

عدم یکپارچگی مدیریت واحد و جلوگیری از موازی کاری، عدم تبادل اطلاعات، عدم اپراتوری صحیح و تدوین دقیق سناریوهای

بحران، عدم وجود سامانه کنترل اضطراری، عدم پایشگری، نامناسب بودن مدیریت بحران، عدم تعمیرات و سامانه امنیت شبکه.

عامل نهایی در ایجاد خاموشی‌های سراسری، عامل سرمایه‌گذاری و بازار است. این عامل به میزان و کیفیت سرمایه‌گذاری و همچنین رویه‌های بازار برق اشاره دارد. این عامل در دسته‌های متنوعی قابل‌بررسی است که به شرح آن پرداخته‌شده است:

سرمایه‌گذاری ناکافی، فرسودگی، سرمایه‌گذاری نادرست، تنظیم مقررات ناصحیح، عدم مدیریت صحیح بازار.

بدین ترتیب با شناخت ضعف‌های شبکه‌ای (سامانه‌ای) در قبال پیامد خاموشی سراسری می‌بایست با بررسی و تحلیل آن بتوان راهکارهای پدافندی را ارائه نمود.

۴- تهدیدات تروریستی

با توجه به مطالب گفته‌شده، ضعف‌های کنترل شبکه که می‌تواند باعث ایجاد خاموشی‌های سراسری توسط اقدامات تروریستی شوند عبارتنداز:

- عدم مدیریت صحیح بحران (سهم ۲۵ درصد از کل)
- عدم پایشگری و شارش صحیح اطلاعات (سهم ۲۲ درصد از کل)
- اپراتوری ناصحیح (سهم ۳۱ درصد از کل)
- عدم وجود سامانه کنترل اضطراری (سهم ۲۲ درصد از کل). البته عوامل سامانه‌ای نیز وجود دارند که اگرچه دارای زمان اثرگذاری بالایی هستند اما پتانسیل بالایی در ایجاد ضعف در شبکه‌دارند، این عوامل را می‌توان به شرح ذیل دسته‌بندی نمود:
- عدم سرمایه‌گذاری کافی
- سرمایه‌گذاری غیر بهینه و ناصحیح
- مدیریت ناصحیح بازار
- تنظیم مقررات ناصحیح و خصوصی‌سازی ناصحیح

جدول ۳- آسیب‌پذیری شبکه برق در راستای پیامدی خاموشی سراسری

عیب اولیه	توسعه خاموشی	
	ضعف شبکه	ضعف کنترل شبکه
خط انتقال	عدم طراحی مناسب شبکه	اپراتوری ناصحیح
پست	عدم طراحی صحیح ادوات حفاظتی	عدم مدیریت بحران صحیح
رشد بار	تولید ناکافی در هر منطقه	عدم وجود سامانه کنترل اضطراری
نیروگاه	عدم عملکرد سامانه کنترل ناپایداری	عدم پایشگری و شارش صحیح اطلاعات

با توجه به آنچه گفته شد تهدیدات بالقوه به ازای هر آسیب‌پذیری را می‌توان به شرح جداول (۳ تا ۶) نمایش داد.

جدول ۴- تهدیدات بالقوه جهت شروع خاموشی

آسیب‌پذیری	نحوه تهدید
عیب در خط	واژگونی دکل‌ها، بمب گرافیتی
عیب در پست	انفجار، حمله سایبری، بمب گرافیتی، بمب لیزری
عیب در نیروگاه	انفجار، حمله سایبری، بمب گرافیتی، بمب لیزری، بمب الکترومغناطیسی
رشد ناگهانی	تحریک مصرف‌کنندگان، ایجاد مصرف مصنوعی

جدول ۵- تهدیدات بالقوه جهت توسعه خاموشی ناشی از ضعف‌های شبکه

آسیب‌پذیری	نحوه تهدید	شرط مؤثر بودن تهدید
عدم عملکرد صحیح ادوات حفاظتی	بمب الکترومغناطیسی	عدم شیلدینگ
	حمله سایبری	پیاده‌سازی خودکارسازی
	استفاده از عدم تنظیم بودن ادوات حفاظتی	شناسایی و مطالعه شبکه توسط متخاصم
عدم طراحی نامناسب شبکه	ایجاد چند خاموشی به‌صورت هم‌زمان	امکان حاکمیت چندساعته بر یک منطقه
	ایجاد اختلال در شبکه تبادل با کشورهای همسایه ایجاد عیب در دارایی‌های که شرط پایداری شبکه اضافه‌بار شدن حداقل یک دارایی دیگر باشد	شناسایی و مطالعه شبکه توسط متخاصم
تولید ناکافی در هر منطقه	ایجاد اختلال در نیروگاه‌ها، خطوط و پست‌های مهم	شناسایی و مطالعه شبکه توسط متخاصم
عدم عملکرد سیستم کنترل پایداری	بمب الکترومغناطیسی	عدم شیلدینگ
	حمله سایبری	پیاده‌سازی خودکارسازی
	ایجاد خطا در مناطق با عملکرد ناصحیح سیستم کنترل ناپایداری	شناسایی و مطالعه شبکه توسط متخاصم

جدول ۶- تهدیدات بالقوه جهت توسعه خاموشی ناشی از ضعف‌های کنترل شبکه

آسیب‌پذیری	نحوه تهدید	شرط مؤثر بودن تهدید
عدم مدیریت بحران صحیح	ایجاد اختلال با دستورات اشتباه	تطمیع یا نفوذ در منابع انسانی
عدم شارش صحیح اطلاعات	بمب الکترومغناطیسی	عدم شیلدینگ
	حمله سایبری	پیاده‌سازی خودکارسازی
	انجام اقدامات خرابکارانه	تطمیع یا نفوذ در منابع انسانی
اپراتوری ناصحیح	ایجاد عیب در دارایی‌ها که سامانه کنترل اضطراری ندارند	شناسایی و مطالعه شبکه توسط متخاصم
عدم وجود سامانه کنترل اضطراری	ایجاد عیب در دارایی‌ها که مدیریت بحران ضعیف دارند	شناسایی و مطالعه سامانه مدیریت توسط متخاصم

۵- نتیجه‌گیری

در این بخش با توجه به مطالعات انجام‌شده راهکارهای پدافند غیرعامل به تفکیک هر یک از تهدیدات شبکه ارائه می‌شود.

دسته اول تهدیدات، حجیم‌سازی دارایی‌ها است: بهترین راهکار در برابر این تهدید کاهش حساسیت خاموشی سراسری از طریق کوچک‌سازی دارایی‌ها و ایجاد پراکندگی در فضای سرزمین ملی و استانی است، بهترین راه تولید برق در شبکه توزیع برق و استفاده از تولیدات پراکنده است. این راهکار باعث امکان جزیره سازی شبکه در هنگام وقوع حادثه می‌شود. راهکارهای پدافند غیرعامل در دسته اول تهدیدات عبارتنداز:

- اصلاح خط و مشی مدیریت تولید به توسعه تولید در توزیع
- امکان جزیره سازی شبکه در هنگام وقوع حادثه
- کوچک‌سازی و ایجاد پراکندگی

دسته دوم تهدیدات، استفاده از بمب‌ها و تهدیدات نوین است: تهدیدات نوین شامل بمب‌های الکترومغناطیسی، گرافیتی و لیزری است که به ترتیب از طریق ایجاد اضافه ولتاژ، اتصال کوتاه و ایجاد حرارت متمرکز نسبت به تخریب دارایی‌های شبکه اقدام می‌کنند. بهترین راهکار در این بخش مقاوم‌سازی شبکه در برابر تهدیدات نوین چون شیلدینگ، کوتینگ و ... و همچنین کاهش حساسیت شبکه به یک دارایی خاص است. بدین ترتیب راهکارهای پدافند غیرعامل در دسته دوم تهدیدات عبارتنداز:

- شیلدینگ تجهیزات کنترلی و الکترونیکی
- کوتینگ و عایق کردن هادی‌ها
- ارتینگ بدنه و تجهیزات و تابلوها و ...

دسته سوم تهدیدات، حمله سایبری است: پس از پیاده‌سازی خودکارسازی و انجام پروژه‌های هوشمند سازی کلیه شبکه صنعت برق به‌صورت دیجیتالی و کامپیوتری فرمان پذیر می‌شوند. بدین ترتیب با حملات سایبری اطلاعات شبکه قابل‌برداشت و تغییر خواهد بود و فرمان‌ها نیز می‌تواند به‌تناسب دلخواه گروه متخاصم تغییر کند. بدین ترتیب پایداری شبکه با اختلال مواجه می‌شود. بدین ترتیب راهکارهای پدافند غیرعامل در دسته سوم تهدیدات عبارتنداز:

- طراحی بهینه شارش اطلاعات شبکه با حفظ امنیت آن‌ها و دسترس‌پذیری آن‌ها برای واحدهای اجرایی و تصمیم گیر [۱۹]
- ایجاد شبکه مخابراتی مستقل جهت بهبود امنیت و پایداری سامانه‌های مخابراتی
- ایجاد مقاوم‌سازی سایبری
- مجهز سازی شبکه به سامانه خودکارسازی و هوشمند سازی جهت افزایش سرعت عمل در هنگام حادثه
- توسعه پایشگری شبکه با ملاحظات دفاع سایبری

دسته چهارم تهدیدات، تحریک مصرف‌کنندگان به مصرف هم‌زمان است: این بخش که ازجمله تهدیدات مردم محوری است با تحریک مردم نسبت به افزایش ناگهانی مصرف شروع می‌شود و با ضعف‌های شبکه‌ای توسعه می‌یابد [۲۰]. معمولاً در طرح‌های شبکه، اضافه‌بار تا حدودی مشخص لحاظ می‌شود؛ بنابراین چهار روش مقابله با این تهدید وجود دارد:

- کنترل بار و مدیریت تقاضای مصرف‌کنندگان به‌ویژه از طریق پارامترهای اقتصادی و قیمت شناور برق
- افزایش تعداد و ظرفیت‌های خازن‌های نصب‌شده در شبکه توزیع جهت تأمین توان راکتیو و در بخش توزیع
- توسعه متوازن مراکز تولید
- توسعه متوازن نیروگاه‌ها با بار متوازن در مناطق جغرافیایی مختلف
- امکان‌سازی حذف بار
- استفاده از روش‌های حذف بار زیر نوین در زمان وقوع خطا یا عیب

دسته پنجم تهدیدات، شناسایی و ایجاد عیب در نقاط ضعف شبکه است: شناسایی نقاط ضعف شبکه یا از طریق برداشت و تحلیل اطلاعات صورت می‌پذیرد و یا با تطمیع عناصر مطلع در سامانه جمع‌آوری می‌شود. نقاطی چون نقاط با حفاظت نامناسب، کنترل پایداری مناسب، ضعف‌های طراحی شبکه چون ضعف در برابر اضافه‌بار و یا سامانه کنترل اضطراری نامناسب ازجمله این نقاط هستند [۶].

بدین ترتیب راهکارهای پدافند غیرعامل در دسته پنجم تهدیدات عبارتنداز:

- اصلاح ساختار شبکه و همچنین اصلاح رویه طراحی
- مدیریت بهینه بهره‌برداری
- مطالعه مجدد شبکه برق
- هماهنگی مطمئن بین حفاظت شبکه و تولید
- کنترل خودکار و دیجیتال سامانه تحریک ژنراتورها
- تعمیر و نگهداری منظم

دسته ششم تهدیدات، ایجاد چند خاموشی و عیب به‌صورت هم‌زمان است: به‌طورمعمول شبکه برق هر کشور باید با خروج هر دارایی (خط، پست و نیروگاه) پایدار باقی بماند؛ اما رفتارهای اقدامات تروریستی نشان می‌دهد که امروز حملات به شبکه برق باهدف از کار انداختن دو دارایی تغییر ماهیت داده‌اند. این مسئله با پیچیده کردن ساختار و توسعه خطوط رزرو و همچنین افزایش ذخیره چرخان قابل

جبران است؛ اما نیاز به هزینه کرد و سرمایه‌گذاری بیشتری است. بدین ترتیب راهکار عملی پدافند غیرعامل در دسته ششم تهدیدات عبارتنداز:

- اصلاح خط‌مشی مدیریت تولید به توسعه تولید در توزیع

دسته هفتم و هشتم تهدیدات، شناسایی و ایجاد عیب در نقاطی که توازن تولید و مصرف وجود ندارد همچنین شناسایی نقاطی که سامانه کنترل اضطراری وجود ندارد. بدین ترتیب راهکارهای پدافند غیرعامل در دسته هفتم و هشتم عبارتنداز:

- مجهز سازی شبکه به سامانه خودکارسازی
- افزایش تعداد، ظرفیت‌ها و توانایی واحدهای اضطراری استارت سریع
- توسعه پایشگری شبکه
- اصلاح خط‌مشی مدیریت تولید به توسعه تولید در توزیع

دسته نهم تهدیدات، نفوذ در منابع انسانی است: راهکارهای مقابله بانفوذ در بدنه اجرایی صنعت برق.

- مدیریت و فرماندهی واحد شبکه
- تقویت اپراتورها برای بهبود توانایی آن‌ها در مقابله با اختلالات
- عدم واگذاری شبکه انتقال به بخش خصوصی

دسته دهم تهدیدات، تحریم است: تحریم‌ها توانایی دولت را در کنترل و اداره امور اقتصادی کاهش می‌دهد، ازلحاظ خرید کالا و خدمات از کشورهای دیگر با محدودیت مواجه می‌کند و درنتیجه سطح خدمات را نسبت به تقاضای جامعه کاهش می‌دهد. به‌منظور مقابله با این تهدید چهار راهکار اساسی وجود دارد.

- کنترل سطح تقاضا
- خودکفایی و اقتصاد مقاومتی
- اصلاح تنظیم مقررات
- پیاده‌سازی ارزیابی اقتصادی و نظارت بر شرکت‌های تابعه وزارت نیرو
- متنوع سازی منابع و استفاده از نیروگاه‌های مختلف
- ایجاد تنوع در منابع خرید خارجی تجهیزات و منحصربه‌فرد
- نبودن منبع تولید و فروش کالا

امید است با توجه به مطالب ارائه‌شده از وقوع خاموشی سراسری چه از طریق عوامل غیرعمدی و یا عمدی در کشور جلوگیری و قدمی مؤثر در پیشرفت کشورمان برداشته باشیم.

۶- منابع

۱. صدرالسادات‌زاده، محمد، متین، تقی، بررسی حادثه مورخ ۱۳۶۹/۵/۷ شبکه سراسری و نتایج تجربی حاصله از آن، شرکت توانیر.

۲. قاشفیعی، محمد، آذری جهرمی، محمدجواد، بررسی نقش رژیم گذرا در انهدام کلید قدرت پست انجیرک، دانشکده مهندسی برق، دانشگاه صنعت آب و برق، بیست‌ویکمین اجلاس بین المللی برق، ۲۰۰۶.

۳. پرنیان، فرزین، تحلیل فروپاشی شبکه سراسری ایران در تاریخ ۱۳۸۰/۲/۳۰، گروه بهره‌برداری شبکه، پژوهشکده برق، پژوهشگاه نیرو، تهران، ایران.

۴. سایت جهانی تولیدات و مصارف انرژیwww.eia.gov

5. Z. Bo, O. Shaojie, Z. Jianhua, S. Hui, W. Geng, and Z. Ming, "An analysis of previous Blackouts in the World," lessons for china's power industry, Renewable and Sustaiable Energy Reviews, 2015.
6. R. G Farmer and E. H. Allen, "Power System Dynamic Performance Advancement from History of North American Blockouts," Power Systems conference and Exposition, 2006.
7. T. Ohno and S.Imai, "The 1987 Tokyo Blackouts," Power Systems Conference and Exposition, 2006.
8. M. Sforna and M. Delfanti, "Overview of the Events and Causes of the 2003 Italian Blackouts," Power Systems Conference and Exposition, 2006.
9. O. P. Veloza and R. H. Cespedes, "Vulnerability of the Colombian Electric System to Blockouts and Possible Remedical Actions," IEEE Power Engineering Society General Meeting, 2006.
10. A. Berizzi, "The Italian 2003 Blackouts," IEEE Power Engineering Society General Meeting, 2004.
11. S. Corsi and C. Sabelli, "General Blackout in Italy Sunday September 28, 2003, h.03:28:00," IEEE Power Engineering Society General Meeting, 2004.
12. M. El-werfelli, R. Dunn, M. Redfern, and J. Brooks, "Analysis of the national 8th November 2003 Libyan Blockout," Univercities Power Engineering Conference, 2008.
13. V. Thanh Dineh and H. Huu Le, "Vietnamese 500Kv Power System and Recent Blockout," Power and Energy Society General Meeting – Conversion and Delivery of Electrical Energy in the 21st Century, IEEE, 2008.
14. M. W. Younas and S. A. Qureshi, "Analysis of Blockout of National Grid System of Pakistan in 2006 and the Application of PSS and FACTS Controllers as Remedial Measures," Internathional Conference on Electrical Engineering, 2007.
15. C. Li, Y. Sun, and V. Lagendijk, "Transnatinal infrastructure vulnerability: The historical shaping of the 2006 European Blackout," Energy Policy, 2015.
16. M. Sanaye-pasand, "Scrutiny of the Iranian national grid, IEEE Power and Energy Magazine," 2007.

17. Y. Hain and I. Schweitzer, “Analysis of the Power Blackout of june 8, 1995 in the Israel Electric Corportion, IEEE Trans,” On Power Systems, 1997.

18. L. L. Lai, H. T. Zhang, C. S. Lai, F. Y. Xu, and S. Mishra, “Investigation on july 2012 Indian Blackout,” 2013 International Conference on Machine Learning and Cyebernetics, 2013.

19. E. V. Vleuten and V. Lagendik, “Transnational Infrastructure Vulnerability: The Hhistorical shaping of the 2006 European Blackout,” Energy Policy, 2015.

20. P. J. Maliszewski and C. Perrings, “Factors in the Resilience of Electrical Power Distribution Infrastructures,” Applied Geography, vol. 32, pp. 668-679, 2012.

The Passive Defense Strategies to Confront the Creation of Blackouts in Iran

S. P. Madani, R. Dashti*

Abstract

The outage of electricity not only has damage to domestic, industrial and agricultural consumption, but also can be considered as a threat to the national security. Nowadays the outage of electricity as an important target of the terrorist groups and hostile governments is being abused to paralyze societies, therefore, it is important and necessary to identify threats and take appropriate strategies in passive defense to have a counteract against them. The purpose of this paper is to explain blackouts around the world and specially Iran, analyze its causes and provide passive defense solutions in order to avoid it and raise the reliability level of the electricity grid.

KeyWords: *Passive Defense, National Security, Blackouts, Reliability*

* Qom University of Technology, (drrezadashti@yahoo.com)- Writer-in-Charge