نشریه علمی پدافند غیرعامل

سال دهم، شماره ۱، بهار ۱۳۹۸، (پیاپی ۳۷): صص ۲۲-۱

# تاب‌آوری، پاسخی برای نگرانی‌های موجود در حوزه پدافند غیرعامل شبکه برق

رضا غفارپور[1*]، محمدرضا جنتی اسکوئی[2]، سجاد نجفی روادانق[3]، حبیب‌اله اعلمی[4]

تاریخ دریافت: ۱۳۹۷/۰۳/۲۸
تاریخ پذیرش: ۱۳۹۷/۰۷/۲۵

## چکیده

سامانه قدرت به‌طور معمول بر مبنای اصول اساسی قابلیت اطمینان، امنیت و کفایت، طراحی و بهره‌برداری می‌شوند. این اصول می‌توانند به‌درستی با خطاهای شناخته‌شده در تجهیزات زیرساخت قدرت تعامل کنند. با این حال، اخیراً با رخداد تهدیدهایی با احتمال وقوع پایین و شدت تخریب بالا (HILP)، نگرانی‌هایی در باب نگرش متداول قابلیت اطمینان‌گرا اوج گرفته است. به‌عنوان یک زیرساخت حیاتی، انتظار می‌رود که سامانه قدرت به‌مراتب در برابر رویدادهای HILP تاب‌آور و برگشت‌پذیر باشد. بنابراین، ارگان‌های مختلف، تلاش‌هایی را در جهت بهبود پاسخگویی شبکه در برابر رویدادهای HILP انجام می‌دهند. در این راستا، راه‌کارهای مختلفی وجود دارد که تصمیم‌گذاران متناسب با علایق و امکانات خود می‌توانند اتخاذ کنند. در این میان، یک نیاز اساسی به‌منظور دسته‌بندی و ارزیابی به‌روز انواع تهدیدها وجود دارد. در این راستا، بررسی انواع تهدیدها، شناخت راه‌کارهای مختلف و درنهایت بهره‌گیری از مفهوم شبکه‌های هوشمند در ارتقا تاب‌آوری شبکه توزیع در این مقاله مرور شده است.

**کلیدواژه‌ها:** شبکه توزیع هوشمند، تاب‌آوری و برگشت‌پذیری، طراحی، برنامه‌ریزی، بهره‌برداری

---

۱- استادیار، دانشگاه جامع امام حسین(ع)، (rghaffarpour@ihu.ac.ir) - نویسنده مسئول
۲- باشگاه پژوهشگران جوان و نخبگان، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران
۳- دانشیار، دانشگاه شهید مدنی آذربایجان، تبریز، ایران
۴- دانشیار، دانشگاه ایوانکی

## ۱- مقدمه

بحران معرف وضعیتی است که به‌صورت طبیعی و یا توسط انسان به‌وجود می‌آید و طی آن، الگوهای معمول زندگی از بین رفته و جامعه انسانی یا محیط‌زیست دچار خسارت می‌شود. برطرف کردن آثار گسترده و مخرب بحران‌ها، نیاز به مدیریت، برنامه‌ریزی و اقدامات اضطراری و فوق‌العاده دارد. امروزه مدیریت بحران به مدیریت هر دو جنبه مخاطرات و پیامدهای پیش و پس از وقوع بحران می‌پردازد و برخلاف گذشته، به امدادرسانی پس از وقوع حادثه محدود نمی‌شود؛ بنابراین، در مدیریت بحران از یک‌سو، از وقوع بحران جلوگیری می‌شود و از سوی دیگر اثرات مخرب ناشی از وقوع آن تا حد امکان کاهش می‌یابد. جامعه مدرن امروزی به‌شدت وابسته به خدماتی است که توسط زیرساخت شبکه‌های مهندسی‌شده فراهم می‌شوند. زمانی که بحرانی روی می‌دهد، غالباً توانایی این شبکه‌ها در ارائه خدمات به دلیل خسارت بر تجهیزات شبکه تنزل پیدا می‌کند. به‌عنوان یک زیرساخت اساسی و حیاتی، امنیت سامانه‌های قدرت به‌عنوان یک چالش جهانی شناخته‌شده است که ارتباط تنگاتنگی باثبات جامعه و بهبود شرایط اقتصادی دارد؛ بنابراین، همواره جز اولویت‌های مسئولین، سازمان‌ها و نهادهای اجتماعی گوناگون در سطوح مختلف بوده است. به‌محض این‌که امنیت سامانه قدرت به‌شدت تحت تأثیر تهدیدهای مختلف قرار می‌گیرد، سامانه قدرت ممکن است به چندین ناحیه تقسیم‌شده و نواحی بزرگ ممکن است با خاموشی سراسری مواجه شوند؛ که نتیجه آن، زیان اقتصادی وسیع است و در بعضی شرایط، زندگی بشری و حتی امنیت ملی به مخاطره می‌افتد. موارد مشابه متعددی در خاموشی‌های اخیر به‌وضوح دیده می‌شود [۱]. علاوه‌بر این، زندگانی بشری در دهه‌های اخیر، وابستگی رو به رشدی به پیوستن دستگاه‌های مختلف وابسته به هم در سطح وسیع پیداکرده است [۲]. برق به‌عنوان منبع انرژی دیگر زیرساخت‌ها، در مرکز قرار گرفته و نقش حیاتی در بهره‌برداری دیگر سامانه‌ها دارد [۳]. به‌منظور تضمین امنیت سامانه‌های قدرت، از دیرباز تهدیدهای مختلف شناخته و بررسی شده‌اند [۴]. تهدید اشاره به یک علت بالقوه از حادثه ناخواسته که ممکن است یک سامانه قدرت را به مخاطره بیندازد، دارد. تهدیدهایی که موجب خاموشی می‌شوند طیف وسیعی از عوامل برون‌زاد و درون‌زاد را شامل می‌شوند [۵]؛ بنابراین، یک نیاز اساسی به‌منظور دسته‌بندی و ارزیابی به‌روز انواع تهدیدها در ملاحظات امنیت سامانه وجود دارد. معمولاً، دسته‌بندی تهدیدها به‌قرار زیر است:

### الف) تهدیدهای طبیعی

بلایای طبیعی اصلاً تحت کنترل انسان نیستند بنابراین، اگر اتفاق بیافتند ممکن است عملکرد سامانه قدرت را درنتیجه ایجاد اختلال تحت تأثیر قرار دهند. علت یک تهدید طبیعی به مکان جغرافیایی اقلیمی بستگی دارد که سامانه قدرت در معرض آن قرار می‌گیرد. تهدیدهای طبیعی ناشی از شرایط بد آب و هوایی ازجمله موج گرما، گردباد، صاعقه و همچنین خطرات زمین‌شناختی ازجمله زلزله، سونامی، رانش زمین، فوران آتش‌فشان است؛ در سراسر دنیا چندین نمونه از خاموشی‌های گسترده که تهدیدهای طبیعی موجب شده‌اند، وجود دارد. قطعی ۱۲ ساعته برق و تحت تأثیر قرار گرفتن نزدیک به ۵۶ میلیون نفر در سراسر ایتالیا، در حین طوفان [۶]، قطع برق بیش از ۴۰۰ هزار مشترک خانگی واقع در جنوب سوئد در نتیجه وقوع طوفان شدید و درنتیجه آن صدها میلیون کرون سوئد زیان اقتصادی [۷]، تحت تأثیر قرار گرفتن نزدیک به ۱۳ استان و خاموشی تقریباً ۱۶۹ شهرستان درنتیجه پایداری دمای پایین، باران و کولاک برف در جنوب چین که زیان اقتصادی آن بالای ۱۰۰ میلیارد یوان برآورد شده است [۸]، بحران هسته‌ای ژاپن در پس وقوع زلزله و سونامی که توجه همه جهانیان را به خود جلب کرد [۹].

### ب) تهدیدهای تصادفی

علت تهدیدهای تصادفی می‌تواند عملکرد نادرست تجهیز، ازجمله: رد عمل بریکر، شکست عایقی، اضافه‌بار ترانس، یا خطای عملیاتی، ازجمله: خطای انسانی یا اشتباه در برنامه‌ریزی سامانه، بهره‌برداری، یا تعمیر و نگهداری، باشد. در ۸-۹ سپتامبر سال ۲۰۱۱، عملکرد نادرست تجهیزات نظارتی منجر به قطع گسترده برق در قسمت‌هایی از کالیفرنیای جنوبی و آریزونا و همچنین شمال غربی مکزیک گردید [۱۰]. خاموشی بخش شمال شرقی در سال ۲۰۰۳ یک نمونه برای اختلال عملیاتی است [۳].

### ج) تهدیدهای مخرب

اقدامات عمدی علیه تأسیسات و عملکرد سامانه قدرت که توسط عوامل مختلف (تروریست، گروه‌های تبهکار، هکرها، سارقان مس، خرابکار، بیمار روانی، نویسنده بدافزار، ...) با به‌کارگیری ابزارآلات گوناگون (مواد منفجره، سلاح قدرتمند، بدافزار، ...) باهدف ایجاد خرابی به‌منظور دست‌یابی به منافع سیاسی یا مادی صورت می‌گیرد. با افزایش روزافزون اهمیت سامانه‌های قدرت، این سامانه به دلایل متنوعی ازجمله اهداف جنایت‌کارانه، نظامی یا سیاسی، به هدف محبوبی برای تهدیدهای مخرب تبدیل‌شده است به‌گونه‌ای که تضعیف یا تخریب آن تأثیر به‌سزایی در تضعیف امینت اقتصادی و امنیت ملی دارد. از این منظر دستگاه‌های قدرت می‌تواند به ۳ زیر لایه تقسیم‌بندی شوند: لایه فیزیکی، لایه انسانی، لایه سایبری. لایه فیزیکی به دارایی‌های محسوس مرتبط با صنعت برق ازجمله،

نیروگاه‌ها، خطوط انتقال و ترانس‌ها، اشاره دارد. لایه انسانی به افرادی که به سامانه‌های قدرت دسترسی دارند اطلاق می‌شود و لایه سایبری شامل: اطلاعات سخت‌افزاری، نرم‌افزار، داده‌ها، و شبکه‌های ارتباطی است که عملکرد سامانه قدرت را پشتیبانی می‌کنند. تهدیدهای مخرب همواره بر/از طریق/توسط سه لایه انجام می‌شود، به‌عنوان‌مثال: تخریب ترانس‌ها در لایه فیزیکی، خسارت ایجادشده توسط افراد بدخواه درون‌سازمانی در لایه تصمیمات انسانی، حمله از طریق بدافزار، و هک در لایه سایبری. از سال ۱۹۹۹ تا ۲۰۰۲، بالای ۱۵۰ حمله روی سامانه قدرت در سراسر جهان رخ داده است [۱۱]. طبق گزارش دپارتمان انرژی آمریکا، سالانه به‌طور متوسط ۳۹ حمله به دارایی‌های بخش انرژی آمریکا مابین سال‌های ۱۹۸۰ تا ۱۹۸۹ صورت گرفته است که بخش اعظم آن سامانه قدرت را هدف قرار داده‌اند [۱۲]. اطمینان است که نرخ حمله امروزه بسیار بیشتر از گذشته باشد. از ۱۱ سپتامبر ۲۰۱۱، منابع و تلاش‌هایی که به‌منظور حفاظت سامانه قدرت در برابر تهدیدهای طبیعی و تصادفی صرف می‌شد به سمت پاسخگویی به نگرانی‌های جهانی در باب تهدیدهای مخرب سوق پیدا کرده است [۱۳].

### د) تهدیدهای نوظهور

تهدیدهایی که در مسیر تکاملی سامانه قدرت از جمله تجمیع انرژی تجدیدپذیر و وابستگی بین سامانه قدرت و دیگر زیرساخت‌ها ظهور پیدا کرده‌اند. هم‌زمان با تکامل، توسعه و گذار خود سامانه قدرت، تهدیدهای نوظهور بروز پیدا کرده‌اند که طبقه‌بندی آن‌ها در سه گروه فوق مشکل خواهد بود. پیشرفت سریع فنّاوری در سال‌های اخیر در حوزه الکترونیک قدرت، رایانه، ارتباطات از راه دور و علم مواد، امیدبخش توسعه روزافزون سامانه قدرت بوده است [۱۴]. از دیگر سو، تغییر و تحولات در دستگاه‌های قدرت نیز فرصتی رو به رشد برای تهدیدهای نوظهور در برابر امنیت سامانه ایجاد کرده است. علاوه براین، تهدید ناشی از حملات انسانی به سامانه‌های قدرت جدی‌تر شده است [۱۵-۱۴]. به‌عنوان مثال، تجمیع تجهیزات شبکه هوشمند مبتنی بر ارتباطات به‌منظور کنترل‌پذیری آن‌ها، امکان حملات سایبری را افزایش داده است [۱۶]؛ و رشد سهم تولیدی منابع انرژی تجدیدپذیر با ماهیت متناوبی در عرضه توان، ماهیت سامانه را دچار تغییر کرده و باعث بروز چالش‌های امنیتی متنوعی شده است [۱۸-۱۷]. شناسایی همه تهدیدهای نوظهور غیرممکن است چراکه بعضی از آن‌ها هنوز مشاهده نشده‌اند؛ اما از منظر عامل داخلی یا خارجی سامانه قدرت، تهدیدهای نوظهور را می‌توان در دو دسته طبقه‌بندی کرد:

#### د-۱) تهدیدهای سامانه‌ای

انرژی‌های نو، ازجمله انرژی بادی و انرژی خورشیدی، به‌طور روزافزون به‌منظور تولید برق استفاده می‌شوند. به دلیل ماهیت متناوبی منابع انرژی تجدیدپذیر، تجمیع‌سازی این منابع در سامانه قدرت، امینت این سامانه را به مخاطره می‌اندازد. به‌عنوان مثال، حفظ تعادل بین تولید توان و تقاضای آنی در دستگاهی بانفوذ بالای منابع تولید متغیر، برای بهره‌بردار سامانه، چالش بزرگی محسوب می‌شود. علاوه‌بر این، این منابع انرژی به‌طور کامل کنترل‌پذیر نیستند و پیش‌بینی آن‌ها از دقت کافی برخوردار نیست [۱۹]. علاوه براین، نفوذ بالای منابع انرژی تجدیدپذیر در بازار برق، ناسازگاری‌هایی بین بازارهای موجود و تقاضای جدید معرفی می‌کند. این ناسازگاری شامل ۳ مورد زیر است:

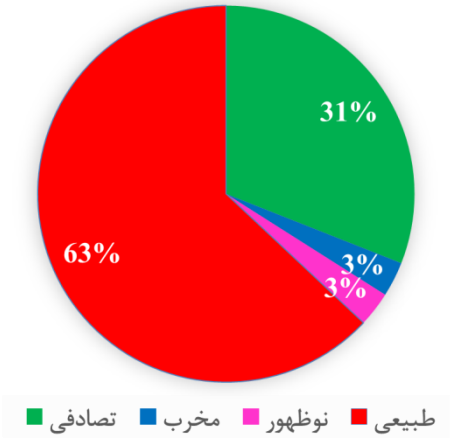
- نرخ بهره‌برداری پایین از ظرفیت شبکه انتقال ممکن است هزینه اتصال انرژی‌های نو را افزایش دهد.
- روش‌های پیش‌بینی تولید باد بهبود نیافته است ولی در طی بهینه‌سازی پخش توان در سامانه استفاده می‌شود، که ممکن است امینت سامانه را کاهش دهد.
- عدم شفافیت در قیود سامانه، در تصمیمات مربوط به سرمایه‌گذاری در شبکه انتقال مؤثر است [۲۰].

یکی دیگر از پیشرفت‌های جدید سامانه قدرت مدرن، شبکه‌های هوشمند است. جهت انجام وظایف گسترده در شبکه‌های هوشمند از سطح تولید تا مشترکین، زیرساخت گسترده رایانه و ارتباطات باید در شبکه‌های هوشمند ایجاد و توسعه یابد که به‌موجب آن، چالش‌های متعدد شامل تعاملات بسیار پیچیده درنتیجه برهم‌کنش و تجمیع دستگاه‌های سایبری و فیزیکی [۲۱] ایجاد می‌گردد. متعاقب آن امنیت سایبری سامانه‌های قدرت به دلیل افزایش حملات سایبری و حوادث بر روی زیرساخت‌های حیاتی به خطر می‌افتد [۲۳-۲۲]. از این میان، سه نوع از تهدیدهای مخرب بر روی زیرساخت مخابراتی سامانه‌های قدرت تحت عنوان در دسترس بودن سامانه، تجمیع داده، و حریم خصوصی اطلاعات در مقاله [۲۴] ارزیابی شده‌اند.

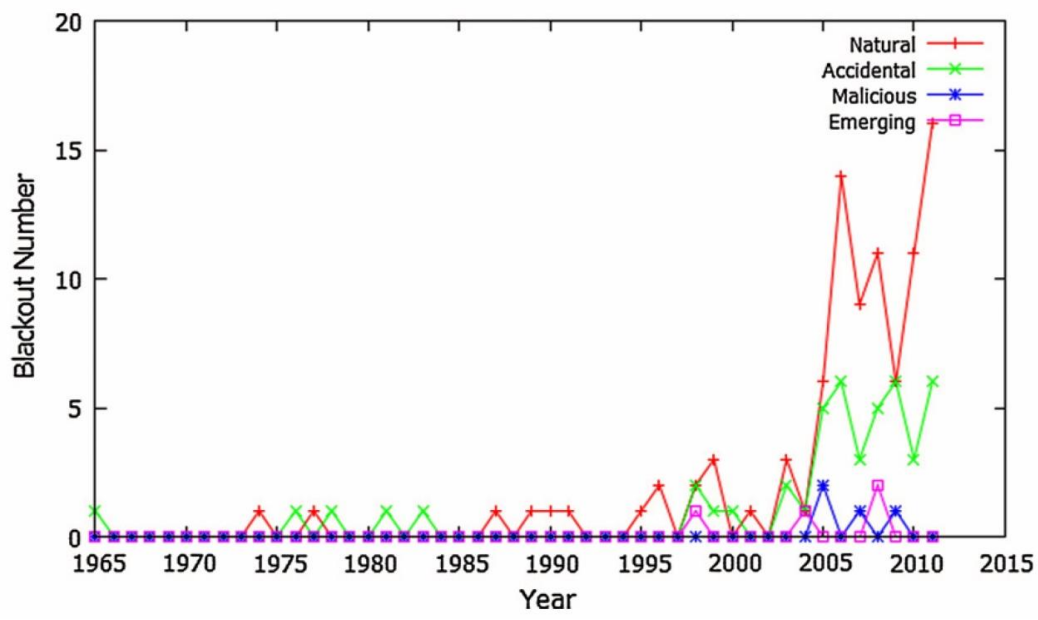
#### د-۲) تأثیر برداری از دیگر زیرساخت‌ها

پیوستگی به هم زیرساخت‌هایی همچون شبکه‌های برق، آب، نفت، تلفن، حمل‌ونقل و گاز طبیعی، روزبه‌روز پیچیده‌تر می‌شود. این وابستگی متقابل به این معنی است که اگر حادثه‌ای که در یک زیرساخت رخ دهد، ممکن است به‌سرعت گسترش یافته و یک اثر کلی در داخل دیگر زیرساخت‌ها ایجاد کند؛ و این تأثیرات به‌صورت

آبشاری گسترش پیدا می‌کند. بنابراین، این وابستگی، تهدیدهای جدیدی به امنیت سامانه قدرت تحمیل خواهد کرد؛ به‌عنوان مثال، وقتی‌که یک مشکل یا خطا در عرضه گاز رخ می‌دهد، ممکن است منجر به از مدار خارج شدن نیروگاه‌های برق با سوخت اولیه گاز گردد [۲۶-۲۵]. شکل (۱) نشان‌دهنده هر یک از چهار دسته‌بندی فوق در ایجاد خاموشی در بازه زمانی بین سال‌های ۱۹۶۵ تا ۲۰۱۱ است. به‌وضوح روشن است که علت اصلی خاموشی‌ها وقوع بلایای طبیعی است که این سهم با توجه به تغییرات آب و هوایی، روند رو به رشدی دارد [۲۷].




(الف)




(ب)

**شکل (۱):** الف) توزیع علل خاموشی‌ها ب) توزیع علل مختلف خاموشی‌ها در سال‌های مختلف

در حالت کلی خاموشی که درنتیجه هر تهدیدی ایجاد می‌شود، می‌تواند با یک زنجیره به‌صورت زیر تعمیم یابد: در مرحله اول، یک حادثه باید درنتیجه تهدیدی خاص رخ دهد؛ این حادثه تأثیرهای متنوعی بر روی سامانه قدرت دارد؛ و سرانجام خاموشی به علت یک پدیده مشخص رخ می‌دهد. حادثه، به دگرگونی ساختاری در سامانه‌های قدرت یا تغییر در وضعیت عملکرد اجزا اشاره دارد. تأثیر نیز بر تغییر حالت سامانه قدرت از منظر کیفیت پارامترهای الکتریکی دلالت دارد و نهایتاً پدیده نیز به یک دلیل اساسی که در نتیجه آن خاموشی رخ می‌دهد، دلالت می‌کند. از منظر سامانه قدرت، می‌توان سه دسته از تهدیدات که جامعه را هدف قرار داده‌اند، برشمرد:

**دسته اول) حمله به سامانه قدرت**

هدف از این تهدیدها، زیرساخت الکتریکی است. به‌عنوان مثال، تروریست‌ها می‌توانند هم‌زمان دو پست برق یا دکل‌های مهم انتقال

را به‌منظور ایجاد خاموشی در یک منطقه وسیع مورد حمله قرار دهند. نمونه دیگری می‌تواند حمله به بازار برق باشد.

**دسته دوم) حمله با سامانه قدرت**

تروریست‌ها با به‌کارگیری بخشی از تجهیزات نصب‌شده در سامانه قدرت می‌توانند جمعیتی را مورد حمله قرار دهند، به‌عنوان مثال، به‌کارگیری برج‌های خنک‌کننده نیروگاه برق به‌منظور اشاعه عوامل شیمیایی و بیولوژیکی

**دسته سوم) حمله از طریق سامانه قدرت**

تروریست‌ها با به‌کارگیری بخشی از تجهیزات نصب‌شده در سامانه قدرت می‌توانند زیرساخت‌های عمرانی را مورد حمله قرار دهند، به‌عنوان‌مثال، تروریست‌ها می‌توانند با ایجاد پالس الکترومغناطیسی از طریق شبکه به زیرساخت‌های رایانه یا ارتباطات از راه دور آسیب بزنند.

در دهه های اخیر، بنا به دلایل مالی و بعضاً سیاسی و مباحث زیست‌محیطی، زیرساخت‌های سامانه قدرت متناسب با رشد تقاضای بار گسترش پیدا نکرده است. براین اساس، سامانه‌های قدرت نزدیک به محدودیت‌های استاتیکی و دینامیکی خود بهره‌برداری می‌شوند [۲۸]. در نتیجه، سامانه‌های قدرت، به‌شدت نسبت به تهدیدها آسیب‌پذیر شده‌اند. مطابق با خاموشی‌های متعددی که گزارش شده است [۲۹-۳۱]، این موضوع تبدیل به موتور محرکی برای دولت ها شده است که راه‌کارهایی را برای ارتقا تاب آوری و برگشت پذیری سامانه های قدرت خود اجرا کنند [۳۲]. تاب‌آوری و برگشت‌پذیری[1] به توانایی سامانه در ایستادگی در برابر وقایعی با احتمال وقوع کم و اثرات تخریبی زیاد (HILP[2]) به‌واسطه به حداقل رساندن خاموشی‌ها و بازگشت به حالت عادی بهره برداری سامانه قدرت اطلاق می شود [۲۸]. این وقایع به طور معمول شامل حوادث شدید ناشی از شرایط بد آب و هوایی و بلایای طبیعی مانند طوفان، زلزله، طوفان برف، سیل، حملات سایبری، حملات مخرب و ... می‌باشند. اصلی‌ترین ویژگی سامانه با ویژگی‌های تاب‌آوری و برگشت‌پذیری، تغییر ساختار سامانه به هنگام مواجهه با حوادث با هدف کاهش تأثیرات و بازگشت سریع به وضعیت قابل قبول پس از اتمام حادثه است. در این راستا، باید راهکارهایی توسط تصمیم گیران سامانه قدرت اتخاذ یا حتی به صفر برسانند شود تا اثرات و عواقب ناشی از رویدادهای HILP را کاهش دهند و. به این راهکارها مدیریت بحران سامانه اطلاق می‌شود. مدیریت بحران سامانه به اقدامات عملیاتی اطلاق می‌گردد که برای مقابله با بحرانی که می‌تواند به وقوع بپیوندد، انجام می‌پذیرد. این اقدامات می‌تواند به‌صورت مستحکم‌سازی، افزونگی، پاسخ همزمان به اقدام خرابکارانه و بازیابی سریع‌تر سامانه باشد. در بین گزینه های موجود، توسعه ریزشبکه ها با توانایی بهره‌برداری در حالت جزیره‌ای می‌تواند به‌عنوان یک راه‌کار مؤثر و عملی به‌منظور ارتقای تاب‌آوری و برگشت‌پذیری مطرح شود [۳۳-۳۲]. به‌طور خلاصه، ریزشبکه به مجموعه‌ای از بارها و حداقل یک منبع انرژی پراکنده قابل کنترل که در یک منطقه جغرافیایی مشخص به هم متصل شده‌اند، اشاره دارد [۳۴] که در مواقع لازم می‌تواند از شبکه اصلی جدا شده و به‌صورت جزیره‌ای بهره‌برداری شود. فناوری‌های مورداستفاده در ریزشبکه‌ها شامل: انواع منابع تولید پراکنده، مبدل‌های دوطرفه، تجهیزات اندازه‌گیری هوشمند، خودکارسازی شبکه توزیع، سامانه‌های کنترلی ریزشبکه، تجهیزات ذخیره‌ساز انرژی پیشرفته، سوئیچ‌های هوشمند، فعال‌سازی خودروهای برقی و هیبریدی و نرم‌افزارهای متناسب با شبکه ازنظر سرعت، دقت و قدرت محاسباتی هستند. ریزشبکه ازنظر فنی به سامانه قدرت مقیاس کوچکی اطلاق می‌شود که توانایی خود تغذیه و جزیره شدن را دارا است و به‌منظور تأمین بار به شیوه اقتصادی و با قابلیت اطمینان بالا، هوش محلی پراکنده برای سامانه قدرت فراهم می کند. ویژگی چشمگیر ریزشبکه توانایی آن در جزیره‌سازی از شبکه توزیع اصلی است. معمولاً جزیره‌سازی برای قطع سریع ریزشبکه از شبکه توزیع تحت خطا و به‌منظور حفاظت تجهیزات ریزشبکه از اختلالات بالادستی و ایجاد فرصتی برای تأمین بی وقفه بارها انجام می‌گیرد. علاوه‌بر این، به‌منظور محافظت بارهای حساس به ولتاژ از افت قابل توجه ولتاژ در زمانی که سریع‌ترین راهکار برای مشکلات ولتاژ شبکه قریب‌الوقوع نیست، جزیره‌سازی انجام می شود. ریزشبکه در حالت متصل به شبکه به طرز اقتصادی بهره برداری می‌شود؛ بااین‌حال، در شرایطی که ریز شبکه نیازمند گذار به حالت جزیره‌ای است همواره باید ظرفیت مناسبی از تولید و/یا ذخیره در دسترس باشد. ریز شبکه با استفاده از کلیدهای بالادستی که در نقطه اتصال مشترک (PCC[3]) نصب می‌باشند از شبکه اصلی جدا می‌شود و بار ریزشبکه کاملاً از منابع محلی تأمین می گردد [۳۵]. مزایای غیرقابل انکار ریزشبکه‌ها باعث شده تا تلاش‌های زیادی در جهت نفوذ هر چه بیشتر آن‌ها در سامانه قدرت انجام شود. هم‌زمان با گسترش سریع آن‌ها، چالش‌های بی‌شماری در مسیر طراحی، کنترل و بهره‌برداری مؤثر ریزشبکه‌ها در حالت متصل به شبکه و نیز در حالت جزیره‌ای پیش‌آمده که موجب تمرکز فعالیت‌های تحقیقاتی گسترده‌ای در این زمینه شده است؛ بنابراین، نیاز به یک دید جامع و شامل از نحوه پیوستن ریزشبکه به سامانه قدرت وجود دارد. زمینه‌های مختلف مربوط به ریزشبکه شامل منابع تولید پراکنده، ارزشمندی ریز شبکه‌ها، استفاده‌های کاربردی الکترونیک قدرت، مباحث اقتصادی، کنترل و بهره‌برداری ریزشبکه، دسته‌بندی

1- Resiliency
2- High Impact-Low Probabilty
3- Point of Common Coupling

ریزشبکه‌ها، حفاظت و زیرساخت‌های مخابراتی مرور شده است [۳۶]. امروزه مدیریت انرژی در مواقع بحرانی یکی از مهم‌ترین موارد از نقطه‌نظر ملاحظات پدافند غیرعامل در صنعت برق است که موجب توسعه گسترده انواع ریزشبکه‌ها شده است. پدافند در مفهوم کلی به مجموعه روش‌ها، برنامه‌ریزی‌ها و فعالیت‌هایی گفته می‌شود که هر نظامی برای دفع و خنثی کردن یا کاهش اثرات اقدامات افندی دشمن یا اثرات ناشی از بلایای طبیعی سهمگین انجام می‌دهد. پدافند به دو دسته شامل پدافند عامل و پدافند غیرعامل تقسیم می‌شود. در پدافند عامل، مقابله مستقیم با دشمن و رویارویی با حملات افندی از طریق به‌کارگیری جنگ‌افزارها صورت می‌پذیرد. پدافند غیرعامل به مجموعه اقداماتی اطلاق می‌شود که مستلزم به‌کارگیری جنگ‌افزار نیستند و با اجرای آن تا می‌توان از وارد شدن خسارات مالی به تجهیزات و تأسیسات حیاتی و حساس نظامی و غیرنظامی و تلفات جانی جلوگیری کرد و یا میزان خسارات و تلفات را تا حد امکان کاهش داد. در دسترس بودن ریزشبکه‌ها در طی بلایای طبیعی و بعد از وقوع، بر دو دسته از تجهیزات که امکان تأمین توان توسط ریزشبکه‌ها را ارتقا می‌دهند، تمرکز دارد: منابع تولید پراکنده و منابع ذخیره‌ساز انرژی محلی. منابع انرژی تجدیدپذیر به‌عنوان منابع تولید پراکنده، در زمان بلایای طبیعی دارایی‌های ارزشمندی تلقی می‌شوند که نیاز به شاهراه‌ها ندارند. با این‌حال، ماهیت تولید متغیر این منابع، نیازمند ذخیره‌سازی محلی چشمگیر است. مازاد ذخیره انرژی محلی می‌تواند به‌عنوان گزینه پشتیبان برای عیوب احتمالی که موجبات خاموشی را فراهم می‌کند، مطلوب باشد چراکه تأثیر عملکرد شاهراه در طی بلایای طبیعی را بر روی دسترس‌پذیری ریز شبکه کاهش می‌دهد. بسیاری از فناوری‌های تولید در ریزشبکه‌ها، مانند میکرو توربین‌ها، به دیگر زیرساخت‌ها که شاهراه نامیده می‌شوند وابسته هستند، مثلاً جاده‌ها یا شبکه توزیع گاز، به‌منظور رسیدن سوخت به این منابع تا بتوانند به عملکرد خود ادامه دهند. این شاهراه‌ها، ممکن است همانند شبکه‌های مرسوم تحت تأثیر بلایا قرار گیرند. یک تحلیل جامع از خطرات بالقوه بر روی ریزشبکه مؤید آن است که انتخاب منابع تولید محلی که شاهراه‌های آن‌ها به‌شدت تحت تأثیر این خطرات قرار نمی‌گیرد، به‌منظور غلبه بر این مشکل مناسب است، مثلاً عرضه گاز طبیعی به طوفان آسیب‌پذیری کمتری نسبت به زلزله دارد. ولی در بعضی مواقع، امکان انتخاب چنین گزینه‌ای وجود ندارد. در این موقعیت‌ها، ذخیره انرژی به‌منظور کاهش وابستگی به شاهراه‌ها می‌تواند ضروری باشد. گزینه دیگر، وابستگی به منابع انرژی تجدیدپذیر است که تابش خورشید یا سرعت باد به چنان شاهراه‌هایی برای رسیدن به ژنراتورهای ریز شبکه محلی وابسته نیستند. با این‌حال، وسعت سطح مورد نیاز، کاربرد منابع انرژی تجدیدپذیر را در مکان‌هایی با فضای کوچک‌تر یا تقاضای توان بالا محدود می‌کند. علاوه براین، خروجی متغیر این منابع، کاربرد آن‌ها را محدود می‌سازد. همانند وضعیت مربوط به وابستگی به شاهراه‌ها، ذخیره انرژی می‌تواند برای غلبه بر این مشکل نیز مؤثر باشد. روشن است که، ادوات ذخیره‌کننده انرژی با تزریق یا جذب انرژی در هنگام عدم تعادل تولید و مصرف نوسانات فرکانس را رفع می‌کنند. در شرایط اضطراری که عدم تعادل تولید و مصرف شدیدتر است، به‌ناچار می‌بایست بار زدایی انجام گیرد. درصورتی‌که بتوان عدم تعادل تولید و مصرف را با تغییر بی‌درنگ در میزان مصرف کنترل کرد، دیگر نیازی به ادوات ذخیره‌کننده انرژی نیز نیست. درزمینه کنترل و تثبیت فرکانس در ریزشبکه‌ها می‌بایست به نکاتی توجه داشت:

الف) عدم قطعیت تولید انرژی بادی و خورشیدی اینرسی کم ریز شبکه

ب) فاصله کوتاه بین منبع تولید و مصرف‌کننده نوسانات فرکانس، ناشی از منابع انرژی نوین مانند توربین بادی

## ۲- اصول کلی ارزیابی تاب‌آوری

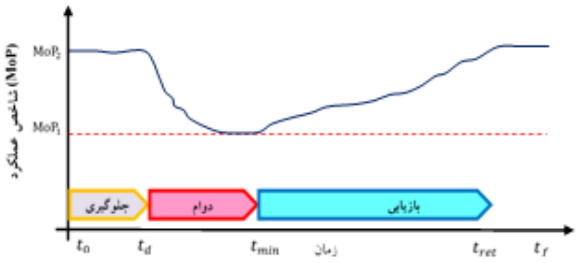
جهت ارزیابی یک ویژگی مانند تاب‌آوری از یک سامانه مهندسی، ابتدا باید شاخص‌های کمی برای توصیف میزان آن ویژگی و اجزای آن تعریف و محاسبه شود. شکل (۲) به‌صورت نوعی شاخص عملکرد یک سامانه را نسبت به زمان و در شرایط وقوع یک اغتشاش شدید نمایش می‌دهد. شاخص عملکرد می‌تواند بار تأمین‌شدهٔ یک سامانه به‌عنوان هدف غایی آن باشد. یا بر حسب نیاز ممکن است ارزش بارهای باقیمانده در شبکه، تعداد تجهیزات سالم و برقدار سامانه و ... به‌عنوان شاخص عملکرد سامانه انتخاب شوند.

همان‌طور که در شکل (۲) مشاهده می‌شود، عملکرد سامانه پس از آغاز اغتشاش در زمان $t_0$ به سرعت پایین نمی‌آید و با توجه به میزان استقامتی که دارد، مدت زمانی طول می‌کشد تا عملکرد سامانه افت نماید. این مرحله از رفتار سامانه را می‌توان مرحلهٔ جلوگیری نامید که به میزان هوشیاری وضعیتی بهره‌بردار و نیز استحکام شبکه بستگی دارد. هرچه بهره‌بردار شبکه نسبت به خطری که سامانه را تهدید می‌کند و آنچه که در حال وقوع است آگاه‌تر بوده و از دانش و تجربهٔ کافی برای مقابله با آن برخوردار باشد و البته سامانه هم از استقامت بیشتری برخوردار باشد، زمان بیشتری طول خواهد کشید تا افت عملکرد سامانه رخ دهد. بنابراین، مدت زمان $t_0$-$t_d$ را می‌توان یک شاخصی کمی جهت توصیف کیفیت مرحلهٔ جلوگیری دانست. با افت عملکرد سامانه و تا زمان استقرار وضعیت در شرایط جدید، عملاً وارد مرحلهٔ دوام می‌شویم. میزان آسیب‌پذیری شبکه که برحسب حداکثر افت شاخص عملکرد شبکه

نسبت به مقدار آن در حالت عادی سنجیده می‌شود، به میزان انطباق‌پذیری سامانه در برابر اغتشاش بستگی دارد. با افزایش انطباق‌پذیری سامانه، روند افت عملکرد کندتر شده و میزان آسیب‌پذیری نیز کاهش می‌یابد. مقدار $\frac{MoP_2 - MoP_1}{MoP_2}$ به‌عنوان یک شاخص کمی نرمال‌شده جهت توصیف میزان آسیب‌پذیری سامانه در برابر یک اغتشاش به‌کار می‌رود. مرحلهٔ بازیابی، پس از استقرار شرایط در وضعیت پس از حادثه آغاز می‌شود. در این مرحله، بهره‌بردار توسط ابزارها و رویه‌های در اختیار و البته دانش و تجربهٔ شخصی خود شروع به به‌کارگیری منابع موجود، بازآرایی شبکه و بازیابی بارهای خاموش می‌نماید. البته پیشتر نیز تاکید گردید که ممکن است مرحلهٔ بازیابی، خود به دو بخش بازیابی اولیهٔ زیرسامانه جدا شده از شبکه و بازیابی کلی مربوط به تشکیل سامانه یکپارچه و بازگشت به شرایط عادی تقسیم گردد. مدت زمان بازیابی نیز می‌تواند شاخصی باشد که کیفیت روند بازیابی را پس از یک اغتشاش مشخص توصیف نماید. در نهایت اگر بخواهیم کل روند بازیابی را توسط یک شاخص کمی اندازه‌گیری نماییم، می‌توان از شاخص نرمال‌شدهٔ زیر بهره برد:

$$R(T) = \frac{\int_0^T P_R(t)dt}{\int_0^T P_T(t)dt} \qquad (۱)$$

که در آن، $P_R(t)$ مقدار واقعی شاخص عملکرد در لحظه $t$ و $P_T(t)$ مقدار مطلوب شاخص عملکرد در همان لحظه می‌باشند.




**شکل (۲):** شاخص عملکرد بر حسب زمان

## ۳- تاب‌آوری ضرورتی انکارناپذیر

از جنگ جهانی دوم تاکنون، شبکه‌های برق یک هدف راهبردی برای حملات نظامی به شمار می‌روند. به‌طورکلی در حمله به شبکه برق، چهار هدف اصلی دنبال می‌شود که عبارت‌اند از: کاهش روحیه شهروندان، تحمیل هزینه به مقامات سیاسی برای القای تغییر موردنظر، اخلال در حمله نظامی و جلوگیری از تولید و ضربه زدن به بدنه اقتصادی کشور. معمولاً حمله به تأسیسات برق آسان و کم‌هزینه بوده و آثار تخریبی زیادی را به دنبال دارد. به همین دلیل سامانه برق همواره جز اهداف نظامی و تروریستی است تا با آسیب رساندن به آن موجبات تضعیف ثبات اقتصادی و اجتماعی یک کشور فراهم شود و نیز می‌تواند سبب آشفتگی روانی ملت، فلج شدن سامانه‌های تدافعی و ملی گردد [۳۷]. لازم به ذکر است که وقوع بلایای طبیعی سهمگین نیز همانند تهدیدهای نظامی اثرات مخربی دارد که به‌مراتب ممکن است سهمگین‌تر و فراگیرتر باشد. مشکلات ایجادشده برای سامانه قدرت هنگام مواجه‌شدن با انواع تهدیدها عبارت‌اند از [۳۸-۳۹]:

- افزایش جریان خطا و تراکم خطوط و آسیب رسیدن به ادوات و تجهیزات نصب‌شده در شبکه.
- با وقوع خطا، ولتاژ و فاز آن دچار نوسان شده و کیفیت توان شبکه افت می‌کند و به تجهیزات الکترونیکی و نظامی متصل به شبکه آسیب وارد می‌شود.

بین سال‌های ۱۹۸۷ تا ۱۹۹۶ میلادی بنا به گزارش‌ها، بیش از ۲۰۰۰۰ حمله فیزیکی ثبت‌شده به شبکه‌های برق انجام شده است که نتیجه آن اختلالاتی در سرویس برق‌رسانی است [۴۰]. از سوی دیگر، بلایای طبیعی می‌توانند موجب خاموشی‌های گسترده شوند. در پرتو تغییرات آب و هوایی، انتظار می‌رود که احتمال وقوع، شدت و مدت‌زمان بلایای طبیعی روند افزایشی داشته باشد. موضوع تأثیرات بلایای طبیعی بر سامانه قدرت مبحثی نو در تحقیقات است که باهدف درک علل خاموشی، تحلیل روش‌های آماده‌سازی و مقاوم‌سازی شبکه، و افزایش تاب‌آوری سامانه قدرت در برابر این‌گونه حوادث انجام می‌شود. هم‌زمان، فناوری‌های نو، مانند شبکه‌های هوشمند، ریز شبکه و به‌کارگیری نظارت گسترده ناحیه‌ای می‌تواند آگاهی‌های ناحیه‌ای را افزایش داده و همین‌طور موجب بازیابی سریع سامانه گردد [۴۱]. تجربه‌های به‌دست‌آمده از بلایای طبیعی حاکی از آن است که سامانه قدرت مرسوم به‌دلیل وسعت جغرافیایی بالا، در ترکیب با تولید و معماری کنترل مرکزی، دستگاه‌های شکننده‌ای هستند به‌گونه‌ای که تخریب کمتر از ۱ درصد از تجهیزات آن‌ها می‌تواند به وقوع خروج‌های بزرگی بیانجامد، بنابراین، انتظار می‌رود که نواحی بزرگ‌تر سامانه قدرت، احتمال بالایی از خروج را تجربه کنند. مشخصاً، ممکن است این‌چنین عملکردی برای تمامی بلایا یا در تمامی نواحی قابل مشاهده نباشد، ولی مدارکی دال بر مشاهده چنین عملکردی در اقصی نقاط جهان در پی بلایای مختلفی همانند طوفان کاترینا، زلزله سیروان چین، زلزله و سونامی ژاپن، وجود دارد [۴۲]. در سال‌های اخیر، تأکید جدی بر روی نیاز به راه‌کارهای اجرایی به‌منظور ارتقا تاب‌آوری - برگشت‌پذیری سامانه قدرت در پاسخ به حوادث HILP وجود داشته است. اگر سامانه قدرت تحت تأثیر این حوادث قرار گرفته و تجهیزات حساس شامل تجهیزات تولید و/ یا زیرساخت‌های توزیع و انتقال، به‌شدت آسیب ببینند، ارائه خدمات ممکن است برای روزها و حتی هفته‌ها

قطع گردد. با توجه به توضیحات ارائه‌شده، سامانه قدرت جزء زیرساخت‌های حیاتی طبقه‌بندی‌شده است، که انهدام یا اختلال در کل یا قسمتی از آن، موجب بروز بحران، آسیب و صدمات قابل‌توجه در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و دفاعی با سطح تأثیرگذاری منطقه‌ای می‌گردد. اهمیت سامانه قدرت به حدی است که به گفته یکی از افسران ارشد هیتلر بمباران نیروگاه‌ها و شبکه‌های انتقال آلمان توسط نیروهای متفقین دلیل اصلی اتمام جنگ جهانی دوم بود. با توجه به توضیحات ارائه‌شده، چنین می‌توان گفت که منظور از تاب‌آوری و برگشت‌پذیری، تأمین انرژی پایدار مورد نیاز مخصوصاً برای زیرساخت‌های از پیش تعریف‌شده و در نتیجه آن ایجاد شرایطی برای استمرار فعالیت‌های اساسی و ضروری مردم، تضمین تداوم نیازهای حیاتی مردم، و سهولت در اداره کشور در شرایط بروز و تهدید بحران ناشی از تجاوزت خارجی در مقابل حملات و اقدامات خصمانه و مخرب دشمن و همین‌طور بروز بلایای طبیعی، از طریق طرح‌ریزی و اجرای طرح‌های دفاع غیرعامل و کاهش آسیب‌پذیری نیروی انسانی، مستحدثات و تأسیسات و تجهیزات حیاتی و حساس کشور است. به‌طور خلاصه می‌توان چنین گفت که تهدیدات نظامی و بلایای طبیعی سهمگین مخاطرات جدی بر سر راه تأمین انرژی مطمئن می‌گذارند و به‌عنوان چالشی قابل‌توجه برای تصمیم‌گیران سامانه قدرت به‌حساب می‌آیند که چگونه می‌توان با طراحی و بهره‌برداری درست این سامانه، اثرات این مخاطرات را به حداقل رساند. در این راستا، طراحی سامانه‌های قدرت باید به‌گونه‌ای باشد که امکان تداوم بی‌وقفه فعالیت‌های ضروری و کاهش آسیب‌پذیری سامانه قدرت فراهم گردد. به‌عبارت دیگر، سامانه قدرت باید به‌گونه‌ای طراحی شود که اهداف زیر حاصل شود:

- کاهش آسیب‌پذیری در برابر تهدیدات
- تأمین انرژی موردنیاز برای مدیریت بحران در شرایط بحران
- تضمین تداوم کارکردهای ضروری مردم در شرایط بحران
- قابلیت بازیابی و باز زیستی سریع سامانه به شرایط عادی بهره‌برداری

تلفیق سیاست‌های دفاعی در برنامه پیشرفت پایدار هم‌راستا با سیاست‌های توسعه و پیشرفت، پایدارترین و ارزان‌ترین روش دفاع و مناسب‌ترین راه‌کار افزایش آستانه مقاومت ملی در شرایط بحران و پشتوانه اقتدار، عزت و پایداری کشور و صلح‌آمیزترین و فطری‌ترین روش دفاع در برابر همه حوادث است. در این راستا، نیاز به سامانه قدرت مطمئن به‌منظور کاهش آسیب‌پذیری در برابر تهدیدات نظامی و بلایای طبیعی، مجموعه‌ای از اقدامات و تدابیر و ملاحظات لازم شامل مکان‌یابی درست تجهیزات مختلف سامانه قدرت، ایجاد پشتیبان‌های لازم برای تأمین انرژی، ایمن‌سازی، تسهیل مدیریت بحران در زیرساخت‌های اساسی استفاده می‌شود. در مبحث مربوط به طراحی سامانه‌های قدرت در هماهنگی با تاب‌آوری و برگشت‌پذیری لزوم توجه به زیرساخت‌های مختلف بر مبنای نوع کاربری آن، اهمیت ویژه‌ای را به خود جلب کرده است. بدین منظور، پاره‌ای از زیرساخت‌هایی که محل استقرار افراد و یا انجام فعالیت‌های کلیدی و مرتبط با امنیت ملی، ارگان حاکمیتی کشور و مراکز تصمیم‌گذار در مدیریت شرایط بحرانی است را باید به‌عنوان مصارف حساس در نظر گرفت. بدین معنی که این مصارف حساس باید موردتوجه جدی طراحان سامانه قدرت قرار گیرند تا همواره، و البته در زمان بحران، برق‌رسانی به آن‌ها با حداکثر قابلیت اطمینان صورت گیرد. به عبارت ساده‌تر، طراحی سامانه قدرت باید به‌گونه‌ای انجام شود که بارهای حساس موجود، در اکثر مواقع از طریق شبکه توزیع برق محلی تغذیه شوند. ذکر این نکته ضروری است که، طرح موفق مبتنی بر تاب‌آوری و برگشت‌پذیری از دید مدافع و به تعبیری بهره‌بردار شبکه، طرحی است که در زمان مواجهه با بحران، شبکه با کمترین اخلال به کار خود ادامه دهد و به عبارتی پاسخگوی نیاز قراردادی مشترکین باشد. علاوه‌بر این، جبران خسارت ناشی از بحران و به عبارتی برگرداندن شبکه به شرایط قبل بحران، با هزینه کمتری صورت پذیرد. مسیریابی فیدرها و انتخاب محل پست‌ها و نیروگاه‌ها و منابع انرژی پراکنده، استفاده از نقاط تغذیه متعدد برحسب نوع و اهمیت مصرف‌کننده، اتوماسیون شبکه، استفاده از هادی‌های تقویت‌شده و انتخاب تعداد مدارات، کابل‌کشی زیرزمینی، مقاوم‌سازی و استفاده از ابزارهای آشکارساز خطا، ایزوله‌سازی و سامانه بازیابی خودکار ازجمله موارد مهمی هستند که برحسب نظر تصمیم گذاران باید در طراحی و برنامه‌ریزی سامانه قدرت بر مبنای تاب‌آوری و برگشت‌پذیری مدنظر قرار داده شوند.

سامانه قدرت در سراسر جهان، به‌طور معمول بر مبنای اصول اساسی قابلیت اطمینان، امنیت و کفایت، طراحی و بهره‌برداری می‌شوند. این اصول می‌توانند به‌درستی با خطاهای شناخته‌شده در تجهیزات زیرساخت قدرت تعامل کنند. بااین‌حال، اخیراً رخداد فجایع طبیعی، نگرانی‌هایی در باب نگرش متداول قابلیت اطمینان گرا اوج گرفته است. بر اساس تجارب به‌دست‌آمده از بلایای طبیعی اخیر، ویژگی‌های اساسی این‌چنین رویدادهایی که آن‌ها را از خطاهای مرسوم سامانه قدرت، متمایز می‌کند، به‌قرار زیر است:

- زمان وقوع و طول مدت این اختلالات شدیداً با عدم قطعیت همراه هستند و ممکن است روزها به طول بیانجامد
- طبیعت کاملاً دینامیکی دارند و پیش‌بینی مؤثر رویدادهای آتی یا توالی وقوع آن‌ها بسیار سخت است
- وقوع آن‌ها ممکن است منجر به خطای چندین تجهیز در زمان کوتاهی شود
- منابع توان ممکن است قابل دستیابی یا در دسترس نباشند

با توجه به ویژگی‌های ذکرشده، به‌منظور داشتن سامانه تاب‌آور، سامانه مورد بحث باید ویژگی‌های زیر را داشته باشد:

- به‌دلیل درجه بالایی از عدم قطعیت‌ها، باید تنوع منابع تأمین‌کننده تا حد ممکن افزایش یابد و از وابستگی به مجموعه محدودی از تجهیزات تأمین قدرت پرهیز شود.
- بایستی انعطاف‌پذیری کافی برای پاسخگویی سریع به رخدادها وجود داشته باشد و براین اساس روش‌های بهره‌برداری حتی در طول زمان‌های کوتاه تنظیم گردد
- به‌دلیل کمبود در منابع در دسترس، اولویت‌ها به‌منظور تأمین بارهای مختلف باید شناسایی و مشخص گردد

تاکنون مطالعات گسترده‌ای در خصوص تاب‌آوری و برگشت‌پذیری سامانه‌های قدرت مخصوصاً در بخش تولید و انتقال انجام شده است و بخش توزیع به‌دلیل ماهیت غیرفعال خود سهم اندکی از این مطالعات را به خود اختصاص داده است. علاوه براین، مقالات موجود در این حوزه بیشتر بر پایه مقاومت‌سنجی سامانه‌های قدرت موجود در مقابل رویدادهای HILP استوار هستند. درحالی‌که باید معیارهای تاب‌آوری و برگشت‌پذیری در مرحله طراحی و برنامه‌ریزی ملاک عمل قرار گیرد، تا از هزینه‌های کلان مقاوم‌سازی ثانویه جلوگیری به عمل آید. همین‌طور با توجه به وابستگی شدید فعالیت‌های اساسی به انرژی الکتریکی باید راه‌کارهایی در جهت محافظت از این ساختار راهبردی به عمل آید. تاب‌آوری کوتاه‌مدت سامانه قدرت در طی اختلالات الکتریکی، وابسته به توانایی سامانه در غلبه مؤثر و سریع با در نظر گرفتن شرایط سامانه یا توانایی آن در کاهش تدریجی تغییر می‌کند. تاب‌آوری میان‌مدت معرف ویژگی‌هایی است که سامانه قدرت تاب‌آور باید قبل (پیش‌شرط مانند تقاضای بار و وضعیت هوا)، در طول (حوادث پی‌درپی) و بعد (بازیابی) از حادثه الکتریکی، به‌ترتیب، مقاومت، افزونگی و بهبودی، داشته باشد. اقدامات میان‌مدت، اقدامات پیشگیرانه و اصلاحی هستند که قبل از، روزها یا هفته‌ها، در طی و بعد از رخداد شدید مربوط به شرایط بد آب و هوایی انجام می‌گیرند. شرکت‌های برق مطابق با پیش‌بینی وضعیت جوی باید تأسیسات در دسترس خود را در مؤثرترین شیوه ممکن به‌منظور رویارویی با رویداد بد آب و هوایی استفاده کنند. اقداماتی که باید انجام گیرد شامل، برنامه‌ریزی ذخیره، برنامه‌ریزی دوباره واحدهای تولیدی، تضمین توانایی شروع مجدد، هماهنگی با شبکه‌های مجاور، ذخیره‌ساز انرژی و مدیریت سمت تقاضا. تاب‌آوری بلندمدت به سازگاری زیرساخت حیاتی به تهدیدهای جدید و تغییر شرایط اشاره دارد. در سامانه‌های قدرت، سازگاری از طریق مطالعات ریسک و قابلیت اطمینان، شامل سناریوهای آتی محتمل، به‌منظور شناسایی تهدیدهای اصلی بر روی پایداری سامانه قدرت حاصل می‌شود. سپس در صورت نیاز، اقداماتی به‌منظور ارتقا تاب‌آوری سامانه در برابر هم حوادث قابل پیش‌بینی و هم حوادث غیرمنتظره انجام می‌گردد. اقدامات بلندمدت، اشاره به برنامه‌ریزی طولانی‌مدت سازگاری به‌منظور ارتقا تاب‌آوری سامانه در برابر رویدادهای وابسته به شرایط جوی و تغییرات آب و هوایی دارد. به بخشی از این اقدامات در زیر اشاره شده است:

- ارزیابی و مدیریت ریسک به‌منظور سنجش و آماده‌سازی در برابر چنین رویدادهایی
- تخمین دقیق محل احتمالی رویداد و شدت آن
- ارتقا طرح برنامه‌های اضطراری و آمادگی
- هرس کردن درختان/ مدیریت زندگی گیاهی به‌منظور پاک کردن خطوط انتقال کنار راهی
- زیرزمینی کردن خطوط توزیع و انتقال
- ارتقا تجهیزات با مواد نیرومندتر
- بالا بردن افزونگی مسیرهای انتقال با احداث تأسیسات انتقال جدید
- تغییر مسیر خطوط انتقال به نواحی که کمتر تحت تأثیر شرایط بد جوی قرار می‌گیرند
- مرتفع ساختن پست تا و تأسیسات کلیدانی به نواحی که کمتر دچار سیل می‌شوند
- انبار و نگهداری کردن از دکل تا و مواد پشتیبان
- افزایش تجسم سازی و آگاهی محیطی از طریق نظارت پیشرفته و ابزار پیش‌بینی

اثربخشی اقدامات پیشگیری و اصلاحی، به‌شدت وابسته به توانایی بهره‌برداران سامانه در درک و فهم درست اطلاعات و داده‌های ورودی، تشخیص مشکل، اولویت‌بندی، شناسایی منابع در دسترس و سرانجام اعمال مناسب‌ترین معیار برای بازیابی سامانه به حالت تاب‌آور است.

در هر سیستم قدرت، شبکه توزیع آن به دلیل نقطه اتصال به مصرف‌کنندگان نهایی دارای جایگاه ویژه‌ای است به‌گونه‌ای که در عرف بین‌الملل حدود ۳۰٪ تا ۵۰٪ از کل هزینه سرمایه‌گذاری یک سامانه قدرت به شبکه توزیع تعلق می‌گیرد. کار آیی یک شبکه توزیع در انجام وظایف محوله برحسب افت ولتاژ، تداوم سرویس‌دهی، قابلیت انعطاف، بازدهی و هزینه آن بیان می‌گردد. با توجه به گستردگی شبکه‌های توزیع الکتریکی، امنیت عرضه انرژی الکتریکی وابستگی شدیدی به این شبکه دارد. طراحی بهینه این شبکه، باعث خواهد شد که تا توان موردنیاز مشترکین در کمترین هزینه ممکن، باقابلیت اطمینان بالا و در کیفیت مطلوب عرضه گردد. با توجه به اهمیت روزافزون شبکه‌های توزیع، تلاش زیادی در راستای طراحی بهینه آن، از دیرباز در حال انجام است. چرا که امروزه و با رشد فنّاوری‌های مختلف، نیاز به برق و در نهایت نیاز به

شبکه عرضه انرژی الکتریکی که بتواند در تمامی شرایط اعم از شرایط عادی و بحرانی عملکرد مطمئنی داشته باشد، یک نیاز اساسی به شمار می‌رود. با توجه به توضیحات ارائه‌شده در باب اهمیت شبکه توزیع در عرضه انرژی مطمئن، لذا باید در کلیه مراحل طراحی و برنامه‌ریزی شبکه توزیع، معیارهای تاب‌آوری جهت افزایش ضریب اطمینان و تداوم نیرورسانی لحاظ گردد. منظور از طراحی بهینه، یافتن راهبرد مبتنی‌بر ارتقا تاب‌آوری و برگشت‌پذیری است که در کمترین هزینه به بهترین شرایط فنی منجر شود. به عبارتی آرمان مهندسی که پیشنهاد طرحی با کمترین هزینه و بیشترین بهره‌وری است، رعایت گردد. تاکنون مطالعات گسترده‌ای در خصوص طراحی سامانه قدرت در سطح توزیع با اهداف مختلف فنی و/ یا اقتصادی انجام شده است. عمده مطالعات انجام‌شده در این زمینه مربوط به شبکه‌های توزیع کنونی با ساختارهای شناخته‌شده است که سال‌ها مورد بهره‌برداری قرارگرفته‌اند. متأسفانه در این مطالعات مقوله ارتقا تاب‌آوری و برگشت‌پذیری بسیار کمرنگ بوده است و به‌ندرت مقاله‌ای در این زمینه می‌توان یافت. در سال‌های اخیر با ظهور مفهوم شبکه‌های هوشمند، مسئله "ارتقا تاب‌آوری و برگشت‌پذیری" در سطح توزیع نیز موردتوجه فراوان قرارگرفته است. در این راستا، رویکردهای نوینی در طراحی، برنامه‌ریزی، بهره‌برداری و کنترل شبکه‌های توزیع هوشمند ایجادشده است. بر اساس مطالعات انجام‌شده پایه اصلی و هسته شبکه‌های توزیع هوشمند، ریز شبکه‌ها خواهند بود. به‌طوریکه در ویرایش چهارم استاندارد IEEE ۱۵۴۷ نیز به این موضوع اشاره شده است. ریزشبکه‌های با اضافه کردن تجهیزات شبکه فعال در سطح توزیع موجب ارتقا انعطاف‌پذیری در عملکرد و کاهش آسیب‌پذیری‌های دستگاه‌های قدرت مرسوم که درنتیجه تولید و معماری کنترل متمرکز و فواصل طولانی بین منابع تولید و بارها ایجاد می‌شوند، شده است. با این شیوه، ریزشبکه‌ها به‌منظور دستیابی به یکی از اهداف شبکه‌های هوشمند مبنی بر "تاب آور و برگشت‌پذیر بودن شبکه در برابر حمله و بلایای طبیعی با توانایی ترمیم و بازیابی سریع" مشارکت می‌کنند. ازاین‌روی، تأثیر رویدادهای HILP می‌تواند با توسعه و گسترش ریز شبکه‌ها به دلیل فراهم بودن امکان تأمین بار محلی در ریز شبکه حتی درزمانی که تأمین توان از شبکه اصلی ممکن نیست، کاهش یابد؛ بنابراین، ظهور ریزشبکه‌ها در دستگاه‌های قدرت مدرن اقدام امیدوارکننده‌ای است که می‌تواند نیاز به تاب‌آوری در سامانه قدرت را برطرف سازد [۴۳]. می‌توان گفت که، با طوفان اخیر در ایالت متحده آمریکا و اختلالات اجتماعی چشمگیر بالقوه جرقه بحث‌های جدی‌تر در مورد ارزش و کاربرد ریز شبکه‌ها در صنعت برق و انرژی زده شد.

بنا به تعاریف موجود، ریزشبکه باید دارای سه مشخصه متمایز باشد [۴۴]:

- مرزهای الکتریکی باید به‌وضوح مشخص باشد
- وجود دستگاه‌های کنترل به‌منظور بهره‌برداری هماهنگ منابع انرژی پراکنده و حفظ ولتاژ و فرکانس در محدوده قابل‌قبول
- تجمیع دقیق ظرفیت نصب‌شده منابع انرژی پراکنده و بارهای قابل‌کنترل به‌منظور تأمین مطمئن تقاضای بحرانی

ریزشبکه‌ها در دو حالت بهره‌برداری می‌شوند [۴۴]:

- متصل به شبکه: در این حالت، ریز شبکه قادر به خریدوفروش انرژی با شبکه بوده و یا می‌تواند هیچ‌گونه تبادل توانی نداشته باشد. این حالت بهره‌برداری معمولاً برای وضعیت عادی (بدون وقوع رخداد احتمالی) طراحی‌شده است، و هدف از آن ارتقا عملکرد سامانه و بهره‌وری به‌وسیله به‌کارگیری منابع انرژی پراکنده محلی است که موجب به تعویق انداختن سرمایه‌گذاری‌ها، کاهش تلفات سامانه و افزایش قابلیت اطمینان محلی می‌شود.
- جدا از شبکه: در این حالت، ریز شبکه قادر است به‌صورت جزیره‌ای از شبکه بهره‌برداری شود. این حالت معمولاً با عنوان جزیره‌سازی عمدی شناخته شده است. این حالت از بهره‌برداری، نیازمند آن است که منابع انرژی پراکنده داخل ریز شبکه به‌گونه‌ای هماهنگ بهره‌برداری شوند که ولتاژ و فرکانس در محدوده استاندارد باشد.

بهره‌برداری جزیره‌ای موفق مستلزم اجرای مدیریت مصرف انرژی برای مثال پاسخگویی بار یا بار زدایی یا استفاده از ذخیره‌سازهای انرژی به‌منظور دستیابی به تعادل تولید- بار است. این حالت از بهره‌برداری برای تأمین توان برای مکان‌های دور (بهره‌برداری جزیره‌ای دائم) و یا تأمین پیوسته توان در طی رخدادی احتمالی (بهره‌برداری جزیره‌ای موقت) است. برای حالت دوم، انتظار می‌رود که ریز شبکه به‌محض رفع رخداد خطا به حالت بهره‌برداری متصل به شبکه بازگردد.

درنتیجه مزایای بی‌شمار متصور برای ریز شبکه‌ها، این مفهوم در سال‌های اخیر موردتوجه بخش بزرگی از محققان قرارگرفته است و مطالعات سودمندی در این حوزه انجام‌شده است.

تقریباً اکثر این مطالعات بر روی یک ریزشبکه تنها و متصل به شبکه اصلی صورت گرفته است. همچنین تمرکز اصلی مطالعات صورت گرفته بیشتر در باب کنترل و بهره‌برداری از ریزشبکه بوده است. با توجه به‌مرور انجام‌شده بر روی مقالات و منابع موجود،

مسئله طراحی شبکه‌های توزیع بر پایه ریزشبکه‌های چندگانه به‌ندرت موردتوجه بوده است و تحقیقات صورت گرفته در این زمینه هم از نظر حجم و هم از نظر عمق بسیار محدود بوده است. علاوه‌بر این، به‌وضوح روشن است که اهداف اصلی تحقیقات موجود نیز، تاب‌آوری و برگشت‌پذیری نبوده است.

دلایل متعددی وجود دارد که چرا باید ریزشبکه متصل‌به‌هم باشند. اولین و ابتدایی‌ترین مزیت، تقسیم ذخیره در شرایط بحرانی (نبود تولید اصلی) به‌منظور کاهش احتمال فروپاشی سامانه، کاهش نیازمندی به بار زدایی اضطراری و ارتقا قابلیت اطمینان کل سامانه است. دومین مزیت، پخش بار اقتصادی ریزشبکه‌های چندگانه است که در هر دو حالت متصل به شبکه و حالت جزیره‌ای اجرایی می‌شود. مزیت سوم تقسیم ذخیره انرژی و خدمات جانبی است. مزیت چهارم، مربوط به نگرانی‌های تاب‌آوری ریزشبکه است. ریزشبکه‌ها ممکن است در مواقع اضطراری با چالش‌های وسیعی مواجه شوند ازجمله جزیره‌سازی غیرعمدی به‌دلیل اختلالی عمده در سمت شبکه بالادستی. اتصال راهبردی و شایسته ریزشبکه‌ها به هم می‌تواند موجب کاهش تأثیرات شرایط اضطراری گردد. علاوه‌بر این، یک ریزشبکه بزرگ با اهداف کنترلی می‌تواند به چندین ریزشبکه متصل‌به‌هم (حلقه) جزبندی شود.

علاوه‌بر این، شبکه توزیع برق به‌عنوان یک زیرساخت حساس و با توجه به اهمیت روزافزون نیرورسانی حتی در مواجهه با رویدادهای HILP، انتظار می‌رود که غالباً تاب‌آور و برگشت‌پذیر باشد. با این حال، تاب‌آوری و برگشت‌پذیری خود مفهوم جدیدی است که برخلاف جذابیت رو به رشد خود، فعلاً به‌طور دقیق موشکافی نشده است.

به‌طور خلاصه می‌توان گفت که، اهمیت تجارب کسب‌شده حامی به‌کارگیری ریزشبکه به‌منظور تأمین بارهای الکتریکی در طی تهدیدها است چراکه اساسی‌ترین مشکل برای مصرف‌کنندگان برق، نبود گزینه‌های جایگزین نیرورسانی (نبود پراکندگی) به‌منظور تأمین پیوسته بارهای خود از طریقی غیر از شبکه مرسوم است.

## ۴- پیشینه نظری و تجربی

نیاز به انرژی، با رشد جوامع بشری به‌طور چشمگیری افزایش‌یافته است که در این مسیر از انواع مختلف انرژی استفاده می‌شود. در این بین، انرژی الکتریکی به‌دلیل دارا بودن مزایایی، از جمله طیف وسیع کاربرد، سهولت تولید و انتقال و ... توجه ویژه‌ای را به خود جلب کرده است، بنابراین، در بین زیرساخت‌های حساس و حیاتی، سامانه قدرت نقشی اساسی در زندگی روزانه جوامع پیشرفته بازی می‌کند. این نقش نه‌تنها به‌دلیل اهمیت انرژی الکتریکی در زندگی روزمره است، بلکه ادامه حیات دیگر زیرساخت‌های حساس و حیاتی نیز وابستگی شدیدی به انرژی الکتریکی دارد. عملیات محتاطانه و سخت‌کوشانه در سطح شبکه این اطمینان را می‌دهد که انتقال و توزیع توان الکتریکی در حداکثر قابلیت اطمینان ممکن انجام پذیرد. درحالی‌که، اخلال در تحویل انرژی الکتریکی منجر به هزینه‌های بالای اقتصادی و اجتماعی می‌شود. مطالعات سازمان اطلاعات انرژی آمریکا در مورد قطع برق، در بین سال‌های ۱۹۹۱ تا ۲۰۰۵ از افزایش نمایی تعداد قطعی‌ها در آمریکای شمالی حکایت دارد. علاوه بر این، اختلال در شبکه توزیع الکتریکی مسئول خاموشی ۸۰ تا ۹۵ درصد مشترکین است [۴۵]. شرح و تحلیل ۹۳۳ مورد از حوادث که بین سال‌های ۱۹۸۴ تا ۲۰۰۶ منجر به قطعی شده‌اند به تفصیل بیان شده است [۴۶]. از طرفی دیگر، صنعت برق، صنعتی تخصصی، هزینه‌بر، زمان‌بر و حیاتی برای یک کشور است. جنگ‌ها و دفاع‌های امروزه، جنگ‌های هوشمند و پیچیده‌ای هستند و تمام تلاش مهاجم در این است که با کمترین هزینه نظامی و جانی بیشترین ضربه را به‌طرف مقابل وارد کند. یکی از این روش‌ها، حمله به مراکز نیروگاهی و تأسیسات تولید انرژی است. به‌عنوان مثال قابل لمس، در جریان جنگ تحمیلی ازآنجایی‌که نیروگاه‌ها اهداف راهبردی تلقی می‌شدند، حمله به آن نه‌تنها به استان‌های مرزی ایران محدود نشده و طیف وسیعی از نیروگاه‌ها را شامل می‌شد. نمونه‌هایی از سابقه تاریخی حملات نظامی عراق را در جریان جنگ تحمیلی گردآوری شده است [۴۷]. این مراکز به‌واسطه بزرگی و متمرکز بودن تجهیزات نصب‌شده، ضریب آسیب‌پذیری بالایی دارند. به لحاظ اهمیت منابع انرژی در شرایط جنگی، مختل کردن سامانه تولید انرژی الکتریکی و دسترس‌ناپذیر کردن نیروگاه‌ها و به‌طورکلی ایجاد بحران انرژی الکتریکی از اهداف اولیه مهاجمان است. یکی از اقداماتی که در زمان جنگ توسط دشمن انجام می‌شود، تخریب زیرساخت‌های حیاتی و گسترده ازجمله ایجاد اخلال در برق‌رسانی به محیط‌های حساس و مهم مانند سایت‌های استقراری نیروهای مسلح است. درنتیجه بروز خاموشی‌های گسترده و طولانی‌مدت در سایت‌های فرماندهی نیروهای مسلح، ارتباط یگان‌ها و عملیات لجستیکی و تدارکات مختل می‌شود. از سوی دیگر برای پادگان‌های دورافتاده مسئله تأمین انرژی الکتریکی برای مصارف نظامی و یا رفاهی، حائز اهمیت است؛ بنابراین، استفاده از منابع انرژی ترکیبی از قبیل منابع تولید پراکنده تجدیدپذیر بادی و خورشیدی برای پایگاه‌های نظامی حساس رواج یافته است تا اینکه بتوان تغذیه پایدار سایت‌های فوق را در شرایط بحرانی تضمین کرد. به‌طور نمونه ارتش امریکا در افغانستان با مشکل تهاجم القاعده به کاروان‌های سوخت‌رسانی برای پایگاه‌های خود مواجه شده که به‌منظور گذر از این بحران به سمت سایت‌های هیبریدی شامل انرژی‌های نو گام برداشته و در این زمینه سرمایه‌گذاری‌های هنگفتی کرده است. به‌طورکلی، گردانندگان وقایع خرابکارانه اغلب بازیگرانی کاملاً

باهوش و راهبردی هستند، آن‌ها می‌توانند آن دسته از وقایع با احتمال کم که سامانه در مقابل آن‌ها محافظت‌شده نیست، ولی درعین‌حال موجب آسیب جدی به سامانه قدرت می‌شوند، را مورد هدف قرار دهند. با توجه به اصل استتار و اختفا که مربوط به حفاظت از نیروها و تأسیسات از دید دشمن است، نیروگاه‌های عمده تولید برق با در نظر داشتن وسعت فضای اشغال‌یافته توسط تجهیزات بخش تولید، عملاً نمی‌توانند بستری برای اجرای این اصل فراهم آورند. حال‌آن‌که منابع انرژی تجدیدپذیر به دلیل عدم نیاز به سامانه‌های خنک‌کننده، مخزن‌های سوخت و غیره، به نسبت توان تولیدی خود، به ابعاد و فضای کمتری برای تولید توان نیاز دارند. ازاین‌رو می‌توان گفت به‌کارگیری این منابع می‌تواند به نحوی دربردارنده اصل اختفا و استتار باشد. همچنین با توجه به توزیع بهتر شرایط لازم جغرافیایی برای بهره‌برداری از این منابع در مقایسه با منابع فسیلی، این منابع با امکان نصب به‌صورت پراکنده قادرند تا حدودی تمرکززدایی لازم را در بخش تولید ایجاد کنند. پراکندگی منابع تولید، خود در زمان بلایای طبیعی نقش مؤثری در تأمین نیرو دارد چراکه اثر بلایای طبیعی به یک منطقه محدود است و دیگر نواحی مصون است. از طرفی دیگر، به‌دلیل گستردگی سامانه قدرت و همچنین محدود بودن امکانات و منابع مالی و انسانی، حفاظت از تجهیزات سامانه قدرت به‌طور کامل امکان‌پذیر نیست. به‌طورکلی می‌توان گفت که، مکان‌یابی بهینه تجهیزات و تسهیلات حیاتی و حساس نظامی و غیرنظامی ازجمله تمهیداتی است که در پدافند غیرعامل بدان پرداخته می‌شود. بر اساس اصول پدافند غیرعامل، تسهیلات باید در مکانی مستقر شوند که امکان اجرای مأموریت در مکان تعیین‌شده وجود داشته باشد. همچنین ایجاد پراکندگی و تمرکززدایی نیروها، تجهیزات و تأسیسات، اصل دیگر پدافند غیرعامل در مکان‌یابی تسهیلات حساس محسوب می‌شود. بر اساس اصل سوم، استقرار تسهیلات باید در مکانی انجام شود که نیاز به تغییر شکل عوارض و محیط پیرامون نباشد. انتخاب مکان بهینه تسهیلات با توجه به چنین اصولی، از یک‌سو از کشف و شناسایی تسهیلات جلوگیری می‌کند و از سوی دیگر حجم خرابی‌های ناشی از حملات دشمن و بلایای طبیعی را کاهش می‌دهد؛ بنابراین، ارائه راه‌کارهایی به‌منظور شناسایی و رتبه‌بندی تجهیزاتی که دارای بالاترین میزان ریسک در برابر حملات تروریستی و بلایای طبیعی هستند، می‌تواند در این زمینه بسیار مفید باشد. همچنین رتبه‌بندی تجهیزات برحسب میزان ریسک به برنامه ریزان سامانه قدرت این امکان را می‌دهد که بتوانند شاخصی برای سطح امنیت تجهیزات شبکه تعیین کرده و اقدامات لازم را به‌منظور کاهش آسیب‌پذیری تجهیزات در برابر تهدیدهای متعدد و متفاوت اتخاذ نمایند [۴۸]. مسئله مهمی که درزمینه ارزیابی امنیت سامانه قدرت با در نظر گرفتن حملات تروریستی وجود دارد بحث عدم قطعیت در این نوع حملات است. اولین عدم قطعیت، مربوط به رخ دادن حملات بر روی سامانه قدرت (میزان احتمال حمله) و دومین عدم قطعیت مرتبط به تأثیر حملات بر روی رفتار و عملکرد سامانه قدرت (نتیجه حمله) است. امنیت زیرساخت‌های الکتریکی با تعریف سناریوهای مختلف حمله موردبررسی و ارزیابی قرارگرفته و روشی برای محاسبه میزان آسیب ناشی از این حملات ارائه‌شده است [۴۹]. درنهایت راه‌کارهایی برای مقاوم‌تر کردن پست‌ها در برابر حملات تروریستی سایبری پیشنهاد شده است. از بین کارهای زیادی که بر روی آسیب‌پذیری سامانه قدرت تمرکز داشته‌اند، مهم‌ترین آن‌ها در ذیل مرور شده است. فرمول‌بندی ریاضی امنیت سامانه برق در مقابل تهدیدهای تروریستی ارائه شده است [۵۰]. تنها نگرانی این مقاله، حملات فیزیکی بر روی خطوط انتقال است با فرض ضمنی که زیرساخت SCADA به میزان نیاز مقاوم‌سازی شده است. در مقاله دیگری با اصلاح روش پیشنهادی [۵۰] و استفاده از روش تجزیه بندرز و استفاده از روش غیر ابتکاری، به حل مسئله مذکور پرداخته است [۵۱]. در تحقیق دیگری [۵۲] مسئله مذکور به‌صورت مسئله برنامه‌ریزی دوسطحی فرمول‌بندی شده است که در آن حمله‌کننده سعی بر آن دارد تا بار از دست‌رفته سامانه با کمترین تعداد حملات، مساوی یا بیشتر از یک سطح معین باشد. با این فرض که بهره‌بردار سامانه تمام اقدامات اصلاحی ممکن را به‌منظور کاهش بار حذف‌شده انجام خواهد داد. روشی برای آنالیز آسیب‌پذیری سامانه قدرت در حضور چندین حادثه احتمالی پیشنهاد داده است [۲۸]. به‌منظور شناسایی خطوط بحرانی یک شاخص برای ارزیابی آسیب‌پذیری برپایه تئوری زنجیره خطا پیشنهاد شده است [۵۳]. چندین کنش و واکنش بین حمله‌کننده و مدافع به‌منظور استنتاج معیار جدید قابلیت اطمینان برای دفاع از سامانه قدرت در مقابل حملات عمدی در نظر گرفته شده است [۵۴]. اصول شبکه‌های پیچیده به‌منظور تعیین شاخص بحران برای ارزیابی آسیب‌پذیری هر خط از شبکه در [۵۵] استفاده شده است. استفاده از تئوری شبکه‌های پیچیده، گراف تک جهته وزن‌دار سامانه قدرت در [۵۶] به‌دست آمده است که برای آنالیز آسیب‌پذیری سامانه قدرت است. روشی برای ارزیابی سامانه قدرت در برابر حملات عمدی و احتمالاتی ارائه شده است [۵۷]. تحقیق دیگری حملات هماهنگ فیزیکی- سایبری را مدنظر قرار داده و مدل جدیدی برای شناسایی حملات فیزیکی غیرقابل‌شناسایی ارائه داده است [۵۸]. کلیدزنی خط انتقال به‌عنوان راه‌کاری مؤثر به‌منظور کاهش تأثیرات حملات عمدی پیشنهاد داده شده است [۵۹]. روشی بر پایه مدافع- مهاجم- مدافع به‌منظور راهنمایی برنامه‌ریز سامانه، به‌عنوان مدافع، ارائه شده است که چگونه مقدار بهینه از منابع دفاعی در دسترس خود را جایابی کند تا آسیب‌پذیری سامانه در برابر حملات هماهنگ کاهش یابد [۶۰]. به‌منظور شناسایی تجهیزی که ازکارافتادگی آن بدترین تأثیر را روی سامانه سایبری- فیزیکی دارد، مقاله [۶۱] از شاخص ناپایداری استفاده

کرده است. واضح است که هدف مهاجم افزایش هزینه بهره‌برداری سامانه و میزان بار حذف‌شده است [۵۱-۵۰]. با توجه به این‌که برای تعمیر تجهیز معیوب زمان لازم است، هزینه‌هایی که سامانه قدرت باید متحمل شود درمجموع باید حساب گردد. در عالم واقعیت، هدف اصلی مهاجم ایجاد اضطراب و رعب و وحشت است. مسائل مالی مانند بار حذف‌شده می‌تواند معیار خوبی برای ارزیابی سطح اضطراب قرار گیرد. به‌منظور ارزیابی رفتار مهاجم، فرض بهره‌بردار مستقل سامانه (ISO) بر این است که مهاجم در طی افق زمانی دارای محدودیت منابع است [۲۸، ۵۰ و ۵۲]. در تحقیقی دیگر [۵۰]، آسیب‌های ناشی از حملات تروریستی بر روی سامانه قدرت بررسی‌شده و راه‌کارهایی برای حفاظت مؤثر از تجهیزات سامانه در برابر تهدیدات تروریستی ارائه شده است. راه‌کارهایی پیشنهاد شده است که توسط آن‌ها بهره‌برداران قادرند تجهیزات سامانه را از نظر میزان ریسک اولویت‌بندی کرده و با ارائه روش‌هایی برای حفاظت تجهیزات در برابر حملات، میزان ریسک ناشی از این حملات را کاهش دهند [۵۱]. در تحقیقی دیگر [۵۲]، با استفاده از تئوری بیزین- گیم و با طرح چندین سناریو مربوط به جمع‌آوری اطلاعات در مورد سامانه قدرت، به نقش اطلاعات و داده‌ها بر روی تجزیه و تحلیل ریسک ناشی از حملات بر روی سامانه قدرت پرداخته شده است. مقاله [۶۲] یک چارچوب مفهومی برای ایجاد یک دید وسیع در مورد تاب‌آوری سامانه‌های قدرت، با تمرکز بر روی حوادث ناشی از شرایط آب و هوایی به‌شدت نامساعد، ارائه کرده است و مفهوم منحنی‌های شکنندگی به‌منظور اعمال احتمال خرابی وابسته به زمان و شرایط آب‌وهوا به تجهیزات سامانه استفاده شده است. ویژگی‌های سامانه تاب‌آور مطابق با تعریف ارائه‌شده در شورای مشورتی ملی زیرساخت آمریکا (NIAC)، مقاومت، کاردانی، بازیابی سریع و سازگاری برشمرده شده است. این تعریف، یک مفهوم عام و مشابه برای تاب‌آوری ارائه می‌دهد که برای تمامی زیرساخت‌های حیاتی قابل اعمال است و علاوه‌بر آن توانایی آن را دارد که از رخدادهای مخرب درس گیرد و به‌منظور جلوگیری یا کاهش تأثیرات حوادث مشابه در آینده، بهره‌برداری زیرساخت حیاتی را با ساختار آن وفق می‌دهد. پاسخ زمانی سامانه قدرت در برابر بلایای طبیعی نمایش داده شده است [۴۶]. روشی برای تخمین قابلیت اطمینان، تاب‌آوری و برگشت‌پذیری، و آسیب‌پذیری منابع آبی ارائه شده است [۶۳]. قابلیت اطمینان به‌صورت احتمال حضور سامانه در شرایط عادی و بدون رخداد خطا، تاب‌آوری و برگشت‌پذیری به‌صورت توانایی سامانه به بازگشت به حالت عادی بعد از وقوع خطا و آسیب‌پذیری به‌صورت محتمل‌ترین خسارت ناشی از رخداد خطا تعریف شده است. با ارتقا مناسب شبکه‌های توزیع می‌توان عملکرد شبکه را در شرایط بعد از رخداد بهبود دهد. در مقاله [۶۴] مسئله طراحی بهینه شبکه توزیع الکتریکی به‌صورت برنامه‌ریزی آماری دوسطحی مدل‌سازی شده است. سناریوهای خسارت مربوط به بلایای طبیعی به‌عنوان مجموعه حوادث آماری مدل‌سازی شده است. در مطالعه [۶۵] روشی پیشنهاد شده است که بهره‌برداران سامانه با استفاده از آن می‌توانند مکان و زمانی که سامانه آن‌ها بیشترین آسیب‌پذیری را به حمله‌های عمدی دارد، ارزیابی کنند.

همان‌طور که می‌دانیم، کاهش منابع سوخت‌های فسیلی، سیاست‌های سخت‌گیرانه در باب کاهش آلودگی‌های زیست‌محیطی، هزینه‌بر بودن ایجاد زیرساخت‌های جدید در شبکه قدرت فعلی، بهره‌وری پایین شبکه موجود، نیاز به ارتقا کیفیت توان، نیاز به افزایش امنیت عرضه، نفوذ گسترده و روزافزون منابع انرژی متغیر تجدیدپذیر، ظهور خودروهای الکتریکی و ... از عوامل محرک به گذار از شبکه قدرت فعلی به شبکه هوشمند می‌باشند. شبکه هوشمند نیازها و توانمندی‌های بازیگران مختلف شبکه اعم از تولیدکنندگان، مصرف‌کنندگان، متصدیان شبکه و عوامل بازار برق را به‌منظور بهره‌برداری هر چه مؤثرتر تمامی قسمت‌های شبکه، کاهش هزینه‌ها، کاهش تأثیرات زیست‌محیطی هم‌زمان با افزایش قابلیت اطمینان، افزایش تاب‌آوری سامانه و بهبود پایداری، هماهنگ می‌کند [۶۶]. برنامه‌ریزی بهینه شبکه توزیع مسئله پیچیده‌ای با توابع هدف متعدد و قیود مختلف است. پیچیدگی مسئله در محیط شبکه‌های هوشمند و به دلیل در نظر گرفتن عدم قطعیت‌های ناشی از بار و تولید افزایش می‌یابد. در مقاله [۶۷] برنامه‌ریزی توسعه‌ای چندمرحله‌ای شبکه‌های توزیع به‌منظور یافتن مکان، زمان و ظرفیت پست‌های فشار متوسط و منابع تولید پراکنده حل شده است. به‌منظور افزایش تاب‌آوری شبکه توزیع الکتریکی در مقابل بلایای طبیعی، مسئله برنامه‌ریزی شبکه توزیع تاب‌آور برای هماهنگی گزینه‌های موجود مقاوم‌سازی و جایابی منابع تولید پراکنده باهدف کاهش هزینه‌های خرابی سامانه پیشنهاد شده است [۶۸]. می‌دانیم که پایه اصلی و هسته شبکه‌های توزیع ریزشبکه‌ها خواهند بود. گذار از شبکه قدرت مرسوم به سمت ریزشبکه‌های هوشمند و استفاده گسترده‌تر از منابع انرژی پراکنده و بارهای قابل‌کنترل، پیش‌بینی می‌شود که به تحول عظیمی در ابعاد مختلف سامانه قدرت منجر شود. با این‌حال، موانع متعددی نیز بر سر راه گسترش سریع و وسیع ریزشبکه‌ها وجود دارد. از جمله این موارد می‌توان به هزینه بالای گسترش ریزشبکه‌ها، نبود دانش کافی مصرف‌کنندگان از تأثیرات منابع تولید پراکنده و الگوهای برنامه‌ریزی بار و مخصوصاً مسائل مالکیت و مقررات اشاره کرد که باید به‌تفصیل موردبررسی قرارگرفته و راه‌کارهای مناسبی اجرایی گردد. بااین‌حال، ریزشبکه‌ها فرصت‌های بی‌نظیری را برای مصرف‌کنندگان و نیز برای بهره‌برداری و طراحی سامانه قدرت، معرفی کرده‌اند [۴۴] که در زیر به چندی از آن‌ها اشاره می‌شود:

- افزایش امنیت
- افزایش تاب‌آوری
- افزایش قابلیت اطمینان
- کاهش آلودگی
- هزینه‌های کاهش‌یافته ارتقا سامانه
- افزایش بهره‌وری انرژی
- بهبود کیفیت توان
- هزینه‌های کاهش‌یافته انرژی
- تعیین ترکیب تولید منابع انرژی پراکنده
- ارتقا شبکه‌ی توزیع
- گسترش کنترل‌کننده ارشد

به‌منظور پایه‌ریزی چارچوبی استوار در باب مفهوم ریزشبکه، تحقیقات گسترده‌ای درباره تشکیلات، ابزار کنترل، ویژگی‌ها و دیگر مشخصات فنی در حال انجام است. گسترش موفق مفهوم ریزشبکه‌ها نیازمند تدوین قوانین مناسب درباره تجمیع آن‌ها در شبکه‌های توزیع است. به‌منظور تدوین آن‌چنان قوانینی، شناسایی هزینه‌ها و سودهایی که یک ریزشبکه ایجاد می‌کند، یک تکلیف حیاتی است. در بین سایر جنبه‌ها، تأثیر ریزشبکه‌ها بر قابلیت اطمینان شبکه توزیع درنتیجه توانایی بهره‌برداری حالت جزیره‌ای در شرایط اضطرار به‌عنوان مزیتی مهم شناخته شده است. مقاله [۶۹]، موقعیت‌هایی را که حضور ریزشبکه، موجب ارتقا شاخص‌های قابلیت اطمینان شبکه توزیع می‌شود، شناسایی می‌کند. مبحث ساخت ریزشبکه در شبکه توزیع فعال از منظر مدیریت انرژی و استفاده بهینه از ظرفیت منابع انرژی تجدیدپذیر موضوع مهمی است که تحقیقات محدودی پیرامون آن انجام شده است. در تحقیق دیگری در ابتدا کاهش تلفات شبکه توزیع فعال را با مکان‌یابی بهینه منابع تولید پراکنده با روش احتمالاتی مورد بررسی قرار داده و سپس هم‌زمان با ساخت ریزشبکه‌ها، منابع ذخیره‌ساز و منابع تولید توان راکتیو به شبکه اضافه نموده است [۷۰]. در این مقاله ایجاد ریزشبکه باهدف کاهش نامتعادلی توان در آن‌ها انجام شده است. از منظر بهره‌برداری ریزشبکه‌های چندگانه، نتیجه آن شده است که در این حالت بیشینه خود کفایت ریزشبکه‌ها به‌منظور کمک به جلوگیری از گسترش خطا از یک قسمت از شبکه به قسمتی دیگر، حاصل می‌شود. موضوع مورداشاره، با در نظرگیری شاخص‌های قابلیت اطمینان، تکمیل شده است [۷۱]. نویسندگان مرجع [۷۲] ایده‌ها و نظرات مراجع [۷۱-۷۰] را گردآوری کرده و بر روی مزیت دیگری از بهره‌برداری شبکه توزیع فعال مبتنی بر ریزشبکه‌های چندگانه تمرکز کرده‌اند. این مرجع چارچوب کاملی برای ایجاد اقدامات کنترلی خودترمیم بهینه در شبکه توزیع فعال در برابر تمامی خطاهای آتی پیشنهاد داده است. این مرجع اشاره دارد که با طراحی مبتنی بر ریزشبکه با هدف افزایش امنیت عرضه انرژی، حداقل اقدامات به‌منظور دست‌یابی به توانایی خودترمیم در شبکه‌های توزیع فعال مورد نیاز است و ریزشبکه‌های منفصل از شبکه می‌توانند در حالت جزیره‌ای با حداقل بار زدایی بهره‌برداری گردند. تقسیم‌بندی شبکه توزیع فعال به مجموعه‌ای از ریز شبکه‌ها و بهره‌برداری بر اساس ریزشبکه‌های چندگانه می‌تواند مزایای متعددی برای شرکت‌های برق، مصرف‌کنندگان برق و صاحبان منابع تولید پراکنده داشته باشد. این مزایا شامل سادگی روش کنترلی، کنترل پراکنده بین ریزشبکه‌ها، جایابی بار و جابجایی بار بین ریزشبکه‌ها، ارتقا قابلیت اطمینان و ... است. علاوه‌بر این، تقسیم‌بندی شبکه قدرت به ریزشبکه‌ها یا جزایر باکفایت بالا (خوداستوار) می‌تواند، انتشار اختلالات را متوقف و از گسترش پی‌درپی حوادث جلوگیری کند [۷۰]. در تحقیق [۷۳]، به‌کارگیری مفهوم ریزشبکه‌های چندگانه در طراحی و بهره‌برداری از شبکه‌های توزیع فعال با مدل‌سازی دومرحله‌ای مبتنی بر شبیه‌سازی احتمالاتی مونت‌کارلو، بررسی شده است. مسئله چندهدفه احتمالاتی مذکور مبتنی‌بر معیارهای فنی متفاوتی ازجمله کفایت، بهره‌وری، پروفیل ولتاژ و قابلیت اطمینان به‌وسیله الگوریتم بهینه‌سازی NSGA II حل شده است [۷۳]. نتایج حاصل مؤید آن است که بهره‌برداری از شبکه توزیع فعال مبتنی بر ریزشبکه‌های چندگانه در مقایسه با شبکه مرسوم در تمامی ابعاد تعریف‌شده مناسب‌تر است. در تحقیق [۳۵] مدلی برای بهره‌برداری بهینه ریز-شبکه با در نظر گرفتن قیود جزیره‌سازی چند دوره‌ای ارائه شده است. کاهش هزینه‌های بهره‌برداری هدف از حل مسئله دوسطحی تعریف شده است. در مقاله [۷۴] مدلی برای حل مسئله طراحی ریزشبکه با در نظر گرفتن عدم قطعیت‌های فیزیکی و مالی ارائه شده است. مسئله طراحی ریزشبکه، توسعه ریزشبکه از منظر اقتصادی را ارزیابی کرده و ترکیب بهینه‌ای از منابع انرژی پراکنده برای نصب را پیشنهاد می‌دهد. خطاهای پیش‌بینی بار، ماهیت متناوبی تولید و قیمت بازار برق درروش بهینه‌سازی مقاوم ارائه‌شده، وارد شده‌اند. با خود جزیره‌سازی ریز شبکه نیز به‌عنوان منبع عدم قطعیت رفتار شده است. با این‌که مطالعات بسیاری درزمینه بهره‌برداری و کنترل بهینه ریزشبکه وجود دارد، ولی تحقیق در باب نقشه راه برنامه‌ریزی سرمایه‌گذاری ریزشبکه محدود است. مدلی برای یافتن ترکیب بهینه از منابع انرژی تجدیدپذیر و منابع تولید انرژی مرسوم در ریزشبکه‌ها پیشنهاد شده است [۷۵]. علاوه‌بر این تأثیر مالیات بر آلودگی را در طراحی سامانه توزیع مطالعه نموده است. خطای پیش‌بینی قیمت سوخت و سرعت متوسط باد با مشخص کردن متغیرهای حساسیت در نظر گرفته شده است. مطالعه‌ای در باب به‌کارگیری منابع انرژی پراکنده در ریزشبکه به‌جای منابع مرسوم تولید انرژی و نیز طراحی انتقال انجام شده است [۷۶]. تحقیق دیگری طراحی و برنامه‌ریزی بهینه از

ریزشبکه‌های هیبرید با در نظر گرفتن چرخه عمر منابع انرژی تجدیدپذیر، را بررسی می‌کند [۷۷]. این مطالعه نشان می‌دهد که ترکیب منابع انرژی‌های نو و منبع دیزلی در ریز شبکه‌ها در مقایسه با ریزشبکه‌های مبتنی بر منابع دیزلی، دارای هزینه خالص فعلی پایین‌تر و آلودگی کربنی کمتری است. مدل‌سازی دوسطحی چندهدفه به‌منظور یافتن منطقه بهینه برای احداث ریزشبکه و مشخص کردن مکان و ظرفیت تعداد مشخصی واحد منابع تولید پراکنده در ریزشبکه استفاده شده است [۷۸]. روشی برای یافتن بهینه مکان و ظرفیت واحدهای منابع تولید پراکنده در ریزشبکه‌ها و ساختار شبکه باهدف ارتقا قابلیت اطمینان در [۷۹] ارائه شده است. مسئله فوق با الگوریتم ذوب فلزات حل‌شده و تقاضای الکتریکی و حرارتی ریزشبکه وارد مدل‌سازی شده است. طراحی توسعه‌ای ریزشبکه باهدف یافتن مکان، ظرفیت و نوع منابع انرژی پراکنده در [۸۰] ارائه شده است. مکان بهینه منابع انرژی پراکنده بر اساس شاخص حساسیت تلفات در هر باس به‌دست‌آمده است. در مسئله فوق افزایش نسبت سود به هزینه هدف‌گذاری شده که با در نظر گرفتن شاخص قابلیت اطمینان نقطه بار حل‌شده است. طراحی توسعه تولید ریز شبکه با در نظر گرفتن اقتصاد مبتنی بر حداقل آلودگی کربنی بررسی‌شده است [۸۰]. نتایج حاکی از آن است که به‌کارگیری مناسب منابع تولید بادی و خورشیدی در ریزشبکه‌ها می‌تواند آلودگی‌های کربنی را محدود کند. روشی دوسطحی برای طراحی و برنامه‌ریزی بهینه ریزشبکه‌هایی با تقاضای بار هم‌زمان حرارت، برودت و توان الکتریکی ارائه شده است [۸۱]. تابع هدف مسئله فوق، کاهش هم‌زمان هزینه کل خالص فعلی و آلودگی کربنی در ریز شبکه‌ها است. یک دید کلی درباره مدل‌سازی، برنامه‌ریزی و مدیریت انرژی ریزشبکه‌هایی با تقاضای بار هم‌زمان حرارت، برودت و توان الکتریکی ارائه شده است [۸۲]. طراحی توسعه سامانه قدرت مبتنی بر ریز شبکه از منظر بهره‌بردار سامانه قدرت حل‌شده است [۸۳]. زیرساخت بهینه ارتباط و کنترل، مبتنی بر مفهوم ریز شبکه، برای شبکه‌های توزیع فعال به‌منظور تسهیل در چارچوب کنترلی قدرتمند منطبق با الگوی شبکه‌های هوشمند ضروری است. روشی نو برای طراحی زیرساخت ارتباط و کنترل در مقاله [۸۴] ارائه شده است. در این طرح، ویژگی‌های مربوط به هر دو شبکه توزیع الکتریکی و سامانه ارتباطی در نظر گرفته شده است. طرح پیشنهادی، تقسیم‌بندی بهینه و نظام‌مند شبکه توزیع به چندین ریزشبکه مجازی با ساختار بهینه ارتباطات و در نظر گرفتن کیفیت توان، را تسهیل می‌کند. روشی برای بهره‌برداری بهینه ریزشبکه‌ها در حضور منابع پراکنده از قبیل مراکز داده، خودروهای الکتریکی و منابع تولید پراکنده ارائه شده است. به‌منظور نیل به هدف بهره‌برداری کارای شبکه، مدل‌سازی چندهدفه پیشنهاد شده است [۸۵]. ریزشبکه‌ها به‌عنوان هسته و خوشه شبکه توزیع هوشمند شناخته شده‌اند. مدلی برای برنامه‌ریزی بهینه و خوشه‌بندی شبکه توزیع هوشمند فشار ضعیف مستقر در یک ناحیه بایر به چندین ریزشبکه خودمختار ارائه شده است [۸۶]. به‌منظور شکل‌دهی و مشخص کردن مرز الکتریکی ریزشبکه‌ها، معیارهای مشخصی از قبیل تعادل توان، امنیت عرضه و چگالی بار اعمال‌شده است. برنامه‌ریزی و توسعه شبکه‌های توزیع بانفوذ بالای ریزشبکه‌های متصل به شبکه فشار متوسط، هدف اصلی مقاله [۸۷] است. در این مقاله تأثیر ریزشبکه‌ها بر ساختار بهینه شبکه، تلفات، قابلیت اطمینان، اتصالات ذخیره، ارتقا شبکه و به تعویق انداختن سرمایه‌گذاری ارزیابی شده است. نتایج مؤید آن است که محل ریزشبکه به عوامل متعددی از قبیل، سیاست‌گذاری دولت، روحیه کارآفرینی، پارامترهای جغرافیایی، جمعیتی و منطقه‌ای وابسته است. برنامه‌ریزی بهینه ریزشبکه‌های چندگانه متصل‌به‌هم موجب ارتقا قابلیت اطمینان و بهره‌برداری اقتصادی مجموعه ریزشبکه‌ها می‌شود [۸۸]. برنامه‌ریزی بهینه، پارامترهای مختلفی از جمله اقتصاد، قابلیت اطمینان، متغیر بودن انرژی تجدیدپذیر، عدم قطعیت‌های مبتنی بر شبکه و منابع، را به‌منظور تطبیق چالش‌های غالب در بهره‌برداری وارد مدل‌سازی کرده است. نتایج حاصل مؤید آن است که روش برنامه‌ریزی متصل‌به‌هم پیشنهادی، ساختار بهینه دقیق و کارآمدی برای خوشه‌ای از ریز شبکه‌ها ارائه می‌دهد و نشان می‌دهد که روش برنامه‌ریزی سازگار می‌تواند به‌سادگی قابل‌اعمال و گسترش به ریزشبکه‌های کاربردی باشد. بهره‌برداری بهینه ریزشبکه‌های متصل‌به‌هم با در نظر گرفتن بازار برق و قابلیت اطمینان شبکه برپایه ریزشبکه‌های چندگانه، تحلیل و بررسی شده است [۸۹]. به دلیل رفتار غیرقابل پیش‌بینی بعضی از منابع انرژی مقیاس کوچک و توان مصرفی ریزشبکه‌ها، مدل‌سازی احتمالاتی به‌عنوان جز لاینفک، اعمال شده است. ارزیابی قابلیت اطمینان ریز شبکه‌ها در هر دو حالت بهره‌برداری متصل به شبکه و جزیره‌ای انجام شده است. همان‌طور که قبلاً نیز اشاره شد، راه‌کار نو و اجرایی برای بحث ارتقا تاب‌آوری و برگشت‌پذیری در سامانه‌های قدرت، گسترش ریزشبکه‌ها است. گسترش ریزشبکه به‌عنوان راه‌کاری که جذابیت روزافزونی برای مشترکین برقی که نمی‌توانند به تأمین برق از شبکه اصلی وابسته باشند، و/ یا به دنبال منافع اقتصادی درنتیجه تولید محلی برق هستند، مطرح است. مشترکین برق در داخل ریزشبکه می‌توانند از تأمین محلی برق در زمان‌هایی که آسیبی در شبکه اصلی موجب قطع عرضه برق شده است، منتفع گردند. اثرات رویدادهای HILP بر مصرف‌کنندگان به‌واسطه گسترش ریزشبکه‌ها که درنتیجه امکان‌پذیر ساختن تأمین توان بارهای محلی حتی در زمان‌هایی که تأمین توان از شبکه بالادستی در دسترس نیست، می‌تواند کاهش یابد [۴۴]. در تحقیق [۴۲]، چگونگی در دسترس بودن ریزشبکه‌ها در طی بلایای طبیعی و بعد

از وقوع، ارزیابی شده است. با استخراج مدل‌سازی ریاضی و در نظر گرفتن پارامترهای قابلیت اطمینان ریزشبکه، دو شاخص برای ارزیابی آسیب‌پذیری سامانه پیشنهاد شده است [۹۰]. مدل‌سازی بازآرایی ریزشبکه در هر دو حالت بهره‌برداری متصل به شبکه و جزیره‌ای و شاخص آسیب‌پذیری، استخراج شده است. در عمل، ریزشبکه‌ها با توانایی خود تغذیه و جزیره‌شدن می‌توانند در زمان وقوع بلایای طبیعی راه را برای بالا بردن تاب‌آوری سامانه قدرت هموار کنند. مزایای بهره‌برداری مبتنی بر ریزشبکه دستگاه‌های قدرت در ارتقا تاب‌آوری در مرجع [۳۲] به‌تفصیل بیان شده است. مدل بهینه‌سازی مقاوم برای بهره‌برداری بهینه ریزشبکه‌ها باهدف ارتقا تاب‌آوری پیشنهاد داده است [۹۱]. این مدل تلاش می‌کند تا بتواند گذاری موفق از حالت بهره‌برداری عادی شبکه به حالت اضطراری داشته باشد و نیز بتواند بعد از رفع شرایط اضطرار به حالت قبل بازگردد. این روش سعی دارد که قطع بار ریزشبکه را در حالت جزیره‌ای کاهش دهد. تجمیع وسیع منابع تولید پراکنده در شبکه‌های فشار ضعیف و متوسط می‌تواند درنتیجه به‌کارگیری مفهوم ریزشبکه‌های چندگانه میسر شود؛ یک معماری جدید از شبکه توزیع شامل سامانه کنترل سلسله مراتبی که منجر به هماهنگی بین واحدهای منابع تولید پراکنده و ریزشبکه‌ها شده و ازاین‌رو، بهره‌برداری از چنین سامانهی در حالت جزیره‌ای را ممکن می‌سازد. بعد از یک خاموشی سراسری، توانایی‌های ریزشبکه‌های چندگانه می‌تواند به‌منظور بازیابی خدمات در شبکه‌های توزیع به‌کار گرفته شود. یک روش جدید برای شروع مجدد ریزشبکه‌های چندگانه ارائه شده است [۹۲]. توالی اقدامات کنترلی تشریح داده‌شده و توسط شبیه‌سازی‌های عددی ارزیابی شده است. یک الگوریتم بهره‌برداری بهینه باهدف ارتقا حاشیه اقتصادی ریزشبکه به‌منظور تأمین بارهای بحرانی در حالت جزیره‌ای پیشنهاد شده است [۹۳]. روش آماری دوسطحی به‌منظور بهره‌برداری بهینه ریزشبکه تاب‌آور در مقاله [۹۴] ارائه شده است. تأثیر بلایای طبیعی بر روی بهره‌برداری ریزشبکه‌ها به‌صورت برنامه‌ریزی آماری مدل‌سازی شده است. مدل ساعتی ارائه‌شده تلاش خود را معطوف به کاهش تأثیرات قطع برق با بهره‌برداری مؤثر ریزشبکه کرده است. مدلی برای مدیریت بار باهدف ارتقا تاب‌آوری ریزشبکه پیرو جزیره‌سازی و با در نظر گرفتن محدودیت‌های ذخیره‌سازی انرژی و پاسخ فرکانسی ارائه شده است [۹۵]. این مرجع ویژگی‌های مدیریت بار پیشرفته ریزشبکه را توسعه داده است که شامل بهره‌گیری از بارهای پاسخگو است که امکان مدیریت سامانه ذخیره‌ساز انرژی ریزشبکه را فراهم می‌کند. در این مرجع روشی برای تنظیم فرکانس اولیه ریزشبکه و بهره‌برداری زمان واقعی ریزشبکه پیشنهاد شده است. بار ازدست‌رفته تحت عنوان شاخص آسیب‌پذیری ارائه شده است که همراه با اهداف تعریف‌شده، تحت عنوان قابلیت اطمینان و اقتصاد، در طراحی بهینه ریزشبکه به‌منظور تضمین بهره‌برداری تاب‌آور در حالت جزیره‌ای، استفاده می‌شود [۹۶]. شاخص ترکیبی از مقاومت-تاب‌آوری به‌منظور ارزیابی قابلیت سامانه قدرت در خود بهبودی به حالت عادی جدید بعد از تجربه رخداد غیرمنتظره مصیبت‌بار ارائه شده است که در مدل‌سازی مسئله چندهدفه بهره‌برداری بهینه ریز شبکه با استفاده از تئوری فازی به‌کار گرفته شده است [۹۷]. نحوه مدل‌سازی استفاده از ذخیره‌ساز انرژی از نوع چرخ طیار به‌منظور تأمین توان تاب‌آور به بارهای بحرانی بحث شده است [۹۸]. روش محاسبه در دسترس‌بودن ریزشبکه در طی بلایای طبیعی بر اساس مدل‌های فضای حالت مارکو ارائه شده است [۴۲]. آسیب‌پذیری در برابر چندین آسیب و توانایی سامانه در برابر حوادث طبیعی و عمدی تحلیل و بررسی شده است [۹۹]. ریزشبکه‌ها با کاهش احتمال حذف بار، می‌توانند موجب ارتقا تاب‌آوری سامانه قدرت شوند. جزیره‌سازی ریزشبکه معمولاً به‌منظور جداسازی ریزشبکه از شبکه توزیع اصلی باهدف حفاظت تجهیزات ریزشبکه از اختلالات در شبکه بالادستی یا حفاظت بارهای حساس به ولتاژ در مقابل افت ولتاژهای شدید در شبکه اصلی انجام می‌شود [۱۰۰]. توانایی جزیره‌سازی ریزشبکه به‌عنوان راه‌کاری ارزشمند به‌منظور ارتقا تاب‌آوری سامانه قدرت شناخته شده و توجه زیادی را در سال‌های اخیر به خود جلب کرده است [۱۰۱]. ارتقا تاب‌آوری به‌عنوان یک ارزش مکمل برای ریزشبکه‌ها که با ترویج پراکندگی منابع توان و جزیره‌سازی فراهم می‌شود، شناخته می‌شود. قیود کفایت به‌منظور تضمین حاشیه مناسب عملکرد در بهره‌برداری اقتصادی ریز شبکه و تأمین بارهای بحرانی در زمان وجود خطا در شبکه بالادستی، در نظر گرفته شده‌اند [۱۰۲]. مفهوم سامانه قدرت خودمختار پراکنده هوشمند باهدف ایجاد ریزشبکه‌ی تاب‌آور و دوستدار طبیعت و با به‌کارگیری مدیریت سمت بار به‌منظور تأمین بارهای حساس در شرایط اضطرار در مرجع [۱۰۳] پیشنهاد شده است. شبکه توزیع با منابع تجدیدپذیر و مبتنی‌بر سوخت‌های فسیلی می‌تواند به‌صورت ریزشبکه در حالت خودمختار و غیر خودمختار بهره‌برداری گردد. بهره‌برداری خودمختار شبکه توزیع نیازمند برنامه‌ریزی محتاطانه است. یک روش تفصیلی برای توسعه ریزشبکه خودمختار مقاوم ارائه شده است [۱۰۴]. روش پیشنهادی، بر پایه جایابی بهینه منابع تولید پراکنده و تغییر در ساختار ریزشبکه‌های خودمختار استوار است که با هدف کاهش تلفات سامانه و بهبود پروفیل ولتاژ حل شده است. روشی جامع و نو برای بهره‌برداری و خود ترمیمی شبکه توزیع دارای منابع تولید قابل/ غیرقابل‌کنترل پیشنهاد شده است [۱۰۵]. هدف از بهره‌برداری در حالت عادی، کاهش هزینه‌های بهره‌برداری و افزایش درآمد است. نتایج حاکی از آن است که تقسیم شبکه توزیع به چندین ریزشبکه موجب ارتقا بهره‌برداری و قابلیت اطمینان شبکه توزیع می‌شود.

روشی مدیریت قطع سلسله مراتبی به‌منظور ارتقا تاب‌آوری سامانه توزیع هوشمند شامل ریزشبکه‌های چندگانه در مقابله با حوادث غیره منتظره پیشنهاد شده است [۱۰۶]. در این راستا، بعد از شناسایی ویژگی‌های اصلی و نیازمندی‌های طرح مدیریت قطع تاب‌آور، چارچوب مناسبی ابداع‌شده و نقش‌ها و وظایف نهادهای مختلف مدیریتی در سامانه ریزشبکه‌های چندگانه معرفی می‌شود. تاب‌آوری سامانه قدرت درنتیجه بهبود روح خود ترمیمی سامانه در برابر خطاها، ارتقا می‌یابد. بازیابی توان در پی وقوع خطاها درنتیجه تغییر در ساختار شبکه توزیع الکتریکی و با حفظ محدودیت‌های بهره‌برداری، بهبود می‌یابد. روشی برای بازیابی توان در شبکه‌های توزیع ارائه‌شده است. روش پیشنهادی، بازیابی محلی را با بهره‌گیری از ریزشبکه‌ها ارتقا می‌دهد. خطای یکتا، خطاهای هم‌زمان، اولویت‌بندی ریز شبکه‌ها و اولویت‌بندی بارها موردمطالعه قرارگرفته و تأثیر آن‌ها ارزیابی شده است [۱۰۷]. در مقاله دیگری روشی مبتنی‌بر ریزشبکه‌های متصل‌به‌هم به‌منظور بازیابی خدمات در شبکه توزیع ارائه داده است [۱۰۸]. برنامه‌نویسی روش خطی مختلط- صحیح با توابع هدف شامل افزایش پاسخگویی بار و کاهش زمان بازیابی و تضمین برقراری قیود بهره‌برداری شبکه توزیع و ریزشبکه‌ها فرمول‌بندی شده است. روشی برای مدیریت انرژی در برنامه‌ریزی روز بعد ریزشبکه‌های متصل‌به‌هم ارائه شده است [۱۰۹]. هزینه بهره‌برداری در روش پیشنهادی کمتر از روش‌های غیرمتمرکز مرسوم و راهبردهای مدیریت انرژی هیبریدی است. درروش پیشنهادی امنیت مشترکین و نیز تاب‌آوری ریزشبکه‌ها منفصل در حالت بهره‌برداری جزیره‌ای ارتقا یافته است. علاوه‌بر این، ریزشبکه‌های AC/DC به‌منظور ارزیابی اثربخشی آن‌ها مطالعه شده‌اند. مقاله‌ای دیگر روشی نو برای بهره‌برداری شبکه توزیع به‌منظور ایجاد ریزشبکه‌های چندگانه دارای منابع تولید پراکنده در شبکه توزیع شعاعی و باهدف بازیابی زمان واقعی بارهای بحرانی در زمان خروج ارائه می‌دهد [۱۱۰]. تأمین بارهای بحرانی و هم‌زمان تضمین محدودیت‌های خود کفایت بهره‌برداری برای پیکربندی ریزشبکه‌ها با کنترل وضعیت کلیدهای کنترل از راه دور و منابع تولید پراکنده، هدف‌گذاری شده است. الگوریتم ارائه‌شده در مقاله [۱۱۱] قادر به محاسبه تاب‌آوری تمامی ساختارهای ممکن شبکه که تمامی بارهای حساس را تأمین می‌کند، است. این روش در طراحی و بهره‌برداری شبکه توزیع در حضور ریزشبکه‌ها مفید است. همان‌طور که میدانیم، مانع اصلی در برابر گسترش سریع ریزشبکه‌ها، هزینه سرمایه‌گذاری بالای منابع انرژی پراکنده است. منابع انرژی پراکنده قابلیت تولید انرژی با هزینه پایین، به‌خصوص در زمان‌های تراکم شبکه‌های انتقال و توزیع وقتی‌که قیمت برق زمان واقعی بالا است، را دارند. به‌هرحال، هزینه سرمایه‌گذاری بالا، می‌تواند مانع گسترش ریزشبکه توسط برنامه‌ریزان شود. به‌منظور تعیین کارایی اقتصادی گسترش ریز شبکه و متناسب با آن تولید بهینه منابع انرژی پراکنده، بایستی مطالعه برنامه‌ریزی طولانی‌مدت ریزشبکه انجام گیرد. مطالعه برنامه‌ریزی بایستی دربرگیرنده تمام گزینه‌های با ارزش از جمله هزینه، قابلیت اطمینان، تأثیرات زیست‌محیطی و پرداخت‌های خدمات جانبی به‌منظور توجیه هزینه‌های سرمایه‌گذاری ریزشبکه باشد. داده‌های نامعلوم که خطاهای پیش‌بینی دربارها، تولید متغیر تجدیدپذیر و قیمت‌های بازار می‌تواند بخشی از آن‌ها باشد باید در این مطالعات در نظر گرفته شوند. وقوع جزیره‌سازی به‌عنوان یک داده نامعلوم که تأثیر به سزایی در تصمیمات مربوط به توسعه و گسترش ریز شبکه‌ها، دارد باید اعمال شود [۷۴].

پیش‌بینی بار طولانی‌مدت یک منبع اصلی عدم قطعیت است. بار ثابت می‌تواند با دقت قابل‌قبولی پیش‌بینی شود. بار انعطاف‌پذیر، از دیگر سو، نمی‌تواند به‌آسانی پیش‌بینی گردد چرا که به تغییرات ساعتی قیمت، شرایط آب و هوایی و تصمیمات مصرف‌کننده وابسته است. تولید متغیر تجدیدپذیر یکی دیگر از منابع عدم قطعیت است. درصد بالایی از منابع انرژی تجدیدپذیر، معمولاً تولید بادی و خورشیدی، که تولید متغیر دارند در ریزشبکه‌ها مورد استفاده قرار می‌گیرند. در دسترس بودن تولید متغیر انرژی تجدیدپذیر معمولاً دارای یک الگوی تکرارشونده در بهره‌برداری روزانه ریز شبکه‌ها نیستند. پیش‌بینی دقیق تولید متغیر، چالشی جدی محسوب می‌شود و به‌شدت به مکان جغرافیایی و شرایط آب و هوا بستگی دارد. پیش‌بینی قیمت بازار درجه بالایی از خطا دارد و دلیل آن تأثیر پارامترهایی است که در جریان پیش‌بینی نقش دارند و خود دارای عدم قطعیت هستند، ازجمله: پیشنهادها قیمت بنگاه‌های تولیدی، گرفتگی خطوط انتقال و مشارکت مصرف‌کنندگانی که قادر به پاسخ به قیمت‌های بازار هستند. قیمت بازار برق (قیمت زمان واقعی برق در نقطه اتصال مشترک ریز شبکه) مهم‌ترین منبع عدم قطعیت در مسئله طراحی ریزشبکه است که بهره‌برداری از منابع مختلف انرژی را تحت تأثیر قرار می‌دهد. آخرین منبع عدم قطعیت مهم، جزیره‌سازی ریز شبکه است. گذار ریزشبکه به حالت جزیره‌ای زمانی رخ می‌دهد که در شبکه توزیع اصلی اختلالی رخ دهد. ریزشبکه می‌تواند به‌محض برطرف شدن اختلال از شبکه، با شبکه اصلی همگام‌سازی شود. زمان و طول مدت این نوع اختلالات برای ریزشبکه مشخص نیست. با این‌که، ریزشبکه به‌ندرت به حالت جزیره‌ای می‌رود، ولی طرح جزیره‌سازی به‌دلیل ذخیره چشمگیر هزینه‌های اجتماعی و ارتقا قابلیت اطمینان محلی در زمان خروج‌های اساسی (مانند طوفان) به‌عنوان بخشی از تصمیمات طراحی ریزشبکه، توجیه‌پذیر است.

## ۵- نتیجه‌گیری

یک سامانه مهندسی معمولاً به‌گونه‌ای طراحی می‌شود که از استقامت لازم در برابر حوادث عادی برخوردار بوده و عملکرد آن در چنین شرایطی به راحتی تحت تأثیر قرار نگیرد. ولی در عین حال، این سامانه باید انعطاف‌پذیری کافی هم داشته باشد تا بتواند خود را متناسب با یک اغتشاش شدید و بدون از دست رفتن کامل عملکرد خود، تطبیق داده و پس از رفع اغتشاش سریعاً خود را بازیابی کند. این ویژگی مهم از رفتار سامانه‌های زیرساختی مانند شبکه‌های برق، تاب‌آوری نامیده می‌شود. رخداد تهدیدهایی با احتمال وقوع پایین و شدت تخریب بالا (HILP)، نگرانی‌هایی را در باب نگرش معمول قابلیت اطمینان‌گرا پدید آورده است؛ بنابراین، ایستادگی در برابر موقعیت‌های دشوار ناخواسته و نادر، به‌عنوان چالشی اساسی شناخته‌شده است؛ بنابراین، ارگان‌های مختلف، تلاش‌هایی را در جهت ارتقا تاب‌آوری و برگشت‌پذیری سامانه قدرت انجام داده‌اند تا در مواجهه با رویدادهای HILP حداقل ممکن قطعی برق اتفاق افتاده و پیرو آن سامانه قدرت به‌سرعت به حالت بهره‌برداری عادی بازیابی گردد. برای این منظور راه‌کارهای مختلفی وجود دارد که در این بین، گسترش ریزشبکه‌ها می‌تواند سودمندتر باشد. ریزشبکه به‌دلیل فراهم آوردن امکان جزیره شدن در زمان رخداد خطا در شبکه بالادستی، قادر است بارهای محلی خود را از طریق منابع در دسترس خود تغذیه کرده و بدین طریق موجب ارتقا تاب‌آوری و برگشت‌پذیری سامانه گردد. مقالات متعددی درباره انواع تهدیدها، ارزیابی آسیب‌پذیری سامانه قدرت، راه‌کارهای ارتقا تاب‌آوری و درنهایت بهره‌گیری از شبکه‌های هوشمند در ایجاد شبکه تاب‌آور وجود دارد که در این مقاله مرور شده‌اند. در این مقاله، مفاهیم مرتبط با تاب‌آوری در برابر اغتشاشات شدید تبیین گردیدند. با ارائهٔ مثال‌هایی ساده ولی واقعی در حوزهٔ سامانه‌های قدرت، ضرورت ارتقا تاب‌آوری تشریح شد. همچنین، اجزای تشکیل دهندهٔ تاب‌آوری و البته شیوهٔ ارزیابی آنها معرفی شدند. به نظر می‌رسد که با توجه به افزایش وابستگی زندگی بشر به پایایی سامانه‌های زیرساختی و نیز روند صعودی وقوع اغتشاشات طبیعی ناشی از HILPs، مطالعات تاب‌آوری بایستی در برنامه‌های آموزشی و پژوهشی دانشگاه‌ها قرار گرفته و منابع و نرم‌افزارهای مرتبط با آن توسط اساتید و صاحب نظران تدوین گردد. این مقاله می‌تواند به‌نوبه خود دید و نگرش قابل‌قبولی از مبحث به‌روز و رو به رشد تاب‌آوری در اختیار خوانندگان قرار دهد و می‌تواند به‌عنوان مرجع اولیه برای مشتاقان به این مبحث باشد.

با توجه به اهمیت موضوع، مخصوصا در کشور عزیزمان ایران، پیشنهاد می‌شود، تحقیقاتی در زمینه یافتن راه‌کارهای موثر و عملیاتی به‌منظور ارتقا تاب‌آوری شبکه موجود کشور انجام شود. از این روی مقاوم‌سازی سامانه قدرت، از اساسی‌ترین اولویت‌های تحقیقاتی باید اتخاذ گردد.

## ۶- منابع


1. G. A. Maas, M. Bial, and J. Fijalkowski, “Final Report-System Disturbance on 4 November 2006,” Union for the Coordination of Transmission of Electricity in Europe, Tech. Rep., 2007.
2. R. M. Steven, J. P. Peerenboom, and T. K. Kelly, “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies,” IEEE Control Systems, vol. 21, no. 1, pp. 11-25, 2011.
3. US-Canada Power System Outage Task Force, “Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations,” US-Canada Power System Outage Task Force, 2004.
4. R. Gaffarpour and A. A. Pourmoosa, “Risk Assessment, Modeling, and Ranking for Power Network Facilities Regarding to Sabotage,” Advanced Defence Sci. & Tech., vol. 2, pp. 127-144, 2015.
5. H. S. Suad, F. Gubina, and A. F. Gubina, “Prediction of Power System Security Levels,” IEEE Trans Power Systems, vol. 24, no. 1, pp. 368-377, 2009.
6. R. Bacher, “Report on the Blackout in Italy on 28 September 2003 [Electronic resource],” Swiss Federal Office of Energy, Berne, Switzerland, 2003.
7. L. Jyrki and P. Holmström, “Electric Power Systems Blackouts and the Rescue Services: The Case of Finland,” Emergency Services College of Finland and State Provincial Office of Western Finland, 2007.
8. South China Bureau of State Electricity Regulatory Commission, “Power System Operation Condition Report during 2008 Snow Disaster,” Guangzhou, China, Tech. Rep., 2008.
9. N. Okada, T. Ye, Y. Kajitani, P. Shi, and H. Tatano, “The 2011 Eastern Japan Great Earthquake Disaster: Overview and Comments,” International Journal of Disaster Risk Science, vol. 2, pp. 34-42, 2011.
10. J. Watson, et al, “Power failure leaves 5 million in the dark,” [Internet]. San Diego: The San Francisco Chronicle, 2011. <http://www.sfgate.com/cgiin/article.cgi?f=/c/a/2011/09/08/MND01L2A1P.DTL> [cited 09.07.12].
11. R. Zimmerman, R. CE, J. S. Simonoff, and L. Lave, “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].
12. Congress, U. S. Office of Technology Assessment, “Physical vulnerability of electric system to natural disasters and sabotage,” OTA-E-453, Washington, DC: US Government Printing Office, 1990.

13. K. E. Merrick, "The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States," Air & Space Power Journal, vol. 18, no. 4, pp. 117-120, 2004.
14. S. Javier, K. Wood, and R. Baldick, "Analysis of Electric Grid Security under Terrorist Threat," IEEE Trans. power systems, vol. 19, no. 2, pp. 905-912, 2004.
15. R. Natalia, N. Xu, L. K. Nozick, I. Dobson, and D. Jones, "Investment Planning for Electric Power Systems Under Terrorist Threat," IEEE Trans. Power Systems, vol. 27, pp. 108-116, 2012.
16. D. J. Kang, J. J. B. Lee, H. Kim, and D. Hur, "Proposal Strategies of Key Management for Data Encryption in SCADA Network of Electric Power Systems," Int. J. Elec. Power, vol. 33, pp. 1521-1526, 2011.
17. D. Yannick and C. Singh, "A Quantitative Approach to Wind Farm Diversification and Reliability," Int. J. Elec. Power, vol. 33, pp. 303-314, 2011.
18. G. Xydis, "Comparison Study between a Renewable Energy Supply System and a Supergrid for Achieving 100% from Renewable Energy Sources In Islands," Int. J. Elec. Power. vol. 46, pp. 198-210, 2013.
19. OECD. Publishing, and International Energy Agency, "Harnessing variable renewables: A guide to the balancing challenge," Organisation for Economic Co-operation and Development, 2011.
20. House of Commons Energy and Climate Change Committee, "A European Supergrid," Seventh Report of Session, vol. 2, pp. 2010–2012, 2012.
21. K. Himanshu, M. Hadley, N. Lu, and D. A. Frincke, "Smart-Grid Security Issues," IEEE Security & Privacy, vol. 8, no. 1, pp. 81-85, 2010.
22. M. R. Anthony and L. Ekl. Randy, "Security Technology for Smart Grid Networks," IEEE Trans. Smart Grid, vol. 1, no. 1, pp. 99-107, 2010.
23. E. N. Göran, "Cyber Security and Power System Communication—Essential Parts of A Smart Grid Infrastructure," IEEE Trans. Power Delivery, vol. 25, no. 3, pp. 1501-1507, 2010.
24. L. Zhuo, X. Lu, W. Wang, and C. Wang, "Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid," Military Communications Conference, pp. 1830-1835, 2010.
25. The North American Electric Reliability Corporation [Internet]. "2011 long term reliability assessment," Nov. 2011. http://www.nerc.com/files/2011LTRA_Final.pdf.
26. M. Shahidehpour, Y. Fu, and T. Wiedman, "Impact of Natural Gas Infrastructure on Electric Power Systems," Proceedings of the IEEE, vol. 93, no. 5, pp. 1042-1056, 2015.
27. B. Ettore, T. Huang, Y. Wu, and M. Cremenescu, "Classification and Trend Analysis of Threats Origins to the Security of Power Systems," IJEPS, vol. 50, pp. 50-64, 2013.
28. A. J. Manuel, "Bilevel Programming Applied to Power System Vulnerability Analysis under Multiple Contingencies," IET generation, transmission & distribution, vol. 4, no. 2, pp. 178-190, 2010.
29. D. L. Gerard, K. G. Uhlen, H. Kjolle, and E. Stale Huse, "Vulnerability Analysis of the Nordic Power System," IEEE Trans. Power Systems, vol. 21, no. 1, pp. 402-410, 2006.
30. D. P. Chassin and C. Posse, "Evaluating North American Electric Grid Reliability Using the Barabási–Albert Network Model," Physica A: Statistical Mechanics and its Applications, vol. 355, no. 2, pp. 667-677, 2005.
31. M. Kia and H. A. Aalami, "A New Approach for Optimal Location of Power Dispatching Centers Based on Passive Defense Criteria Using EAHP," Advanced Defense Sci. & Tech., vol. 5, pp. 19-29, 2014.
32. A. Gholami, F. Aminifar, and M. Shahidehpour, "Front Lines against the Darkness: Enhancing the Resilience of the Electricity Grid through Microgrid Facilities," IEEE Electrification Magazine, vol. 4, no. 1, pp. 18-24, 2016.
33. R. Haghmaram, "Application of Interconnected Microgrids to Increase the Continuation of Electrification in Distribution Networks under Emergencies Situations," Advanced Defence Sci. & Tech, vol. 8, pp. 235-250, 2018.
34. C. Liang, M. Khodayar, and M. Shahidehpour, "Only connect: Microgrids for Distribution System Restoration," IEEE Power and Energy Magazine, vol. 12, no. 1, pp. 70-81, 2014.
35. A. Khodaei, "Microgrid Optimal Scheduling with Multi-Period Islanding Constraints," IEEE Trans. Power Systems, vol. 29, no. 3, pp. 1383-1392, 2014.
36. S. Parhizi, H. Lotfi, A. Khodaei, and S. Bahramirad, "State of the Art in Research on Microgrids: A Review," IEEE Access, vol. 3, pp. 890-925, 2015.
37. M. Bruch, V. Mnch, M. Aichinger, M. Kuhn, M. Weymann, and G. Schmid, "Power Blackout Risks: Risk Management Options Emerging Risk Initiative," Position Paper, CRO Forum, 2011.
38. Y. Lie and A. Campbell, "Behavior Investigations of Superconducting Fault Current limiters in Power Systems," IEEE Trans. applied Superconductivity, vol. 16, no. 2, pp. 662-665, 2006.
39. Y. Shirai, K. Furushiba, Y. Shouno, M. Shiotsu, and T. Nitta, "Improvement of Power System Stability by Use of Superconducting Fault Current Limiter with Zno Device and Resistor in Parallel," IEEE Trans. Applied Superconductivity, vol. 18, no. 2, pp. 680-683, 2008.
40. A. Amy, P. W. Parfomak, and D. A. Shea, "Electric Utility Infrastructure Vulnerabilities: Transformers Towers and Terrorism," CRS Report for Congress, Congressional Research Service, 2004.
41. W. Yezhou, C. Chen, J. Wang, and R. Baldick, "Research on Resilience of Power Systems under Natural Disasters—A Review," IEEE Trans. Power Systems, vol. 31, no. 2, pp. 1604-1613, 2016.
42. A. Kwasinski, V. Krishnamurthy, J. Song, and R. Sharma, "Availability Evaluation of Micro-Grids for Resistant Power Supply during Natural Disasters," IEEE Trans. Smart Grid, vol. 3, no. 4, 2007-2018, 2012.
43. US DOE, "The NETL Modern Grid Initiative. A Vision for the Modern Grid", Mar. 5, 2012. http://enterprise. alcatel-

58. L. Zhiyi, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks On Power Systems," IEEE Trans. Smart Grid, vol. 7, no. 5, pp. 2260-2272, 2016.
59. Z. Long and B. Zeng, "Vulnerability Analysis of Power Grids With Line switching," IEEE Trans. Power Systems, vol. 28, no. 3, pp. 2727-2736, 2013.
60. A. Natalia, A. Delgadillo, and J. M. Arroyo, "A Trilevel Programming Approach for Electric Grid Defense Planning," Computers & Operations Research, vol. 41, pp. 282-290, 2014.
61. C. X. Maggie, M. Crow, and Q. Ye, "A Game Theory Approach To Vulnerability Analysis: Integrating Power Flows With Topological Analysis," JEPS, vol. 82, pp. 29-36, 2016.
62. P. Mathaios and P. Mancarella, "Modeling and Evaluating the Resilience of Critical Electrical Power Infrastructure to Extreme Weather Events," IEEE Systems Journal, vol. 11, no. 3, pp. 1733-1742, 2015.
63. K. T. Rodding and D. Rosbjerg, "Choice of Reliability, Resilience and Vulnerability Estimators For Risk Assessments Of Water Resources Systems/Choix D'estimateurs De Fiabilité, De Résilience Et De Vulnérabilité Pour Les Analyses De Risque De Systèmes De Ressources En Eau," Hydrological sciences journal, vol. 49, no. 5, 2004.
64. Y. Emre, R. Bent, and S. Backhaus, "Designing Resilient Electrical Distribution Grids," arXiv preprint arXiv: 1409.4477, 2014.
65. S. Sayyadipour, G. R. Yousefi, and M. A. Latify, "Mid-Term Vulnerability Analysis of Power Systems under Intentional Attacks," IET Generation, Transmission & Distribution, vol. 10, no. 15, pp. 3745-3755, 2016.
66. Smart Grids Scope, History and Prospects Update on Smart Metering Activities Note to the GA 0, July 0226 (v.) Available at: http://www.ure.gov.pl/download.php?s=4&id=0154 NETL Modern Grid Strategy Powering our 04st-Century Economy Advanced Metering Infrastructure Conducted by the National Energy Technology Laboratory for the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability February 0221, http://www.smartgrid.gov/sites/default/files/pdfs/advanced_metering_infrastruure_20-0221.pdf.
67. S. N. Ravadanegh, N. Jahanyari, A. Amini, and N. Taghizadeghan, "Smart Distribution Grid Multistage Expansion Planning Under Load Forecasting Uncertainty," IET Generation, Transmission & Distribution, vol. 10, no. 5, pp. 1136-1144, 2016.
68. Wei. Yuan, J. Wang, F. Qiu, C. Chen, C. Kang, and B. Zeng, "Robust Optimization-Based Resilient Distribution Network Planning Against Natural Disasters," IEEE Trans. Smart Grid, vol. 7, no. 6, pp. 2817-2826, 2016.
69. C. P. Moises and M. A. Matos, "Assessing the Contribution of Microgrids to the Reliability of Distribution Networks," EPSR, vol. 79, no. 2, pp. 382-389, 2009.
70. S. A. Arefifar, Y. Abdel-Rady, I. Mohamed, and T. H. M. El-Fouly, "Supply-Adequacy-Based Optimal Construction of Microgrids in Smart Distribution lucent.com/private/active_docs/NETL%20Vision%20for%20the%20Modern%20Grid.pdf.
44. S. Bahramirad, A. Khodaei, J. Svachula, and J. R. Aguero, "Building Resilient Integrated Grids: one Neighborhood at a Time," IEEE Electrification Magazine, vol. 3, no. 1, pp. 48-55, 2015.
45. Y. Koç, A. Raman, M. Warnier, and T. Kumar, "Structural Vulnerability Analysis of Electric Power Distribution Grids," International Journal of Critical Infrastructures, vol. 12, no. 4, pp. 311-330, 2016.
46. P. Hines, J. Apt, and S. Talukdar, "Trends in the History of Large Blackouts in the United States," Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE. IEEE, 2008.
47. H. A. Aalami and H. Ramezani, "Presentation of a New Algorithm for the Operation of DG Resources in Electrical Interconnection Grids over the Critical Conditions," Passive Defence Sci. & Tech, vol. 3, pp. 231-241, 2012.
48. T. Nilsen and T. Aven, "Models and Model Uncertainty in the Context of Risk Analysis," Reliability Engineering & System Safety, vol. 79, no. 3, pp. 309-317, 2003.
49. T. Carol, A. Krings, and J. Alves-Foss, "Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening," Proc. ACM Workshop on Scientific Aspects of Cyber Terrorism, (SACT), Washington DC, vol. 64, 2002.
50. S. Javier, K. Wood, and R. Baldick, "Analysis of Electric Grid Security under Terrorist Threat," IEEE Trans. power systems, vol. 19, no. 2, pp. 905-912, 2004.
51. R. E. Alvarez, "Interdicting Electrical Power Grids," Diss. Monterey, California. Naval Postgraduate School, 2004.
52. A. M. Jose and F. D. Galiana, "On the Solution of the Bilevel Programming Formulation of the Terrorist Threat Problem," IEEE trans. Power Systems, vol. 20, no. 2, pp. 789-797, 2005.
53. W. Ansi, Y. Luo, G. Tu, and P. Liu, "Vulnerability Assessment Scheme for Power System Transmission Networks Based on the Fault Chain Theory," IEEE Trans. power systems, vol. 26, no. 1, pp. 442-450, 2011.
54. C. Guo, "Exploring Reliable Strategies for Defending Power Systems against Targeted Attacks," IEEE Trans. Power Systems, vol. 26, no. 3, pp. 1000-1009, 2011.
55. D. Ajendra and X. Yu, "A Maximum-Flow-Based Complex Network Approach for Power System Vulnerability Analysis," IEEE Trans. Ind. Informatics, vol. 9, no. 1, pp. 81-88, 2013.
56. C. Guo, Z. Y. Dong, D. J, Hill, and Y. S. Xue, "An Improved Model for Structural Vulnerability Analysis of Power Networks," Physica A: Statistical Mechanics and its Applications, vol. 388, no. 19, pp. 4259-4266, 2009.
57. C. Guo, Z. Y. Dong, D. J. Hill, G. H. Zhang, and K. Q. Hua, "Attack Structural Vulnerability of Power Grids: A Hybrid Approach Based On Complex Networks," Physica A: Statistical Mechanics and its Applications, vol. 389, no. 3, pp. 595-603, 2010.

Systems," IEEE trans. smart grid, vol. 3, no. 3, pp. 1491-1502, 2012.

71. S. A. Arefifar, A-RI M. Yasser, and T. HM. El-Fouly, "Optimum Microgrid Design for Enhancing Reliability and Supply-Security," IEEE Trans. Smart Grid, vol. 4, no. 3, pp. 1567-1575, 2013.
72. S. A. Arefifar, A-RI M.Yasser, and T. H. M. El-Fouly, "Comprehensive Operational Planning Framework for Self-Healing Control Actions in Smart Distribution Grids," IEEE Trans. Power Systems, vol. 28, no. 4, pp. 4192-4200, 2013.
73. H. Haddadian and R. Noroozian, "Multi-Microgrids Approach for Design and Operation of Future Distribution Networks Based on Novel Technical Indices," Applied Energy, vol. 185, pp. 650-663, 2017.
74. A. Khodaei, S. Bahramirad, and M. Shahidehpour, "Microgrid Planning under Uncertainty," IEEE Trans. Power Systems, vol. 30, no. 5, pp. 2417-2425, 2015.
75. S. Wencong, Z. Yuan, and Mo-Y. Chow, "Microgrid Planning and Operation: Solar Energy and Wind Energy," Power and Energy Society General Meeting, 2010 IEEE 2010.
76. J. Driesen and F. Katiraei, "Design for Distributed Energy Resources," IEEE Power and Energy Magazine, vol. 6, no. 3, pp. 30-40, 2008.
77. O. Hafez and B. Kankar, "Optimal Planning and Design of a Renewable Energy Based Supply System for Microgrids," Renewable Energy, vol. 45, pp. 7-15, 2012.
78. K. Buayai, W. Ongsakul, and N. Mithulananthan, "Multi- Objective Micro- Grid Planning by NSGA- II in Primary Distribution System," European Transactions on Electrical Power, vol. 22, no. 2, pp. 170-187, 2012.
79. M. R. Vallem and M. Joydeep, "Siting and Sizing of Distributed Generation for Optimal Microgrid Architecture," Power Symposium, 2005. Proceedings of the 37th Annual North American. IEEE, 2005.
80. Y. Xuewei and W. Tian, "Microgrid's Generation Expansion Planning Considering Lower Carbon Economy," Power and Energy Engineering Conference (APPEEC), 2012 Asia-Pacific. IEEE, 2012.
81. L. Guo, L. Wenjian, C. Jiejin, H. Bowen, and W. Chengshan, "A Two-Stage Optimal Planning and Design Method for Combined Cooling, Heat and Power Microgrid System," Energy Conversion and Management, vol. 74, pp. 433-445, 2013.
82. G. Wei, Z. Wu, R. Bo, W. Liu, G. Zhou, W. Chen, and Z. Wu, "Modeling, Planning and Optimal Energy Management of Combined Cooling, Heating and Power Microgrid: A Review," IJEPS. vol. 54, pp. 26-37, 2014.
83. A. Khodaei and M. Shahidehpour, "Microgrid-Based Co-Optimization of Generation and Transmission Planning in Power Systems," IEEE Trans. power systems, vol. 28, no. 2, pp. 1582-1590, 2013.
84. S. A. Arefifar, Y. Abdel-Rady, I. Mohamed, and T. El-Fouly, "Optimized Multiple Microgrid-Based Clustering Of Active Distribution Systems Considering Communication and Control Requirements," IEEE Trans. Ind. Electron, vol. 62, no. 2, pp. 711-723, 2015.
85. C. Guido, F. Mottola, D. Proto, and A. Russo, "A Multi-Objective Approach for Microgrid Scheduling," IEEE Trans. Smart Grid, vol. 8, no. 5, pp. 2109-2118, 2017.
86. S. Mojtahedzadeh, S. N. Ravadanegh, and M. R. Haghifam, "A Framework For Optimal Clustering of a Greenfield Distribution Network Area Into Multiple Autonomous Microgrids," Journal of Power Technologies, vol. 96, no. 4, pp. 219-228, 2016.
87. R. Millar, "Impact of MV connected microgrids on MV distribution planning," IEEE Transactions on Smart Grid, vol. 3, no. 4, pp. 2100-2108, 2012.
88. M. R. John, S. Kazemi, M. Lehtonen, and E. Saarijarvi, "Optimal Interconnection Planning of Community Microgrids with Renewable Energy Sources," IEEE Trans. Smart Grid, vol. 8, no. 3, pp. 1054-1063, 2015.
89. N. Nikmehr and S. N. Ravadanegh, "Reliability Evaluation of Multi-Microgrids Considering Optimal Operation of Small Scale Energy Zones under Load-Generation Uncertainties," IJEPS, vol. 78, pp. 80-87, 2016.
90. Z. Xin, T. Xiang, H. Chen, B. Zhou, and Z. Yang, "Vulnerability Assessment and Reconfiguration of Microgrid through Search Vector Artificial Physics Optimization Algorithm," IJEPS, vol. 62, pp. 679-688, 2014.
91. A. Khodaei, "Resiliency-Oriented Microgrid Optimal Scheduling," IEEE Trans. Smart Grid, vol. 5, no. 4, pp. 1584-1591, 2014.
92. R. F. O. Gil and J. A. Lopes, "Service Restoration on Distribution Systems Using Multi-Microgrids," European Transactions on Electrical Power, vol. 21, no. 2, pp. 1327-1342, 2011.
93. T. G. Antonis and N. D. Hatziargyriou, "Operation of Microgrids with Demand Side Bidding and Continuity of Supply for Critical Loads," European Transactions on Electrical Power, vol. 21, no. 2, pp. 1238-1254, 2011.
94. A. Gholami, T. Shekari, F. Aminifar, and M. Shahidehpour, "Microgrid Scheduling with Uncertainty: The Quest for Resilience," IEEE Trans Smart Grid, vol. 7, no. 6, pp. 2849-2858, 2016.
95. C. Gouveia, J. Moreira, C. L. Moreira, and P. J. A. Lopes, "Coordinating Storage and Demand Response for Microgrid Emergency Operation," IEEE trans. smart grid, vol. 4, no.4, pp. 1898-1908, 2013.
96. X. Xu, M. Joydeep, C. Niannian, and M. Longhua, "Planning of Reliable Microgrids in the Presence of Random and Catastrophic Events," International Trans. Electrical Energy Systems, vol. 2, no. 8, pp. 1151-1167, 2014.
97. C. A. Sergio, M. R. V. Spakovsky, A. Fuentes, C. L. Prete, B. F. Hobbs, and L. Mili, "Multi-Objective Optimization for the Sustainable-Resilient Synthesis/Design/Operation of A Power Network Coupled To Distributed Power Producers Via Microgrids," ASME 2012 International Mechanical Engineering Congress and Exposition. American Society of Mechanical Engineers, 2012.
98. R. Arghandeh, M. Pipattanasomporn, and R. Saifur, "Flywheel Energy Storage Systemsf Ride-Through Applications in a Facility Microgrid," IEEE Trans. smart grid, vol. 3, no. 4, pp. 1955-1962, 2012.
99. D. J. Cox, "Microgrid Infrastructure Modeling for

Residential Microgrids," Power Engineering Society General Meeting, 2007. IEEE. IEEE, 2007.

100. M. Shahidehpour, "Role of Smart Microgrid in A Perfect Power System," Power and Energy Society General Meeting, 2010 IEEE. IEEE, 2010.
101. M. Victor, C. Myres, and N. Bakshi, "The Vulnerabilities of The Power-Grid System: Renewable Microgrids as an Alternative Source of Energy," Journal of business continuity & emergency planning, vol. 4, no. 2, pp. 142-153, 2010.
102. T. G. Antonis and N. D. Hatziargyriou, "Operation of Microgrids with Demand Side Bidding and Continuity of Supply for Critical Loads," European Transactions on Electrical Power, vol. 21, no. 2, pp. 1238-1254, 2011.
103. R. Saifur, "Framework for a Resilient and Environment-Friendly Microgrid with Demand-Side Participation," Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE. IEEE, 2008.
104. K. M. Venkata, S. A. Daniel, and S. Gurunathan, "A Methodology for Transforming an Existing Distribution Network into a Sustainable Autonomous Micro-Grid," IEEE Trans. Sustainable Energy, vol. 4, no. 1, pp. 31-41, 2013.
105. W. Zhaoyu and J. Wang, "Self-Healing Resilient Distribution Systems Based on Sectionalization into Microgrids," IEEE Trans. Power Systems, vol. 30, no. 6, pp. 3139-3149, 2015.
106. F. Hossein, M. Fotuhi-Firuzabad, and M. Moeini-Aghtaie, "Enhancing Power System Resilience through Hierarchical Outage Management in Multi-Microgrids," IEEE Trans. Smart Grid, vol. 7, no. 6, pp. 2869-2879, 2016.
107. N. J. Anuranj, K. M. Rohit, S. Ashok, and S. Kumaravel, "Resiliency Based Power Restoration in Distribution Systems Using Microgrids," Power Systems (ICPS), 2016 IEEE 6th International Conference on. IEEE, 2016.
108. A. Anmar and Z. Wang, "Service Restoration in Resilient Power Distribution Systems with Networked Microgrid," Power and Energy Society General Meeting (PESGM), 2016. IEEE, 2016.
109. A. Hussain, H. Bui, and M. Kim, "A Resilient and Privacy-Preserving Energy Management Strategy for Networked Microgrids," IEEE Trans. Smart Grid, 2016.
110. C. Chen, J. Wang, F. Qiu, and D. Zhao, "Resilient Distribution System by Microgrids Formation After Natural Disasters," IEEE Trans. smart grid, vol. 7, no. 2, pp. 958-966, 2016.
111. B. Prabodh, S. Chanda, and A. K. Srivastava, "A Novel Metric to Quantify and Enable Resilient Distribution System using Graph Theory and Choquet Integral," IEEE Trans. Smart Grid, 2016.

# Resiliency, an Answer to Existing Passive Defense Concerns About the Classical Reliability-Oriented View in Electric Power Networks

**R. Ghaffarpour[*], M. R. Jannati Oskuee, S. Najafi Ravadanegh, H. Alami**

## Abstract

Power systems have been traditionally designed and operated based on the main principles of reliability, i.e. security and adequacy. These principles can properly deal with identified failures in the power infrastructure components. However, recently occurred high impact low-probability (HILP) threats have raised the concerns about the classical reliability-oriented view. As a critical infrastructure, power systems are more and more expected to be resilient to HILPs. So, the related governmental organizations put their endeavors to enhance the resiliency of these networks against HILPs. For this purpose, there is a great need to identify different threats and evaluate their impacts. The investigation of different threats, identification of different ways to enhance the resiliency and finally introducing smart grid concept as an efficient way to increase the resiliency of the distribution networks are reviewed in this paper.

**Key Words:** *Smart Distribution Network, Resiliency, Design, Planning, Operation*

[*] Imam Hossein Comprehensive University- (rghaffarpour@ihu.ac.ir) - Writer-in-Charge