مفاهیم و مبانی ارزیابی تاب‌آوری در شبکه‌های برق

فرخ امینی‌فر[1] **متین فرهومندی[2]**

۱- استادیار- دانشکده مهندسی برق و کامپیوتر- دانشگاه تهران- تهران- ایران
faminifar@ut.ac.ir
۲- دانشجوی کارشناسی ارشد- دانشکده مهندسی برق و کامپیوتر- دانشگاه تهران - تهران- ایران
matin.farhoumandi@ut.ac.ir

چکیده: حفظ امنیت سیستم‌های زیرساختی مانند شبکه‌های برق در برابر وقوع حوادث عادی که با اثر کم و البته احتمال زیاد رخ می‌دهند، از دیرباز مدنظر طراحان و بهره‌برداران این سیستم‌ها بوده است. اما، عملکرد این سیستم‌ها همچنان با وقوع اغتشاشات شدید به شدت مختل می‌گردد. بنابراین ضروری است که هم در مرحلهٔ طراحی و هم در مرحلهٔ بهره‌برداری از این سیستم‌ها، رفتار سیستم در شرایط وقوع حوادث شدید مطالعه شده و در صورت نیاز تمهیدات لازم جهت رفع کاستی‌ها اندیشیده شود. این رفتار به عنوان یک ویژگی جدید با نام تاب‌آوری یک سیستم زیرساختی شناخته می‌شود. تاب‌آوری به عملکرد زمانی یک سیستم شامل استقامت، آسیب‌پذیری و برگشت‌پذیری در شرایط وقوع یک اغتشاش شدید اشاره دارد. این مقاله مفاهیم و مبانی ارزیابی تاب‌آوری را تبیین نموده و تفاوت‌های اساسی آن را با مفاهیم شناخته‌شده‌تری مانند امنیت و قابلیت اطمینان تشریح می‌نماید. با توجه به افزایش نرخ وقوع حوادث طبیعی که از نوع حوادث با اثر زیاد و احتمال کم قلمداد می‌شوند و اثرات فاجعه‌بار خاموشی‌های هرچند کوتاه مدت، مطالعات تاب‌آوری بایستی به عنوان یک ضرورت در برنامه‌های عملیاتی نهادهای مرتبط قرار گیرد.

کلمات کلیدی: تاب‌آوری، حوادث با اثر زیاد و احتمال کم، استقامت، برگشت‌پذیری

تاریخ ارسال مقاله: ۱۳۹۶/۰۴/۰۵
تاریخ پذیرش مشروط مقاله: ۱۳۹۶/۰۸/۲۱
تاریخ پذیرش مقاله: ۱۳۹۶/۰۹/۱۸
نام نویسنده‌ی مسئول: فرخ امینی‌فر
نشانی نویسنده‌ی مسئول: ایران – تهران –خیابان کارگر شمالی – پردیس دانشکده‌های فنی دانشگاه تهران – دانشکده‌ی مهندسی برق و کامپیوتر

[Downloaded from jiaeee.com on 2025-08-19]
[DOR: 20.1001.1.26765810.1397.15.3.8.0]
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.15- No.3-Fall 2018

۱- مقدمه

با توجه به نقش حیاتی سیستم‌های زیرساختی از جمله شبکه‌های برق، سیستم‌های مخابراتی، سامانه‌های حمل و نقل، شبکه‌های بانکی و تبادلات مالی و ... در زندگی بشر امروزی، افزونگی[۱] به عنوان یکی از مهمترین ملاحظات، از دیرباز در طراحی این سیستم‌ها مدنظر قرار گرفته است [۱]. هدف از افزونگی مقاوم[۲] نمودن یک سیستم در شرایط وقوع خرابی یک یا چند تجهیز است. برای مثال، فیدرهای توزیع برق فشار متوسط[۳] توسط دو ترانسفورماتور موازی تغذیه می‌شوند و ظرفیت این ترانسفورماتورها به نحوی انتخاب می‌گردد که هر یک از ترانسفورماتورها به تنهایی قادر به تأمین بار فیدرهای توزیع باشند تا در شرایط خرابی، تعمیر و یا تست ترانسفورماتور دیگر، مصرف‌کنندگان با خاموشی مواجه نگردند. در سیستم‌های بزرگ با تجهیزات فراوان، که در هر لحظه برخی از آنها ممکن است خارج از سرویس باشند و البته نقطهٔ کار سیستم نیز دائماً در حال تغییر است، مطالعات تحلیل پیشامد به صورت دوره‌ای انجام می‌پذیرد تا از حفظ امنیت[۴] سیستم در شرایط وقوع پیشامدهای خروج یگانه اطمینان حاصل گردد. به عبارت دیگر، حفظ امنیت یک سیستم زیرساختی و مقاوم ساختن عملکرد آن در برابر حوادث با اثر کم و احتمال زیاد[۵] به عنوان یک ضرورت بهره‌برداری[۶]، از گذشته متداول بوده است[۲].

در سال‌های اخیر، تغییرات آب و هوایی[۷] و گرم شدن کرهٔ زمین[۸] منجر به افزایش وقوع حوادث طبیعی شده است[۳]. تابستان‌های بسیار گرم و طولانی، زمستان‌های بسیار سرد همراه با یخبندان‌های شدید، سیلاب‌های ناگهانی و خسارت بار، طوفان‌های با سرعت بالا و مخرب، تندبادهای گسترده و فاجعه‌بار و ... همگی از رخدادهایی هستند که برای همگان آشنا بوده و در اقصی نقاط کرهٔ زمین مرتباً در حال وقوع می‌باشند. بسته به موقعیت جغرافیایی یک منطقه، وقوع برخی از این حوادث محتمل‌تر و برخی دیگر بعید است؛ اما، افزایش وقوع آنها بر اساس مستندات موجود، واقعیتی انکارناپذیر است [۴]. به عنوان مثال، در گذشته وقوع طوفان در شهر تهران بسیار به ندرت مشاهده می‌گردید؛ اما، امروزه وقوع این پدیده در شهر تهران دور از انتظار نبوده و حداقل چندین مورد اخیر در اذهان شهروندان تهرانی موجود است. حوادث طبیعی با توجه به گستردگی جغرافیایی خود تجهیزات فراوانی را به صورت همزمان تحت تأثیر قرار داده و می‌توانند با خروج همزمان چندین تجهیز، عملکرد سیستم را با اختلال جدی مواجه کرده و حتی منجر به فروپاشی[۹] کلی سیستم شوند. از سویی دیگر با تقویت زیرساخت‌های اطلاعاتی شبکه‌های برق جهت پایش، حفاظت و کنترل بهتر این سیستم‌ها و در یک کلام هوشمندتر کردن آنها، نقاط نفوذ اطلاعاتی به این سامانه‌ها بیشتر شده است. حملات[۱۰] و خرابکاری‌های[۱۱] فیزیکی و سایبری نیز از جملهٔ حوادث با اثر شدید و احتمال کم[۱۲] می‌باشند که در صورت وقوع می‌توانند خاموشی‌های گسترده‌ای را رقم بزنند [۵].

بدیهی است شبکه‌های برق از دیرباز در معرض حوادث طبیعی آسیب‌پذیر[۱۳] بوده‌اند؛ اما، هم نرخ وقوع حوادث طبیعی در گذشته کمتر بوده است و هم وابستگی زندگی بشر به پایایی خدمات برق‌رسانی، به اندازه شرایط کنونی نبوده است. امروزه زندگی شهری و حتی روستایی به نحوی به دسترسی به انرژی الکتریکی گره خورده است که وقوع خاموشی‌های گستردهٔ هرچند کوتاه‌مدت نیز عواقب سنگین اقتصادی و انسانی به‌همراه دارد. از سوی دیگر به دلیل وابستگی عملکرد صحیح سیستم‌های زیرساختی به یکدیگر، با وقوع یک خاموشی چندین ساعته در یک منطقه، عملکرد سایر سیستم‌های زیرساختی مانند شبکه‌های آب‌رسانی یا سیستم‌های مخابراتی نیز مختل شده و عواقب وقوع خاموشی برق، گسترده‌تر و شدیدتر می‌شود. بدیهی است در چنین شرایطی، حفظ امنیت بهره‌برداری یک سیستم قدرت در شرایط رخداد حوادث با اثر کم و احتمال زیاد دیگر کافی نبوده و باید یک ویژگی دیگر از این سیستم که رفتار آن به حوادث با اثر زیاد و احتمال کم را منعکس می‌نماید مدنظر قرار گیرد. این ویژگی که از آن با عنوان *تاب‌آوری*[۱۴] یاد می‌شود میزان استقامت[۱۵]، آسیب‌پذیری[۱۶] و برگشت‌پذیری[۱۷] یک سیستم زیرساختی را در برابر یک حادثه شدید نشان می‌دهد [۳].

این مقاله به تبیین مفاهیم و تشریح روش‌های ارزیابی تاب‌آوری سیستم‌های زیر ساختی می‌پردازد. ابتدا حوادث و اغتشاشاتی که امکان وقوع دارند شناسایی شده و با توجه به ویژگی‌های مختلف مورد طبقه‌بندی قرار می‌گیرند. تحلیل امنیت و ارزیابی قابلیت اطمینان به عنوان دو روش مطالعاتی سنتی برای بررسی رفتار یک سیستم در حوادث مختلف مرور می‌شوند و کاستی‌های این مطالعات مورد کنکاش قرار می‌گیرند. در ادامه، مفهوم تاب‌آوری تبیین شده و اجزای تاب‌آوری معرفی می‌گردد. همچنین ضمن تشریح تمایزات تاب‌آوری با مفاهیم شناخته شده‌تری مانند استقامت، امنیت و قابلیت اطمینان، روش ارزیابی تاب‌آوری و نیز بهره‌برداری تاب‌آور از یک سیستم زیرساختی معرفی می‌شود. اگر چه غالب مباحث مطرح شده در این مقاله مرتبط با سیستم‌های قدرت و شبکه‌های برق می‌باشند، تعمیم آنها برای دیگر سیستم‌های زیرساختی مهندسی به راحتی و با تغییرات اندکی ممکن خواهد بود.

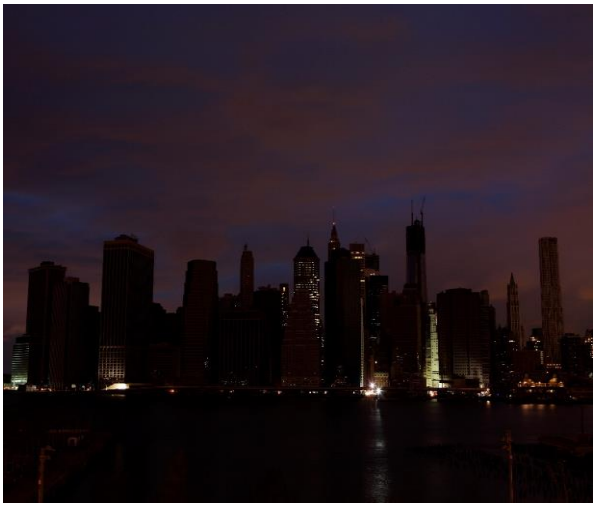
۲- طبقه‌بندی حوادث

تجهیزات مهندسی همواره در معرض خرابی و آسیب قرار دارند و انتظار عملکرد صددرصدی و بدون وقفه از یک تجهیز مهندسی واقع‌بینانه نیست. اما، به دلیل لحاظ نمودن افزونگی در طراحی سامانه‌های زیرساختی مهندسی، عموماً در دسترس نبودن برخی از تجهیزات برای عملکرد کلی سیستم مشکل جدی ایجاد نمی‌کند. در شبکه‌های برق، هر روزه تجهیزات متعددی از واحدهای تولید برق گرفته تا فیدرهای فشار ضعیف توزیع برق به دلایل گوناگونی از مدار خارج می‌شوند و پس از تعمیر مجدداً وارد مدار می‌گردند؛ در حالی که برق‌رسانی به مشترکین عموماً در این شرایط تحت تأثیر قرار نمی‌گیرد. هر از گاهی

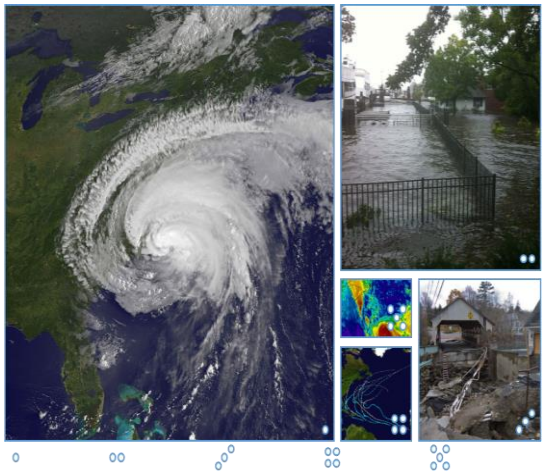
[Downloaded from jiaeee.com on 2025-08-19]
[DOR: 20.1001.1.26765810.1397.15.3.8.0]

هم حوادث طبیعی و یا انسانی شدیدی در نقطه‌ای از جهان گزارش می‌شوند که اثرات به مراتب شدیدتر و گسترده‌تری را بجا می‌گذارد و بخش اعظمی از ساکنین آن منطقه را با مشکل و خاموشی مواجه می‌سازد. ندرتاً هم حوادث تجربه نشده‌ای رخ می‌دهد که در سوابق گذشته آن منطقه هیچ رد پایی از آن موجود نمی‌باشد. در ادامه، مثال‌هایی از این حوادث ذکر می‌گردد.

تندباد سندی[۱۸] در سال ۲۰۱۲ میلادی در ایالات متحدهٔ امریکا بیش از ۷/۵ میلیون مشترک برق در ۱۵ ایالت و واشنگتن D.C. را با قطعی برق مواجه ساخت. نهادهای قانونی گزارش داده‌اند که بازیابی شبکهٔ برق و سیستم حمل و نقل شهر نیویورک پس از تندباد سندی، بزرگترین چالشی بوده است که این کلان شهر ایالات متحده تاکنون به خود دیده است. چندین روز پس از تندباد سندی، هنوز حدود ۳ میلیون مشترک در ایالت‌های نیویورک و نیوجرسی و حدود ۷۰۰ هزار مشترک در ۱۱ ایالت دیگر از ماساچوست تا ویرجینیا و میشیگان بدون برق بودند. به دلیل قطعی گستردهٔ برق در منطقهٔ منهتن شهر نیویورک، مردم برای شارژ گوشی‌های تلفن همراه خود به کافی شاپ‌ها و رستوران‌ها هجوم می‌بردند. قطعی برق در نیوجرسی ایستگاه‌های پمپ بنزین را از کار انداخته بود و علیرغم فراوانی سوخت، مردم ساعت‌های طولانی در صف می‌ایستادند تا سوخت مورد نیاز برای ژنراتورهای اضطراری خود را تهیه نمایند [۶]. شکل ۱ یک منطقه در شهر نیویورک را پس از تندباد سندی نمایش می دهد. در شرایطی مشابه در سال ۲۰۱۱، ساکنین ایالت کنتیکت در اثر طوفان استوایی آرین[۱۹] و در پی آن وقوع کولاک برف[۲۰]، با خاموشی گسترده و طولانی مواجه شدند (شکل ۲). در این وقایع، هزاران درخت شکسته و با آسیب به شبکه‌های برق، برخی از شهرها را برای بیش از دو هفته بی‌برق کردند و میلیون‌ها دلار خسارت به بار آوردند [۷]. از سال ۲۰۰۳ تا سال ۲۰۱۲ میلادی، ۶۷۹ حادثهٔ خاموشی با منشاء عوامل طبیعی که بیش از ۵۰ هزار مشترک را تحت تأثیر قرار داده است در ایالات متحده رخ داده است که توزیع زمانی آنها نیز حاکی از سیر صعودی این رخدادها در طول سالیان اخیر است [۸].



شکل (۱): شهر نیویورک؛ ۱۳ اکتبر سال ۲۰۱۲ میلادی



شکل (۲): طوفان آرین؛ ۹ ژوئن سال ۲۰۱۱ میلادی

حملهٔ سایبری سال ۲۰۱۵ به شبکه برق کشور اوکراین که در خلال مداخلهٔ نظامی روسیه در اوکراین پس از انقلاب مردم اوکراین در سال ۲۰۱۴ صورت پذیرفت نمونهٔ دیگری از این حوادث با اثر زیاد و احتمال کم است که البته این بار نه با یک منشاء طبیعی بلکه با یک منشاء انسانی شکل گرفت. در این حمله، هکرها با ایجاد اختلال در ۳۱ پست برق منجر به خاموشی بیش از ۲۲۵ هزار مشترک شدند [۹]. در کشور خودمان نیز قطعی برق ۱۱ شهر استان خوزستان در بهمن ماه سال ۱۳۹۵ و به دنبال آن از کارافتادن شبکه‌های آب رسانی شهری و اختلال در سامانه‌های مخابراتی مثال گویایی از اثرات حوادث طبیعی بر سیستم‌های زیرساختی است. در این حادثه، آلودگی[۲۱] سطح مقره‌ها (که به دلیل محدودیت منابع مالی به موقع شستشو نشده بودند) با رطوبت ۹۷ درصدی هوا ترکیب شده و موجب کاهش استقامت عایقی و وقوع اتصال کوتاه و خروج تجهیزات از مدار گردید. از نمونه‌های داخلی با منشاء انسانی نیز می‌توان به حملهٔ سایبری بدافزار[۲۲] مخرب استاکس‌نت[۲۳] به تأسیسات نیروگاه بوشهر و سایر تأسیسات مرتبط در تیر ماه سال ۱۳۸۹ اشاره کرد که با آلوده نمودن تجهیزات یارانه‌ای، علاوه بر افشای برخی از اطلاعات محرمانه، خسارات فیزیکی سنگینی نیز به بار آورد.

بدیهی است برای تبیین و ارزیابی تاب‌آوری یک سیستم زیرساختی، ابتدا باید خطرات و تهدیدهای مرتبط شناسایی شوند. در این راستا، حوادث ممکن را می‌توان بر حسب شدت اثرگذاری و احتمال (یا امکان) وقوع به سه دستهٔ زیر طبقه‌بندی نمود:

- **دستهٔ اول** حوادثی هستند که احتمال وقوع مشخص دارند و اثرات آنها نیز محدود بوده و به راحتی قابل برآورد است. این حوادث به دلیل کثرت وقوع دارای پایگاه دادهٔ غنی می‌باشند و با بکارگیری قانون اعداد بزرگ[۲۴] و فرض برقراری قضیهٔ حد مرکزی[۲۵]، احتمال وقوع آنها با استخراج توابع توزیع احتمال[۲۶] از روی پایگاه دادهٔ غنی قابل محاسبه می باشد. برای مثال در یک شبکهٔ برق، نرخ خروج اضطراری

[Downloaded from jiaeee.com on 2025-08-19]
[DOR: 20.1001.1.26765810.1397.15.3.8.0]
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.15- No.3-Fall 2018

یک واحد تولید مشخص یا واحد طول یک تیپ معین از خطوط انتقال معلوم بوده و مقادیر آنها به صورت سالیانه بروزرسانی می‌شود [۱۰]. این دسته از حوادث را حوادث شناخته شده[۲۷] می‌نامند.

- **دستهٔ دوم** حوادثی را شامل می‌شوند که به ندرت رخ می‌دهند و به همین دلیل پایگاه دادهٔ غنی از این حوادث موجود نمی‌باشد که بتوان مقادیری برای تابع توزیع احتمال وقوع آنها استخراج نمود. اما، عواقب وقوع این حوادث حدوداً قابل برآورد می‌باشد. برای نمونه می‌توان وقوع یک طوفان با سرعتی معین در شهر تهران را مثال زد. اگرچه احتمال وقوع چنین طوفانی برای ما نامعلوم است؛ اما در صوت وقوع، می‌توان اثرات و عواقب آن را بر روی سیستم‌های زیرساختی تخمین زد چراکه موارد مشابهی در گذشته تجربه شده است. این دسته از حوادث را با نام‌های حوادث شناخته نشده[۲۸] یا قوی خاکستری[۲۹] یاد می‌کنند. بدیهی است استفاده از نظریهٔ احتمال[۳۰] برای تحلیل حوادث این دسته عملی نمی‌باشد؛ اما، نظریهٔ امکان[۳۱] که می‌تواند مبتنی بر قضاوت‌های مهندسی و نظری کارشناسان نیز باشد به خوبی قابل پیاده‌سازی و بهره‌برداری است [۱۱].
- **دستهٔ سوم** حوادث تجربه نشده‌ای می‌باشند که طبیعتاً عواقب رخداد آنها نامشخص است. با توجه به اینکه در این موارد حتی یک نمونهٔ مشابه در گذشته وجود نداشته است، صحبت از احتمال وقوع این حوادث عملاً بی‌معنی است؛ هرچند که می‌توان در مورد امکان وقوع آنها بحث نمود. برای مثال، زلزله در شهر تهران حادثه‌ای است که وقوع آن از نظر علمی کاملاً ممکن است ولی نمی‌توان احتمالی برای این رخداد تعیین نمود و عواقب چنین فاجعه‌ای نیز غیرقابل تصور است. در مقابل، وقوع سونامی در شهر تهران اساساً از نظر فیزیکی غیرممکن است و لذا هرگز نباید مورد بحث قرار گیرد. شایان ذکر است که پس از وقوع حادثه‌ای از این دسته، این حادثه از آن پس به دستهٔ دوم منتقل می‌گردد؛ چراکه یک بار تجربه شده است و عواقب رخداد آن تا حدودی قابل تصور است. به این دسته از رخدادها، حوادث غیرقابل شناسایی[۳۲] یا قوی سیاه[۳۳] اطلاق می‌شود.

۳- تحلیل امنیت و قابلیت اطمینان

اگرچه از نظر تعاریف کلاسیک، امنیت زیر مجموعهٔ تعریف جامع قابلیت اطمینان است، ولی عملاً تحلیل امنیت در حوزه بهره‌برداری و راهبری سیستم‌های قدرت و مطالعات قابلیت اطمینان در حوزه مطالعات و برنامه‌ریزی این سیستم‌ها به انجام می رسد و لذا می‌توان این دو تعریف را تفکیک نمود. تحلیل امنیت در شبکه‌های قدرت معمولاً شامل مطالعات پیشامد خروج یگانه[۳۴] می‌باشد. ویژگی امنیت عموماً با عنوان معیار N-۱ در بهره‌برداری سیستم‌های قدرت شناخته می‌شود که در آن N تعداد تجهیزات سیستم است؛ به این معنی که اگر معیار N-۱ در یک سیستم قدرت رعایت گردد، این سیستم می‌تواند در شرایط پیشامد خروج یگانهٔ هر یک از تجهیزات، با N-۱ تجهیز باقیمانده بدون هرگونه اختلالی به عملکرد خود ادامه دهد. یا اگر بهره‌برداری یک سیستم با رعایت معیار N-۲ انجام گیرد، پیشامد خروج همزمان دو تجهیز[۳۵] در عملکرد صحیح این سیستم نقصی ایجاد نمی‌کند. در صورتی که در یک شرایط بهره‌برداری با ساختار متناظر با آن لحظه برخی از قیود بهره‌برداری یا الزامات تأمین بار شبکه نقض گردد، بهره‌بردار شبکه برحسب ریسک‌پذیری، ظرفیت موجود سیستم و قابلیت پذیرش افزایش هزینهٔ بهره‌برداری، دو رویکرد متفاوت پیشِ رو دارد. رویکرد اول که پیشگیرانه[۳۶] می‌باشد شامل جابجایی نقطه کار فعلی شبکه به نقطه‌ای است که در آن معیار N-۱ ارضا گردد، تا در صورت وقوع یک پیشامد، شرایط پس از حادثه همچنان از نظر قیود بهره‌برداری یا الزامات تأمین بار مجاز باشد. با فرض وجود ظرفیت کافی در سیستم، انتخاب این رویکرد به معنای پذیرش افزایش هزینهٔ بهره‌برداری به صورت دائمی و البته کاهش ریسک خاموشی در شرایط وقوع پیشامدها است. رویکرد دوم، اصلاحی[۳۷] است که در آن بهره‌بردار شبکه آمادگی دارد با بکارگیری ابزارهای مناسب اقدامات ضروری جهت برطرف نمودن نقض قیود پس از رخداد یک حادثه را پیاده نماید. بازتوزیع[۳۸] توان بین واحدهای در مدار پس از پیشامد خروج یک واحد تولید از جملهٔ این اقدامات است. همچنین، برخی از اقدامات اصلاحی ممکن است پس از تشخیص وقوع حادثه به صورت خودکار اجرا شوند. برای مثال حذف بخشی از بار شبکه توسط رله‌های حذف بار فرکانسی[۳۹] مثال دیگری برای رویکرد اصلاحی جهت ارضای قیود بهره‌برداری فرکانس شبکه است. در این رویکرد، افزایش دایمی هزینهٔ بهره‌بردای مطرح نبوده، ولی در مقابل، ریسک نقض قیود شبکه و امکان خاموشی بار بالاتر است [۲].

دیدگاه فوق جهت ارزیابی و تضمین امنیت سیستم‌های زیرساختی کاملاً بر یک تحلیل قطعی[۴۰] مبتنی است و هیچ حساسیتی به احتمال وقوع حوادث ندارد و عملاً با حوادث با احتمال کم و یا زیاد به صورت مشابه برخورد می‌کند. در حالی که طراحی و برنامه‌ریزی[۴۱] توسعهٔ این سیستم‌ها معمولاً توسط روش‌های مبتنی بر تحلیل‌های احتمالاتی[۴۲] انجام می‌شوند. در مطالعات مبتنی بر روش‌های احتمالاتی، که از آنها با عنوان ارزیابی قابلیت اطمینان[۴۳] نیز یاد می‌شود، احتمال خروج تجهیزات نیز در محاسبات وارد شده و میزان مقاوم ساختن یک سیستم در مقابل یک حادثهٔ با احتمال زیاد، بیشتر از میزان مقاوم ساختن سیستم در برابر یک حادثهٔ با احتمال کم است [۱۲]. روش‌های احتمالاتی با پذیرش بار محاسباتی سنگین‌تر و البته نیازمندی اطلاعاتی بیشتر، نتایجی نزدیک‌تر به مشاهدات دنیای واقعی دارند. در حقیقت این روش‌ها امکان تخمین دقیق هزینه و سود[۴۴] طرح‌های

[Downloaded from jiaeee.com on 2025-08-19]
[DOR: 20.1001.1.26765810.1397.15.3.8.0]

توسعه و همچنین قابلیت مدل‌سازی عدم قطعیت‌های مختلف را فراهم می‌کنند [۱۰]. در سال‌های اخیر با گسترش منابع تجدیدپذیر انرژی که با عدم قطعیت‌های ذاتی همراه هستند، بکارگیری انواع این روش‌ها در مطالعات سیستم‌های قدرت بیش از پیش رونق یافته است.

پر واضح است که تحلیل امنیت شبکه، تنها پیشامدهای یگانه (و شایدً برخی از پیشامدهای دوگانهٔ محتمل یا خطرساز) را در نظر می‌گیرد. همچنین، ارزیابی قابلیت اطمینان نیز تنها پیشامدهایی را منظور می‌کند که مرتبهٔ پایینی[۴۵] داشته و احتمال وقوع آنها معین و البته زیاد است. بنابراین می‌توان نتیجه گرفت که حوادثی که در تحلیل امنیت و ارزیابی قابلیت اطمینان مطالعه می‌شوند، به دسته اول حوادث طبقه‌بندی شده در بخش قبل محدود می‌شوند. در این دسته از حوادث، هم احتمال وقوع و هم عواقب رخداد آنها از اهمیت برخوردار است. نکتهٔ مهم دیگر آن است که در مطالعات امنیت و ارزیابی قابلیت اطمینان، معمولاً رفتار استاتیکی شبکه مد نظر قرار می‌گیرد و از رفتار دینامیکی آن در حین حادثه و پس آن صرف نظر می‌شود. به عبارت دیگر، نقطهٔ کار جدید سیستم پس از رخداد، مبنای ارزیابی عملکرد آن قرار می‌گیرد.

۴- تاب‌آوری

۴-۱- تعریف

تاب‌آوری مفهومی است که پیش از مطرح شدن در حوزه‌های مهندسی، در زمینه‌های اجتماعی، اقتصادی و مدیریتی مورد کنکاش قرار گرفته است. در سیستم‌های اجتماعی، تاب‌آوری به توانایی یک جامعه برای ایستادگی در برابر فشارها و حوادث ناشی از تغییرات سیاسی، اجتماعی و اقتصادی در آن جامعه اطلاق می‌گردد [۱۳]. در یک سیستم اقتصادی منظور از تاب‌آوری عبارت است از: پاسخ به خطرات مختلف به گونه‌ای که افراد و گروه‌های مختلف بتوانند خود را از برخی تلفات اقتصادی در بازار حفظ کنند [۱۴]. در زمینه‌های مدیریتی و سیستم‌های سازمانی، توانایی یک سازمان در شناسایی ریسک‌های مختلف و مدیریت حوادث را تاب‌آوری می‌نامند [۱۵]. آنچه که در این تعاریف کاملاً پررنگ می‌باشد، وجود تعابیری مانند ایستادگی در برابر حوادث، محفوظ ماندن از تلفات و مدیریت حوادث است. به عبارت دیگر تأکید اصلی این تعاریف بر عدم آسیب‌پذیری در برابر حوادث است و اشاره‌ای هرچند ضمنی به وجه بازیابی پس از آسیب نشده است. دلیل این امر لختی بسیار زیاد سیستم‌های اجتماعی، اقتصادی و مدیریتی و کندی فرآیندهای تغییرات مثبت در آنهاست. به این معنی که متخصصان این سیستم‌ها به درستی، رویکرد پیشگیرانه را مدنظر خود قرار می‌دهند و فرآیند درمان پس از وقوع یک آسیب جدی را نوشدارویی پس از مرگ سهراب دانسته و چندان اثرگذار نمی‌دانند. به عنوان مثال، اگر جامعه‌ای مراقبت فرهنگی لازم را ننماید و فرهنگ در آن جامعه آسیب ببیند، دیگر بازیابی فرهنگی و برگشت به دوره شکوفایی فرهنگی در آن جامعه به راحتی و به سرعت ممکن نخواهد بود. یا اگر فساد در یک ساختار اقتصادی ریشه بدواند، دیگر اصلاح آن ساختار اقتصادی در کوتاه مدت دور از انتظار است. اما، در سیستم‌های مهندسی و بخصوص سیستم‌های زیرساختی، مسئله متفاوت است.

در یک سیستم مهندسی که تجهیزات آن در معرض خرابی است و عوامل مختلف ذاتی، طبیعی و انسانی دائما سلامت تجهزات را تهدید می‌نمایند، نمی‌توان تنها با تمهیدات پیشگیرانه به عملکرد صحیح سیستم امیدوار بود. در این سیستم‌ها، نگهداری و تعمیرات تجهیزات جزء جداناپذیری از فرآیند بهره‌برداری می‌باشد. همچنین، پس از وقوع یک حادثه و افت عملکرد سیستم، بازیابی سرویس و ترمیم ساختار شبکه ضرورتی گریزناپذیر و البته از نظر عملی امکان‌پذیر است. بنابراین، تعریف تاب‌آوری در سیستم‌های زیرساختی بایستی هر دو وجه استقامت در برابر حادثه و بازیابی سریع پس از حادثه را در کانون توجه خود قرار دهد. توانایی سیستم برای کاهش مدت و شدت اغتشاشات؛ یا به عبارت دیگر، توانایی سیستم در پیش‌بینی، تحمل و تطبیق با اغتشاشات مختلف و بازیابی سریع *تاب‌آوری* نامیده می‌شود [۱۶]-[۱۹].

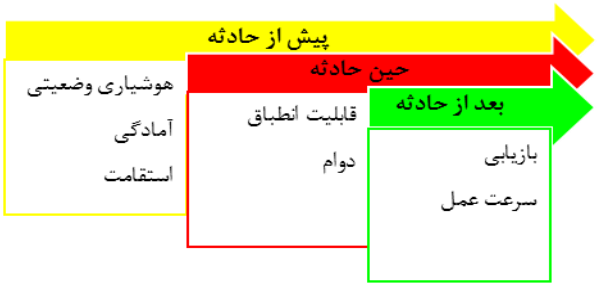
در مورد سیستم‌های قدرت، اگرچه تعریف فوق برای تاب‌آوری صحیح و قابل استفاده است، باید تأکید گردد که منظور از اغتشاش، حوادث با اثر زیاد و احتمال کم (دستهٔ دوم و سوم در طبقه بندی بخش ۲) می‌باشد. این حوادث که می‌توانند منشاء طبیعی یا انسانی داشته باشند، یا به ندرت اتفاق می‌افتند و یا هرگز تجربه نشده‌اند. رخداد اینگونه از اغتشاشات محدودهٔ جغرافیایی وسیعی را دربر گرفته و تجهیزات متعددی را به صورت همزمان از مدار خارج می‌سازند و فرآیند بازیابی را پیچیده و البته طولانی می‌نمایند. به عبارت دیگر این اغتشاشات آثار همبستهٔ مکانی زمانی[۴۶] برجای می‌گذارند. ویژگی منحصر به فرد دیگر این اغتشاشات این است که اگر منشاء طبیعی داشته باشند، چندین سیستم زیرساختی مانند شبکهٔ برق، سیستم مخابراتی، زیرساخت تأمین و توزیع گاز، شبکهٔ آب‌رسانی و ... را به صورت همزمان تحت تأثیر قرار می‌دهند. این شرایط بحرانی از طرفی عمق فاجعه رخ داده را بیشتر می‌کند و از سوی دیگر فرآیند بازیابی را دشوارتر می‌سازد.

برخلاف مطالعات قابلیت اطمینان که مجموعه‌ای از حوادث را به صورت یکجا مد نظر قرار داده و رفتار سیستم را توسط شاخص‌هایی کلی ارائه می‌دهد، مطالعهٔ تاب‌آوری به صورت اختصاصی برای یک حادثه انجام می‌گیرد. ممکن است طراحی سیستم به گونه‌ای باشد که تاب‌آوری سیستم در برابر یک حادثه بیشتر شود ولی همزمان تاب‌آوری آن در برابر یک حادثه دیگر کاهش یابد. برای مثال اگر طراح شبکه برای تاب‌آور ساختن آن در برابر طوفان و تندباد تصمیم بگیرد فیدرهای توزیع برق را توسط کابل‌های زیرزمینی اجرا نماید، تاب‌آوری سیستم در مقابل سیل و آب‌گرفتگی (نسبت به حالتی که از فیدرهای هوایی استفاده شود) کمتر می‌شود.

[Downloaded from jiaeee.com on 2025-08-19]
[DOR: 20.1001.1.26765810.1397.15.3.8.0]
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.15- No.3-Fall 2018

۴-۲- اجزای تاب‌آوری

شکل ۳ اجزای تشکیل دهندهٔ تاب‌آوری یک سیستم را در شرایط وقوع یک اغتشاش شدید نمایش می‌دهد. در ادامه، به تشریح این اجزاء می‌پردازیم.



شکل (۳): اجزای تشکیل دهنده تاب‌آوری

۴-۲-۱- هوشیاری وضعیتی[۴۷] و آمادگی

با بهره‌مندی از ابزارهای پایش گسترده و تقریباً بلادرنگ[۴۸] که هم داده‌داده‌های مربوط به سیستم مورد نظر و هم داده‌های محیطی را جمع‌آوری و به مرکز کنترل ارسال می‌نمایند، بهره‌برداران از شرایط واقعی سیستم و تهدیدات بالقوه آن آگاه می‌شوند. امروزه در سیستم‌های قدرت و در سطح تولید و انتقال، هوشیاری وضعیتی توسط طراحی و پیاده‌سازی سامانهٔ اندازه‌گیری گسترده[۴۹] بهبود چشمگیری یافته است که این مهم با توسعه و نصب واحدهای اندازه‌گیری فازوری[۵۰] و لینک‌های مخابراتی فیبر نوری محقق شده است. واحدهای اندازه‌گیری فازوری، مجهز به آنتن GPS هستند و با داشتن مرجع زمانی یکسان (با دقت بهتر از یک میکروثانیه) امکان اندازه‌گیری زاویهٔ فاز کمیت‌های فازوری را نیز دارند. علاوه بر آن در سامانهٔ اندازه‌گیری گسترده کلیهٔ داده‌ها دارای برچسب زمانی‌اند؛ بنابراین بدون توجه به تأخیر انتقال داده، می‌تواند تصویری کاملاً همگام[۵۱] و همگن[۵۲] از سیستم را ایجاد نماید [۲۰]. از سوی دیگر، به دلیل بهره‌مندی این سامانه از ارتباطات فیبر نوری با پهنای باند بسیار وسیع، نرخ گزارش‌دهی[۵۳] این سامانه‌ها از مرتبهٔ چند ده پکت داده در ثانیه می‌باشد که به هیچ عنوان با نرخ یک پکت در چند ثانیه سامانه‌های پایش قدیمی قابل قیاس نیست. این ویژگی برتری مهم دیگری است که امکان پایش پدیده‌های دینامیکی را فراهم نموده و بهره‌برداران را به صورت واقعی از آنچه در سیستم در حال وقوع است آگاه می‌نماید [۲۱]. بنابراین بهره‌بردار قادر خواهد بود که بجای وضعیت غیرفعال[۵۴] و واکنشی[۵۵] کنونی، به صورت فعال[۵۶] و حتی پیشگامانه[۵۷] به مدیریت سیستم پیش از، در حین و پس از رخداد اغتشاش بپردازد و از این طریق تاب‌آوری شبکه تحت بهره‌برداری خود را ارتقاء بخشد.

۴-۲-۲- استقامت

این جزء، مربوط به پیش از وقوع حادثه می‌باشد. تمامی ابزارها و تمهیدات زیرساختی باید قبل از وقوع حادثه اندیشیده شوند تا عواقب رخداد احتمالی محدود شود. زیرساخت تجهیزاتی شبکه باید تقویت شود تا از ایستادگی مناسبی در مقابل اغتشاشات شدید برخوردار باشد و به این ترتیب سیستم نیز استقامت بیشتری در برابر این اغتشاشات از خود نشان خواهد داد. برای نمونه اگر هدف، ارتقای تاب‌آوری یک سیستم در برابر طوفان و تندباد است، برج‌های انتقال و تیرهای توزیع برق باید از نظر استحکام مکانیکی قوی‌تر باشند و یا اینکه از شبکهٔ زیرزمینی برای انتقال و توزیع انرژی الکتریکی بهره برد. استقامت به طراحی و برنامه‌ریزی یک سیستم مربوط می‌شود و روشی غیرفعال و سخت‌افزاری جهت ارتقای تاب‌آوری محسوب می‌گردد. غالباً اینگونه تصور می‌شود که استقامت و تاب‌آوری مفاهیمی مترادف هستند که برداشت صحیحی نمی‌باشد. اگرچه استقامت را باید جزئی از تاب‌آوری دانست؛ ولی تاب‌آوری مفهومی جامع‌تر است که علاوه بر استقامت، آسیب‌پذیری و بازیابی را نیز دربر دارد. استقامت مفهومی است که در یک لحظه از زمان قابل تعریف است؛ به این معنی که اگر درختی با وزش یک طوفان نشکند، در برابر آن استقامت دارد. در مقابل، تاب‌آوری مفهومی است که در بستر زمان تعریف شده و شامل استقامت و طول مدت آن، میزان و نحوهٔ آسیب‌پذیری و همچنین سرعت و روند بازیابی است. برای روشن‌تر شدن موضوع می‌توان رفتار یک درخت بلوط و یک درخت نی را در برابر طوفان مثال زد. درخت بلوط درختی بسیار تنومند و محکم است که در برابر طوفان‌های معمولی مستحکم بوده و به عبارتی استقامت دارد. ولی اگر طوفان شدیدتری بوزد، درخت بلوط به دلیل ساختار شکننده‌ای که دارد شکسته و از بین می‌رود. در مقابل، درخت نی از استقامت کمی برخوردار است و حتی در برابر وزش بادهای عادی نیز مقداری تکان می‌خورد؛ ولی درخت نی به دلیل ساختار انعطاف‌پذیری که دارد در برابر شدیدترین طوفان‌ها نیز خم شده و پس از سپری شدن طوفان به حالت اولیهٔ خود باز می‌گردد. رفتار درخت نی در حوزهٔ زمان با مفهوم تاب‌آوری توصیف می‌گردد.

۴-۲-۳- قابلیت انطباق[۵۸] و دوام[۵۹]

با وقوع یک اغتشاش شدید، ابتدا سیستم به دلیل تمهیداتی که در مرحلهٔ طراحی اندیشیده شده است مقداری استقامت از خود نشان می‌دهد. در ادامه با طولانی شدن یا تشدید اغتشاش، برخی از اجزای سیستم صدمه دیده و از مدار خارج می‌شوند و به این ترتیب سطح عملکرد سیستم کاهش می‌یابد. در این مرحله اگر سیستم نتواند خود را با حادثه تطبیق دهد، عملکرد کلی آن مختل شده و حتی بسیاری از تجهیزاتی که آسیب ندیده‌اند هم از مدار خارج شده و بلااستفاده می‌مانند. خاموشی سراسری شبکهٔ برق مثال مناسبی برای این شرایط است که در آن اگرچه غالب تجهیزات سالم‌اند، ولی به دلیل نبود قابلیت انطباق در سیستم و البته عملکرد نادرست برخی از رله‌های

[Downloaded from jiaeee.com on 2025-08-19]
[DOR: 20.1001.1.26765810.1397.15.3.8.0]

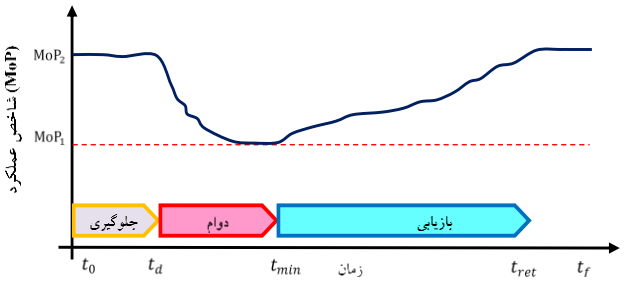
حفاظتی، سیستم کاملاً دچار فروپاشی می‌شود. در حالی که اگر سیستم قابلیت انطباق با اغتشاش و یا به اصطلاح دوام داشته باشد، سیستم‌های حفاظتی و طرح‌های دفاعی[۶۰] فقط تجهیزات و بخش‌های آسیب دیده را از مدار خارج می‌کنند و از گسترش اغتشاش در شبکه جلوگیری می‌نمایند [۲۲]. بنابراین، سایر بخش‌های سالم در مدار باقی مانده و حداقل بخشی از بار سیستم را تأمین می‌نمایند. در این شرایط، منطقی است تغذیه بارهای مهم و حیاتی سیستم در اولویت قرار گیرند. قابلیت انطباق یک سیستم در برابر حوادث شدید نیازمند آن است که بخش‌های باقی مانده در سیستم در صورتی که از بدنهٔ اصلی سیستم جدا شده باشند، بتوانند به کار خود ادامه دهند. به عبارت دیگر، یک سیستم تاب‌آور باید از مجموعه‌ای از زیرسیستم‌های کوچک‌تر تشکیل شده باشد که در حالت عادی به صورت یکپارچه و در حالت اضطراری به صورت جداگانه قابل بهره‌برداری باشند. این فلسفهٔ طراحی را در مهندسی نوین، ایجاد *سیستمی از سیستم‌ها*[۶۱] یا *شبکه‌ای از شبکه‌ها*[۶۲] می‌نامند [۲۳]. در این راستا، امروزه در اقصی نقاط جهان تلاش می‌شود تا شبکه‌های برق مراکز بیمارستانی، امنیتی، نظامی، مسکونی، اداری و صنعتی به صورت ریزشبکه‌هایی[۶۳] که قابلیت کار جدا از شبکهٔ سراسری را دارند طراحی و پیاده‌سازی شوند [۳]. شایان ذکر است که قابلیت انطباق علاوه بر الزامات طراحی و تعبیهٔ ابزارهای مورد نیاز در ساختار سیستم، دارای وجه بهره‌برداری پررنگی نیز می‌باشد. به این معنی که تجربهٔ بهره‌برداران و رویه‌های تدوین شده برای آنها نقش مهمی در این امر دارند. در این راستا، ابزارهای تحلیلی و نرم‌افزارهایی که مراکز کنترل هوشمند[۶۴] در اختیار بهره‌برداران قرار می‌دهند می‌توانند بسیار موثر باشند [۲۴]. برای روشن‌تر شدن موضوع به مثالی از سیستم‌های قدرت اشاره می‌شود. فرض نمایید بخشی از تولید توان یک سیستم قدرت توسط واحدهای بادی صورت گیرد و اغتشاش مورد بررسی، وزش یک طوفان باشد. واحدهای بادی تنها در بازهٔ مشخصی از سرعت باد قابل بهره‌برداری هستند و در صورت وزش باد شدید، توربین آنها برای ممانعت از آسیب فیزیکی به پره‌ها قفل شده و توان تولیدی آنها صفر می‌شود. در چنین شرایطی به دلیل حذف مقدار قابل توجهی از تولید سیستم، ممکن است فروپاشی فرکانسی رخ دهد و یا سهم عمده‌ای از بار شبکه از دست برود. حال آنکه بهره‌بردار شبکه می‌تواند با توجه به الگوهای هواشناسی و هوشیاری وضعیتی که از شبکه در اختیار دارد، به صورت پیشگیرانه عمل نماید و تولید واحدهای بادی را قبل از رسیدن طوفان به مزرعهٔ بادی، کاهش داده و سهم آنها را به واحدهای دیگر منتقل کند. با این اقدام، دیگر قفل شدن توربین واحدهای بادی به عنوان تهدید فرکانسی برای شبکه قلمداد نخواهد شد. بدیهی است این مثال از انطباق‌پذیری یک سیستم در برابر یک اغتشاش، هم جنبهٔ سخت‌افزاری طراحی را شامل می‌شود و هم نیازمند اقدامات نرم افزاری بهره‌برداران می‌باشد.

۴-۲-۴- بازیابی[۶۵] و سرعت عمل[۶۶]

پس از رخداد یک اغتشاش و آسیب دیدن تعدادی از تجهیزات، سیستم بر حسب قابلیت انطباقی که دارد خود را به نحو مناسبی با شرایط پس از حادثه تطبیق می‌دهد تا میزان خاموشی و وقفه در خدمت‌رسانی حداقل گردد. در چنین شرایطی، بهره‌بردار سیستم بایستی ابزار کافی در اختیار داشته باشد که از وسعت و شدت آسیب وارد شده، تجهیزات سالم، منابع تولید موجود و بارهای دچار خاموشی و وقفه آگاه شود. سپس، بهره‌بردار برحسب منابعی که در اختیار دارد و نیز شناخت و تجربهٔ خود شروع به بازیابی بارهای خاموش شده می‌نماید. البته ممکن است به دلیل محدویت منابع، بخشی از بارهای شبکه قابل بازیابی نباشند و برگشت خدمات به آنها تا تعمیر و اصلاح بخش‌های آسیب دیده به تعویق افتد. شایان ذکر است مشابه ویژگی انطباق‌پذیری، بازیابی و سرعت عمل نیز هم به ابزارها و تمهیدات سخت‌افزاری و هم به اقدامات بهره‌برداری نیاز دارد.

۴-۳- ارزیابی تاب‌آوری

جهت ارزیابی یک ویژگی مانند تاب‌آوری از یک سیستم مهندسی، ابتدا باید شاخص‌های کمی برای توصیف میزان آن ویژگی و اجزای آن تعریف و محاسبه شود. شکل ۴ به صورت نوعی شاخص عملکرد یک سیستم را نسبت به زمان و در شرایط وقوع یک اغتشاش شدید نمایش می‌دهد. شاخص عملکرد می‌تواند بار تأمین شدهٔ یک سیستم به عنوان هدف غایی آن باشد. یا بر حسب نیاز ممکن است ارزش بارهای باقیمانده در شبکه، تعداد تجهیزات سالم و برقدار سیستم و ... به عنوان شاخص عملکرد سیستم انتخاب شوند [۲۵].



شکل (۴): شاخص عملکرد بر حسب زمان

همانطور که در شکل ۴ مشاهده می‌شود، عملکرد سیستم 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 سیستم افت نماید. این مرحله از رفتار سیستم را می‌توان مرحلهٔ جلوگیری[۶۷] نامید که به میزان هوشیاری وضعیتی بهره‌بردار و نیز استحکام شبکه بستگی دارد. هرچه بهره‌بردار شبکه نسبت به خطری که سیستم 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 سیستم هم از استقامت بیشتری برخوردار باشد، زمان بیشتری طول خواهد کشید تا افت

[Downloaded from jiaeee.com on 2025-08-19]
[DOR: 20.1001.1.26765810.1397.15.3.8.0]
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.15- No.3-Fall 2018

عملکرد سیستم رخ دهد. بنابراین، مدت زمان t_0-t_d را می‌توان یک شاخصی کمی جهت توصیف کیفیت مرحلهٔ جلوگیری دانست.

با افت عملکرد سیستم 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 سیستم در برابر اغتشاش بستگی دارد. با افزایش انطباق‌پذیری سیستم، روند افت عملکرد کندتر شده و میزان آسیب‌پذیری نیز کاهش می‌یابد. مقدار $\frac{MoP_2 - MoP_1}{MoP_2}$ به عنوان یک شاخص کمی نرمال شده جهت توصیف میزان آسیب‌پذیری سیستم در برابر یک اغتشاش بکار 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 بکارگیری 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 زیرسیستم جدا شده از شبکه و بازیابی کلی مربوط به تشکیل سیستم 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 نرمال شدهٔ 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.

۵- نتیجه‌گیری

یک سیستم مهندسی معمولاً بگونه‌ای 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 سیستم 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 سیستم‌های زیرساختی مانند شبکه‌های برق، تاب-آوری نامیده می شود. در این مقاله، مفاهیم مرتبط با تاب‌آوری در برابر اغتشاشات شدید تبیین گردید. با ارائهٔ مثال‌هایی ساده ولی واقعی در حوزهٔ سیستم‌های قدرت، تفاوت‌های تاب‌آوری با مفاهیم شناخته شده-تری مانند امنیت و قابلیت اطمینان تشریح شد. همچنین، اجزای تشکیل دهندهٔ تاب‌آوری و البته شیوهٔ ارزیابی آنها معرفی شد. به نظر می‌رسد که با توجه به افزایش وابستگی زندگی بشر به پایایی سیستم-های زیرساختی و نیز روند صعودی وقوع اغتشاشات طبیعی ناشی از تغییرات آب و هوایی، 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.

مراجع

[1] Billinton, R., & Allan, R. N., Reliability evaluation of engineering systems, pp. 155-173, New York: Plenum press, 1992.

[2] Shahidehpour, M., Tinney, F., & Fu, Y., Impact of security on power systems operation. Proceedings of the IEEE, Vol. 93, No. 11, pp. 2013-2025, 2005.

[3] Gholami, A., Aminifar, F., & Shahidehpour, M., 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.

[4] Wang, Y., Chen, C., Wang, J., & Baldick, R, Research on resilience of power systems under natural disasters—A review. IEEE Transactions on Power Systems, Vol. 31, No. 2, pp. 1604-1613, 2016.

[5] Madani, V., Das, R., Aminifar, F., McDonald, J., Venkata, S. S., Novosel, D., ... & Shahidehpour, M., Distribution automation strategies challenges and opportunities in a changing landscape. IEEE Transactions on Smart Grid, Vol. 6, No. 4, pp. 2157-2165, 2015.

[6] National Hurricane Center. Hurricane Sandy, [Online], 2012. Available: http://www.nhc.noaa.gov/

[7] Hurricane Adrian, [Online], 2011. Available: https://en.wikipedia.org/wiki/Hurricane_Adrian_(2011)

[8] Severe Impact Resilience Task Force, Severe impact resilience: Considerations and recommendations, [Online], 2012. Available: http://www.nerc.com/comm/OC/Pages/SIRTF/Severe-Impact-Resilience-Task-Force.aspx

[9] Analysis of the Cyber Attack on the Ukrainian Power Grid, [online]. Available: http://www.nerc.com/pa/CI/ESISAC/Docum ents /E-ISAC_SANS_Ukraine_DUC_18Mar2016 .p d f, 2016.

[10] Billinton, R., Power system reliability evaluation. Taylor & Francis, 1970.

[11] Zadeh, L. A., Fuzzy sets as a basis for a theory of possibility. Fuzzy sets and systems, Vol. 1, No. 1, pp. 3-28, 1978.

[۱۲] صالحی دوبخشری احمد، فتوحی فیروزآباد محمود. برنامه ریزی توسعه واحد های تولیدی در حضور نیروگاه های بادی از نقطه نظر قابلیت اطمینان. مجله مهندسی برق و الکترونیک ایران. ۱۳۸۷; ۵

[13] Adger, W. N., Social and ecological resilience: are they related?. Progress in human geography, Vol. 24, No. 3, pp. 347-364, 2000.

[14] Perrings, C., Resilience and sustainable development. Environment and Development Economics, Vol. 11, No. 4, pp. 417-427, 2006.

[15] Hollnagel, E., Woods, D. D., & Leveson, N., Resilience engineering: Concepts and precepts. Ashgate Publishing, Ltd, 2007.

[16] Brown, G., Carlyle, M., Salmerón, J., & Wood, K., Defending critical infrastructure. Interfaces, Vol. 36, No. 6, pp. 530-544, 2006.

[17] Panteli, M. & Mancarella, P., 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.

[Downloaded from jiaeee.com on 2025-08-19]

[DOR: 20.1001.1.26765810.1397.15.3.8.0]

[18] Mensah, A. F. & Dueñas-Osorio, L., Efficient Resilience Assessment Framework for Electric Power Systems Affected by Hurricane Events. Journal of Structural Engineering, Vol. 142, No. 8, 2016.
[19] Arghandeh, R., Meier, A. V., Mehrmaneshb, L., & Mili, L., On the Definition of Cyber-physical Resilience in Power Systems. Renewable and Sustainable Energy Reviews, Vol. 58, pp. 1060-1069, 2016.
[20] Torkashvand, A., Ghasemi, H., & Aminifar, F., Parameters Estimation of Classical Model of Generator Using PMU Data. Journal of Iranian Association of Electrical and Electronics Engineers, Vol. 14, No. 1, pp. 73-82, 2017.
[21] Khazaei, M. H. & Haghjoo, F., A Comprehensive PMU-Based Fault Location Algorithm for Double Circuit and Multi-Terminal Transmission Lines. Journal of Iranian Association of Electrical and Electronics Engineers, Vol. 14, No. 1, pp. 1-10, 2017.
[22] Begovic, M. et al., Defense plan against extreme contingencies. CIGRE TF–Summary for Electra. C, 2, pp. 02-24, 2007.
[23] Zhu, J., & Mostafavi, A., Performance Assessment in Complex Engineering Projects Using a System-of-Systems Framework. IEEE Systems Journal, 2017.
[24] Vaahedi, E., Practical power system operation. John Wiley & Sons, 2014.
[25] Madni, A. M., & Jackson, S., Towards a conceptual framework for resilience engineering. IEEE Systems Journal, Vol. 3, No. 2, pp. 181-191, 2009.

زیرنویس‌ها

[1] Redundancy
[2] Robust
[3] Medium-Voltage Distribution Feeders
[4] Security
[5] Low-Impact High-Probability (LIHP) Events
[6] Operation
[7] Climate Changes
[8] Global Warming
[9] Collapse
[10] Attacks
[11] Vandalisms
[12] High-Impact Low-Probability (HILP) Events
[13] Vulnerable
[14] Resilience
[15] Robustness
[16] Vulnerability
[17] Recoverability
[18] Sandy
[19] Tropical Storm Irene
[20] Snowstorm
[21] Contamination
[22] Virus or Malware
[23] Stuxnet
[24] Law of Large Numbers
[25] Central Limit Theorem
[26] Probability Distribution Function (PDF)
[27] Known Events
[28] Unknown Events
[29] Gray Swan
[30] Probability Theory
[31] Possibility Theory
[32] Unknowable Events
[33] Black Swan
[34] Single-Outage Contingency
[35] Concurrent Double-Outage Contingency
[36] Preventive
[37] Corrective
[38] Redispatch
[39] Under-Frequency Load Shedding (UFLS)
[40] Deterministic
[41] Design and Planning
[42] Probabilistic
[43] Reliability Assessment
[44] Cost and Benefit
[45] Uncertainty
[46] Correlated Spatiotemporal Effects
[47] Situational Awareness
[48] Near Real-Time
[49] Wide-Area Measurement System (WAMS)
[50] Phasor Measurement Units (PMUs)
[51] Synchronized
[52] Homogenous
[53] Reporting Rate
[54] Passive
[55] Reactive
[56] Active
[57] Proactive
[58] Adaptability
[59] Survivability
[60] Defense Plans
[61] System of the Systems
[62] Grid of the Grids
[63] Microgrids
[64] Smart Control Center
[65] Recoverability
[66] Rapidity
[67] Avoidance

[Downloaded from jiaeee.com on 2025-08-19]
[DOR: 20.1001.1.26765810.1397.15.3.8.0]