مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال ششم، شماره ۴، زمستان ۱۳۹۴؛ ص ۲۹۷- ۲۸۹

ارائه شاخصی برای ارزیابی آسیب‌پذیری سامانه قدرت در برابر تهدیدات تروریستی

محمدحسین رنجبر[۱]، ابوالفضل پیرایش[۲*]

۱- دانشجوی دکتری، ۲- استادیار، دانشگاه شهید بهشتی

(دریافت: ۹۴/۰۳/۲۵، پذیرش: ۹۴/۰۷/۰۸)

چکیده

در سال‌های اخیر گروه‌های تروریستی خطر بزرگی برای کشورهای جهان محسوب می‌شوند. این گروه‌ها با حمله به زیرساخت‌های اساسی خسارات فراوانی ایجاد می‌کنند. یکی از زیرساخت‌های اساسی هر کشور سامانه قدرت آن است که برای گروه‌های تروریستی هدفی جذاب محسوب می‌شود. تجربه حملات تروریستی نشان می‌دهد که حمله به زیرساخت سامانه قدرت می‌تواند سبب قطع بار گسترده و همچنین اختلال در سایر زیرساخت‌ها شود. ارزیابی آسیب‌پذیری و تعیین نقاط ضعف سامانه قدرت در برابر این تهدیدات جهت اتخاذ تصمیمات صحیح برای مقابله با آن ضروری است. هدف این مقاله بررسی روش‌های موجود ارزیابی آسیب‌پذیری و ارائه شاخصی جدید برای ارزیابی آسیب‌پذیری سامانه قدرت بر اساس ترکیب شاخص انرژی تأمین نشده با شاخص‌های دیگر است. نتایج شبیه‌سازی نشان می‌دهد استفاده از شاخص جدید برای تعیین آسیب‌پذیری سامانه به جواب‌های مطلوب منجر می‌شود.

کلید واژه‌ها: آسیب‌پذیری، زیرساخت اساسی، شاخص آسیب‌پذیری ، رتبه‌بندی حوادث، انرژی تأمین نشده.

A New Vulnerability Evaluation Index for Power System due to Terrorist Threats

M. H. Ranjbar, A. Pirayesh[*]
Shahid Beheshti University

(Received: 15/06/2015; Accepted: 30/09/2015)

Abstract

In recent years, terrorist groups have become a major Threats for the world. These terrorist groups attack critical infrastructures and cause substantial damages. One of the most critical infrastructures is power system which is an attractive target to terrorists. The experience of terrorist attacks shows the crippling effects of such attacks which could lead to public discontent. Vulnerability evaluation and identification the weak points of power system due to such threats are necessary in order to make appropriate decisions to defend against them. The aim of this article is to review common methods of vulnerability evaluation and present a new index for vulnerability evaluation of power system based on combination of expected energy not supplied index and other indices. The simulation results show using the new index leads to favorable outputs for determining the vulnerability of power system.

Keywords: Vulnerability, Critical Infrastructure, Vulneraility Index, Contingency Ranking, Energy Not supplied.

[*]Corresponding Author E-mail: A_pirayesh@sbu.ac.ir

۱. مقدمه

زندگی در جوامع مدرن و توسعه‌یافته امروزی متأثر از زیربناهای اساسی آن جوامع است به‌نحوی‌که کارکرد پیوسته و بدون اختلال این زیربناها بر کیفیت زندگی انسان‌ها، رفاه عمومی و ثروت عمومی اثر بسیار زیادی می‌گذارد. در صورت عدم وجود و یا اختلال در زیربناهای اساسی نظیر شبکه برق، گاز، آب، فاضلاب، مخابرات، حمل و نقل، بانک و ... در یک کشور و یا کارکرد نامطمئن آن‌ها، آن جامعه به‌سوی توسعه و پیشرفت حرکت نمی‌کند و با خسارات فراوان مواجه می‌شود.

مسئله امنیت و قابلیت اطمینان زیربناهای اساسی در برابر حوادث طبیعی و غیر طبیعی و همچنین مسئله بهبود و توسعه زیرساخت‌های اساسی موجود توجهات زیادی را در طول سال‌های اخیر به خود جذب کرده است [۶-۱]. زیرساخت شبکه برق (سامانه قدرت) یکی از مهم‌ترین و شاید اساسی‌ترین زیرساخت‌های هر کشور است [۷]. می‌دانید سامانه قدرت در برابر تهدیدات طبیعی و غیر طبیعی آسیب‌پذیر است که باید حفاظت شود. تهدیدات طبیعی به حوادث درون شبکه‌ای نظیر خطا و خرابی تجهیزات و برون شبکه‌ای مانند برخورد صاعقه، طوفان، اشتباه عوامل انسانی و ... اطلاق می‌شود. در سالیان متمادی مسئله امنیت و قابلیت اطمینان سامانه قدرت در برابر تهدیدات طبیعی در نظر گرفته شده و راهکارهای مقابله با آن شناخته شده است.

تهدیدات غیر طبیعی به اقداماتی اطلاق می‌شود که عامدانه و از روی عناد برای ایجاد اختلال در زیرساخت سامانه قدرت انجام می‌شود. عملیات تروریستی، خرابکارانه، نظامی و اخیراً حملات سایبری از نمونه‌های حوادث غیر طبیعی هستند. خسارات و اختلالات چنین تهدیداتی می‌تواند بسیار زیاد و تأثیرگذار باشد. نمونه‌هایی از حملات به سامانه‌های قدرت در جنگ‌های اخیر اهمیت موضوع را نشان می‌دهد. همچنین در سال‌های اخیر گروه‌های تروریستی خطر بزرگی برای کشورهای جهان محسوب می‌شوند و خسارات فراوانی را بر ملت‌ها تحمیل نموده‌اند. نگرانی از وجود چنین گروه‌هایی و خطرات بالقوه آن‌ها بر سامانه قدرت در سالیان اخیر افزایش یافته است [۱۰-۸]. به ویژه در منطقه خاورمیانه که کشور ما در آن قرار دارد این خطر و نیاز مقابله با آن بیشتر احساس می‌شود.

در کشورهای مختلف برنامه‌هایی برای دفاع از سامانه قدرت در برابر تهدیدات نظامی و تروریستی وجود دارد. هدف از برنامه‌های دفاع از سامانه قدرت در برابر تهدیدات نظامی و تروریستی، مقابله با اقدامات عامدانه‌ای است که توسط دشمنان و بدخواهان یک کشور بر علیه سامانه قدرت و شبکه برق‌رسانی آن انجام می‌پذیرد. این اقدامات به صورت حمله مستقیم به تأسیسات الکتریکی و نابود کردن آن‌ها انجام می‌پذیرد. در مورد حملات سایبری این اقدامات با ایجاد اختلال در عملکرد صحیح و پیوسته اجزای سامانه انجام می‌پذیرد. انواع حملات هوایی، موشکی، بمب‌های گرافیتی، بمب‌گذاری و ... از جمله تهدیدات امنیتی سامانه قدرت می‌باشند. در این حملات به تأسیساتی نظیر نیروگاه، پست‌های الکتریکی و خطوط انتقال آسیب رسانده می‌شود.

برای مقابله با حملات مستقیم به سامانه قدرت جدای از اقدامات نظامی و اطلاعاتی که مسئولیت آن با نیروهای نظامی حافظ امنیت کشور است، راهکارهایی توسط بهره‌بردار سامانه قدرت انجام می‌پذیرد تا اثرات و عواقب ناشی از حملات را کاهش دهد و یا حتی به صفر رساند. 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 به صورت مستحکم‌سازی، افزونگی[1]، پاسخ هم‌زمان به اقدام خرابکارانه و بازیابی سریع‌تر سامانه باشد [۱۱].

فیروزی [۱۲] محورهای راهبردی مدیریت پایایی شبکه از دیدگاه مدیریت بحران ناشی از جنگ را معرفی کرده است. در آن مقاله با ذکر جنگ‌های اخیر و حملات به سامانه قدرت، آثار چنین حوادثی و لزوم دفاع از سامانه قدرت نشان داده شده است و نمونه‌ای از برنامه دفاع از سامانه قدرت و مدیریت بحران سامانه قدرت در برابر حملات نظامی در دو محور ارائه شده است.

در تمامی برنامه‌های مدیریت بحران سامانه قدرت در برابر تهدیدات غیر طبیعی، اولین گام شناسایی نقاط گلوگاهی یا ارزیابی آسیب‌پذیری سامانه قدرت است [۱۳]. محور اول برنامه مقاله ذکر شده نیز شناسایی نقاط گلوگاهی در جهت مستحکم‌سازی سامانه و تحمل ضربه اول ناشی از حمله یا حملات دشمن است [۱۲].

در این تحقیق آسیب‌پذیری سامانه قدرت در برابر تهدیدات نظامی و تروریستی بررسی شده است. در فصل دوم مفهوم آسیب‌پذیری و نمونه‌هایی از روش‌های ارزیابی آسیب‌پذیری سامانه قدرت بیان شده است. در فصل سوم روشی محاسباتی برای ارزیابی آسیب‌پذیری سامانه قدرت و تعیین نقاط گلوگاهی آن ارائه شده است. در فصل چهارم اعمال شبیه‌سازی و نتایج ارائه شده است و در فصل آخر نیز نتیجه‌گیری بیان شده است.

۲. مفهوم آسیب‌پذیری

در یک مقایسه درباره مفهوم آسیب‌پذیری در مقالات دیده می‌شود که مراجعی آسیب‌پذیری را "استعداد، آمادگی و قابلیت" زیان دیدن و متضرر شدن از حادثه که همان احتمال وقوع اتفاق نامطلوب (حادثه) است، معنا کرده‌اند. دسته‌ای دیگر آن را "شدت نتایج و عواقب حاصل از حادثه" تعریف کرده‌اند. در غالب مقالات تعریف دوم برای آسیب‌پذیری در نظر گرفته شده است [۱۴].

در اینجا مشاهده می‌شود که برای یک حادثه نامطلوب دو مفهوم وجود دارد. یکی احتمال وقوع حادثه و دیگری عواقب و نتایج آن است. در حقیقت آسیب‌پذیری پاسخ سامانه به حادثه و مقابله سامانه

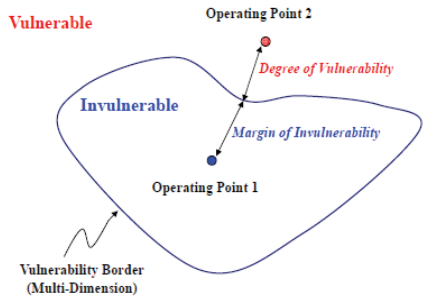
[1] Redundancy

با آن سناریوی مشخص است و به زبان ساده نتایج و عواقب حاصل از حادثه می‌باشد. در این تحقیق تعریف دوم برای آسیب‌پذیری پذیرفته شده است. در این صورت تنها عواقب ناشی از وقوع حادثه بررسی می‌شود و فرض می‌شود که یک حادثه اتفاق افتاده است و حال نتایج و عواقب ناشی از آن بررسی می‌شود. به‌طور مثال برای یک سامانه قدرت با فرض وقوع حمله به اجزائی از سامانه و نابودی و از دست رفتن آن جزء، میزان عواقب و خسارت ناشی از آن بررسی شود. این اجزاء می‌توانند خطوط انتقال، مولد، ترانسفورماتور و ... باشند. بر این اساس می‌توان اجزاء و تأسیسات سامانه قدرت را برحسب اهمیت اولویت‌بندی کرد و اجزاء گلوگاهی شبکه را مشخص کرد. اجزاء گلوگاهی به اجزائی گفته می‌شود که در صورت از دست رفتن آن‌ها خسارت بیشتری حاصل می‌شود. در برخی از مراجع شاخص‌هایی برای ارزیابی و اندازه‌گیری آسیب‌پذیری به نام شاخص‌های آسیب‌پذیری ارائه شده است. این شاخص‌ها بر اساس عواقب و نتایج اتفاقات و حوادث مثلاً میزان بار تأمین نشده، میزان هزینه از دست رفته و یا میزان اختلال و انحراف در عملکرد سامانه تعیین می‌شوند [۱۵ و ۱۶].

در ادامه چند نمونه از این شاخص‌ها در زمینه ارزیابی آسیب‌پذیری بیان می‌شود. ارزیابی آسیب‌پذیری به معنی دریافت درک مفهومی و دانش به صورت کمی یا کیفی از آسیب‌پذیری یک سامانه است. ارزیابی آسیب‌پذیری یکی از گام‌های برنامه دفاع از زیرساخت سامانه قدرت و در واقع اولین گام برنامه است. به این علت که اجزاء گلوگاهی سامانه را مشخص می‌کند و به بهره‌بردار این دید را می‌دهد که در صورت وقوع حمله موفقیت‌آمیز و نابودی هر کدام از اجزاء سامانه، خسارت و عواقب حاصله چه میزان است.

۲-۱. شاخص فاصله از مرز آسیب‌پذیری

کیم و همکاران [۱۷] آسیب‌پذیری را اینگونه تعریف کرده‌اند که اگر سامانه قدرتی بعد از وقوع حوادث مشخص همچنان بتواند به صورت پیوسته و بدون نقض قیود، توان را تأمین کند، غیر آسیب‌پذیر و در صورت وقوع حوادثی یا یک حادثه، قیود آن نقض شود، سامانه آسیب‌پذیر است. میزان و درجه آسیب‌پذیری سامانه توسط شاخص‌هایی تعریف می‌شود که به آن‌ها شاخص‌های امنیت یا شاخص‌های آسیب‌پذیری می‌گویند. در شکل (۱) شاخص فاصله تا مرز آسیب‌پذیری نشان داده شده است.



شکل ۱. شاخص فاصله تا مرز آسیب‌پذیری [۱۷]

شاخص‌های امنیت رفع خطای بحرانی (CCT[1]) و حاشیه انرژی (EM[2]) مرسوم‌ترین شاخص‌های امنیت هستند. شاخص CCT زمان سپری شده از شروع خطا تا جدا کردن خطا برای پایدار ماندن سامانه است [۱۸]. این روش بسیار محاسباتی است و برای تعداد بسیار حالات سامانه و سناریوهای حوادث مختلف مناسب نیست. شاخص EM یک روش مستقیم است که پایداری سامانه را از طریق تابع انرژی سامانه و مقایسه آن با یک انرژی از پیش تعیین شده، تشخیص می‌دهد. این روش محدودیت‌های ذاتی دارد که کاربرد آن را برای سامانه‌های بسیار بزرگ محدود می‌سازد [۱۷].

کاساباالیدیس و همکاران [۱۹] روشی برای تعیین فاصله از مرز آسیب‌پذیری معرفی کرده‌اند. روش کار به این صورت است که در ابتدا وضعیت امنیت سامانه با توپولوژی مشخص و بازه زمانی مشخص توسط شبکه عصبی پیش‌بینی می‌شود. این وضعیت امنیت می‌تواند به صورت هر شاخص دلخواهی مانند CCT یا EM باشد. سپس توسط بهینه‌سازی دسته ذرات (PSO[3]) نزدیک‌ترین مرز با کمینه‌سازی از نقطه وضعیت امنیت، به‌دست می‌آید.

از روشی مشابه و البته با تقریب در شرکت‌های برق شمال آمریکا استفاده می‌شود [۲۰]. مزیت این روش آن است که یک درک شهودی به اپراتور سامانه می‌دهد و وضعیت پارامترهای سامانه قدرت مانند ولتاژ توان عبوری و ... را نسبت به مرز آسیب‌پذیری درک می‌کند و اقدامات لازم را انجام می‌دهد. در شاخص‌های CCT و EM پارامترهای زمان و انرژی اینچنین درک شهودی را نمی‌دهد.

۲-۲. رتبه‌بندی حوادث

یکی از مفاهیم مطرح در زمینه بهره‌برداری و امنیت سامانه قدرت، بحث تحلیل حوادث است. تحلیل حوادث به بررسی وضعیت سامانه قدرت بعد از وقوع حوادث می‌پردازد و به بهره‌بردار سامانه دانش کافی در خصوص وضعیت سامانه بعد از وقوع حوادث مشخص را می‌دهد [۲۳-۲۱]. تحلیل حوادث به سه بخش تعریف حوادث، رتبه‌بندی حوادث[4] و ارزیابی حوادث تقسیم می‌شود [۲۲]. رتبه‌بندی حوادث روشی است که با استفاده از شاخص‌های کارایی[5] مشخص، تأثیر حوادث بر کل سامانه را توصیف می‌کند و حوادث را به ترتیب فاجعه‌بار بودن اولویت‌بندی می‌کند. در گام بعد بهره‌بردار با توجه به این اولویت‌بندی و با استفاده از تمهیداتی، حتی‌الامکان از وقوع حوادث فاجعه‌بار جلوگیری می‌کند. روش استاندارد مطالعه حوادث، استفاده از مسئله پخش بار بعد از وقوع حادثه و بررسی نقض قیود سامانه است.

یکی از این شاخص‌های کارایی، شاخص کارایی شارش توان حقیقی است. یک سامانه قدرت را در نظر بگیرید که به صورت پایدار

[1] Critical Clear Time
[2] Energy Margin
[3] Particle Swarm Optimization
[4] Contingency Ranking
[5] Performance Index

کار می‌کند. در صورتی که یک یا چند خط انتقال آن بر اثر سوانح طبیعی و یا غیر طبیعی قطع شده و از مدار خارج شوند، ممکن است برخی از دیگر خطوط دچار اضافه‌بار شوند. این اضافه‌بار می‌تواند حاشیه پایداری را به مخاطره بیندازد و یا سامانه را به حالت ناپایدار ببرد. همچنین این اضافه‌بار موجب خسارت فیزیکی به خطوط انتقال می‌شود. این شاخص به صورت زیر تعریف شده است [۲۱]:

$$PIw_i = \sum_{j=all\ other\ branches} \left(\frac{P_{flow\ j}}{P_j^{\max}} \right)^{2n} \quad (۱)$$

که در آن، PIw_i شاخص کارایی شارش توان حقیقی سامانه در صورت خروج خط انتقال i است. $P_{flow\ j}$ شارش توان در خط انتقال j بعد از خروج خط انتقال i می‌باشد. P_j^{max} بیشینه توان قابل‌انتقال خط انتقال j است. n هر عدد طبیعی دلخواه می‌تواند باشد (۱، ۲، ۳ و...).

شاخص دیگر که در مطالعات حوادث مورد استفاده قرار می‌گیرد، شاخص کارایی ولتاژ است. بعد از وقوع حادثه ولتاژ نقاط مختلف سامانه تغییر می‌کند و ممکن است در برخی از نقاط ولتاژ از محدوده مجاز خارج شود. این امر سبب اختلال در عملکرد سامانه می‌شود. میزان انحراف ولتاژ از محدوده مجاز توسط شاخص کارایی ولتاژ به صورت زیر مشخص می‌شود [۲۱]. این شاخص اختلاف ولتاژ شینه‌ها قبل از وقوع حادثه و بعد از وقوع آن را نسبت بیشینه انحراف ولتاژ مجاز مدنظر قرار می‌دهد.

$$PIv_i = \sum_{k \in \alpha} \left(\frac{\left(V_k^{pre} - V_k^{post}\right)}{\max volt\ drop} \right)^{2n} \quad (۲)$$

که در آن، PIv_i شاخص کارایی شارش ولتاژ سامانه در صورت خروج خط انتقال i است. α مجموعه باس‌هایی که ولتاژ آن‌ها بعد از خطا خارج از محدوده مجاز می‌رود. V_k^{pre} ولتاژ باس k قبل از خروج خط انتقال i و V_k^{post} ولتاژ باس k بعد از خروج خط انتقال i است. n هر عدد طبیعی دلخواه می تواند باشد.

۲-۳. شاخص انرژی مورد انتظار تأمین نشده[1]

از آنجایی‌که برای حفظ پایداری سامانه و برای پاسخ هم‌زمان به حمله تروریستی به سامانه قدرت، یکی از مؤثرترین و مهم‌ترین راهکارها قطع بار است و همچنین هدف حملات نظامی و تروریستی نیز قطع هر چه بیشتر بار ست، شاخصی که میزان بار تأمین نشده را در صورت حمله به سامانه قدرت به عنوان شاخص آسیب‌پذیری بیان کند می‌تواند بسیار مفید باشد و مورداستفاده مستقیم بهره‌بردار قرار گیرد. در صورت وقوع یک حمله، اگر بهره‌بردار میزانی مشخص از بار را قطع کند می‌تواند تعادل تولید و مصرف را حفظ سازد و سامانه را از حوادث پی‌درپی و بعدی و فروپاشی نجات دهد. اگر میزان باری که بهره‌بردار مجبور به قطع آن است، بیشتر باشد سامانه در برابر آن حادثه مشخص آسیب‌پذیرتر است و خسارت بیشتری متحمل می‌شود. در اینجا خسارت و عواقب ناشی از حمله برابر با میزان بار قطع شده است. این شاخص در برخی از مراجع استفاده شده است و بسیار کارآمد می‌باشد [۱۷ و ۲۴].

۳. روش تحقیق

همان‌طور که در فصل قبل بیان شد، شاخص میزان بار تأمین نشده شاخصی بسیار مناسب و ملموس برای ارزیابی آسیب‌پذیری و تعیین اجزاء گلوگاهی شبکه است. اما این شاخص به تنهایی نمی‌تواند بیانگر میزان خسارت وارده بر سامانه قدرت در صورت وقوع حمله باشد. به طور مثال یک سامانه فرضی دارای دو عنصر "الف"و "ب" است که حمله به عنصر "الف" منجر به قطعی بار بیشتری می‌شود. در این صورت و با استفاده از شاخص میزان بار تأمین نشده سامانه در صورت حمله به عنصر اول تا حمله به عنصر دوم آسیب‌پذیرتر است. حال فرض کنید که قیمت و ارزش عنصر "ب"چندین برابر ارزش عنصر "الف" است. در این صورت نمی‌توان خسارت ناشی از حمله را تنها بار تأمین نشده ببینید، زیرا ممکن است ارزش دارایی از دست رفته به علاوه ارزش بار تأمین نشده در صورت حمله به عنصر "ب" بسیار بیشتر از عنصر "الف" شود.

بنابراین شاخص آسیب‌پذیری باید به صورت ترکیبی از شاخص‌ها که بیانگر دقیق میزان خسارات باشد، تعیین شود. فیروزی [۱۲] عنوان کرده است که بر اساس مطالعات انجام شده شاخص‌های زیر به منظور شناسایی گلوگاه‌های سامانه استفاده می‌شود:

۱- تأثیر خروج جزء بر مشخصه کفایت سامانه (P_{loss}): میزان انحراف مصرف و تولید و در واقع میزان بار تأمین نشده را بیان می‌کند.

۲- تأثیر خروج جزء بر امنیت سامانه ($P_{security}$): تأثیر خروج جزء بر فروپاشی مناطق و شبکه را نشان می‌دهد. این شاخص نشان می‌دهد که در صورت خروج جزء آیا منطقه‌ای دچار فروپاشی می‌شود و اگر می‌شود چه تعداد از مناطق تحت تأثیر قرار می‌گیرند.

۳- کمیت و کیفیت بار تأمین نشده ($POP_{affected}$) و ($Area_{affected}$): تعداد جمعیت تحت تأثیر از قطعی بار و همچنین نوع منطقه‌ای که دچار قطعی می‌شود را بیان می‌کند. این مناطق می‌تواند شهری، روستایی، سیاسی، صنعتی، نظامی و ... باشد.

۴- مدت زمان بازیابی شبکه ($T_{recovery}$): مدت زمان قطعی را بیان می‌کند.

۵- ارزش دارایی از دست رفته (F_{loss}): ارزش دلاری (ریالی) خسارت وارد شده در هنگام حمله را نشان می‌دهد.

۶- تأثیر بی‌برقی بر سایر زیرساخت‌ها (I): تأثیر قطعی بر سایر زیرساخت‌ها را نشان می‌دهد.

۷- تأثیر بر محیط‌زیست (E): تأثیر زیست‌محیطی وقوع حمله و خرابی را نشان می‌دهد. این مورد می‌تواند بیانگر میزان آلودگی محیط‌زیست در صورت نشت روغن و یا موارد مشابه محاسبه شود.

[1] Expected Energy Not Supplied

می‌توان با استفاده از شاخص میزان بار تأمین نشده و ترکیب آن با شاخص‌های بالا به شاخصی برای تعیین آسیب‌پذیری سامانه دست یافت. در این تحقیق شاخص اولیه برای ارزیابی آسیب‌پذیری سامانه قدرت به صورت ترکیبی از کمیت و کیفیت بار قطع شده، مدت زمان بازیابی شبکه، تأثیر حمله بر مشخصه کفایت سامانه و ارزش دارایی‌های از دست رفته تعریف می‌شود. این شاخص بر حسب میزان خسارت وارده مالی (ریال) محاسبه می‌شود.

$$U = \left[P_{loss} \times VOLL \times T_{recovery} \right] + F_{loss} \quad \text{(Rial)} \qquad (۳)$$

که در آن، P_{loss} مشخصه تأثیر حمله بر مشخصه کفایت سامانه و در واقع میزان بار تأمین نشده بر حسب مگاوات است.

$Area_{affected}$ تأثیر حمله بر کیفیت بار تأمین نشده است. در واقع این شاخص بیان می‌کند که منطقه‌ای که دچار خاموشی یا قطعی می‌شود، شهری، روستایی و یا جدایی‌طلب است. این شاخص می‌تواند به این صورت در نظر گرفته شود که به هر یک از مناطق ارزش بار از دست رفته (VOLL[1]) جداگانه‌ای اختصاص یابد. VOLL (ارزش بار از دست رفته) بر حسب (Rial/MWh) است که برای هر منطقه میزان مشخصی دارد.

$$VOLL = \begin{cases} VOLL_1 & \text{Re}\,gion = Rural \\ VOLL_2 & \text{Re}\,gion = Urban \\ VOLL_3 & \text{Re}\,gion = Political \end{cases} \qquad (۴)$$

$T_{recovery}$ مدت زمان بازیابی شبکه بر حسب ساعت است. F_{loss} میزان دارایی از دست رفته بر حسب ریال است. این ارزش بیانگر ارزش سخت‌افزاری از دست رفته در اثر حمله است.

برای در نظر گرفتن کمیت بار تأمین نشده ($POP_{affected}$) باید جمعیتی که دچار قطعی می‌شوند را در نظر گرفت. برای این کار می‌توان از ضرایب وزنی استفاده کرد. بدین منظور متناسب با جمعیتی که تحت تأثیر قطعی بار قرار می‌گیرند، ضریب وزنی (w) در ارزش بار از دست رفته (VOLL) ضرب می‌شود. این ضرایب وزنی را می‌توان به صورت زیر در نظر گرفت:

$$w = \begin{cases} .9 & Population \le 50000 \\ 1 & 50000 \le Population \le 500000 \\ 1.1 & Population \ge 500000 \end{cases} \qquad (۵)$$

حال شاخص آسیب‌پذیری به صورت زیر کامل می‌شود:

$$U = \left[P_{loss} \times w \times VOLL \times T_{recovery} \right] + F_{loss} \quad \text{(Rial)} \qquad (۶)$$

در این تحقیق تأثیر قطعی بر سایر زیرساخت‌ها و تأثیر حمله بر محیط‌زیست در نظر گرفته نمی‌شود. در تحقیقات بعدی بر روی این موارد کار خواهد شد.

[1] Value of Lost Load

برای محاسبه این شاخص و تعیین دقیق میزان بار تأمین نشده بر مبنای تحلیل غیر خطی شبکه، از روش ارائه شده توسط رنجبر [۲۵] استفاده می‌شود. در آن پایان‌نامه بار تأمین نشده با استفاده از پخش بار بهینه و با نرم‌افزار matpower محاسبه شده است. نقطه قوت روش ارائه شده سرعت بالای محاسبات، امکان تغییر آسان در برنامه و توپولوژی سامانه، در نظر گرفتن دقیق توپولوژی شبکه همراه با تمام عناصر غیر خطی و جبران‌ساز و همچنین در نظر گرفتن تأثیر وجود توان ذخیره در سامانه قدرت بر بار تأمین نشده است.

متأسفانه در اکثر تحقیقات گذشته میزان بار تأمین نشده با استفاده از روش پخش بار DC (مدل ساده شده پخش بار) محاسبه شده است [۲۸-۲۶]. استفاده از تحلیل خطی برای محاسبه میزان بار تأمین نشده به خطا می‌انجامد که در فصل بعد نشان داده شده است. همچنین وجود توان ذخیره به عنوان بخشی از اقدام مدیریت بحران در پاسخ هم‌زمان به حمله در تعیین آسیب‌پذیری مؤثر است.

۴. نتایج و بحث

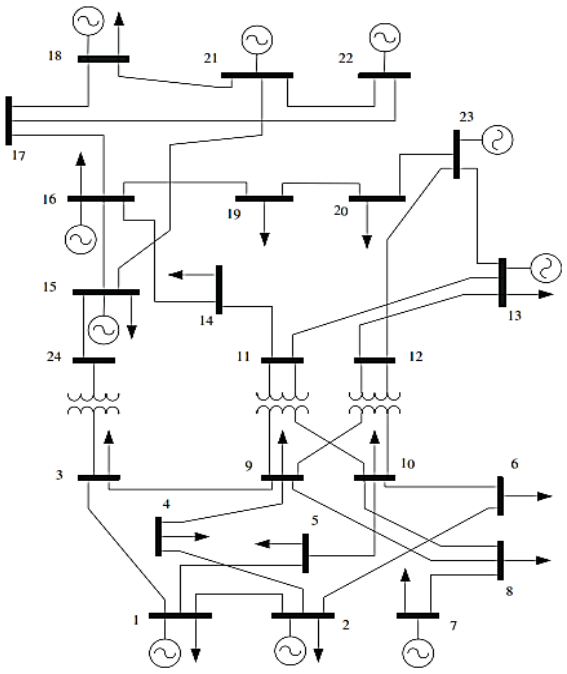
کاربرد روش ارائه شده بر روی شبکه آزمایش ۲۴ باسه IEEE انجام‌شده است [۲۹]. این شبکه در شکل (۲) نشان داده شده است. در اینجا آسیب پذیری خطوط انتقال مورد مطالعه قرار می‌گیرد و در واقع تأثیر حمله به خطوط انتقال و خسارت ناشی از آن بر سامانه قدرت بررسی می‌شود.

با استفاده از شاخص کارایی شارش توان حقیقی، تأثیر خروج خطوط انتقال شبکه محاسبه شده است. توسط پخش بار، میزان شارش توان در خطوط انتقال پس از وقوع حادثه محاسبه شده و با استفاده از رابطه (۱) شاخص کارایی (PI) به دست آمده است. در آن رابطه n=5 در نظر گرفته شده است. هشت خط انتقالی که خروج آن‌ها بیشترین اضافه‌بار را در سایر خطوط انتقال ایجاد می‌کند، به ترتیب مشخص شده و در جدول (۱) نشان داده شده است.

برای شاخص کارایی ولتاژ نیز همین روند با استفاده از رابطه (۲) و n=1 انجام شده و در جدول (۲) هشت خط انتقال پر اهمیت به‌دست آمده توسط این شاخص گزارش شده است. برای محاسبه هر دو شاخص از پخش بار AC استفاده شده است.

جدول ۱. هشت خط انتقال با بیشترین اهمیت به‌دست آمده از شاخص کارایی توان حقیقی

به باس	از باس	PI_w	شماره خط
۲۱	۱۵	۱۹/۳۲	۲۵
۱۷	۱۶	۱۷/۹۲	۲۷
۱۰	۶	۶/۴۹	۱۰
۲۳	۲۰	۱/۳۳	۳۳
۱۳	۱۱	۱/۱۴	۱۸
۲۴	۱۵	۰/۷۴	۲۶
۲۴	۳	۰/۷۴	۷
۱۲	۱۰	۰/۷۰	۱۷



شکل ۲. شبکه آزمایش ۲۴ باسه IEEE

جدول (۱) برای شاخص کارایی شارش توان حقیقی اینگونه تفسیر می‌شود که قطع خطوط انتقال ۲۵، ۲۷ و ۱۰ یک یا چند خط انتقال دیگر را دچار اضافه‌بار شدید می‌کند و ممکن است آن خط یا خطوط نیز از مدار خارج شوند. حمله به خط انتقال ۳۳ تنها یک خط انتقال دیگر را دچار اضافه‌بار آن هم تا نزدیکی مقدار بیشینه‌اش می‌کند و قطع تمامی خطوط انتقال به جز این ۴ خط انتقال باعث اضافه‌بار دیگر خطوط نمی‌شود. این نتیجه با توجه به ظرفیت نسبتاً زیاد خطوط انتقال و بار نسبتاً کم سامانه منطقی به نظر می‌رسد. بنابراین با این شاخص، خروج خطوط انتقال ۲۵، ۲۷ و ۱۰ در این شرایط از سامانه فاجعه‌بار تلقی می‌شود.

جدول ۲. هشت خط انتقال با بیشترین اهمیت به‌دست آمده از شاخص کارایی ولتاژ

به باس	از باس	PI_V	شماره خط
۱۰	۶	۸۴/۹۴	۱۰
۲۴	۱۵	۱۰/۲۱	۲۶
۸	۷	۶/۵۲	۱۱
۲۴	۳	۴/۲۷	۷
۴	۲	۱/۸۹	۴
۳	۱	۰/۲۷	۲
۱۶	۱۴	۰/۲۰	۲۳
۱۷	۱۶	۰/۰۶۵	۲۷

از سوی دیگر با استفاده از شاخص کارایی ولتاژ، حمله به خطوط ۱۰، ۲۶، ۱۱ و ۷ ولتاژ باس یا باس‌هایی از سامانه را از محدوده مجاز خارج می‌کند و سبب عمل کردن رله‌های حفاظتی ولتاژ می‌شود. با استفاده از این شاخص خروج خط این چهار خط انتقال فاجعه‌آمیز است. همچنین خروج خطوط انتقال ۴، ۲، ۲۳ و ۲۷ نیز سبب انحراف جزئی ولتاژ باس یا باس‌هایی از سامانه خارج از محدوده مجاز می‌شود. مشاهده می‌شود که نتیجه به‌دست آمده توسط دو شاخص با یکدیگر مشابه نیست. در این شرایط با استفاده از روش‌های ترکیبی دو یا چند شاخص را با هم ترکیب کرده و حوادث را بر اساس بیشترین خسارت ترکیبی رتبه‌بندی می‌کنند. می‌توان تأثیر حمله هم‌زمان به دو یا چند خط انتقال را نیز با استفاده از همین شاخص‌های کارایی محاسبه کرد.

حال استفاده از شاخص انرژی تأمین نشده با استفاده از راهکار ارائه شده توسط رنجبر [۲۵] برای همین سامانه نشان داده شده است. استفاده از این شاخص به جدول (۳) منجر خواهد شد. زمان بازیابی شبکه برای خروج تمامی خطوط انتقال جهت سادگی مسئله ۱۰ ساعت در نظر گرفته شده است. برای تعیین صحیح زمان بازیابی شبکه به ازای خروج هر خط انتقال باید مطالعات تجربی و همچنین مطالعات دینامیکی انجام گیرد. نکته قابل توجه این است که جواب به‌دست آمده توسط این روش (جدول (۳)) تمامی خطوط بحرانی به‌دست آمده از شاخص‌های کارایی ولتاژ و توان حقیقی را شامل می‌شود.

نکته قابل توجه دیگر حساسیت آسیب‌پذیری سامانه به میزان بار کل سامانه است. اگر بار کل سامانه را به صورت یکنواخت بر روی تمامی باس‌های سامانه به میزان ۴ درصد کاهش دهید، اولویت اهمیت خطوط دچار تغییر می‌شود. همچنین این کاهش بار سبب می‌شود تا تنها سامانه به شش خط انتقال آسیب‌پذیر باشد و در صورت قطع دیگر خطوط سامانه، انرژی تأمین نشده سامانه برابر صفر شود. این مطلب لزوم صرفه‌جویی توسط مصرف‌کنندگان و همچنین لزوم کاهش تلفات سامانه توسط بهره‌بردار را در شرایط بحرانی (تهدید تروریستی) نشان می‌دهد.

جدول ۳. هشت خط انتقال با بیشترین اهمیت به‌دست آمده از شاخص انرژی مورد انتظار تأمین نشده و بار کل ۳۴۲۰ مگاوات

به باس	از باس	EENS(MWh)	شماره خط
۸	۷	۳۶۱۰	۱۱
۱۷	۱۶	۲۵۵۷	۲۷
۲۱	۱۵	۲۵۰۳	۲۵
۱۰	۶	۱۶۶۴	۱۰
۲۳	۲۰	۸۵۹	۳۳
۱۶	۱۴	۸۱۱	۲۳
۲۴	۳	۷۷۴	۷
۲۴	۱۵	۷۷۴	۲۶

ارزیابی آسیب‌پذیری سامانه با استفاده از روش ارائه شده در این مقاله با محاسبه رابطه (۶) انجام می‌پذیرد. در اینجا نیز فرض شده است که زمان بازیابی شبکه برای خروج تمام خطوط انتقال برابر ۱۰ ساعت است. می‌توان به سادگی زمان‌های متفاوت را که از مطالعات تجربی و دینامیکی به‌دست می‌آید، در رابطه (۶) جایگزین کرد. از آنجا که فرض شده است در صورت حمله به خطوط انتقال تنها قسمتی از خط انتقال

دچار آسیب می‌شود و آسیب به طول خط مربوط نمی‌شود، می‌توان قیمت دارایی از دست رفته (F_{loss}) را برای تمام خطوط (چه خطوط کوتاه چه خطوط بلند) برابر در نظر گرفت. البته اگر فناوری ساخت خطوط با هم متفاوت باشند، قیمت دارایی از دست رفته برای خطوط متفاوت است. در اینجا فرض می‌شود قیمت دارایی از دست رفته در صورت حمله به خطوط انتقال برابر ۵۰ میلیون تومان است.

جمعیت تحت تأثیر از قطعی بار و همچنین نوع منطقه دچار قطعی شده به صورت جدول (۵) فرض می‌شود. واحد ارزش بار از دست رفته (VOLL) تومان بر کیلووات ساعت است.

جدول ۴. هشت خط انتقال با بیشترین اهمیت به‌دست آمده از شاخص انرژی مورد انتظار تأمین نشده و بار کل ۳۲۸۰ مگاوات

به باس	از باس	EENS (MWh)	شماره خط
۲۱	۱۵	۲۲۳۶	۱۱
۱۷	۱۶	۱۶۸۱	۱۰
۱۸	۱۷	۱۳۱۳	۲۷
24	۳	۱۲۶۱	۲۵
۲۴	۱۵	۱۹۷	۵
۲۱	۱۸	۱۳	۲۶
۲۳	۱۳	۰	۱۸
۱۹	۱۶	۰	۲۳

جدول ۵. جمعیت متصل، نوع منطقه و ارزش بار از دست رفته باس بارها

باس	جمعیت	منطقه	VOLL
۱	۴۰۰۰۰	سیاسی	۴۰۰
۲	۳۵۰۰۰	سیاسی	۴۰۰
۳	۱۰۰۰۰۰	شهری	۲۰۰
۴	۱۵۰۰۰	روستایی	۴۰
۵	۱۰۰۰۰	روستایی	۴۰
۶	۸۰۰۰۰	شهری	۲۰۰
۷	۷۰۰۰۰	سیاسی	۴۰۰
۸	۱۰۰۰۰۰	شهری	۲۰۰
۹	۱۵۰۰۰۰	شهری	۲۰۰
۱۰	۲۰۰۰۰۰	شهری	۲۰۰
۱۳	۴۰۰۰۰۰	شهری	۲۰۰
۱۴	۳۰۰۰۰۰	شهری	۲۰۰
۱۵	۶۰۰۰۰۰	شهری	۲۰۰
۱۶	۳۰۰۰۰	روستایی	۴۰
۱۸	۷۰۰۰۰۰	شهری	۲۰۰
۱۹	۳۰۰۰۰۰	شهری	۲۰۰
۲۰	۱۰۰۰۰۰	شهری	۲۰۰

هشت خط انتقال پر اهمیت به‌دست آمده توسط روش ارائه شده در جدول (۶) نشان داده شده است. نتیجه استفاده از پخش بار DC برای محاسبه میزان بار تأمین نشده (P_{loss}) در روش ارائه شده، در جدول (۷) نشان داده شده است. مشخص است که نتیجه به‌دست آمده توسط پخش بار DC در مقایسه با نتیجه به‌دست آمده توسط پخش بار بسیار متفاوت است.

جدول ۶. هشت خط انتقال با بیشترین اهمیت به‌دست آمده از روش ارائه شده

به باس	از باس	خسارت (میلیون تومان)	شماره خط
۸	۷	۱۰۷۳	۱۱
۲۱	۱۵	۴۷۹	۲۵
۱۷	۱۶	۴۶۵	۲۷
۱۰	۶	۳۸۵	۱۰
۲۳	۲۰	۲۲۱	۳۳
۱۶	۱۴	۲۱۲	۲۳
۲۴	۳	۲۰۵	۷
۲۴	۱۵	۲۰۴	۲۶

جدول ۷. هشت خط انتقال با بیشترین اهمیت به‌دست آمده از روش ارائه شده و با استفاده از پخش بار DC

به باس	از باس	خسارت (میلیون تومان)	شماره خط
۸	۷	۱۰۰۱	۱۱
۲۱	۱۵	۵۳۸	۲۵
۱۷	۱۶	۵۲۶	۲۷
۱۸	۱۷	۹۰	۲۹
۵	۱	۸۸	۳
۱۶	۱۵	۸۸	۲۴
۱۴	۱۱	۸۷	۱۹
۱۱	۱۰	۸۷	۱۶

در پایان آسیب‌پذیری سامانه در صورت حمله به پست‌های سامانه بررسی می‌شود. با توجه به شکل (۲) مشخص است که ترانسفورماتورهای متصل به باس‌های ۱۱، ۱۲ و ۲۴ سطح ولتاژ سامانه را از ۲۳۰ کیلوولت به ۱۳۲ کیلوولت تبدیل می‌کنند. فرض می‌شود حمله به باس‌های ۱۱، ۱۲ و ۲۴ صورت پذیرفته است که سبب نابودی باس، ترانسفورماتور مربوطه و خطوط انتقال متصل به هر کدام می‌شود. در این صورت با استفاده از شاخص انرژی مورد انتظار تأمین نشده و با فرض بار کل ۳۴۲۰ مگاوات، آسیب‌پذیری سامانه در صورت وقوع حمله به پست‌های آن محاسبه شده است. نتیجه در جدول (۸) نشان داده شده است.

جدول ۸. آسیب‌پذیری سامانه در حمله به پست‌های سامانه توسط شاخص انرژی مورد انتظار تأمین نشده

پست (باس بار)	EENS (MWh)
۲۴	۲۶۰۵
۱۲	۸۳۸
۱۱	۷۲۴

نتیجه حاصله در مقایسه با نتیجه به‌دست آمده از جدول (۳) قابل تفسیر است. در صورت حمله به پست باس ۲۴، ترانسفورماتور و خطوط انتقال ۲۷ و ۷ هم‌زمان از دست می‌رود. در این صورت انرژی تأمین نشده کوچک‌تر از مجموع انرژی‌های تأمین نشده در صورت حمله جداگانه به خطوط انتقال ۲۷ و ۷ می‌باشد.

در صورت استفاده از شاخص ارائه شده برای محاسبه آسیب‌پذیری سامانه در حمله به پست‌های آن، با توجه به اینکه حمله به پست‌ها هزینه از دست رفته میلیارد تومانی ایجاد می‌کند، میزان آسیب‌پذیری بسیار زیاد می‌شود.

۵. نتیجه‌گیری

در این مقاله نمونه‌ای از روش‌های ارزیابی آسیب‌پذیری و تحلیل حوادث سامانه قدرت مورد بررسی قرار گرفته و نتایج استفاده از این روش‌ها ارائه شده است. استفاده از روش انرژی تأمین نشده به عنوان شاخصی مناسب برای ارزیابی آسیب‌پذیری سامانه قدرت در صورت وقوع حمله به خطوط انتقال سامانه مورد تأکید قرار گرفت و نتیجه مطلوب استفاده از این شاخص نشان داده شده است. نتیجه استفاده از شاخص انرژی تأمین نشده به صورت ترکیبی از نتیجه به‌دست آمده از شاخص کارایی ولتاژ و شاخص کارایی شارش توان حقیقی به‌دست آمده است. روش ارائه شده در این مقاله، آسیب‌پذیری سامانه قدرت را به صورت ترکیبی از شاخص انرژی تأمین نشده به همراه میزان خسارت مالی ایجاد شده در صورت وقوع حمله، میزان جمعیتی که تحت تأثیر قطعی بار قرار می‌گیرند، منطقه‌ای که بار آن قطع می‌شود و ... محاسبه کرده است. این رویکرد برای محاسبه و ارزیابی آسیب‌پذیری با توجه به تعریف آسیب‌پذیری که میزان کل خسارات ایجاد شده در صوت وقوع حمله است، منطقی به نظر می‌رسد.

حساسیت زیاد آسیب‌پذیری سامانه قدرت به شرایط مختلف سامانه و میزان بار مصرفی کل سامانه نشان داده شده است. این حساسیت بیانگر این مطلب است که اولویت خطوط انتقال بحرانی (اجزاء بحرانی) سامانه با تغییر شرایط سامانه دچار دگرگونی می‌شود که این مطلب ضرورت بازنگری بهره‌بردار در ارزیابی آسیب‌پذیری سامانه با تغییر شرایط سامانه را نشان می‌دهد. این بازنگری باید با توجه به تغییر مداوم شرایط سامانه در کمترین زمان ممکن و با بیشترین سرعت صورت گیرد. در مطالعات آسیب‌پذیری و تحلیل حوادث سامانه قدرت، از روش‌های حساسیت خطی (پخش بار DC) برای رسیدن سریع به جواب استفاده می‌شود. این روش‌ها به علت ساده‌سازی سامانه قدرت، انحراف ولتاژ باس‌های سامانه قدرت را تحلیل نمی‌کنند و تمامی ولتاژها را برابر واحد در نظر می‌گیرند. بنابراین برای سامانه‌هایی که ولتاژ آن‌ها نیز در شرایط بحرانی قرار می‌گیرد، از پخش بار AC استفاده می‌شود [۳۰]. در بخش پایانی این مقاله خطای استفاده از پخش بار DC نسبت به پخش بار AC نشان داده شده است. می‌توان نتیجه گرفت که ارزیابی آسیب‌پذیری سامانه قدرت با استفاده از پخش بار DC مناسب نیست و به خطای فاحش می‌انجامد. بنابراین استفاده از روش‌های پخش بار AC به همراه کاهش سناریوها برای رسیدن سریع‌تر به جواب مناسب است. در یک سامانه قدرت بزرگ، سناریوها ترکیبات مختلف از وقوع حملات به اجزاء مختلف سامانه قدرت است که می‌تواند بسیار زیاد باشد.

۶. مراجع

[1] Johansson, J. "Risk and Vulnerability Analysis of Interdependent Technical Infrastructures"; PhD. Thesis, Lund University, Dep. Measurement Tech. and Industrial Electrical Eng., 2010.

[2] Amin, M. "Toward Secure and Resilient Interdependent Infrastructures"; J. Infrastructure Syst. 2002, 67-75.

[3] Yusta, J. M.; Correa, G. J.; Arantegui, R. L. "Methodologies and Applications for Critical Infrastructure Protection: State-of-the-Art"; Energy Policy 2011, 10, 6100-6119.

[4] Haimes, Y. Y.; Longstaff, T. "The Role of Risk Analysis in the Protection of Critical Infrastructures against Terrorism"; Risk Anal. 2002, 22, 439-444.

[5] Zerriffi, H. "Electric Power Systems Under Stress: An Evaluation of Centralized Versus Distributed System Architectures"; PhD. Thesis, Carnegie Mellon Univ., Carnegie Institute of Tech. 2004.

[6] Apostolakis, G. E.; Lemon, D. M. "A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due To Terrorism"; Risk Anal. 2005, 25, 361-376.

[7] Amin, M. "Security Challenges for the Electricity Infrastructure"; Computer, 2002, 35, 8-10.

[8] Zimmerman, R.; Restrepo, C.; Dooskin, N.; Hartwell, N.; Miller, L.; Remington, W. "Electricity Case: Main Report - Risk, Consequences, and Economic Accounting"; CREATE, Tech. Rep., 2005.

[9] Li, H.; Rosenwald, G. W.; Jung, L.; Liu, C. C. "Strategic Power Infrastructure Defense"; In Proc. of the IEEE, 2005, 93, 918-933.

[10] Johns, L. S.; Blair, P. D. "Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage"; Office of Tech. Assessment, U.S. Congress, Washington, DC, Tech. Rep OT A-E-453, June 1990.

[11] Holmgren, A.; Jenelius, E.; Westin, J. "Evaluating Strategies for Defending Electric Power Networks Against Antagonistic Attacks"; IEEE T. Power Syst. 2007, 22, 76-84.

[12] Firouzi, H. "Introduction of Strategic Aspects of Electricity Network's Reliable Management from the Perspective of Crisis Management"; Passive Defensc Quarterly 2013, 14, 11-18 (In Persian).

[13] Garrick, B. L.; Hall, L. E.; Kilger, M.; Mcdonald, L. C.; O'Toole, T.; Probst, P. S.; Parker, E. R.; Rosenthal, R. "Confronting the Risks of Terrorism: Making the Right Decisions"; Reliab. Eng. Syst. Safe. 2004, 86, 129-176.

[14] Albert, L.; Nakarado, G. L.; Albert, R. "Structural Vulnerability of The North American Power Grid"; Physical Review 2004, 69.

[15] Kim, M.; EI-Sharkawi, M. A.; Marks, R. J. "Vulnerability Indices For Power Systems"; In 13th Int. Conf. Intelligent Systems Application to Power Systems 2005, 335 - 341.

[16] Mccalley, J. "Security Boundary Visualization for Systems Operation"; IEEE T. Power Syst. 1997, 12, 940- 947.

[17] Kim, M.; EI-Sharkawi, M. A.; Marks, R. J. "Vulnerability Indices For Power Systems"; IEEE T. Power Syst. 2006, 335 - 341.

[18] Kundar, P. "Power System Stability and Control"; Mcgraw-Hill, 1994.

[19] Kassabalidis, I. N.; El-Sharkawi, M. A.; Marks, R. J.; Alves Da Silva, A. P. "Dynamic Security Border Identification Using Enhanced Particle Swarm Optimization"; IEEE T. Power Syst. 2002, 723-729.

[20] Mccalley, J. "Security Boundary Visualization for Systems Operation"; IEEE T. Power Syst. 1997, 12, 940-947.

[21] Eiebe, G. C.; Wollenbera, B. F. "Automatic Contingency Selection"; IEEE T. Power Syst. 1979, 92-104.

[22] Maharana, M. K. Malakar, S. "Sensitivity Based Network Contingency Ranking Using Newton Raphson"; Int. J. of Scientific Eng. and Tech. 2015, 4, 45-49.

[23] Brandwajn, V.; Lauby, M.G. "Complete Bounding Method For Complete AC Contingency Screening"; IEEE T. Power Syst. 1989, 724–729.

[24] Anji, M.; Jiaxi, Y.; Zhizhong, G. "Electric Power Grid Structural Vulnerability Assessment"; In IEEE Power Eng. Society General, 2006.

[25] Ranjbar, M. H. "Optimal Allocation of Reserve Power In Electricity Market"; M.S. Thesis, Shahid Beheshti Univ. Dep. Electrical and Computer Eng., 2012 (In Persian).

[26] Salmeron, J.; Wood, K.; Baldick, R. "Analysis of Electric Grid Security under Terrorist Threat"; IEEE T. Power Syst. 2004, 19, 905–912.

[27] Wood, K.; Baldick, R.; Salmeron, J. "Analysis of Electric Grid Security under Terrorist Threat"; IEEE T. Power Syst. 2004, 19, 905-912.

[28] Chen, G.; Dong, Z. Y.; Hil, D. L.; Xue, Y. S. "Exploring Reliable Strategies for Defending Power Systems Against Targeted Attacks"; IEEE T. Power Syst. 2011, 26.

[29] "The IEEE Reliability Test System-1996"; IEEE T. Power Syst. 1999, 14, 1010–1020.

[30] Wood, A. J.; Wollenberg, B. J. "Power Generation, Opertaion and Control"; Wiley, Third Ed. 2013