فصلنامه علمی-ترویجی پدافند غیرعامل
سال پنجم، شماره ۴، زمستان ۱۳۹۳، (پیاپی ۲۰)؛ صص ۲۹-۴۰

مدل‌سازی و شبیه‌سازی سیستم قدرت با رویکرد پدافند غیرعامل در مقابل حملات الکترومغناطیسی

رمضانعلی آزاده‌دل[۱]، حسن منصف[۲]، حمید دهقانی[۳]

تاریخ دریافت: ۱۳۹۳/۰۶/۰۵
تاریخ پذیرش: ۱۳۹۳/۰۹/۱۲

چکیده

زیرساخت‌های کلیدی به‌ویژه سیستم‌های قدرت از بدو پیدایش تاکنون، بخش جدایی‌ناپذیر زندگی جوامع بشری محسوب می‌شوند؛ بنابراین از لحاظ مواجهه با خطر از سوی عوامل تهدید از پتانسیل بالایی برخوردارند. به همین دلیل، امنیت سیستم‌های مربوط به آنها، به امنیت ملی کلان جامعه گره می‌خورد و تلاش برای حفظ این امنیت، اهمیت زیادی نزد مدیران و تصمیم‌گیرندگان عالی‌رتبه دارد. عوامل تهدیدِ سیستم‌های قدرت، شامل حوادث طبیعی و انسان‌ساز است. هدف اصلی این مقاله، مدل‌سازی و شبیه‌سازی سیستم قدرت با رویکرد پدافند غیرعامل در مقابل تهدیدات الکترومغناطیسی و بررسی راه‌کارهای افزایش ایمنی و امنیت آن در برابر این نوع تهدیدات خواهد بود. شناسایی تهدیدات با تعیین سناریوهای وقوع آن‌ها به‌منظور ارائه راهکارهای حفاظتی و جلوگیری از اختلال یا تخریب در سیستم قدرت برای حفظ و تداوم فرایندهای کاری، سرمایه‌ها و منابع مربوطه، امری ضروری می‌نماید. در این مقاله، منظور از سیستم قدرت، یک ایستگاه فشار قوی دارای اتاق فرمان و تهدیدات مورد نظر برای آن نیز از نوع انفجارات اتمی بالای سطح زمین (HEMP) و فرستنده‌های توان بالا(HPEM) است. با توجه به اینکه تجهیزات مهم سیستم قدرت مورد نظر این تحقیق، شامل محفظه‌های مربوط به سیستم الکترونیکی، رک‌های کنترلی و سازه‌های بتنی برای ایستگاه قدرت می‌باشد، لذا میزان کیفیت حفاظت‌سازی (SE) در هریک از آن‌ها از طریق نرم‌افزار شبیه‌ساز CST، مورد بررسی قرار می‌گیرد. نتایج به‌دست‌آمده نشان می‌دهد که روزنه‌های مستطیلی عریض تعبیه‌شده در ساختارهای محفظه‌ها و رک‌های یادشده، دارای کمترین و روزنه‌های دایروی دارای بیشترین حفاظت الکترومغناطیسی است. نتایج شبیه‌سازی برای سازه ایستگاه‌ها نشان می‌دهد که ساختمان‌های بتنی، تقریباً هیچ‌گونه حفاظتی در برابر تهدیدات ندارند؛ اما در صورتی که در ساختارشان از بتن مسلح استفاده شود، میزان پارامتر SE در فرکانس‌های پایین، بهبود می‌یابد. مروری بر راهکارهای حفاظتی، بر اساس نتایج به‌دست‌آمده از تحقیقات قبلی و شبیه‌سازی‌های انجام‌گرفته، مفاد بخش پایانی این مقاله را تشکیل می‌دهد.

کلیدواژه‌ها: سیستم قدرت، تهدیدات، HEMP، HPEM، کیفیت حفاظت‌سازی (SE)

۱- دانشجوی کارشناسی ارشد برق الکترونیک دانشگاه آزاد اسلامی واحد تهران مرکز Azadehdelir@yahoo.com - نویسنده مسئول
۲- دانشیار و عضو هیئت علمی دانشگاه آزاد اسلامی واحد تهران مرکز
۳- استادیار و عضو هیئت علمی دانشگاه صنعتی مالک اشتر

۱- مقدمه

در دو دهه اخیر، نگرانی نسبت به حملات خصمانه علیه زیرساخت‌های مختلف به‌ویژه سیستم قدرت، رو به افزایش نهاده است؛ به‌ویژه، به‌دلیل به‌کارگیری نیروهای ناتو از این تهدید در طول جنگ‌های بالکان و دوم خلیج فارس، این نگرانی رو به افزایش گذارده است[۱۳]. به‌دلیل وابستگی سایر زیرساخت‌ها به زیرساخت‌های قدرت الکتریکی، تامین و حفظ امنیت آن‌ها از جایگاه مهمی برخوردار می‌باشد [۱۴-۱۶]. از این‌رو، برآورد و مدل‌سازی آسیب‌پذیری‌ها در این زیرساخت (و سایر زیرساخت‌ها)، موضوع مهم کارهای تحقیقاتی اخیر بوده است[۱۷، ۱۸، ۲۲-۲۵]؛ چراکه با بروز هرگونه آسیب به این زیرسخت‌ها، جامعه با چالش‌های متنوعی مواجه خواهد شد[۱] و هرچه وابستگی جامعه به این سیستم بیشتر باشد، چالش‌های مذکور نیز از شدت و پیچیدگی بیشتری برخوردار خواهد شد [۲]. در مجموع، حوادثی که به‌طور بالقوه می‌توانند تهدیدی برای سیستم قدرت باشند، به دو دسته طبیعی و انسان‌ساز تقسیم می‌شوند. حوادث طبیعی می‌تواند در قالب سیل، طوفان، زلزله و آذرخش و حوادث انسان‌ساز نیز می‌تواند به‌صورت پدیده‌هایی نظیر جنگ، خرابکاری و حادثه صنعتی، تهدیدات جدی برای عملکرد سیستم مذکور مطرح شوند [۱۸-۲۰].

حملات خصمانه‌ای که با دخالت عامل انسانی و با هدف ایجاد خسارات و تلفات رخ می‌دهد، در زمره حوادث انسان‌ساز (عمدی) قرار دارد. یعنی در شکل‌گیری این نوع حوادث، انگیزه، آگاهی و هدف نقش مهمی دارند. بنابراین، وجود مدیریت در سیستم قدرت در برابر وقوع این نوع حملات برای امنیت زیرساخت‌ها، بسیار حیاتی خواهد بود؛ چراکه پیامدهای ناشی از این حملات از جنبه‌های مختلف عملیاتی، مالی، روانی، اجتماعی و سیاسی بر جامعه تحمیل می‌گردد. برخی از ویژگی‌های مربوط به این نوع حوادث به شرح زیر است[۲۱]:

- تهدیدات خصمانه، حوادث انسان‌سازی هستند که پیامد آن‌ها ایجاد خسارات و تلفات جبران‌ناپذیر بر زیرساخت‌ها می‌باشد.
- این نوع حملات، عامل واقعی تهدیدات و باعث ایجاد خسارات موثر است.
- این نوع تهدیدات، انتخابی‌اند و اگر هدفی بتواند اثرات مخرب‌تری در سطح جامعه داشته باشد، بدون شک مورد هجوم قرار خواهد گرفت.
- حملات در قالب فرایندهایی شکل می‌گیرند که در آنها، اقدام مهاجمان و مدافعان از یکدیگر تبعیت کرده و بر هم اثرگذارند. به بیان دیگر، یک حمله، زنجیره‌ای از رویدادهای آفندی و پدافندی و وابستگی متقابل است.

این مقاله، بر روی یکی از مهم‌ترین مصادیق مربوط به تهدیدات انسان‌ساز عمدی یعنی تهدیدات ناشی از امواج الکترومغناطیسی و تاثیر آن‌ها بر عملکرد سیستم قدرت متمرکز می‌باشد. تهدیدی که می‌تواند عملکرد اجزای مرتبط با این سیستم را به شدت تحت تاثیر عملکرد سوء خود قرار دهد. لازم به ذکر است که تهدیدات ناشی از امواج الکترومغناطیسی- به‌عنوان یکی از تهدیدات جدید در حیطه زیرساخت‌ها و سیستم‌های قدرت- می‌تواند به‌صورت طبیعی و انسان‌ساز وجود داشته باشد. این امواج، در رنج‌های مختلف به‌صورت مستقیم و تابشی، اجزای سیستم را تحت تاثیر قرار می‌دهند و موجب آسیب آن‌ها می‌شوند.

شناسایی تهدیدات و سناریوهای تهدید احتمالی، به‌منظور ارائه راه‌کارهای حفاظت الکترومغناطیسی و جلوگیری از اختلال یا تخریب اجزای پست‌های برق، حفظ و نگهداری از فرایندهای کاری، منابع و سرمایه‌ها، امری ضروری است. به همین دلیل، آسیب‌شناسی و انجام فعالیت‌های مدیریت ریسک برای مقابله با آثار سوء ناشی از تهدیدات، همچنین اتخاذ تدابیر لازم برای ارتقاء پایداری و قابلیت اطمینان اجزاء سیستم قدرت، ضرورت بسیاری پیدا می‌کند. مدل‌سازی و در پی آن، تدوین و به‌کارگیری هوشمندانه رویکردهای پدافند غیرعامل می‌تواند راهکاری مناسب برای این منظور باشد.

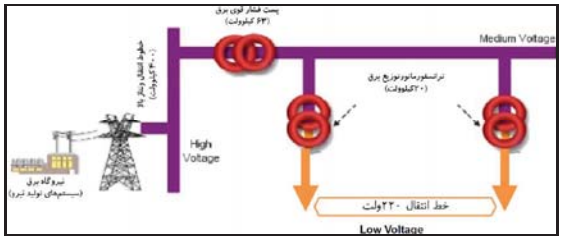
در این مقاله، با مروری بر مولفه‌های کلیدی سیستم قدرت و شناسایی تهدیدات الکترومغناطیسی ناشی از انفجارات اتمی بالای سطح زمین[۱](HEMP) و فرستنده‌های توان بالا[۲](HPEM)، به شبیه‌سازی میزان کیفیت حفاظت‌سازی (SE) در اجزای این سیستم و ارائه دیدگاهی برای به‌کارگیری اصول پدافند غیرعامل در مواجهه با تهدیدات مورد نظر مبادرت می‌گردد. در این راستا، بخش دوم به مروری بر اجزاء سیستم قدرت، بخش سوم به پدافند غیرعامل، بخش چهارم به تاثیر تداخل پالس‌های الکترومغناطیسی بر عملکرد سیستم قدرت و بخش پنجم نیز به شبیه‌سازی میزان کیفیت حفاظت‌سازی[۳] (SE) در اجزای این سیستم اختصاص دارد. سرانجام در بخش ششم، پس از ارائه نتیجه‌گیری، راه‌کاری با هدف تحقق راهبردهای پدافند غیرعامل جهت مقابله با تهدیدات مورد نظر در سیستم قدرت معرفی خواهد گردید.

۲- مروری بر اجزاء سیستم قدرت: پست برق ۶۳ کیلوولت

سیستم قدرت مورد نظر این مقاله، یک پست فشار قوی (۶۳ کیلوولت) دارای اتاق فرمان و سایر اجزای مربوطه است. اصولاً، هر پست یا ایستگاه[۴] فشار قوی برق به‌عنوان یکی از قسمت‌های مهم شبکه تولید، انتقال و توزیع نیرو، مکانی است که در آن، مجموعه‌ای

1- High Altitude Electromagnetic Pulse
2- High Power EM
3- Shielding Effectiveness
4- Substation

از تجهیزات الکتریکی وجود دارد و برای افزایش یا کاهش سطح ولتاژ، قطع و وصل خطوط، انتقال و توزیع برق مورد استفاده قرار می‌گیرد. ولتاژ تولیدی نیروگاه‌ها باید مطلوب مصرف‌کننده‌های نهایی باشد، ولی به جهت وجود موانع زیاد از جمله بُعد مسافت بین نیروگاه و مصرف‌کننده، و نیز ایجاد تلفات خط انتقال و افت ولتاژ، افزایش ولتاژ در نیروگاه و تقلیل این افزایش در مکان دیگر، لازم و ضروری است. هدف از ایجاد این پست‌ها، برآوردن وظیفه دوم است[۳]. شکل (۱)، نمایشی از جایگاه سیستم قدرت مورد نظر این مقاله را در یک شبکه تولید، انتقال و توزیع برق نشان می‌دهد.



شکل ۱- نمایشی از جایگاه سیستم قدرت مورد نظر این مقاله در شبکه تولید، انتقال و توزیع نیرو

در یک دسته‌بندی کلی، پست‌های برق از حیث محل نصب به دو دستهٔ پست سرپوشیده یا داخلی[1] و پست نصب‌شده در فضای آزاد یا خارجی[2] تقسیم می‌شوند. در این صورت، هر پست برق به‌طور کلی از دو قسمت اصلی تشکیل می‌گردد: ۱) قسمت فشار قوی یا همان فضای بیرون پست که تجهیزات فشار قوی در آن قرار می‌گیرد و ۲) قسمت‌های حفاظتی و کنترلی آن شامل تجهیزات حفاظتی، کنترلی و مخابراتی که داخل ساختمان آن قرار دارد. پست داخلی که مورد نظر این مقاله است، شامل انواع بخش‌های الکتریکی، الکترونیکی و کنترلی است. کلیه این بخش‌ها در داخل یک ساختمان سرپوشیده نصب می‌گردند[۳]. اجزای سیستم قدرت مورد نظر این مقاله شامل ساختمان کنترل، سیستم‌های حفاظتی/ کنترلی و سیستم‌های ارتباطی (نظیر PLC[3]) می‌باشد.

۲-۱- ساختمان کنترل: محل نصب و استقرار تجهیزات حفاظتی و کنترلی

اصولاً حفاظت و کنترل تجهیزات پست (شامل ترانسفورماتورهای قدرت، سیستم‌های جبران و سوئیچ‌گیرها) و اندازه‌گیری پارامترهای مورد نیاز پست، توسط وسایلی که از طریق کابل‌های مناسب به سیستم‌های فرمان تجهیزات و ترمینال‌های فشار ضعیف ترانسفورماتورهای اندازه‌گیری ارتباط دارد، انجام می‌شود. کلیه وسایل مذکور به همراه سیستم‌های تغذیه جریان متناوب و مستقیم، در داخل مکانی قرار می‌گیرند که به آن ساختمان کنترل می‌گویند. این مکان، دارای کلیه تجهیزات جانبی برای کار اپراتورهای پست می‌باشد. به‌طور کلی یک ساختمان کنترل ممکن است از اتاق‌های مختلف زیر تشکیل شود [۱۴ و ۱۵]:

۱) *اتاق فرمان*: محلی برای استقرار اپراتورها و انجام عملیات کنترل تجهیزات.

۲) *اتاق حفاظت*: مکانی برای جاسازی رله‌ها و وسایل حفاظتی.

۳) *اتاق باطری*: مکانی برای سیستم‌های تغذیه اضطراری.

۴) *اتاق تغذیه*: محل نصب تابلوهای مربوط به سیستم‌های تغذیه.

۲-۲- سیستم کنترل نظارتی و دستیابی به اطلاعات

"سیستم کنترل نظارتی و دستیابی به اطلاعات" که برای مدیریت و نظارت بر کنترل و جمع‌آوری اطلاعات طراحی شده، برای مانیتورینگ، مدیریت تصمیم‌گیری‌ها در کنترل، و اعلام اخطار برای مواقع مورد نیاز می‌باشد. سیستم اسکادا[4] که برای این منظور طراحی می‌گردد، از سطح ناظر به فرایند کنترل و مانیتورینگ می‌پردازد و کنترل تجهیزات شبکه از نقاط مرکزی را برعهده دارد. هسته اصلی سیستم اسکادا، بسته‌های نرم‌افزاری است که بر روی سخت‌افزارهای استاندارد و مشخص از قبیل کنترل‌کننده قابل برنامه‌ریزی[5] (PLC) و یا واحد پایانه‌های دوردست[6] (RTU) قرارگرفته است. اولی، جانشینی برای سیستم‌های منطقی رله‌ای و تایمری غیرقابل تغییر توسط کاربر به حساب می‌آید و دومی نیز کلیه عملیات جمع‌آوری اطلاعات پست و اعمال فرامین مرکز کنترل را مدیریت می‌نماید[۳، ۴ و ۷].

۲-۳- سیستم‌های ارتباطی

به کمک سیستم‌های ارتباطی و به‌منظور کنترل یا حفاظت از راه دور سیگنال‌های مخابراتی، می‌توان آن‌ها را به نقاط دیگر شبکه، ارسال و متقابلاً سیگنال‌های مشابه را دریافت نمود. این سیگنال‌ها، عمدتاً در انواع سیستم‌های زیر وجود دارند [۳]:

الف) سیستم PLC به کمک این سیستم، می‌توان کنترل از راه دور بار را به کمک انتقال اطلاعات انجام داد و علاوه‌بر آن، سیگنال‌های لازم برای حفاظت تجهیزات را ارسال یا دریافت نمود. با این سیستم، مکالمات تلفنی با دیگر مراکز کنترلی نیز انجام می‌گیرد.

ب) سایر سیستم‌های مخابراتی از نوع بی/ باسیم ارائه‌شده توسط شرکت مخابرات.

1- In-Door
2- Out-Door
3- Power Line Communication

4- Supervisory Control And Data (SCADA)
5- Programmable Logic Controller
6- Remote Terminal Unit

۳- پدافند غیرعامل: مهم‌ترین راهکار برای حفظ امنیت سیستم قدرت

پدافند (یا دفاع)، به دو صورت عامل[1] (یعنی انجام عملیات تدافعی با جنگ‌افزار) و غیرعامل[2] (یعنی انجام عملیات تدافعی بدون جنگ‌افزار) تعریف می‌گردد. به بیان ساده‌تر، پدافند غیرعامل به کلیه اقدامات یا تدابیری اطلاق می‌گردد که بدون استفاده از سلاح، موجب کاهش آسیب‌پذیری، تلفات، خسارات و افزایش پایداری شود. در تعریف فوق، دو مفهوم اقدامات یا تدابیر و کاهش آسیب‌پذیری وجود دارد که به‌طور خلاصه به‌صورت زیر تشریح می‌شوند[۶]:

الف) اقدامات و تدابیر: این مفهوم که در مواردی نظیر دستورالعمل، طرح و نقشه، تدبیر و روش، نظامات و برنامه، مدیریت بحران دفاعی، پروژه‌ها/ فناوری‌های خاص و استفاده از شکاف فناوری خلاصه می‌شود، شامل راه‌کارهایی نظیر استتار و اختفا، پراکندگی، مقاوم‌سازی و استحکامات، تفرقه، موانع، فریب، پوشش، آمایش سرزمینی و اعلام خبر می‌باشد.

ب) کاهش آسیب‌پذیری: این مفهوم نیز شامل مواردی نظیر کاهش میزان ریسک، کاهش احتمال وقوع تهدید، کاهش خسارات بر اماکن و تاسیسات، کاهش تلفات نیروی انسانی و کاهش خسارت بر تجهیزات است. در آسیب‌پذیری، معمولاً مواردی نظیر آنالیز تهدید و امکان حمله، درجه‌بندی ریسک، آنالیز اهمیت و حساسیت و نیز آنالیز فوریت و اولویت باید اجرا گردد.

از نقطه نظر مدیریتی، اقدامات مورد نظر برای اجرای اصول پدافند غیرعامل، عمدتاً قبل از حادثه انجام می‌شود؛ هرچند ممکن است برخی از اقدامات آن، حین و پس از حادثه نیز صورت گیرد[۴]. بنابراین با توجه به اهمیت سیستم قدرت در حفظ و تداوم فعالیت‌های جامعه لازم است تا تدابیر امنیتی کافی برای کم‌اثر نمودن تهدیدات و کاهش آسیب‌پذیری‌ها اتخاذ گردد؛ در این حالت، پدافند غیرعامل می‌تواند نقش مهمی در استمرار فعالیت چرخه تولید تا مصرف انرژی الکتریکی ایفا نماید. برخی از اقدامات پدافندی شامل "پراکندگی"، "تفرقه"، "مستحکم‌سازی"، "آمایش سرزمینی" و "فریب"، می‌تواند برای ارتقاء ایمنی و امنیت سیستم قدرت در در مواجهه با تهدیدات مورد نظر این مقاله اجرایی شوند.

۴- تأثیر تداخل پالس‌های الکترومغناطیسی بر عملکرد سیستم قدرت

تداخل الکترومغناطیسی که غالباً به اختصار، «تداخل» نامیده می‌شود، یکی از مباحث اساسی در حوزه الکترومغناطیس است. با توجه به شکل (۲)، مهندسی سازگاری الکترومغناطیسی[3] (EMC) با پرداختن به یک مدل تداخل شامل منبع تداخل (فرستنده)، سازوکار تزویج و ادوات حساس (گیرنده)، توسعه یافته است. تداخل الکترومغناطیسی، فرایندی است که به‌وسیله آن، ارسال انرژی الکترومغناطیسی به‌صورت سهوی[4] (EMI) یا عمدی[5] (IEMI) از یک سیستم به سیستم دیگر صورت می‌پذیرد. سامانه‌های الکتریکی به همراه قطعات الکترونیکی، عمدتاً سامانه‌های حساسی هستند که می‌توانند توسط پالس‌های الکترومغناطیسی (EMP) و از طریق تداخل هدایتی یا تشعشعی، مورد آسیب قرارگیرند[۷ و ۲۶]. پارامتر SE که در ادامه به آن پرداخته می‌شود، در چارچوب مباحث یادشده و مستقیماً در ارتباط با حفاظت محفظه‌ها در مقابل امواج الکترومغناطیسی بیرونی و تأثیر تراوش امواج از ادوات درونی محفظه، مطرح می‌گردد.

در حالت کلی، EMP نوعی موج الکترومغناطیسی ضربه‌ای با دامنه زیاد است. یکی از عوامل ایجادکننده پالس الکترومغناطیسی، انفجار اتمی است که می‌تواند منجر به تولید پالس الکترومغناطیس هسته‌ای[6] (NEMP) شود[۲۷]. پالس الکترومغناطیسی حاصل از انفجارات هسته‌ای انواع مختلفی دارد که مهم‌ترین و مؤثرترین انواع آن، HEMP می‌باشد که به‌دلیل وقوع انفجارات هسته‌ای در ارتفاع چند ده کیلومتری تا چند صد کیلومتری از زمین رخ می‌دهد[۲۰]. HPEM نیز به‌عنوان یکی از منابع مایکروویوی توان بالای انسان‌ساز، مهم‌ترین نوع بمب الکترومغناطیسی محسوب می‌گردد. این سلاح، به‌عنوان یک سلاح راهبردی در جنگ‌های امروزی و آینده، مطرح می‌باشد [۷]. فناوری‌های مورد استفاده در طراحی بمب‌های الکترومغناطیسی (E-BOMB)، متفاوت از فناوری‌های به‌کاررفته در سلاح‌های هسته‌ای است. این فناوری‌ها از تنوع زیادی برخوردارند و مهم‌ترین آن‌ها شامل مواردی نظیر: مولدهای فشرده‌ساز شار مغناطیسی[7] (FCG)، مولدهای هیدرودینامیکی/ مغناطیسی[8] (MHD) و منبع مولد امواج مایکروویوی توان بالا[9] (HPM) می‌باشد [۸، ۲۸ و ۲۹].

۴-۱- مقایسه تهدیدات ناشی از HEMP و HPEM

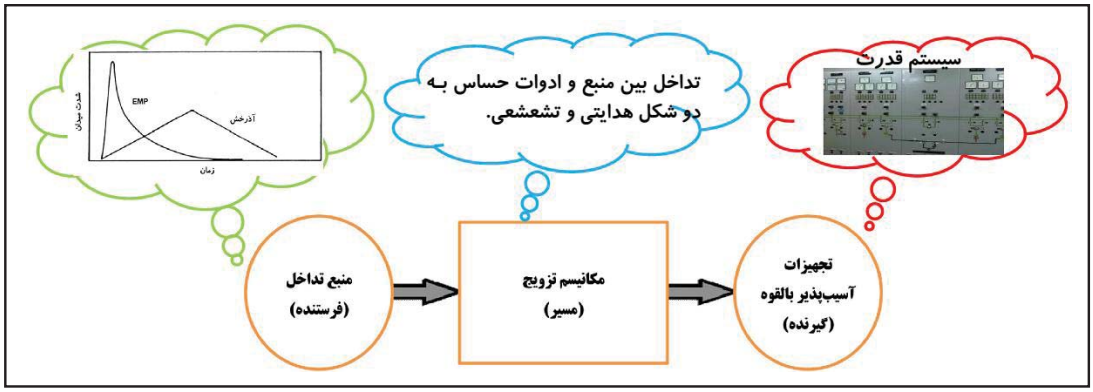
تحقیقات انجام‌شده در این زمینه نشان می‌دهد که HEMP و HPEM، بیشترین اثرات تشعشعی بر روی سامانه‌های الکتریکی و الکترونیکی را دارند. پس از آزمایشات انجام‌شده درخصوص اثرات پالس الکترومغناطیسی ناشی از HEMP در دهه‌های گذشته، امروزه، تهدید HPEM نیز به‌عنوان یک تهدید جدید برای زیرساخت‌های قدرت الکتریکی مطرح شده است. اصطلاح HPEM، به‌طور کلی بر

1- Active Defense
2- Passive Defense
3- Electromagnetic Compatibility

4- Electromagnetic Interference
5- Intentional Electromagnetic Interference
6- Nuclear EMP
7- Flux Compression Generator
8- Magneto Hydro Dynamic
9- High Power Microwave

گذر یک موج الکترومغناطیسی با دامنه قوی و چگالی بالا دلالت دارد. هدف این بخش، مقایسه بین دو تهدید HEMP و HPEM است. در حالت کلی به‌منظور تحلیل اثرات HEMP و HPEM، لازم است تا خصوصیات کلی شامل: منابع تولید، سطح پوشش، رفتار در حوزه زمان، طیف فرکانس و شدت میدان، مورد بررسی قرارگیرد.

جدول (۱) نشان می‌دهد که بیشینه‌دامنه در تهدید HEMP به اندازه ۵۰ کیلوولت بر متر و در تهدید HPEM، ۱۰۰ کیلوولت بر متر می‌باشد. با توجه به اینکه رایانه‌های امروزی و دیگر ادوات وابسته به مدارات مجتمع و میکروکنترولرها در برابر تابش حدود ۳۰ v/m آسیب‌پذیر نشان می‌دهند[۳۳]، لذا تحمیل چنین میدانی بر سیستم قدرت می‌تواند در کسری از ثانیه، اجزای آن را به نابودی بکشاند. در مجموع، میزان دامنه موج رسیده به تجهیزات و دستگاه‌های آسیب‌پذیر، متاثر از عوامل فیزیکی بسیاری چون فاصله از منبع تهدید، پلاریزاسیون موج تابشی، منبع تولیدکننده، شرایط جوی، جنس زمین، محل قرارگیری اجزای سیستم و غیره می‌باشد.



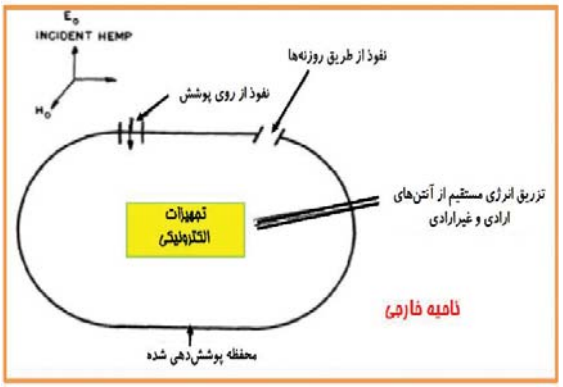
شکل ۲- مدل مربوط به مهندسی سازگاری الکترومغناطیسی (EMC) [۲۶]

جدول ۱- نتیجه مقایسه بین HEMP و HPEM [۸ و ۳۰-۳۲]

مشخصه / تهدید	منبع تولید	سطح پوشش	رفتار در حوزه زمان	طیف فرکانسی	شدت میدان
HEMP	انفجار در ارتفاع ۱۰۰تا۴۰۰ کیلومتر	بسیار گسترده مثلاً یک قاره	برای E1: • زمان صعود در حد چند نانوثانیه؛ • زمان پیک چند ده نانوثانیه • پهنای پالس چند نانوثانیه.	برای E1: ۱ مگا تا ۱ گیگاهرتز	برای E1: ۵۰کیلوولت بر متر
HPEM	آنتن‌های متصل به مولدهای فرکانس بالا	ناحیه تحت پوشش توسط آنتن	۱- فرم باند باریک (HPM): زمان صعود ۱۰۰نانوثانیه؛ ۲- فرم باند پهن (UWB): الف) UWB تک‌قطبی: • زمان صعود ۹۰تا۲۵۰ پیکوثانیه؛ • پهنای پالس چند نانوثانیه. ب) UWB دو قطبی: • زمان صعود ۵۰-۲۵۰ پیکوثانیه؛ • زمان بین حداقل و حداکثر شدت میدان ۱۰۰تا۵۰۰ پیکوثانیه	۱- فرم باند باریک (HPM): ۵۰۰ مگاهرتز تا ۵ گیگاهرتز ۲- فرم باند پهن (UWB): ۱-۱۰ گیگاهرتز	۱- فرم باند باریک (HPM): ۱تا۱۰۰ کیلوولت بر متر ۲- فرم باند پهن (UWB): ۱تا ۱۰۰ کیلوولت بر متر

۴-۲- مدل‌سازی پالس الکترومغناطیسی

راه‌های نفوذ پالس الکترومغناطیسی به سیستم قدرت از طرق مختلف امکان‌پذیر است؛ لذا در صورت جلوگیری از ورود امواج الکترومغناطیسی به داخل پست، می‌توان از تجهیزات پست در مقابل آسیب‌پذیری ناشی از آن‌ها حفاظت نمود. راه‌های نفوذ پالس الکترومغناطیسی به ساختمان پست می‌تواند شامل دیوارها، درب، کانال‌های تهویه، آنتن، زمین و مسیر عبور کابل‌ها باشد؛ در این حالت، میزان نفوذ امواج به داخل تجهیزات و اثرگذاری بر آن‌ها را می‌توان تابع دو پارامتر شدت میدان مغناطیسی و نحوه پوشش (طرح حفاظتی در برابر امواج الکترومغناطیسی) دانست [۹]. به‌طور کلی، مطابق شکل (۳)، مدهای نفوذ و تزویج امواج الکترومغناطیسی تابش میدان خارجی به یک محفظه پوشش‌داده‌شده (نظیر تجهیزات الکتریکی/ الکترونیکی یک سیستم قدرت) را می‌توان در قالب سه روش مختلف زیر بیان نمود:



شکل ۳- سه مود نفوذ و تزویج امواج به محفظه پوشش‌داده‌شده[۳۴]

الف) انتشار از روی پوشش[1]: میدان‌های حاصل از EMP به‌دلیل اثر پوستی، از دیواره‌های هادی غیر ایده‌آل و قفسه‌های پوشش‌دهی (شیلد) شده عبور می‌کند. عبور سیگنال از دیواره‌های محفظه، معمولاً یک پدیده پایین‌گذر به حساب می‌آید؛ چرا که با افزایش فرکانس، عمق پوستی[2] کم می‌شود و عبور سیگنال‌های مختلف از پوشش کاهش می‌یابد؛ بنابراین انتشار از روی پوشش بیشتر شامل میدان‌های مغناطیسی فرکانس پایین می‌باشد. در حالت کلی، قابلیت نسبی یک پوشش، برای ممانعت از ورود میدان‌های الکتریکی و مغناطیسی و همچنین موج‌های صفحه‌ای است. طبق تعریف، توانایی یک محفظه برای کاهش تشعشع یا بهبود ایمنی تجهیزات الکتریکی و الکترونیکی در قبال تداخل‌های فرکانسی، از طریق پارامتری تحت عنوان پارامتر SE یا "کیفیت حفاظت‌سازی" تعریف می‌گردد. در سنجش مذکور، این پارامتر بر حسب نسبت شدت میدان ورودی قبل از حفاظت‌سازی (E1) به شدت میدان اندازه‌گیری‌شده پس از حفاظت‌سازی (E2) تعریف می‌شود که معمولاً برحسب دسی‌بل و به‌صورت زیر بیان می‌گردد [۷ و ۳۴]:

$$SE = 20 \log_{10}|E1/E2| \qquad (۱)$$

در رابطه فوق، SE مثبت است؛ زیرا انتظار می‌رود که شدت میدان اندازه‌گیری‌شده پس از حفاظت‌سازی (E2) بیشتر از شدت میدان ورودی قبل از حفاظت‌سازی (E1) باشد؛ مثلاً اگر SE، ۱۲۰ دسی‌بل باشد، به این معنی است که دامنه E2 نسبت به دامنه E1 با یک عامل 10^{6} کاهش می‌یابد. علاوه‌بر موارد یادشده، درخصوص ملاحظات مربوط به انتشار امواج الکترومغناطیسی از روی پوشش نیز می‌توان به نوع مصالح ساختمانی به‌کاررفته در پست برق اشاره کرد؛ زیرا این مصالح می‌توانند در نفوذپذیری EMP و آسیب‌پذیری اجزای پست، نقش به‌سزایی داشته باشند؛ لذا این موارد نیز باید به دقت مورد بررسی قرار گیرند. به‌منظور بررسی دقیق پارامترهای نفوذپذیری[3] (ε) و هدایت الکتریکی[4] (σ)، مصالح به‌کاررفته در ساختمان، به‌صورت گروه‌های متنوعی نظیر: بتن، آجر، شیشه و چوب تقسیم‌بندی می‌شوند[۷].

به‌طور مثال، استفاده از بتن به‌عنوان یک حفاظ، به خصوصیات الکترومغناطیسی آن که شامل هدایت الکتریکی (σ)، ضریب نفوذپذیری (ε) و گذردهی نسبی[5] (ε'_r) است، بستگی دارد. بتن یک ماده غیرمغناطیسی است که میزان گذردهی نسبی آن برابر با یک است. در بررسی میزان کیفیت حفاظت‌سازی (SE) ساختمان‌ها، بتن به‌عنوان یک دی‌الکتریک ساده در نظر گرفته می‌شود که دارای ضریب گذردهی نسبی $\varepsilon_r(w) = \varepsilon'(w) - j\varepsilon''(w)$ می‌باشد. مطابق [۱۰ و ۳۵]، اگر بتن به‌صورت مواد "دبای" مدل‌سازی گردد، آنگاه وابستگی نفوذپذیری نسبی به فرکانس از روابط زیر پیروی خواهد کرد:

$$\varepsilon'_r(w) = \varepsilon_\infty + \frac{\Delta\varepsilon}{1+(\omega/\omega_r)^2} \qquad (۲)$$

$$\varepsilon''_r(\omega) = \frac{(\omega/\omega_r)\Delta\varepsilon}{1+(\omega/\omega_r)^2} \qquad (۳)$$

در روابط (۲) و (۳)، $\Delta\varepsilon = \varepsilon_{static} - \varepsilon_\infty$ است. ε_∞ و ε_{static} نیز

1- Diffusion Through the Shield
2- Skin Depth

3- Permittivity
4- Electrical Conductivity
5- Relative Permittivity

به‌ترتیب، مقادیر نهایی و اولیه نفوذپذیری در بازه فرکانسی مورد نظر خواهند بود. W_{ap} فرکانس زاویه‌ای منحنی می‌باشد که برحسب رادیان بر ثانیه بیان می‌گردد.

ب) نشت از روزنه‌ها[1] (در رک‌ها و سایر تجهیزات الکترونیکی و الکتریکی پست): هر پوششی به ناچار دارای درها، پنجره‌ها، حفره‌ها و درزهایی است که می‌تواند منشأ ورود امواج و تشکیل میدان‌های الکتریکی/ مغناطیسی باشد. نشت میدان از یک روزنه به اندازه/ نوع ساختار و مکان روزنه‌های روی محفظه، بستگی دارد. از طرفی، چون حملات EMP باند پهن، محدوده وسیعی از فرکانس را دربرمی‌گیرد، لذا به‌منظور مقابله با حملات EMP، باید برای چنین روزنه‌هایی، تمهیداتی اندیشیده و در مورد اثر آن‌ها بر روی پوشش، تجدید نظر کرد [۷ و ۳۴].

ج) ورود از طریق آنتن‌های ارادی و غیرارادی[2]: اصولاً، آنتن‌ها برای جمع‌آوری انرژی الکترومغناطیسی در محدوده فرکانسی خاص طراحی می‌شوند؛ ولی از آنجائی‌که EMP می‌تواند از پهنای باند و دامنهٔ بسیار بزرگی برخوردار باشد، لذا احتمال طراحی در فرکانس‌های خارج از محدوده و دریافت انرژی قابل توجه از یک حمله EMP در جهات خارج از جهت اصلی نیز وجود دارد. از آنجائی‌که آنتن‌ها، اساساً محل ورود انرژی الکترومغناطیسی به سیستم هستند، نمی‌توان آن‌ها را با قفسه‌ها پوشش داد؛ بلکه آن‌ها باید کاملاً در معرض دریافت امواج قرار بگیرند؛ اما از طرفی انتظار نمی‌رود که دامنه موج ورودی از مقدار تقریبی خاصی بالاتر باشد؛ زیرا در این صورت، بر اساس دامنه سیگنال ورودی، سیستم‌های دریافت و پردازش سیگنال بعد از آنتن سطوح مختلف، آسیب‌دیدگی را تجربه خواهند کرد و این تخریب در برابر امواج EMP، بسیار شدید و حتمی خواهد بود؛ اما آنتن‌های غیرارادی، شامل لوله‌ها، خطوط برق، کابل‌های اطلاعات و کلاً تمام هدایت‌کننده‌های الکتریکی گستره وسیعی دارند و برخلاف آنتن‌های ارادی، ناشناس هستند. در نتیجه، مقابله با آنها، انرژی و دقت بیشتری را می‌طلبد. این نوع آنتن‌ها در صورت داشتن طول زیاد، می‌توانند با انباشت مقدار زیاد انرژی در خود، هنگام ورود به داخل محفظه، انرژی الکترومغناطیسی قابل توجهی با خود همراه داشته و صدماتی به اجزای سیستم قدرت وارد نمایند [۷ و ۳۴].

۵- شبیه‌سازی سیستم قدرت در مقابل تهدیدات الکترومغناطیسی

مبنای فعالیت‌های مدل‌سازی و شبیه‌سازی در این بخش، براساس نفوذ امواج الکترومغناطیسی به درون اجزای یک سیستم قدرت از طریق روزنه‌ها و پوشش آن‌ها خواهد بود. از آنجائی‌که این روزنه‌ها در فرکانس‌های مربوط به امواج الکترومغناطیسی، نقش یک آنتن با کارایی تشعشعی بالا را ایفا می‌کنند، اغلب به‌عنوان منابع اصلی تداخل الکترومغناطیسی (EMI) منظور می‌گردند؛ بنابراین تحلیل و شناسایی نسبت اندازه میدان در حضور روزنه، نسبت به اندازه میدان در غیاب آن، به‌عنوان معیاری از نفوذ امواج الکترومغناطیسی به درون تشدیدکننده‌های حفره‌ای در حضور روزنه‌های مختلف، مسئله‌ای کلیدی است. این نکته، مبین تحلیل پارامتر کیفیت حفاظت‌سازی (SE) است. همان‌طور که قبلاً نیز اشاره شد، توانایی یک محفظه برای کاهش تشعشع یا بهبود ایمنی تجهیزات الکتریکی و الکترونیکی در قبال تداخل‌های فرکانسی، از طریق پارامتری تحت عنوان پارامتر SE تعریف می‌گردد؛ در واقع، معیار اصلی تعیین میزان حفاظت سیستم‌ها، پارامتر SE است. به‌منظور تحلیل و بررسی میزان کیفیت حفاظت‌سازی (SE) در سیستم قدرت مورد نظر این مقاله، موضوع به سه بخش زیر تقسیم می‌گردد:

الف) بررسی یک محفظه در دو حالت؛

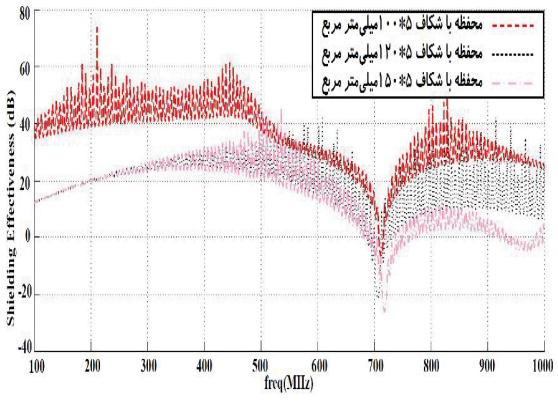
ب) یک رک نوعی در اتاق فرمان در چهار حالت؛

ج) اتاق فرمان با دو نوع سازه.

۵-۱- شبیه‌سازی میزان SE برای یک محفظه

۵-۱-۱- یک محفظه چهارگوش کوچک با یک روزنه

این محفظه با ابعاد ۳۰۰×۳۰۰×۱۲۰ میلی‌متر مکعب، دارای روزنه مستطیلی‌شکل در سه بعد مختلف می‌باشد. با توجه به شکل (۴)، در فرکانس ۷۰۰ مگاهرتز، هر سه محفظه با رزونانس مواجه می‌گردند که در این حالت، هیچ‌گونه حفاظت الکترومغناطیسی نخواهند داشت. لازم به ذکر است که در کلیه آزمون‌ها، پلاریزاسیون موج صفحه‌ای تابانیده‌شده به محفظه در جهت محور Y و پروب نیز در جهت این محور قرار دارد.



شکل ۴- نمایشی از نتیجه شبیه‌سازی برای یک محفظه با سه نوع شکاف

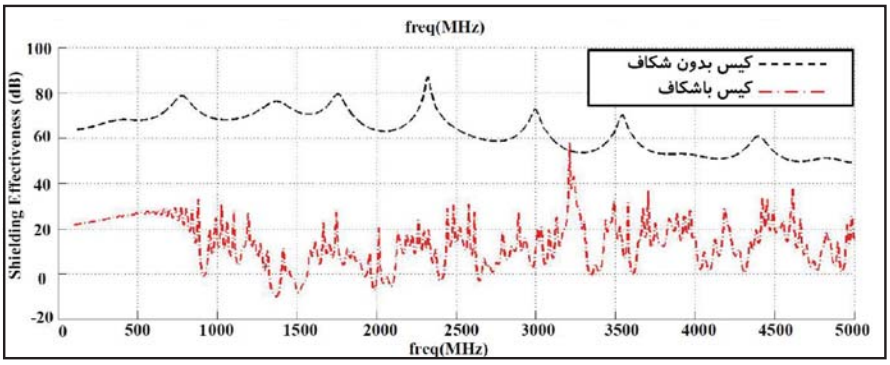
1- Leakage Through Aperture
2- Intentional and Inadvertent Antenna

۵-۱-۲- یک کیس رایانه

این کیس با ابعاد ۱۸۰×۴۲۰×۴۴۵ سانتی‌متر مکعب، دارای روزنه‌های دایره‌ای‌شکل به قطر ۲ میلی‌متر و فاصله مرکز تا مرکز ۷ میلی‌متر است. مختصات اولین روزنه در قسمت جانبی، درست در مرکز مختصاتی محفظه قرار دارد و مختصات اولین روزنه در قسمت پشتی کیس از مرکز مختصاتی ۳۰ میلی‌متر در جهت Y و ۷۰ در جهت Z است. در قسمت پشت کیس، تعداد ۶۴ عدد روزنه به‌صورت ماتریس ۸×۸ و در قسمت جانبی آن نیز، تعداد ۱۲۱ روزنه با مشخصات فوق، به‌صورت ماتریس ۱۱×۱۱ طراحی شده است. میزان SE، یکبار با تابش موج صفحه‌ای به قسمت جانبی و بار دیگر به قسمت عقب، محاسبه می‌گردد (پروب در مرکز کیس قرار دارد). در حالت بعد، سه شکاف مستطیلی‌شکل (محل نصب کارت‌های سخت‌افزاری)، با ابعاد ۵× ۱۰۰ میلی‌متر مربع ایجاد می‌گردد. مطابق شکل (۵)، مقدار SE برای حالت بدون شکاف‌های مستطیلی‌شکل، تقریباً بیش از ۵۰ دسی‌بل است و برای حالت با شکاف‌های مستطیلی‌شکل، محدوده SE به‌شدت کاهش می‌یابد. آزمایش نشان می‌دهد که با افزایش فرکانس، پارامتر یادشده، روال کاهشی را با شدت بیشتری ادامه می‌دهد[۱۱].

۵-۲- یک رک نوعی در اتاق فرمان

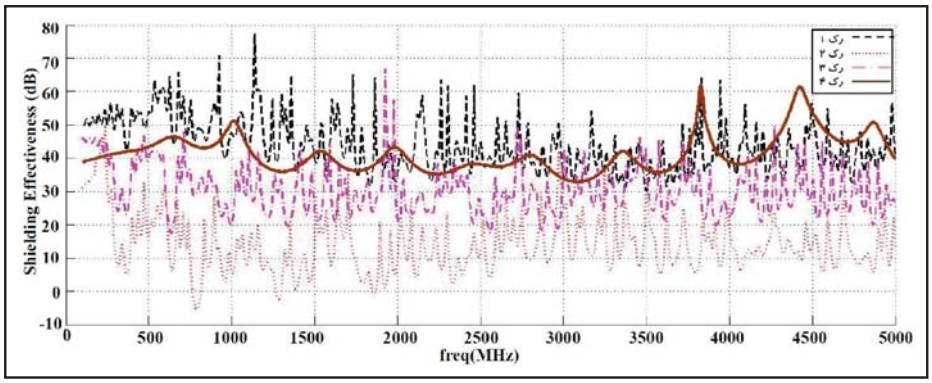
در این بخش، از مشخصات رک SR328B با ابعاد ۶۰۰×۸۰۰×۱۶۰۰ میلی‌متر مکعب استفاده می‌شود. جدول (۲) و شکل (۶)، مشخصات آزمون و تغییرات SE در این رک را در شرایط مختلفی که مورد آزمون قرار گرفته، نشان می‌دهند:



شکل ۵- نتیجه شبیه‌سازی برای کیس رایانه با روزنه‌های مختلف

جدول ۲- تغییرات SE در رک SR328B برای شرایط مختلف

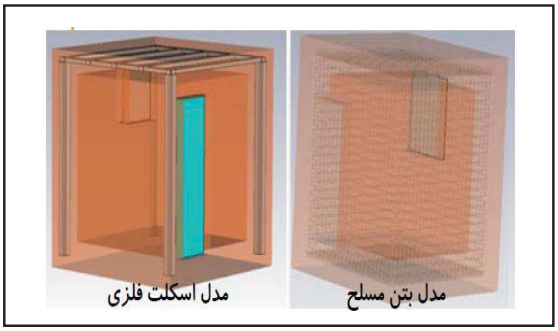
شماره آزمون/ رک	تعداد روزنه	نوع روزنه	مشخصات روزنه	نحوه قرارگیری روزنه	نتیجه آزمون
۱	۶	دایروی	• قطر هر روزنه: ۱۰ میلی‌متر • فاصله مرکز تا مرکز : ۲۰ میلی‌متر	دو ردیف سه‌تایی	مقدار SE در همه فرکانس‌ها، مقداری مثبت و تقریباً بیش از ۴۰ دسی‌بل است.
۲	۶	چهارگوش	• ابعاد: ۱۵۰*۵ میلی‌متر • فاصله مرکز تا مرکز : ۱۰۰ میلی‌متر	دو ردیف سه‌تایی	وجود روزنه‌های چهارگوش، باعث ایجاد رزونانس‌های زیادی می‌شود و مقدار SE در فرکانس ۸۰۰ مگاهرتز منفی است.
۳	۲۵۶	دایره‌ای	• قطر هر روزنه: ۱۰ میلی‌متر • فاصله مرکز تا مرکز : ۲۰ میلی‌متر	۴ ماتریس ۸*۸ در یک گوشه	مقدار SE در همه فرکانس‌ها، مقداری مثبت و تقریباً بیش از ۲۵ دسی‌بل است.
۴	۴+۲۵۶	چهارگوش+ دایروی	• ابعاد چهارگوش ماتریسی: ۱۰*۱۰ میلی‌متر • ابعاد چهارگوش تکی: ۲۰*۲۰ میلی‌متر • قطر روزنه دایره‌ای: ۲۰ میلی‌متر	• ۴ ماتریس ۸*۸ در چهارگوشه • دو ردیف دوتایی	مقدار SE در همه فرکانس‌ها، مقداری مثبت و تقریباً بیش از ۳۵ دسی‌بل است.



شکل ۶- نمایشی از نتیجه شبیه‌سازی برای یک رک با چهار نوع روزنه

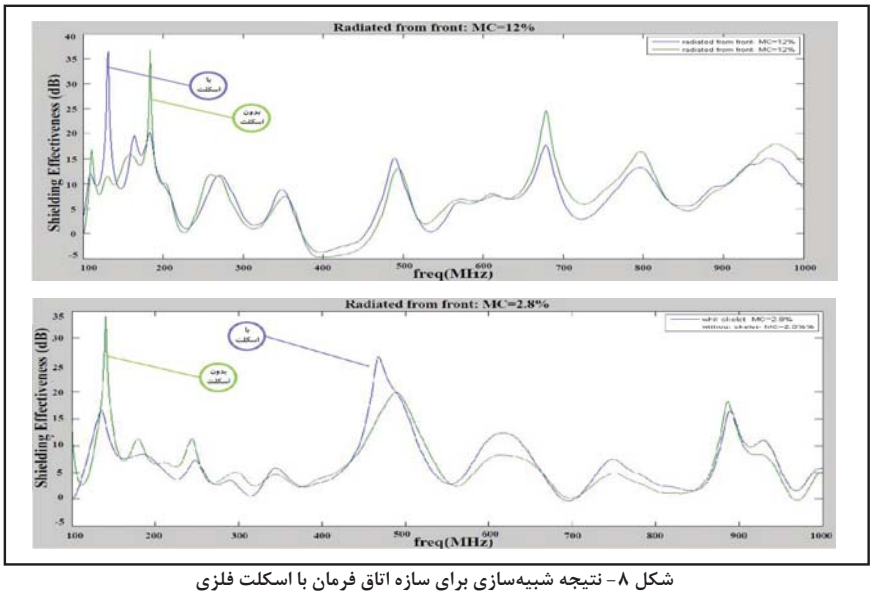
۵-۳- شبیه‌سازی میزان SE برای اتاق فرمان با دو نوع سازه

در این قسمت به بررسی یک اتاق فرمان نوعی به ابعاد ۲×۲×۲ متر دارای در و پنجره، مطابق شکل (۷)، در دو حالت با ساختار اسکلت فلزی و بتن مسلح پرداخته می‌شود.



شکل ۷- مدل‌سازی اتاق فرمان در دو حالت

الف) اتاق فرمان با ساختار اسکلت فلزی: در اولین آزمون این بخش، ساختار بتنی با/ بدون وجود اسکلت فلزی مورد بررسی قرار می‌گیرد. اسکلت فلزی، متشکل از ۴ ستون است که در فاصله ۲/۱۵ متری از یکدیگر قرار داده شده‌اند. همچنین در سقف اتاق نیز تیرچه‌هایی به ابعاد ۵×۱۰×۲۴۰ سانتی‌مترمکعب به فاصله ۶۰ سانتی‌متری از یکدیگر قرار داده شده‌اند. برای این اتاق، یک در و پنجره فلزی به ترتیب با ابعاد ۷۰× ۱۸۵ سانتی‌متر مربع و ۷۰×۷۰ سانتی‌متر مربع طراحی شده است. شکل (۸)، میزان SE اتاق فرمان را در دو حالت با / بدون اسکلت و دو نوع بتن با دو رطوبت ۱۲ و ۲/۸ درصد را نشان می‌دهد. همان‌طور که مشاهده می‌شود، وجود اسکلت تاثیر چندانی در ارتقای میزان SE سازه ندارد.



شکل ۸- نتیجه شبیه‌سازی برای سازه اتاق فرمان با اسکلت فلزی

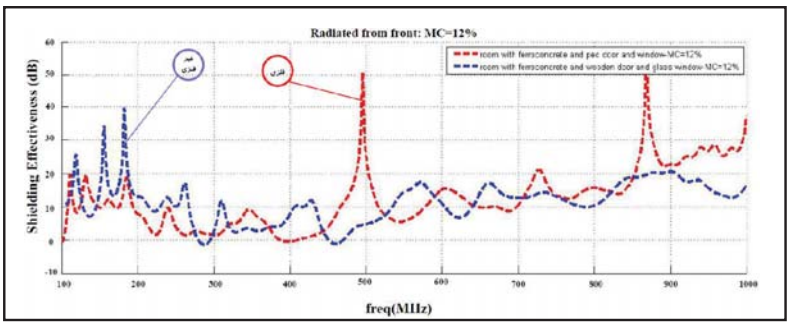
ب) اتاق فرمان با ساختار بتن مسلح: در دومین آزمون این بخش، برای ایجاد سازه بتن مسلح، از میله‌گردهای استیلی با قطر ۱cm و فاصله ۷/۵cm از یکدیگر استفاده می‌گردد. بتن به‌کاررفته در این سازه، مثل آزمون قبل دارای دو میزان رطوبت ۱۲ و ۲/۸ درصد است. ابعاد درب و پنجره اتاق فرمان برای این حالت نیز مشابه حالت قبل بوده و جنس‌شان در حالت اول از چوب و در حالت دوم از فلز است. شکل (۹)، نتیجه شبیه‌سازی برای حالتی که میزان رطوبت ۱۲٪ است را نشان می‌دهد. همان‌طور که در شکل مشاهده می‌شود، میزان SE در هر دو نمونه تا فرکانس ۴۵۰MHz، تقریباً یکسان و در حدود چند دسی‌بل است؛ اما در بازه فرکانسی بالاتر از این مقدار، میزان SE برای سازه دارای در و پنجره فلزی با افزایش بیشتری نسبت به سازه با در و پنجره غیرفلزی (چوبی) مواجه می‌گردد.

۶- نتایج و پیشنهادات

۶-۱- نتیجه‌گیری

با گسترش به‌کارگیری تهدیدات الکترومغناطیسی از سوی کشور هدف، لازم است برای محافظت از اجزای سامانه فرماندهی و کنترل قدرت، راه‌کارهایی در مراحل مختلف فرایند پدافند غیرعامل، توسعه و اجرایی گردد. هرچند به‌کارگیری راه‌کارهای مورد نظر برای مقابله با این تهدیدات از نظر اقتصادی بسیار پرهزینه است، ولی منافع ناشی از این اقدامات در زمان‌های بحرانی، قابل توجه خواهد بود. در این مقاله، بررسی تاثیر تهدیدات الکترومغناطیسی بر روی اجزای یک سیستم قدرت و ارائه راه‌کارهای نظام‌مند برای بهره‌برداری از اصول پدافند غیرعامل با هدف تقویت حوزه فرماندهی و کنترل، یک نوآوری در این مقاله قلمداد می‌شود. در این حالت، قبل از اجرای بسیاری از این راه‌کارها می‌توان ابتدا از طریق مدل‌سازی و شبیه‌سازی، آن‌ها را مورد آزمون قرار داد و سپس پیاده‌سازی نمود؛ هرچند ارزیابی پارامتر SE یک تشدیدگر حفره‌ای واقعی، اغلب یکی از مسائل پیچیده در حوزه الکترومغناطیس است و مقدار این پارامتر به پارامترهای متعددی از قبیل منبع موج الکترومغناطیس خارجی، ابعاد و هندسه محفظه، تعداد و هندسه و ابعاد روزنه‌ها، فرکانس کار و غیره وابسته است. در مجموع نتایج مورد نظر در این مقاله را می‌توان در موارد زیر خلاصه کرد:

- میزان SE، علاوه‌بر عوامل محیطی، به طراحی محفظه شیلد، شکل و ابعاد روزنه‌ها، چگونگی چینش روزنه‌ها، جنس محفظه، زاویه تابش موج و مشخصات موج بستگی دارد.
- از آنجائی‌که روزنه‌های دایروی نسبت به روزنه‌های چهارگوش حفاظت الکترومغناطیسی بالاتری دارند، لذا روزنه‌های تعبیه‌شده برای کلیدهای سکسیونر، بریکر، پنل‌های نمایش و اندازه‌گیری باید به‌صورت دایروی طراحی شوند.
- میزان SE در نزدیکی روزنه کمتر است؛ از این‌رو، مدارهای حساس واقع در داخل رک‌ها تا حد امکان باید از روزنه‌ها دورتر باشند.
- روزنه‌هایی که در راستای هم قرارگرفته‌اند، پارامتر SE را پایین می‌آورند.
- اگر ساختار بتن مسلح از نوع PEC (هادی کامل) باشد، آنگاه موجب افزایش SE خواهد شد. با اضافه کردن پودر آلومینیوم به بتن مسلح این امر محقق خواهد شد.
- در فرکانس‌های پایین، میزان SE توسط ساختار مش‌گونه موجود در بتن تعیین می‌شود و در فرکانس‌های بالاتر، میزان رطوبت و ساختار سایر اجزای اتاق (یعنی جنس در و پنجره) بر میزان SE تاثیرگذارند.
- وجود اسکلت فلزی، تقریباً هیچگونه تاثیری در میزان SE ساختمان ندارد.
- از آنجائی‌که تجهیزات الکترونیکی در رایانه‌ها، مدارات مجتمع و میکروکنترلرها معمولاً در حضور میدان الکتریکی بیشتر از ۳۰ ولت بر متر عملکرد درستی ندارند، لذا دامنه میدان داخل سیستم قدرت باید کمتر از حد آسیب‌پذیری اجزای آن باشد.
- از آنجائی‌که میدان ناشی از تهدیدات الکترومغناطیسی موردنظر این تحقیق (HPEM وHEMP)، بین ۵۰ الی ۱۰۰ کیلوولت بر متر است، لذا ایجاد حفاظت بین ۶۰ تا ۸۰ دسی‌بل در سیستم قدرت، منطقی و مطلوب است.



شکل ۹- نتیجه شبیه‌سازی برای سازه اتاق فرمان با بتن مسلح

۶-۲- ارائه راهکار

قبل از پیشنهاد چند راهکار، لازم است سه راهبرد حفاظتی برای اجزای یک سیستم قدرت مورد بررسی قرار گیرند. این راهکارها به‌منظور تداوم کار در زمان بحران تعیین شده‌اند. این راهبردها که متناسب با عملکرد اجزای سیستم قدرت منظور می‌گردند، به شرح زیر می‌باشند [۱۲]:

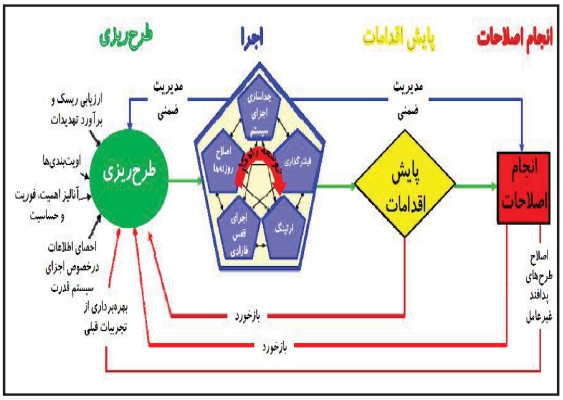
راهبرد حفاظتی اول: در این راهبرد، علاوه‌بر کل فرایند تولید و اجرای فعالیت‌های مهم، تجهیزات و ساختارهای مورد نیاز برای ادامه فعالیت در شرایط وقوع بحران، مقاوم‌سازی می‌شوند.

راهبرد حفاظتی دوم: تنها تجهیزات ضروری موردنیاز فعالیت پست قدرت حفاظت می‌شوند.

راهبرد حفاظتی سوم: در این راهبرد، تنها تجهیزات پشتیبان تولید برق حفاظت می‌شوند تا پس از وقوع بحران نیز مجدداً راه‌اندازی گردند.

به‌منظور تحقق راهبردهای حفاظتی فوق، مدل مطابق شکل (۱۰) پیشنهادی می‌گردد. این مدل، با الهام از چرخه فرماندهی و کنترل، برای پوشش‌دهی به اقدامات پدافند غیرعامل، در قالب گام‌های اساسی زیر ارائه می‌گردد:

الف) طرح‌ریزی: در گام ابتدایی، باید در جست‌وجوی اطلاعات جدید و درک شرایطی که موجود است، بود. جمع‌آوری اطلاعات به همراه ارزیابی و تحلیل آن‌ها در این مرحله، آگاهی تیم اجرایی را از وضعیت موجود، ارتقاء می‌بخشد.



شکل ۱۰- مدل پیشنهادی برای تحقق راهبردهای پدافند غیرعامل در سیستم قدرت جهت مقابله با تهدیدات الکترومغناطیسی

ب) اجرا: در گام بعد، بر اساس نیازمندی‌ها به توسعه راه‌کارها مبادرت می‌گردد.

ج) پایش اقدامات: در این گام، از طریق جمع‌آوری گزارشات، دسته‌بندی و تحلیل آنها، به پایش محیط اقدام پرداخته می‌شود.

د) انجام اصلاحات: نتیجه تحلیل‌ها در گام قبلی، میزان اصلاح طرح‌های پدافند غیرعامل را به دست خواهد داد و از طریق اخذ بازخورد این چرخه تا جائی‌که نیازمندی‌ها را مرتفع سازد، ادامه می‌یابد.

مراجع

۱. تواضع، محمدحسین و سایر؛ حفاظت از ساختمان‌ها و تجهیزات الکترونیکی در برابر تهدیدات EMP؛ همایش سراسری پدافند غیرعامل در علوم مهندسی با تأکید بر استتار، اختفا و فریب، تهران، دانشگاه جامع امام حسین (ع)، (**۱۳۹۲**).

۲. سپهری، محمد و سایر؛ اقدامات پدافند غیرعامل در تاسیسات نیروگاهی و برق‌رسانی، همایش سراسری پدافند غیرعامل در علوم مهندسی با تاکید بر استتار، اختفا و فریب؛ تهران، دانشگاه جامع امام حسین(ع)، (**۱۳۹۲**).

۳. سلطانی، مسعود؛ تجهیزات نیروگاه؛ انتشارات دانشگاه تهران، جلد ۱، صص. ۸۷- ۱۲۰، (**۱۳۸۳**).

۴. فهیمی، شهرام؛ آشنایی با سیستم‌های کنترل DCS؛ گروه صنعتی ندا. http://www.nedaco.com

۵. مهرابی، زهرا؛ انتقال برق از ایستگاه تا کنترل دیسپاچینگ؛ برق منطقه‌ای فارس، (**۱۳۸۴**).

۶. سند راهبردی پدافند غیرعامل کشور (۱۳۸۵-۱۴۰۵)، سازمان پدافند غیرعامل کشور؛ (**۱۳۸۶**).

۷. دانایی، محمد مهدی و سایر؛ تحلیل و بررسی حساسیت پارامترهای حفاظت اتاق کامپیوتر در برابر تهدیدات الکترومغناطیس و ارائه راهکارهای حفاظتی مناسب؛ پنجمین همایش سراسری پدافند جنگ‌های نوین، دانشگاه جامع امام حسین(ع)، تهران، (**۱۳۹۱**).

۸. آشنایی با EMP و اثرات آن؛ نشریه پدافند غیرعامل؛ قرارگاه پدافند هوایی خاتم‌الانبیاء (ص)، شماره ۲، (**۱۳۸۳**).

۹. صادقی‌زاده، وحید؛ کوثری، سعید؛ معرفی روش‌های حفاظت از ساختمان و تجهیزات الکترونیکی در مقابل تهدیدات EMP؛ همایش مدیریت بحران در صنعت ساختمان، سازه‌های زیرزمینی و شریان‌های حیاتی، اصفهان، (**۱۳۹۱**).

۱۰. آبروش، حسن؛ معرفی و شبیه‌سازی روش جدید اندازه‌گیری ضریب تلفات عایقی و پرمتیویته نسبی، نشریه دانشکده فنی، دانشگاه تهران، جلد ۴۱ ، شماره ۵، صص ۵۴۰-۵۳۵، (**۱۳۸۶**).

۱۱. دانایی، محمد مهدی؛ آذرآبادگان، مرتضی؛ مقاوم‌سازی تجهیزات الکترونیکی در برابر تهدیدات الکترومغناطیسی؛ کنفرانس جنگ الکترونیک ایران، دانشگاه جامع امام حسین(ع)، (**۱۳۹۱**).

۱۲. سازمان پدافند غیرعامل کشور، دستورالعمل‌های اجرایی پدافند غیرعامل: مقابله با بحران‌های EMP در وزارت‌خانه نیرو، کد آئین‌نامه: ۱۲۰و ۱۱۹- ۲۱۲۳، نوع دستورالعمل دوم.

13. Zimmerman, Rea; Critical infrastructure and interdependency; McGraw-Hill Homeland Security Handbook (David G. Kamien, Editor), Ch. 34; pp.523-545; New York; (**2006**).
14. Peerenboom, James P. and Fisher, Ronald E.; Analyzing cross-sector interdependencies; Proceeding of 40th Hawaii International Conference on System Sciences; pp.112-121; (**2007**).
15. Zimmerman, Rea; Decision making and the vulnerability of interdependent critical infrastructure; IEEE International Conference on Systems, Man and Cybernetics; Vol.5; pp.4059-4063; (**2004**).
16. Johnsson, Jonas; Risk and Vulnerability analysis of interdependent technical infrastructures: Addressing Socio-Technical Systems; PH.D. Dissertation, Department of Measurement Technology and Industrial Electrical Engineering, Lund University, Sweden; (**2010**).
17. Ezell, Barry C.; Infrastructure Vulnerability assessment model (I-VAM), Risk Analysis; Vol.27; No.3; pp.571-583; (**2007**).
18. Amin, Massud; Security Changes for the electricity infrastructure; Computer; Vol.35; pp.8-10; (**2002**).
19. Physical vulnerability of electric systems to natural disasters and sabotage, Tech. Rep. OTA-E-453; US Congress, Office of Technology Assessment; Washington; DC; (**1990**).
20. Hu, Xiaofeng, et al; Modeling of Attacking and Defending Strategies in Situations with Intentional Threats; Proceedings of the 9th International ISCRAM Conference – Vancouver; Canada; (**2012**).
21. Bompard, Ettore, et al; Risk assessment of malicious attacks against power systems; IEEE Transaction on Systems, Man, and Cybernetics; vol. 39; No. 5; pp. 1074-1085; (**2009**).
22. Sierla, S.A. et al; Security risk analysis for smart grid automation; IEEE 23rd International Symposium on Industrial Electronics (ISIE); pp. 1737 – 1744; (**2014**).
23. Koc, Yaku, et al; Structural vulnerability assessment of electric power grids; IEEE 11th International Conference on Networking, Sensing and Control (ICNSC); pp. 386 – 391; (**2014**).
24. Jian, Zhou, et al; Electric Grid Vulnerability Assessment under Attack-Defense Scenario Based on Game Theory; IEEE PES Asia-Pacific on Power and Energy Engineering Conference (APPEEC); pp. 1-5; (**2013**).
25. Zhu, Yihai, et al; Risk-aware vulnerability analysis of electric grids from attacker's perspective; IEEE PES on Innovative Smart Grid Technologies (ISGT); pp. 1-6; (**2013**).
26. Hasse, peter; Overvoltage Protection of Low Voltage Systems; institution of Engineering and technology; second edition; Vol. 33; pp.2,43,67; (**2008**).
27. Radasky, William A.; Introduction to the Special Issue on High-Altitude Electromagnetic Pulse (HEMP); IEEE Transactions on Electromagnetic Compatibility; vol.55; No.3; pp. 410-411; (**2013**).
28. Kopp, C.; The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction; http://www.globalsecurity.org/military/library/report/apjemp.htm
29. Cheldavi, Ahmad, and Danaei, Mohammad.M.; Capacitive Flux Compression Generator; Journal of IJE Transaction A: Basis; Vol.16; No.4; pp.337-342; (**2003**).
30. IEC 61000-2-9; Electromagnetic compatibility (EMC) – Part 2: Environment – Section 9: Description of HEMP environment – Radiated disturbance; (1998-**2002**).
31. Eng, C.D.; Development of the Time Dependence of the Nuclear (E1) HEMP Electric Field; IEEE Transactions on Electromagnetic Compatibility; vol.53; No.3; pp.737-748; (**2011**).
32. IEC 61000 -1-5; Electromagnetic compatibility (EMC) - part 1: High power electromagnetic (HPEM) effects on civilian systems; (**2004**).
33. Lovetri, J. et al; Microwave interaction with a personal computer: experiment and modeling; Proc. of the 13th Int. Zurich Symp. On EMC; Zurich, Switzerland; pp. 203–206; (**1999**).
34. Vijayaraghavan, G., et al; Practical grounding, bonding, shielding and surge protection; Elsevie;pp.193-206; (**2004**).
35. Ogunsola, Ade, et al; Modeling shielding properties of concrete; 17th International Zurich Symposium on Electromagnetic Compatibility; Singapore; pp.34-37; (**2006**).

Power System Modeling and Simulation of Power Systems with Passive Defense Approachagainst Electromagnetic Attacks

R. Azadehdel[1]
H. Monsef[2]
H. Dehghani[3]

Abstract

Key infrastructures especially electrical power systems, from their inception to the present, have been an integral part of life in human society; therefore, have great potential to put at risk by threatfactors; for this reason, the security of their systems is tied to the national security of the overall community and trying to maintain this securityis of utmost importance to senior managers and decision makers. The factors threatening power systems include natural and human disasters. The main purpose of this paper will be modeling and simulating power systems based on passive defense against electromagnetic threats, and studying measures to enhance safety and security strategies against these types of threats.

Threat detectionby determining their occurrence scenarios in which they provide guidelines to protect against interference or degradation in the power system to maintain business processes, assets and related resources is necessary. In this paper,the purpose ofpower system is a high voltage substation with a control room and the threats to that are High Altitude EMP (HEMP) and High Power EMP (HPEM). Since the major components of the power system in this paper, includeelectronic cabinets, control racks and concrete structures are for a high voltage substation, and therefore; the Shielding Effectiveness (SE) in each of them will be examined using simulation. The resultsshow thatwiderectangular windows mounted in the said chambers structures and racks havethe lowest and the circular windows have the highestelectromagnetic shielding. Simulation results for substations structure show that the concrete structures have almost no protection against threats, but when used in reinforced concrete structure, the parameter SE at low frequencies will be improved. A review of the protective measures, based on the results of previous studies and conducted simulations, constitute provisions of the final section of this paper.

Key Words: *Power System, Threats, HEMP, HPEM, Shielding Effectiveness*

1- MS Candidate of electricity & Electronics, Islamic Azad University, South Tehran Branch (Azadehdelir@yahoo.com)- Writer-in-Charge
2- Associate Professor and Academic Member of Malek Ashtar Technological University
3- Assistant Professor and Academic Member of Malek Ashtar Technological University