فصلنامه علمی-ترویجی پدافند غیرعامل

سال سوم، شماره ۲، تابستان ۱۳۹۱، (پیاپی ۱۰): صص ۲۳-۲۸

تهدیدات الکترومغناطیسی پر قدرت برای سامانه‌های الکترونیکی و روش‌های مقابله با آن‌ها

سید رسول میرمطهری[۱]

ضرغام رستمی[۲]

علی طالبی[۳]

زین‌العابدین نوروزی[۲]

تاریخ دریافت: ۹۱/۰۲/۲۰

تاریخ پذیرش: ۹۱/۰۴/۲۷

چکیده

سلاح تولید انرژی الکترومغناطیس پر قدرت (HPM)، نوعی فناوری است که تهدیدی علیه سامانه‌های الکترونیکی به‌حساب می‌آید. با تولید پالس HPM، انرژی زیادی با قدرت نفوذ بالا در زمان کوتاه ایجاد و باعث برقراری یک جریان ناپایدار با ولتاژ بالا می‌گردد که قطعات الکترونیکی سامانه‌ها، مانند نیمه‌هادی‌ها را از بین می‌برد. در این مقاله ابتدا روش‌های تولید انرژی الکترومغناطیس پر قدرت را بیان کرده و یک معرفی اجمالی از این سلاح، ساختار و روش تولید آن ارائه شده است. پارامترهای سلاح مایکروویو پرقدرت و چگونگی نفوذ آن به درون سامانه‌های الکترونیکی را بیان کرده و تأثیر آن را بر این سامانه‌ها بررسی خواهیم کرد. در پایان چگونگی حفاظت از سامانه‌ها با توجه به نوع آسیب‌پذیری در مقابل پالس‌های انرژی توان بالا، بررسی و راه‌کارهای مناسب برای حفاظت ارائه شده است.

کلیدواژه‌ها: مایکروویو پر قدرت، سلاح HPM، حفاظت الکترومغناطیسی، تزویج الکترومغناطیسی

۱- دانش‌آموخته کارشناسی ارشد مهندسی پدافند غیرعامل- گرایش آفا (CCD) rmir321@ gmail.com - نویسنده مسئول

۲- استادیار و عضو هیئت علمی دانشکده فناوری اطلاعات و ارتباطات- دانشگاه جامع امام حسین(ع)

۳- دانش‌آموخته کارشناسی ارشد مهندسی پدافند غیرعامل- گرایش آفا (CCD)

۱- مقدمه

با پیشرفت تکنولوژی، زندگی روزمره ما بیش از پیش به تجهیزات الکترونیکی وابسته شده است. تجهیزات الکترونیک در بیمارستان‌ها، شبکه‌های مخابراتی، بانک‌ها و مؤسسات بزرگ، نیروهای نظامی و... مورد استفاده قرار گرفته و اگر روزی در اثر یک تهدید الکترومغناطس پر قدرت از کار بیفتند عملاً زندگی ما فلج می‌شود. پالس‌های الکترومغناطیسی پرقدرت، تهدیدی هستند که می‌توانند سامانه‌های الکترونیکی را مورد هدف قرار داده و آسیب‌های بسیار جدی روی سامانه‌های الکترونیکی ایجاد کنند. برای اینکه بدانیم این پالس‌ها چگونه به سامانه‌های الکترونیکی آسیب می‌رسانند لازم است ویژگی‌های پالس‌های الکترومغناطیس توان بالا را بدانیم و نحوهٔ اثر آن‌ها را روی تجهیزات شناسایی کنیم.

در این تحقیق ابتدا سلاح HPM[1] را معرفی کرده و سپس روش‌های مقابله با این سلاح و حفاظت از تجهیزات را مورد بررسی قرار داده‌ایم.

۲- سلاح‌های مایکروویو پر قدرت

انرژی الکترومغناطیسی پر قدرت به دو روش انفجار هسته‌ای و غیرهسته‌ای یا گسیل مایکروویو تقسیم می‌شوند. در انفجار هسته‌ای، پالس الکترومغناطیسی ارتفاع بالا (HEMP)[2]، یک میدان انرژی الکترومغناطیسی آنی در اتمسفر بر اثر انفجار هسته‌ای به‌وجود آورده و این امواج روی تجهیزات الکترونیکی می‌توانند آسیب جدی برسانند [۱].

اما سلاح دوم، انرژی الکترومغناطیسی مایکروویو توان بالا (HPM) است که موضوع بحث ما می‌باشد و توسط یک وسیله الکتریکی خاص با قدرت باطری یا واکنش شیمیایی، یک موج مایکروویو شدید ایجاد می‌نماید.

۳- معرفی سلاح HPM

سلاح HPM از نظر اندازه کوچک و با تکنولوژی خیلی پایین‌تری قابل دسترسی می‌باشد که می‌تواند یک میدان بسیار قوی هدایت شده انرژی مایکروویوی ایجاد نماید که برای حمله به یک هدف طراحی شده‌اند و این سلاح در محدوده فرکانسی ۳۰۰MHZ تا ۳۰۰GHZ مطابق با طول موج‌هایی از ۱m تا ۱mm می‌باشد، که قادر است حداکثر توانی بیش از ۱۰۰MW تولید نماید. به‌طور کلی سلاح HPM جهت تخریب فیزیکی سیستم‌های الکترونیکی، جمینگ، کورکردن مایکروویوی فرستنده‌های رادیویی و رادارهای فریب و اختلال در حافظه یا بخش منطقی سیستم‌های الکترونیکی به‌کار می‌رود.[۲]

۴- ساختار سلاح‌های HPM

یک سیستم مایکروویوی توان بالا (HPM) از بخش‌های مختلفی تشکیل شده‌است [۳]:

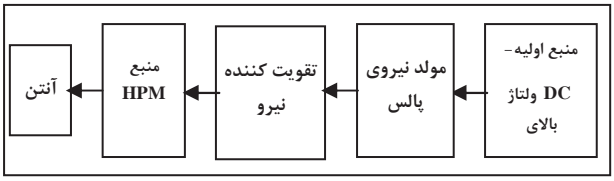
۱- منبع تغذیه اولیه: از یک باطری، ژنراتور الکتریکی و... با توان پایین و پالس طولانی استفاده می‌شود.

۲- منبع تغذیه پالس: که انرژی توان پایین را ذخیره نموده و در زمان بسیار کوتاه یک پالس با توان بالا تولید می‌نماید.

۳- تقویت‌کننده انرژی: پالس تولید شده را با توجه به نیاز منبع HPM به ولتاژ، جریان، زمان خیز و شکل تنظیم می‌نماید.

۴- منبع HPM: پالس تقویت شده را به موج الکترومغناطیسی برای رهاسازی روی هدف منتقل می‌کند.

۵- آنتن: برای انتشار پالس HPM متمرکز نمودن روی هدف [۳].



شکل ۱- طرح کلی منبع HPM

۵- پارامترهای مشخصه پالس HPM

با توجه به مشخصات پالس تولید شده از سلاح HPM که شامل زمان اوج، شدت میدان الکتریکی و فرکانس که از مشخصه‌های پالس تولید شده از سلاح HPM هستند، مقدار تخریب در یک سامانه الکترونیکی را تعیین می‌کنند [۴].

فاصله نقطه انفجار از سامانه و هم‌چنین تدابیر حفاظتی آن هم در میزان تخریب نقش دارد.

ارتباط پارامترهای موج با اثرشان در یک مدار به‌صورت زیر می‌باشد.

- زمان اوج: یک فاکتور مهم برای حفاظت سامانه‌ها به‌شمار می‌رود؛ به‌طوری که کمتر از چند هزارم ثانیه باشد، مدارات داخل به شدت آسیب خواهند دید.
- شدت میدان الکتریکی: جریان القاء شده در مدارات الکترونیکی، به شدت میدان الکتریکی بستگی دارد و با ورود انرژی به درون مدارات آسیب دیدگی به‌وجود خواهد آمد.
- فرکانس: اگر فرکانس پالس سلاح HPM با فرکانس مدارات سامانه مورد نظر یکی شوند بیشترین آسیب را به سامانه خواهد زد [۴].

۶- نفوذ سلاح HPM به درون سامانه

هنگامی که پرتو HPM به طرف سامانه انتشار می‌یابد به دو

1- High Power Microwaves
2- High Altitude Electromagnetic Pulse

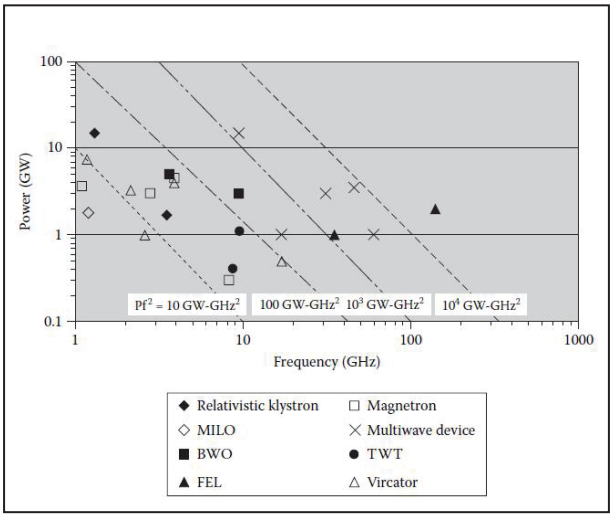
صورت front door و Back door می‌تواند آسیب برساند [۴].
Front door: به زبان خیلی ساده از طریق مسیرهای خارجی مثل آنتن نفوذ می‌کنند که به روش تزویج (جفت شدگی) به نیمه رساناهای RF در گیرنده و فرستنده آسیب می‌رسانند. [۵، ۶].
Back door: نفوذ امواج یا پالس از طریق روزنه‌ها یا شکاف‌ها یا کابل های سیستم که به منابع تغذیه و ابزارهای دریافت و ارسال داده‌ها آسیب می‌رساند [۵،۴].

۷- اثرات سلاح HPM بر روی سامانه‌ها

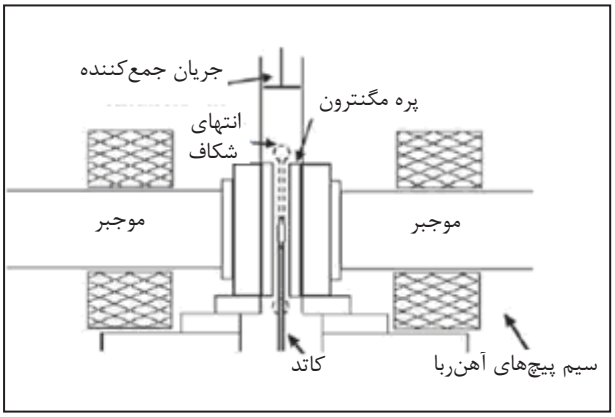
هنگامی که پالس ایجاد شده از سلاح HPM به یک سامانه می‌رسد اثرات مختلفی روی سیستم‌های الکترونیکی آن به‌وجود می‌آورد که شامل ایجاد اختلال، آشفتگی و آسیب می‌شود [۷].
ایجاد اختلال: اختلال در ردگیری، هدایت چرخه های کنترل پایگاه‌ها، اختلال در سنسورهای رادار، ارتفاع‌سنج و نیز تداخل در تصویر و صدا به‌وجود می آید که باعث از بین رفتن مأموریت‌ها می‌شود.
ایجاد آشفتگی[1]: عمل‌کرد نادرست سیستم‌های الکترونیکی باعث از دست رفتن اطلاعات مهم می‌شود که در زمان کوتاه اثر می‌گذارد.
ایجاد آسیب: از بین رفتن سیستم‌های الکترونیکی، هم از نظر سخت‌افزاری و هم از نظر نرم‌افزاری که توسط پالس قوی HPM از طریق تزویج‌های Back door یا Front door اتفاق می‌افتد.
مکانیسم آسیب اجزای سیستم‌ها می‌تواند شامل موارد زیر شود:
حرارت بیش ازحد: باعث ذوب شدن خازنها، مقاومت‌ها و... می‌شود.
ولتاژ بیش ازحد: هنگامی که ولتاژگذرای از HPM از حد آستانه سیستم مورد نظر تجاوز کند، باعث اختلال در بین اتصالات مدارها می‌شود.
تخریب مستقیم: تجهیزات الکترونیکی مانند ICها چون در ولتاژ خیلی کم و جریان حدود چند میلی‌آمپر کار می‌کنند در اثر تابش پالس HPM به علت جریان و ولتاژ بالا کاملاً می‌سوزند.

۸- مولدهای تولید HPM

قبل از اینکه منابع تولید HPM را توضیح دهیم باید دانست که منابع مایکروویو دارای اجزایی از قبیل آنتن، موجبر، دیود (آند و کاتد) می باشد. اولین منابع تولید پالس HPM، مگنترون و کلایسترون و منابع جدید تولید HPM نوسانگر کاتد مجازی (ویرکتیور)- ژایروترون، لیزر الکترون آزاد و مولد پرتو پلاسمایی می‌باشد [۲].
مگنترون نسبیتی، یکی از منابع مایکروویو توان بالا (در باندهای L و X) می‌باشد. این منابع قادرند توان‌هایی از مرتبه چند گیگاوات در فرکانس پایین و توان هایی از مرتبه چند صدمگا وات در فرکانس های بالا تولید کنند و بازده کمتری نسبت به مگنترون غیر نسبیتی دارند. در مگنترون نسبیتی پالس های با دوره تناوب KHz تولید می شود. یکی از پارامترهای اساسی در تولید مایکروویو، به‌وسیله مگنترون نسبیتی جریانی (حدود چند کیلو آمپر) است که از آند می‌گذرد [۸،۳].



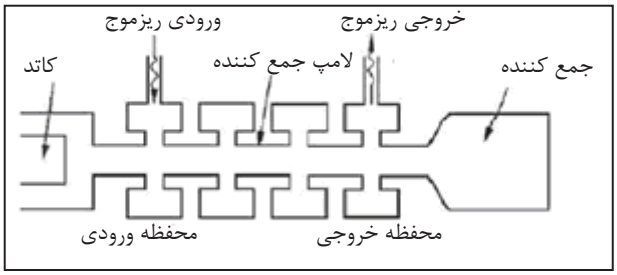
شکل ۲- طبقه‌بندی انواع سلاح‌های مایکروویو توان بالا از نظر توان



شکل ۳- مگنترون نسبیتی

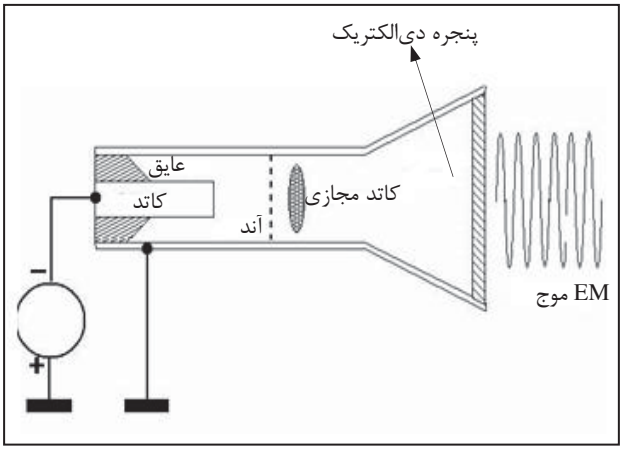
کلایسترون: با استفاده از محفظه‌های تشدید در طول بیم الکترونی می‌تواند مایکروویو توان بالا تولید کند و از اجزاء بیم الکترونیکی، محفظه تشدید و موجبر، کوپلر خروجی و ورودی برای مایکروویو و کلکتور بیم تشکیل شده است. سیگنال مایکروویو ورودی به‌عنوان سیگنال ورودی، یک مد الکترومغناطیسی محفظه تشدید را تحریک می‌کند [۳].

1- Upset



شکل ۴- پیکربندی کلایسترون

ویرکتیـــور: مکـانیزم تولیـد مـایکروویو ویرکتیـور بـه دو روش الکترون‌های بازگشتی و نوسان کاتد مجازی می‌باشد که در شکل (۵) نشان داده شده و از اجزای آنتن، موجبر، مولد پالس و دیود (کاتـد و آند) تشکیل شده است. ویرکتیور یکی از معروف‌ترین ابزار موجـود در تولید مایکروویو می‌باشد [۹،۸].



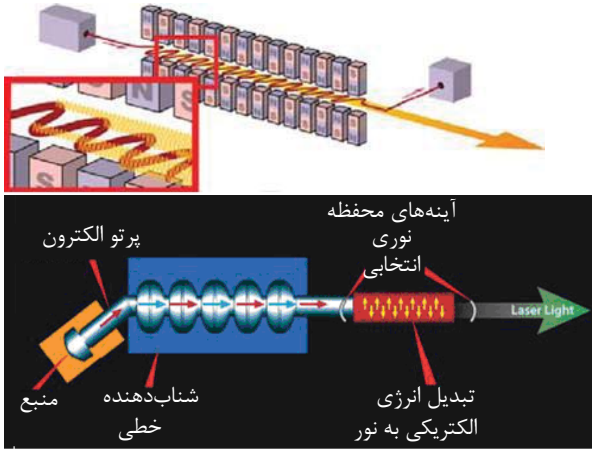
شکل ۵- شماتیک ویرکیتور

لیزر الکترون آزاد: (FEL)[1] یکی از منابع مایکروویو با ساختار پیچیده می‌باشد. این لیزر با روش تکثیر الکترومغناطیس، همدوس توان‌هـای بسیار بالایی را تولید می‌کند که بیشترین محدوده فرکانـسی را دارد. فرقی که با لیزرها دارنـد ایـن اسـت کـه در آن‌هـا الکتـرون‌هـا بـین حالت‌های انرژی در اتم برانگیخته می‌شوند ولی لیزر الکترون آزاد بـا استفاده از بیم الکترونی نسبیتی کار می‌کند [۳].

تکنولوژی FEL به‌عنوان سلاح‌های انرژی مستقیم به‌کار می‌رود.

ژایروترون: یک لامپ مایکروویو است که بـا الکتـرون خوشـه شـده با حرکت سیکلترونی در میدان قـوی مغناطیـسی مـوج میلـی‌متـری تولید مـی‌کنـد و ایـن دسـتگاه توانـایی تولیـد امـواجی بـا فرکـانس ۲۵۰GHZ- ۲۰ (مـایکروویو تـا هرتـز) را دارد. تـوان خروجـی ایـن دستگاه بین ۱۰KW تا چند گیگاوات است و ژایروترون‌ها، هم پـالس الکترومغنـاطیس و هـم مـوج پیوسـته الکترومغناطیـسی تولیـد می‌کنند [۸].

1- Free-Electron Laser



شکل ۶- شماتیک لیزر الکترون آزاد

شکل ۷- ژایروترون در فرکانس 170 GHz

جدول ۱- مشخصات سلاح‌های مایکروویو توان بالا از نظر تکنولوژی

منبع	فرکانس کار	بازده	پیچیدگی	سطح توسعه
مگنترون	1-9GHz	10-30%	پایین	بالا
ویرکیتور	3-60GHz	10-50%	متوسط به بالا	بالا
لیزر الکترون آزاد	8GHz-up	35%	بالا	متوسط به بالا
کلایسترون نسبیتی	1-11GHz	25-50%	متوسط به بالا	متوسط

۹- محافظت از سامانه‌های الکترونیکی در مقابل HPM

انتشار امواج HPM به‌صورت هدایتی و تشعشعی وارد سیستم شده و به سیستم‌ها آسیب می‌رساند.

روش‌های متنوعی برای کاهش اثر امواج روی سامانه‌ها وجود دارد که برخی از آن‌ها عمومی است و برخی دیگر برای حفاظت بیشتر و مقابله با تهدیدات HPM اتخاذ می‌شوند. روش‌های پر کاربرد و مورد توجه به‌صورت زیر می‌باشند:

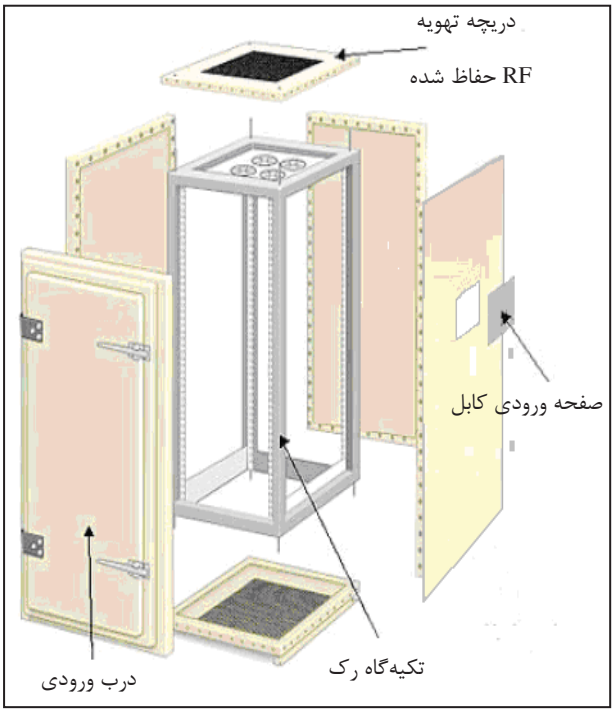
- **زمین کردن:** عملکرد صحیح سیستم ها در مقابل بار اضافی می‌باشد و علاوه بر چاه ارت از چاه ارت RF به‌منظور کاهش تداخل الکترومغناطیس استفاده می‌گردد.
- **فیلترگذاری:** یکی از مشخصات اصلی فیلترها محدود کردن پهنای باند می‌باشد که عموماً برای حفاظت سیستم‌های الکترونیک در برابر امواج الکترومغناطیس استفاده می شوند. با کاهش نویز الکترومغناطیس در سیستم ها اثرات تهدید را کاهش می‌دهند.

مشخصه یک فیلتر، به پارامترهای محدوده ولتاژ، محدوده جریان، محدوده فرکانس و... بستگی دارد.

- **بتون:** هنگام ساخت ساختمان برای سامانه‌ها، با افزودن کک و سایر انواع کربن به بتون می‌توان تا اندازه زیادی خاصیت حفاظ‌سازی را بالا برد.
- **فولاد:** با استفاده از فولاد یا شبکه های سیمی، در بتون یا آرماتور دوبل به‌کار رفته و به‌صورت یک شبکه کل رسانا انجام می‌گیرد که برای حفاظ‌سازی امواج مورد استفاده واقع می‌شود.
- **حفاظ‌گذاری**[1]: با حفاظ‌گذاری می‌توان از نفوذ میدان‌های EM به درون تجهیزات الکترونیکی یا الکتریکی جلوگیری کرد. مواد ساختاری حفاظ‌ها به‌طور کلی، مواد فلزی می‌باشند.

حفاظ‌گذاری به چند صورت قابل انجام است که در زیر به توضیح آن‌ها پرداخته‌ایم.

- ❑ حفاظ گذاری سراسری، به معنی پوشش کامل تجهیزات مورد نظر می‌باشد که همان قفس فارادی که کل تجهیزات در داخل یک محفظه قرار می‌گیرد و برای ارتباط و با انتقال داده‌ها به داخل یا خارج محفظه از فیبرهای نوری استفاده می‌شود.
- ❑ حفاظ‌گذاری کابل فلزی یا هادی که جهت حفاظت کابل هایی که از یک ناحیه به ناحیه دیگر منتقل می شود به‌کار می‌رود (مثلاً فیبرنوری).
- ❑ حفاظ‌گذاری در محل ورودی جهت دسترسی به تجهیزات اتاق شیلد یا ارتباط تجهیزات با بیرون، نصب درب یا دریچه مناسب در اتاق شیلد ضروری است.



شکل ۸- محفظه شیلد برای محافظ یک رک مخابراتی در برابر پالس‌های توان بالا

استفاده از درزگیرها، جاذب‌های هادی و قطعات حفاظتی مثل سوئیچها نیز برای مقابله با اثرات امواج مایکروویو پر قدرت ضروری است.

برای محافظت از سامانه‌ها و میزان آسیب‌پذیری آن‌ها، علاوه بر طبقه‌بندی، به کاربرد و محل قرارگیری آن نیز باید توجه کرد. یعنی از دو دستگاه مشابه در مرکز مخابرات، ممکن است یکی نقش حیاتی و دیگری با همان مشخصات نقش مهم داشته باشد. هر دو دارای آسیب‌پذیری یکسانی از لحاظ استانداردهای تست و اندازه‌گیری می‌باشند، اما با توجه به محل به‌کارگیری و اهمیت کاربری آن‌ها، نیاز به سطح حفاظت متفاوت خواهند داشت. بر همین اساس، ملاک‌های انتخاب نوع حفاظت برای سامانه‌ها به دو صورت زیر قابل طبقه‌بندی است.

۱- عمومی: طبق استانداردهای تست و اندازه‌گیری (IEC61000 و MIL-STD-461E) میزان آسیب‌پذیری هر دستگاه در برابر پالس‌های مزاحم و تداخلی، مقاوم‌سازی می‌شوند.

معیار اصلی جهت تعیین میزان حفاظت سامانه‌ها پارامتر SE[2] ضریب حفاظت می‌باشد. پارامتر کیفیت حفاظ‌سازی (SE) به‌صورت نسبت شدت میدان در حالت عدم حضور محافظ به شدت میدان در حالت وجود محافظ تعریف می‌شود. این پارامتر یک کمیت نسبی برای سنجش میزان مقاومت یک حفاظ در برابر نفوذ امواج تداخلی به‌شمار

1- Shielding

2- Shielding Effectiveness

می‌رود. به‌دلیل گستردگی این تعریف آن را به‌صورت زیر تعریف می‌نمایند.

$$SE = 20\log(E_1/E_2)$$

متغیرهای E_1 به‌ترتیب شدت میدان‌های الکتریکی بدون محافظ و E_2 در حالت حضور محافظ هستند.

۲- اختصاصی: براساس اهمیت کاربردی هر دستگاه (حیاتی، حساس و مهم) باید اقدامات حفاظتی تکمیلی، مثل حفاظ‌گذاری سراسری صورت گیرد.

با توجه به نوع کاربرد، می‌توان یک سامانه الکترونیکی را به چند صورت زیر محافظت نمود.

- ❑ فقط تجهیزات حساس را شیلد نمود.
- ❑ فقط بخش الکترونیکی سیستم را شیلد نمود.
- ❑ کل سیستم را شیلد نمود.
- ❑ یا همه موارد با هم شیلد شوند.

پس حفاظت مورد نیاز سیستم را اهمیت عمل‌کرد آن تعیین می‌کند. استفاده از قطعات حفاظتی نیز که برای مقابله با حملات پالس الکترومغناطیسی طراحی شده‌اند برای تکمیل طرح پدافندی از یک سامانهٔ الکترونیکی باید مورد توجه قرار گیرد. این موضوع از آن جهت ضروری است که محفظه‌های شیلد شده، روزنه‌ها و منفذهایی برای ورود امواج الکترومغناطیسی پر قدرت دارند که با قطعات محافظتی می‌توان اثر آن‌ها را به حداقل ممکن رساند.

۱۰- نتیجه‌گیری

سلاح مایکروویو پر قدرت در مقایسه با سایر سلاح‌های متعارف، توانایی بسیار بالایی برای از بین بردن قطعات الکترونیکی دارد. با گسترش این نوع تهدیدات، روش‌های مقابله‌ای به منظور حفاظت از تجهیزات الکترونیک توسعه یافته و همچنین تکنولوژی‌های آن نیز در حال گسترش است. استفاده از این نوع تکنیک‌های پدافندی برای مقابله با تهدیدات از نظر اقتصادی بسیار پر هزینه است. با علم به اینکه قدرت تخریب این سلاح بسیار بالاست و به راحتی در دسترس خرابکاران می‌تواند قرار گیرد، دولت‌ها و صنایع خصوصی باید متقاعد شوند تا سامانه‌های حیاتی، مراکز حساس و مهم خود را در برابر حملات احتمالی آینده مقاوم سازند.

با استفاده از شبیه‌سازی، می توان بسیاری از مطالعات را بدون هزینهٔ طراحی و ساخت آزمود. با برقراری حریم زمینی و هوایی برای مراکز حیاتی کشور نیز می‌توان تا حدود زیادی از آسیب دیدن سیستم ها در مقابل این نوع تهدیدات جلوگیری به‌عمل آورد.

مراجع

1. Eileen M. Walling, "High Power Microwaves: Strategic and Operational Implications for Warfare," (Maxwell AFB AL: Air University, **2000**)
2. Benford, J. and Swegle, J., "High Power Microwaves", Artech House, Norwood, MA, (**1992**).
3. Benford, J. and Swegle, J., Schamiloglu, E. "High Power Microwaves", Book Second Edition, (**2007**).
4. Steven H. Gold, Gregory S. Nusinovich "Review of high-power microwave source research" AIP Journal, P.3945-3974, (**1997**).
5. D. J. Sullivan, "High Power Microwave Generation from a Virtual Cathode Oscillator"IEEE Trans. Nucl. Sci. NS-30, (**1983**).
6. Wilson C.; "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments" CRS Report for Congress ; order code RL32544; (**2008**).
7. Kopp C.; Pose R.; "The Impact of Electromagnetic Radiation Considerations on Computer System Architecture"; Monash University ; AUSTRALIA
8. LOVETRI, J., WILBERS, ATM. and ZWAMBORN, APM. Microwave Interaction with a Personal Computer: Experiment and Modeling. Proceedings of the (**1999**) Zurich EMC Symposium.
9. Kopp C.; Pose R.; "The Impact of Electromagnetic Radiation Considerations on Computer System Architecture"; Monash University ; AUSTRALIA

High Power Electromagnetic (HPM) Threats against Electronic Systems and Their Countermeasures

S. R. Mir Motahari[1]

Z. Rostami[2]

A. Talebi[3]

Z. Norouzi[2]

Abstract

The high power electromagnetic weapon (HPM) is the technology that is considered a threat to electronic systems. By producing HPM pulse, an enormous energy with high penetrating power in is released a short time which causes an unstable current with high voltage to be established which in turn destroys the electronic parts of systems such as semi-conductors. This article first explains methods of producing high power electromagnetic energy and then a brief introduction of this weapon along with its structure and the way it is produced, is presented. The parameters of the high power electromagnetic weapon and how it can penetrate the electronic systems are further expressed and its effect on these systems is reviewed, as well. Finally, measures taken to protect these systems, taking into account the kind of vulnerability against high power energy pulses, are also reviewed and the appropriate solutions are further presented.

Key Words: *High Power Microwave, HPM Weapon, Electromagnetic Protection, Electromagnetic injection*

1- MS in Passive Defense Engineering, CCD Major, Writer in Charge (Email: rmir321@ gmail.com)
2- Assistant Professor and Academic Member of the Faculty of ICT, Imam Hossein Comprehensive University (Pbh)
3- MS in Passive Defense Engineering, CCD Major, Imam Hossein Comprehensive University (Pbh)