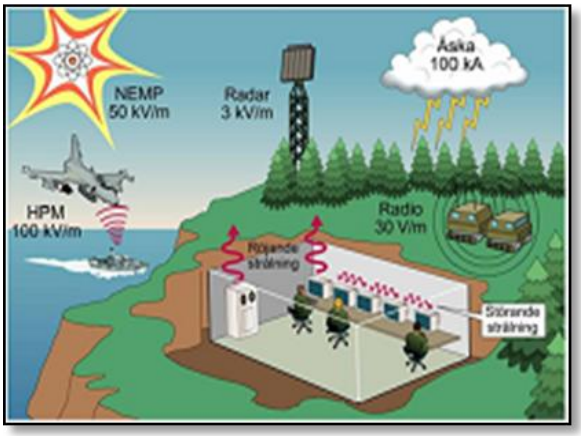
به نام خدا

پدافند غیر عامل در حوزه تهدیدات الکترومغناطیسی



فهرست

مقدمه

گسترش روزافزون سیستم‌ها و تجهیزات الکتریکی و الکترونیکی، همچنین وابستگی بسیاری از خدمات و ارتباطات دنیای امروز به این قطعات، حساسیت نسبت به حفظ ایمنی و پایداری این قبیل تجهیزات را افزایش داده است.

«تهدیدات الکترومغناطیسی» که موضوع اصلی حفاظت الکترومغناطیس می باشد؛ توسط دشمن خارجی و یا ستون پنجم، در زمان جنگ و صلح می‌تواند بوسیله سلاح الکترومغناطیسی از نوع بمب و یا سیستم های سیار کوچک در حد یک وانت یا کامیون، سرویس های یک سازمان حیاتی را هدف قرار داده و مختل نماید[۱].

هدف در اینجا، آشنایی اولیه با اصول و دستورالعمل های حفاظت الکترومغناطیسی و آموزش می‌باشد؛ با انجام دستورالعمل‌های حفاظت الکترومغناطیس می توان علاوه بر تهدیدات مذکور،اثرات ناشی از مخاطرات دیگری مانند امواج هدایتی و انتشاری ناشی از رعد و برق، ژنراتورهای برق، سیگنال سیستم های مخابراتی و... را نیز به حداقل رساند.

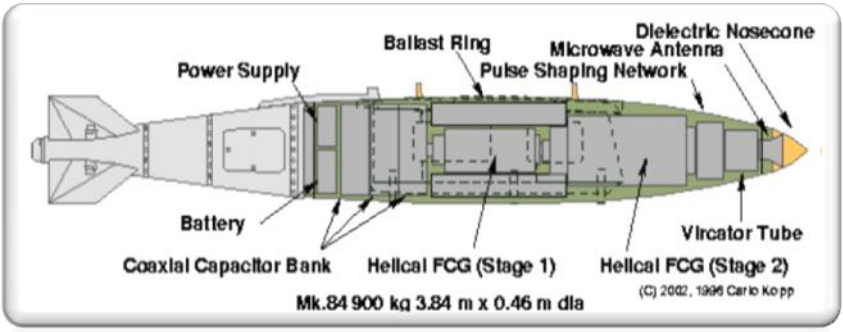
---

[۱] طیف فرکانسی تهدیدات طبیعی و ناخواسته محدودتر از طیف تهدیدات الکترومغناطیسی است. بنابراین حفاظت در مقابل سلاح الکترومغناطیسی، سایر موارد را نیز پوشش می دهد.

فصل ۱ – تهدیدات الکترومغناطیسی

تهدید الکترومغناطیسی عبارت است از تولید امواج الکترومغناطیسی مخرب که از طریق یک سلاح الکترومغناطیسی ایجاد می شود. این امواج به صورت پالس های ضربه ای بوده و دارای انرژی زیادی می باشد. میدان الکترومغناطیسی حاصل، هزاران ولت را به صورت لحظه ای بر کلیه رساناهای موجود، نظیر سیم‌ها، مدارات و لوازم الکتریکی و الکترونیکی القاء می نماید. این پالس باعث سوزاندن و یا مختل کردن اتصالات نیمه هادی و در محدوده وسیع تر ایجاد اختلال در سیستم های الکترونیکی و ارتباطی می گردد. بحران پالس الکترومغناطیسی در دسته بندی سلاح های غیر کشنده قرار می گیرد و به صورت پرتابه ای (یک بار مصرف) و یا ثابت و سیار (استفاده مداوم) – نمایش داده شده در شکل‌ها– مورد استفاده قرار می گیرد. شایان ذکر است انفجارات اتمی نیز چنین پالسی را در محدوده های جغرافیایی وسیع تری ایجاد می کنند. این تسلیحات در فرکانس های چند هرتز تا چند گیگا هرتز توان تولید پالس های قوی در حدود چند ده کیلو ولت بر متر و یا چند گیگا وات را دارند.

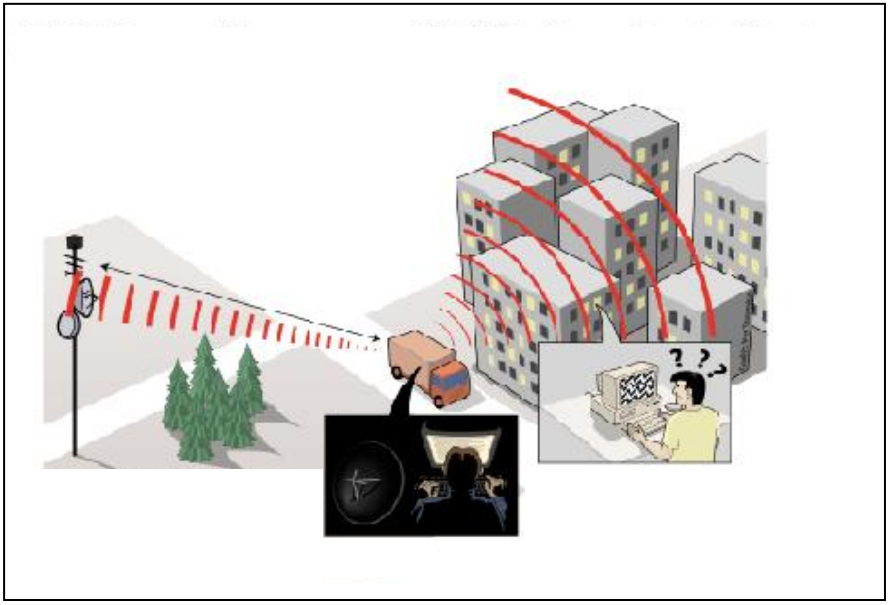
۱- تسلیحات الکترومغناطیسی به صورت پرتابه ای



یک نمونه تسلیحات الکترومغناطیسی بصورت موشک

نحوه عملکرد بمب الکترومغناطیسی در یک منطقه شهری

۲- تسلیحات الکترومغناطیسی بصورت ایستگاه های ثابت و متحرک



تسلیحات الکترومغناطیسی بصورت ایستگاه متحرک

فصل ۲ – آسیب پذیری در اثر بحران الکترومغناطیسی

بطور کلی تجهیزات الکتریکی و الکترونیکی در اثر بحران الکترومغناطیسی دچار دو نوع آسیب می شوند:

- آسیب گذرا :

این آسیب درسیستم های دیجیتال رخ می دهد و خطای بیت درهنگام ارسال یا پردازش اطلاعات نامیده می شود. آسیب گذرا موجب اعلام پیام خطا، عملکرد اشتباه و در بدترین شرایط راه اندازی مجدد[۱] سیستم ها می گردد.

- آسیب دائمی:

این آسیب شامل از کار افتادن و سوختن المانها و قطعات پردازشی و کنترلی(آنالوگ ودیجیتال) می باشد.
عدم حفاظت الکترومغناطیسی ویا عدم کفایت حفاظت تجهیزات مرتبط، آنها را به نقاط آسیب پذیر سیستم تبدیل می کند. این تجهیزات عبارتند از :
۱- تجهیزات الکترونیکی، مخابراتی و ارتباطی
۲- تجهیزات کنترلی ، اعلام خطر و هشدار

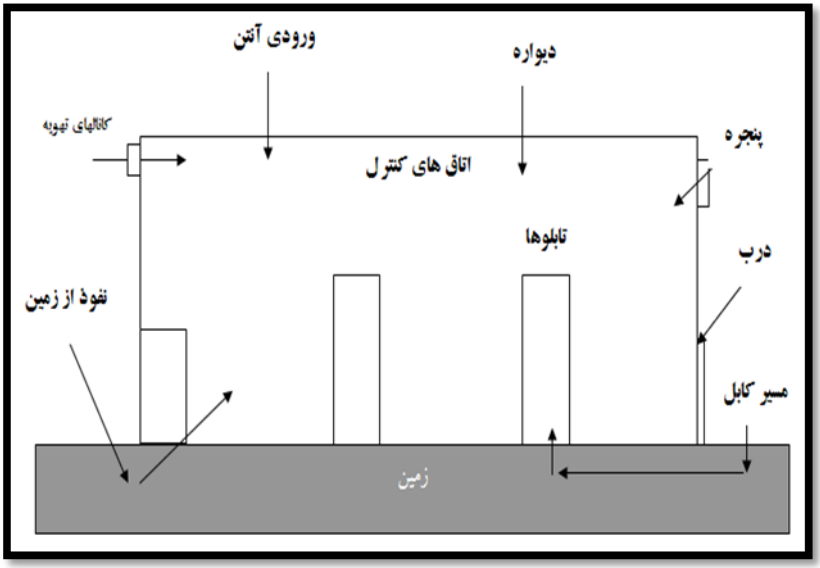
---

[۱] Reset

۳- انواع پردازنده ها، رایانه ها و سرورها

۴- منابع تغذیه مستقیم[۱] و متناوب[۲]

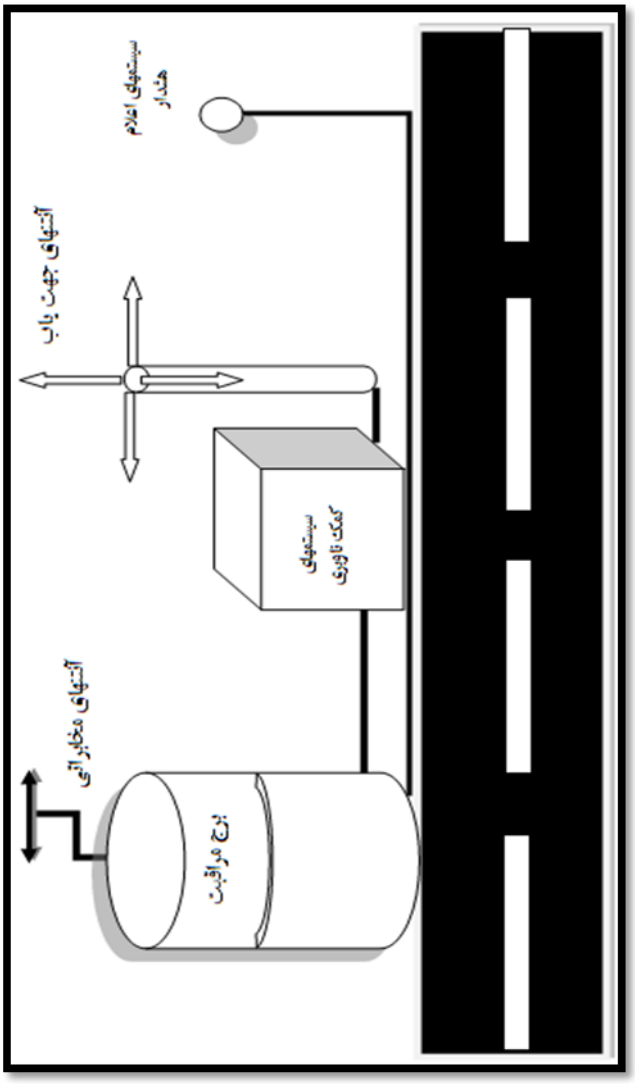
نفوذ پالس به این تجهیزات می تواند از طریق بدنه یا دیواره، روزنه یا شکاف و کابل ورودی/خروجی باشد. مدل کلی نفوذ پالس الکترومغناطیسی به تجهیزات، در شکل، نمایش داده شده است.



مدل کلی نفوذ پالس الکترومغناطیسی(محیط داخل)

[۱] DC

[۲] AC



مدل کلی نفوذ پالس الکترومغناطیسی در یک فرودگاه (محیط بیرون)

فصل ۳ – راهبرد های حفاظتی و سطوح مقاوم سازی

سه راهبرد حفاظتی برای سیستم‌ها، تجهیزات، ساختارها و فرایندهای اجرایی فعالیت های آسیب‌پذیر و تأسیسات دربرابر بحران الکترومغناطیسی پیشنهاد می شود که عبارتند از:

۱- راهبرد حفاظتی اول

در این راهبرد، کل فرآیند تولید و اجرای فعالیت های مهم، حفاظت می گردد. همچنین تجهیزات و ساختارهای مورد نیاز برای ادامه فعالیت در شرایط وقوع بحران مقاوم می شوند.

۲- راهبرد حفاظتی دوم

در این راهبرد، روند تولید و اجرای فعالیت های مهم، حفاظت می‌گردند و تنها تجهیزات ضروری محافظت می شوند.

۳- راهبرد حفاظتی سوم

در این راهبرد، سیستم ها و تجهیزات پشتیبان تولید، حفاظت می شوند تا پس از وقوع بحران بتوان مجددا سیستم ها و تجهیزات مورد نیاز را راه اندازی نمود.

به منظور دستیابی به هریک از راهبردهای حفاظتی مورد نیاز، رعایت سطوح مقاوم سازی در محدوده فرکانسی چند مگاهرتز تا ۱۰ گیگاهرتز ضروری است. این سطوح مقاوم سازی عبارتند از :

- سطح اول مقاوم سازی

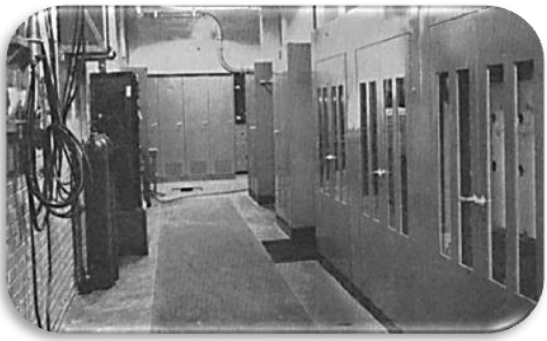
مقدار این سطح از حفاظت در حدود ۸۰ الی ۱۰۰ دسی بل می باشد.

- سطح دوم مقاوم سازی

مقدار این سطح از حفاظت در حدود ۶۰ الی ۸۰ دسی بل می باشد.

- سطح سوم مقاوم سازی

این سطح از حفاظت در حدود ۴۰ الی ۶۰ دسی‌بل می باشد.



فصل ۴ – دستورالعمل های پدافند غیر عامل

❖ دستورالعمل های قبل از بحران

رعایت یک سری از نکات و پیاده سازی آنها در شرایط صلح و قبل از وقوع بحران، به صورت موثری می تواند هزینه های ناشی از آسیب دیدگی تجهیزات در شرایط وقوع بحران را کاهش دهد. نکات مورد نظر شامل موارد ذیل می باشد:

- برنامه ریزی استراتژیک و تدوین دستورالعمل‌های مدیریتی: این برنامه ریزی‌ها به تدوین دستورالعمل های مدیریتی و اجرایی منجر خواهد شد. برخی از نکات مهم که در این دستورالعمل ها باید رعایت شوند عبارتند از:
  - توزیع افراد بر اساس تخصص فنی مورد نیاز جهت تعمیر، نگهداری و پشتیبانی برای هر بخش صورت گرفته شود.
  - دفترچه های تعمیر و راه‌اندازی سیستم های آسیب‌پذیر مربوط به هربخش با استفاده از تیم خبره فنی آماده شود.
  - توجه دقیق به دستورالعمل راه‌اندازی سیستم ها و تجهیزات هر بخش در شرایط وقوع بحران و پس از بحران صورت گیرد.

- در صورتی که توسعه سایت مد نظر باشد، پیاده سازی و اجرای تجهیزات جدید باید منطبق با اصول پدافند غیر عامل در حوزه بحران الکترومغناطیسی باشد.

- ارزیابی آسیب شناسی، مقاوم سازی و دستورالعمل های نگهداری:

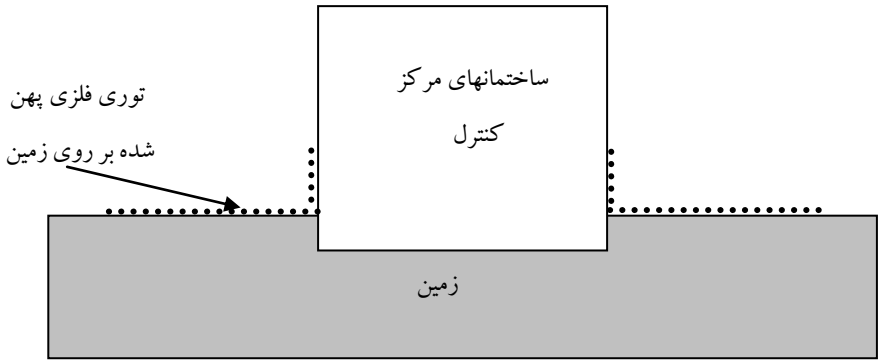
این اقدام که با همراهی افراد متخصص در آسیب شناسی و افراد مجری بخش باید انجام شود، منجر به تهیه چک لیست اولیه از لحاظ نوع آسیب، میزان آسیب پذیری، راهکار رفع آسیب(تعمیر، تعویض یا خاموش و روشن نمودن مجدد)، زمان مورد نیاز جهت راه اندازی و هزینه رفع آسیب خواهد شد.

- مقاوم سازی الکترومغناطیسی ساختار ها و تجهیزات:

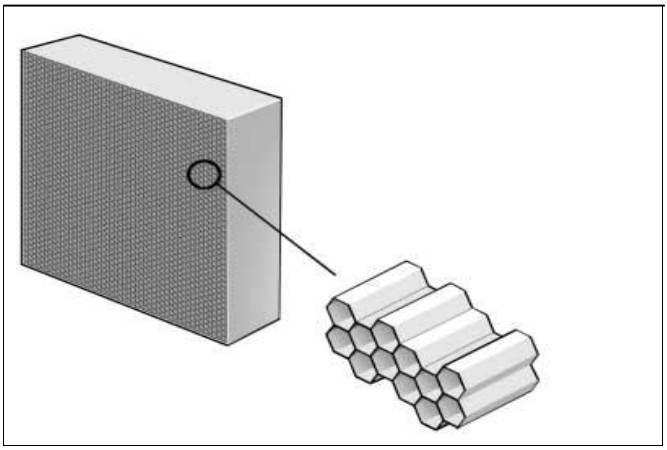
این اقدامات به دو گروه عمومی و اختصاصی تقسیم می گردند.

گروه عمومی: اقداماتی که در مورد کلیه سطوح مقاوم سازی لازم الاجرا هستند، که به ترتیب اولویت عبارتند از:

- دیواره های محافظ
- درب های محافظ
- مدارات محافظت کننده
- فیلترهای کانال تهویه
- اتصال زمین مناسب
- دکلها و آنتن ها و ...



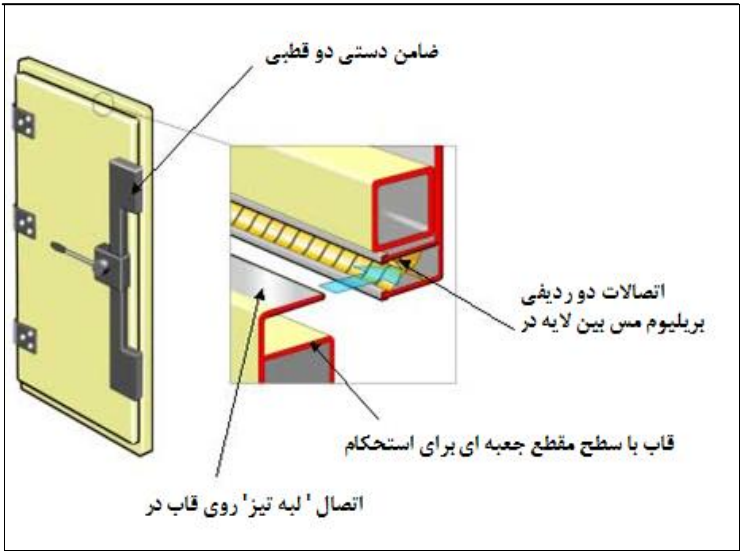
نصب توری روی زمین در اطراف ساختمان به عنوان یک راهکار
حفاظتی عمومی



تصویر نمونه از دریچه های لانه زنبوری به منظور استفاده در بخشهای ورودی تهویه هوا
برای تضعیف امواج

گروه اختصاصی: اقدامات خاص که برای رسیدن به سطوح اول، دوم یا سوم مقاوم سازی لازم الاجرا هستند؛ مانند: سطح دوم شیلد دیواره، استفاده از توری و شیشه هادی در پنجره و ...

چند نمونه از اقدامات حفاظتی گروه اختصاصی در شکل های بعد نشان داده شده است.



یک نمونه از نحوه نصب درزگیر به منظور استفاده در درب ورودی

یک نمونه محفظه طراحی و ساخته شده از جنس آلومینیوم با ضخامت حدود ۱ تا ۱.۵ میلی متر برای حفاظت تجهیزات حساس

نمایش کیف حافظ با ابعاد متوسط جهت حفاظت موبایل، لپ تاپ، هارد دیسک و ...

شبکه هشدار دهندگی:

سنسورهای هشدار دهنده پالس‌های الکترومغناطیسی می توانند هرگونه مخاطره الکترومغناطیسی در باند پایین فرکانسی و مایکروویو را اعلام نمایند. این هشدار برای شروع آماده باش و عملیات پدافندی لازم است.

هشداردهنده‌ها می‌بایست از نظر انتشار امواج الکترومغناطیسی و فضای سیستم‌های خودی در محل‌های مناسبی تعبیه شوند.

یک نمونه هشدار دهنده بحران الکترومغناطیسی

- آموزش بصورت توسعه ای و کلاسیک:

مفاهیم بحران الکترومغناطیسی، منابع بحران، آسیب پذیری‌ها و راهکارهای مقاوم سازی در سطوح کارشناسی و مدیریتی می بایست به کاربران مرتبط آموزش داده شود. این آموزش ها می تواند بصورت کارگاه های آموزشی کوتاه مدت برای مدیران و دوره های میان مدت برای کارشناسان فنی برگزار گردد.

بروشورها و دفترچه های حاوی اطلاعات کلیدی که دارای نکات مفید در خصوص اصول پدافند غیرعامل در حوزه مورد نظر می باشند بایستی تهیه و در اختیار افراد مسئول هر بخش قرار داده شود.

همچنین می بایست تمهیداتی جهت آگاه نمودن تیم های تخصصی و ارائه آموزش های مستمر جهت راه اندازی مجدد بخش های آسیب پذیر با کمترین هزینه در شرایط وقوع بحران و پس از بحران اندیشیده شود.

موضوعات اصلی این آموزش ها شامل موارد زیر می باشد:

- آموزش نصب و قرائت هشدار دهنده ها
- آزمایش دوره ای چاه و اتصال زمین
- آزمایش دوره ای اتصالات

❖ دستورالعمل های حین وقوع بحران

این دستورالعمل‌ها می بایست از لحظه وقوع بحران الکترومغناطیسی بکار گرفته شود. فعال شدن سیستم هشداردهنده همراه با وقوع اختلال در عملکرد سیستم ها و تجهیزات الکترونیکی، کنترلی و مخابراتی حساس سایت ها از جمله نشانه های بروز چنین بحران هایی می باشد. اختلال در عملکرد، سبب وقوع حوادث غیر قابل پیش بینی برای سیستم ها و تجهیزات «مقاوم نشده» می گردد و تا زمانیکه سیستم ها به حالت طبیعی بازنگردند احتمال وقوع هرگونه حادثه وجود دارد.

در شرایط وقوع تهدید الکترومغناطیسی، موارد اساسی ذیل می بایست در اسرع وقت توسط کارشناسان و مدیران مربوطه انجام گیرد:

۱- به علائم هشداردهنده ها توجه شود:

در زمان بحران، هنگامی که بخش های فرآیندی و عملکردی تجهیزات الکترونیکی و ... دچار مشکل شده اند، اولین اقدام، بررسی وضعیت سیستم هشداردهنده می باشد. اگر این سیستم، فعال باشد(وجود اعلام خطر)، باید دستورالعمل های مربوط

به زمان بحران، اجرا شود. در غیر اینصورت باید به دستورالعمل های معمول مربوط به تعمیر و نگهداری سیستم ها و تجهیزات مراجعه نمود.

۲- صحت عملکرد گیرنده ها و بخش های مختلف که دارای دریافت کننده های داده می باشند، بررسی شود.

۳- برنامه های اجرایی و بخش های مختلف الکترونیکی وکامپیوتری بررسی شود.

۴- دستگاه هایی که قابلیت خاموش شدن دارند، خاموش شوند.

۵- سیستم‌های اطفاء حریق و عملکرد آنها بررسی شود.

❖ دستورالعمل های پس از وقوع بحران

- توجه به هشدار دهنده ها:

پس از گذر از زمان بحران، می بایست هشدار دهنده ها بررسی شده، راه اندازی مجدد یا در صورت خرابی جایگزین شوند.

- برآورد آسیب های وارده:

در صورت وقوع بحران و ایجاد اختلال در عملکرد سیستم ها و تجهیزات سایت به دلیل آسیب، مراحل ذیل باید به اجرا در آید:

- مراجعه تکنیسین بخش آسیب دیده به همراه کارشناسان فنی
- شناسایی نوع آسیب گذرا یا دائمی بوجود آمده برای بخش
- ارزیابی عملکرد المان، قطعه یا سیستم آسیب دیده با توجه به مشخصات تعریف شده برای سیستم مورد نظر[1]
- ارائه گزارش مربوط به دسته بندی سیستم ها یا قطعات آسیب دیده به همراه بیان نیازمندی ها و ضرورت ها، بمنظور برآورد آسیب جهت راه اندازی مجدد.

---

[1] محتمل ترین بخش آسیب دیده در هر سیستم، قسمت های ورودی یا خروجی(تغذیه، دیتا، مخابراتی و کامپیوترها) می باشد. این قسمتها جهت ارزیابی در اولویت اول قراردارند.

- راه اندازی مجدد سیستم ها:

بر اساس گزارش تهیه شده توسط کارشناسان فنی و نوع آسیب ایجاد شده مراحل ذیل باید اجرا شود.

- بخش های آسیب دیده به لحاظ ایجاد توقف در عملکرد کلی سیستم بایستی اولویت بندی شوند .
- با توجه به اولویت بندی صورت گرفته، نسبت به راه‌اندازی آنها اقدام شود.
- در صورتی که آسیب از نوع گذرا باشد، تغذیه سیستم قطع و وصل گردد. در این شرایط امکان راه اندازی و بازگشت به حالت عادی برای سیستم، محتمل‌خواهدبود.
- در صورت عدم بازگشت به حالت عادی، متخصصین بخش تعمیر و نگهداری با توجه به دستورالعمل های حفاظتی اقدام نمایند.
- در صورتیکه آسیب از نوع دائمی قابل مشاهده باشد، متخصصین بخش تعمیر و نگهداری با توجه به دستورالعمل های حفاظتی اقدام نمایند.

- استفاده از سیستم های پشتیبان حفاظت شده:

در شرایط وقوع بحران، امکان آسیب دیدگی برای تجهیزات حساس الکترونیکی و مخابراتی که در انبار قطعات نگهداری می شوند نیز وجود دارد. بمنظور نگهداری تجهیزات در انبار می بایست اصول مربوط به مقاوم سازی را اجرا نمود. در صورت نیاز به قطعات و تجهیزات (وجود آسیب دیدگی) جهت تعمیر یا تعویض، می بایست از قطعات و تجهیزات پشتیبان حفاظت شده استفاده نمود.

- راه اندازی مجدد فعالیت ها:

پیش از وقوع بحران، تجهیزات و سیستم های آسیب پذیری که تداوم فعالیت های اصلی وابسته به آنها می باشد، می بایست شناسایی شوند. راه اندازی مجدد فعالیت ها در دو حالت می تواند رخ دهد.

حالت اول:

این حالت مربوط به دسته ای از فعالیت ها می باشد که تنها با استفاده از نیروی انسانی و سیستم های ارتباطی[۱] می توانند تحت شرایطی مجدد راه اندازی شوند.

[۱] سیستم های ارتباطی باید همانند سیستم های پشتیبان حفاظت شوند.

جهت راه اندازی این فعالیت ها نیازی به سیستم ها و تجهیزات نبوده و این عمل بصورت معمول در یک زمان کوتاه و با استفاده از نیروی انسانی امکان پذیر است.

حالت دوم:

در این حالت، فعالیت هایی که جهت تداوم تولید، نیاز به استفاده سیستم و تجهیزات موجود دارند، با رعایت اصول فنی سایت مورد نظر، راه اندازی مجدد می شوند.