حفاظت پشتیبان (بخش اول)

مقدمه

مقاله ای که در ادامه آورده شده ، یکی از رکن های اساسی سیستمهای حفاظتی به نام "حفاظت پشتیبان" را مورد بحث و بررسی قرار می دهد . لازم به ذکر است که این مقاله در دو بخش تنظیم گردیده که بخش اول آن در ادامه آورده شده و بخش دوم نیز به زودی ارائه خواهد گردید .

استفاده از حفاظت پشتیبان بر یک اصل ساده استوار است : استفاده از دو یا چند تجهیز ، به جای اعتماد به عملکرد یک تجهیز ! در نتیجه ، در صورت عدم عملکرد صحیح یک تجهیز ، پشتیبان آن عمل نموده و خواسته ما را از عملکرد صحیح یک سیستم برآورده خواهد نمود . استفاده از سیستمهای پشتیبان ، نقش اساسی در بالا بردن قابلیت اعتماد به سیستم حفاظتی را دارا می باشند . مسلما اثر منفی عدم عملکرد صحیح یک تجهیز حفاظتی در هنگام لزوم ، بسیار کمتر از زمانی است که دو سیستم حفاظتی به صورت همزمان به یک خطا عکس العمل نشان می دهند . در صورتی که از دو تجهیز حفاظتی با عملکرد یکسان نیز استفاده شده باشد ، این تاثیر منفی (عملکرد همزمان دو سیستم حفاظتی به صورت موازی) به مقدار بسیار زیادی کاهش خواهد یافت (مانند استفاده از دو رله دیستانس به صورت اصلی و پشتیبان) . با وجود اینکه معمولا از حفاظتهای پشتیبان محلی (Local) استفاده میشود ، حفاظتهای پشتیبان دوردست (Remote) نیز در برخی سیستمها میتوانند به خوبی عملکرد حفاظتی را بهبود بخشند .

از نظر هر طراح یا کاربر سیستم حفاظتی ، اصطلاح حفاظت پشتیبان ممکن است به صورت خاصی تعریف گردد . برخی ، این سیستمها را (سیستم ۱) و (سیستم ۲) و برخی دیگر (سیستم A) و (سیستم B) و برخی دیگر (حفاظت اصلی) و(حفاظت پشتیبان) می نامند . البته نامیدن سیستمهای فوق به نام حفاظت اصلی و پشتیبان این معنی را به صورت ناخودآگاه نشان میدهد که حفاظت دوم عملا از سیستم خارج بوده و فقط در صورت معیوب شدن حفاظت اصلی به صورت پشتیبان به سیستم وارد شده و عملکرد خواهد داشت در صورتیکه همانطور که میدانیم ، در عمل ، حفاظتهای پشتیبان به اینصورت طراحی و استفاده نشده و به صورت موازی با یکدیگر و دائما در سرویس قرار دارند .

قابلیت اعتماد (Reliability) : ترکیبی از قابلیت اطمینان (Dependability) به شبکه و امنیت (Security) می باشد . توجه داشته باشید که قابلیت اعتماد (Reliability) عبارتست از عملکرد صحیح

آدرس: شیراز خیابان مشیر نو _ صندوق پستی: ۱۱۹۵-۷۳۱۳۶۵ _ کد پستی: ۱۴۷۱۵-۷۱۷۳۶ تلفن: ۴-۲۳۰۸۷۵۲-۰۷۱۱
فاکس: ۰۷۱۱-۲۳۰۸۷۵۵ Web: www.fpmc.co.ir E-mail: info@fmpc.co.ir

حفاظت در مقابل خطاها (قابلیت اطمینان : Dependability) و اطمینان از عدم عملکرد اشتباه سیستم حفاظتی در مقابل شرایط عادی شبکه (امنیت : Security) .

علل استفاده از حفاظت پشتیبان :

از حفاظت پشتیبان به دلایل متعددی استفاده میشود که برخی از آنها عبارتند از : ۱-درخواست سیستم دولتی یا بهره برداری ۲-افزایش قابلیت اطمینان ۳-افزایش رضایت مشتری ۴-پایداری بیشتر شبکه ۵-اهداف تعمیراتی

از آنجاییکه سیستم حفاظتی به طور مستقیم درآمد زا نمی باشد و فقط به منظور پیشگیری از اشکالات اتفاقی و غیر مکرر در شبکه استفاده میگردد ، میتوان آنرا شبیه به یک سیستم بیمه در نظر گرفت که از صدمه رسیدن به تجهیزات اصلی شبکه جلوگیری کرده و همچنین مدت زمان خاموشیها را کاهش میدهد . مانند تمامی سیستمهای بیمه ، میزان سود به دست آمده نسبت به هزینه انجام شده در سیستم حفاظت ، توسط مهندسان و مدیران شبکه محاسبه میگردد .

توجه داشته باشید که روشهای دیگری به غیر از روشهای محاسباتی بیمه ای را نیز میتوان در تجزیه و تحلیل سیستمهای پشتیبان به کار برد .

از آنجاییکه سیستمهای قدرت معمولا در حداکثر ظرفیت خود به کار گرفته می شوند ، مدت زمان بسیار کم و محدودی جهت اعمال خاموشیهای برنامه ریزی شده به منظور انجام تعمیرات و همچنین برای خاموشیهایی که در اثر خرابی تجهیزات به وقوع می پیوندد در اختیار ما قرار دارد . از همین رو ، وجود سیستمهای حفاظت پشتیبان که اجازه تعمیر تجهیزات حفاظتی بدون اعمال خاموشی را به ما داده و همچنین باعث حفظ پایداری شبکه در هنگام خرابی تجهیزات حفاظتی اصلی می گردد ، بسیار حیاتی و ضروری می باشد .

تاثیر حفاظت پشتیبان بر قابلیت اعتماد (Reliability) شبکه :

همانطور که پیش تر نیز گفته شد ، قابلیت اعتماد شبکه ترکیبی از قابلیت اطمینان (Dependability) و امنیت (Security) می باشد . از دید کاملا تئوری و با در نظر نگرفتن مسائل عملی ، می توان دیدگاه فوق را به صورت دو حد بالا و پایین بیان نمود : سیستم با ۱۰۰٪ قابلیت اطمینان و سیستم با ۱۰۰٪ قابلیت امنیت .

آدرس: شیراز خیابان مشیر نو _ صندوق پستی: ۱۱۹۵-۷۳۱۳۶۵ _ کد پستی: ۷۱۷۳۶-۱۴۷۱۵ تلفن: ۴-۲۳۰۸۷۵۲-۰۷۱۱
فاکس: ۰۷۱۱-۲۳۰۸۷۵۵ Web: www.fpmc.co.ir E-mail: info@fmpc.co.ir

سیستم با قابلیت ۱۰۰٪ اطمینان : در این حالت باید سیستم حفاظتی به صورت ثابت و دائم در حالت صدور فرمان تریپ قرار داشته باشد تا اطمینان حاصل شود که هیچ خطایی از دید سیستم پنهان نخواهد ماند !

سیستم با قابلیت ۱۰۰٪ امنیت : در این حالت باید سیستم حفاظتی به طور کامل غیر فعال گردد تا اطمینان حاصل شود که در هیچ صورتی به اشتباه فرمان تریپ صادر نخواهد نمود !

از تعاریف فوق مشخص می گردد ، با وجود اینکه ما همواره خواستار سیستمی با قابلیت اطمینان بالا و امنیت بالا می باشیم این قابلیت ها هیچگاه نمیتوانند به میزان ۱۰۰٪ تامین شوند و موارد فوق همواره باید کمتر از ۱۰۰٪ در نظر گرفته شوند . نکته مهم در اینجاست که باید توجه نمود که با در نظر گرفتن تعاریف فوق ، افزایش قابلیت اطمینان ، باعث کاهش امنیت و افزایش امنیت باعث کاهش قابلیت اطمینان در عملکرد تجهیزات حفاظتی می گردد .

با این وجود ، توجه نمایید که افزایش قابلیت اطمینان در یک سطح مشخص باعث کاهش قابلیت امنیت دقیقا به همان میزان نخواهد گردید و هدف نهایی ما یافتن مقادیر بهینه پارامترهای فوق به منظور دستیابی به حداکثر قابلیت اعتماد در سیستم حفاظتی خواهد بود .

برای نشان دادن تاثیر حفاظت پشتیبان بر قابلیت اطمینان و امنیت در شبکه از مثال DTT (Direct Transfer Trip) استفاده می نماییم . در این حالت امنیت به میزان ۹۹.۹۹۹۹٪ و قابلیت اطمینان به میزان ۹۹.۹۹٪ تامین می گردد.

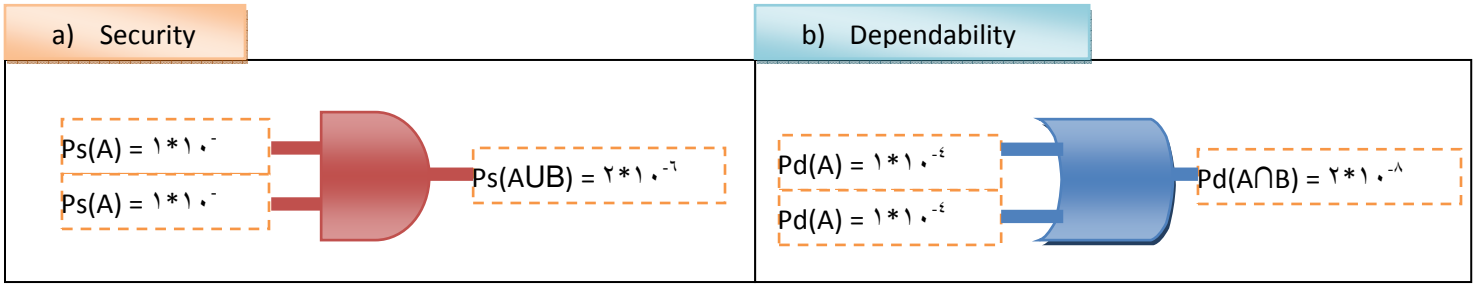
در صورتی که در این حالت خطایی در سیستم رخ دهد و توسط سیستم پشتیبان (B) رفع گردد ، عدم عملکرد سیستم حفاظت اولیه (A) نشانگر عملکرد اشتباه این سیستم نمی باشد . در عین حال ممکن است این عدم عملکرد نشانگر احتمال وجود اشکال در سیستم حفاظتی اولیه (A) باشد . توجه نمایید که در این مثال ، حفاظت پشتیبان (B) به طور کامل از حفاظت اولیه (A) مستقل بوده و درصد احتمال خرابی سیستمهای حفاظت اصلی و پشتیبان کاملا از یکدیگر مستقل می باشد و همچنین خرابی در یک سیستم به هیچ وجه دیگری را تحت تاثیر قرار نخواهد داد . مورد مهم دیگر اینکه یک عامل مشترک باعث از کار افتادن دو سیستم حفاظتی اصلی و پشتیبان به صورت همزمان نخواهد گردید . در این حالت میتوان قابلیت اطمینان و امنیت را به صورت متغیرهای آمار و احتمالات بیان نمود . در اینجا احتمال صدور یک فرمان قطع اشتباه (Ps) برابر با 10^{-6} و احتمال عدم عملکرد حفاظت در شرایط خطا (Pd) برابر با 10^{-4} خواهد بود .

آدرس: شیراز خیابان مشیر نو _ صندوق پستی: ۱۱۹۵-۷۳۱۳۶۵ _ کد پستی: ۱۴۷۱۵-۷۱۷۳۶ تلفن: ۴-۲۳۰۸۷۵۲-۰۷۱۱
فاکس: ۰۷۱۱-۲۳۰۸۷۵۵ Web: www.fpmc.co.ir E-mail: info@fmpc.co.ir

تاثیر حفاظت پشتیبان بر امنیت (Security) و قابلیت اطمینان (Dependability) شبکه :

در صورت استفاده از حفاظت پشتیبان و به شرط یکسان بودن و همچنین مستقل بودن دو سیستم اصلی و پشتیبان ، احتمال صدور فرمان اشتباه تریپ در این سیستم برابر است با مجموع احتمال صدور فرمان اشتباه تریپ توسط هر یک از سیستمها (شکل a). به این ترتیب ، میزان امنیت سیستم از ۹۹.۹۹۹۹٪ به ۹۹.۹۹۹۸٪ کاهش پیدا خواهد کرد .

در مورد قابلیت اطمینان ، با توجه به یکسان بودن و مستقل بودن دو سیستم اصلی و پشتیبان ، باید هر دو سیستم به صورت همزمان معیوب شده و قادر به صدور فرمان تریپ نباشند تا فرمان تریپ صادر نشود . بر همین اساس ، احتمال عدم صدور فرمان تریپ در این سیستم برابر است با حاصلضرب احتمال عدم صدور فرمان تریپ در هریک از سیستمها . (شکل b)



در نتیجه ، قابلیت اطمینان در این سیستم از ۹۹.۹۹٪ به ۹۹.۹۹۹۹۹۹٪ افزایش می یابد .

جدول زیر (جدول ۱) به طور خلاصه تاثیر استفاده از حفاظت پشتیبان بر روی قابلیت اطمینان و امنیت در سیستم مورد مثال (دارای احتمال تریپ اشتباه : $۱۰^{-۶}$ و احتمال عدم تریپ : $۱۰^{-۴}$ برای هر یک از حفاظتها (اصلی و پشتیبان)) را نشان میدهد .

Scheme	Probability of a false trip	Security	Probability of a missed trip	Dependability
Single	$۱۰^{-۶}$	۹۹.۹۹۹۹٪	$۱۰^{-۴}$	۹۹.۹۹٪
Redundant	$۲x۱۰^{-۶}$	۹۹.۹۹۹۸٪	$۱۰^{-۸}$	۹۹.۹۹۹۹۹۹٪

جدول-۱

جدول بالا دلیل اهمیت وجود حفاظت پشتیبان در افزایش سطح قابلیت اطمینان در سیستم حفاظتی را به وضوح نشان میدهد . همانطور که مشاهده می شود ، با افزودن حفاظت پشتیبان ، احتمال بروز یک تریپ اشتباه ۲ برابر افزایش می یابد ، در صورتی که احتمال عدم صدور فرمان صحیح تریپ به میزان ۱۰۰۰۰ برابر کاهش یافته است !

آدرس: شیراز خیابان مشیر نو _ صندوق پستی: ۱۱۹۵-۷۳۱۳۶۵ _ کد پستی: ۱۴۷۱۵-۷۱۷۳۶ تلفن: ۴-۲۳۰۸۷۵۲-۰۷۱۱
فاکس: ۰۷۱۱-۲۳۰۸۷۵۵ Web: www.fpmc.co.ir E-mail: info@fmpc.co.ir

طرح حفاظت پشتیبان به روش رأی گیری :

یکی از طرحهایی که به منظور افزایش اطمینان از عملکرد سیستم حفاظتی شبکه مورد استفاده قرار می گیرد ، طرح حفاظت پشتیبان به روش رای گیری ۲ از ۳ میباشد . این روش باعث افزایش همزمان قابلیت اطمینان و امنیت خواهد گردید . در این طرح از تعداد ۳ عدد رله یا بیشتر (تعداد رله ها باید فرد باشد) استفاده می گردد . عملکرد سیستم به این صورت است که به منظور صدور فرمان تریپ باید بیش از نصف تعداد رله ها فرمان تریپ صادر کرده باشند در غیر اینصورت فرمان تریپ اصلی تایید نشده و صادر نمی گردد . معمولا این طرح با استفاده از تعدادی از کنتاکتهای تریپ خروجی رله های حفاظتی که به صورت سری با یکدیگر قرار گرفته اند اجرا می گردد . توجه داشته باشید که در این طرح باید شرایط زیر رعایت شده باشد :

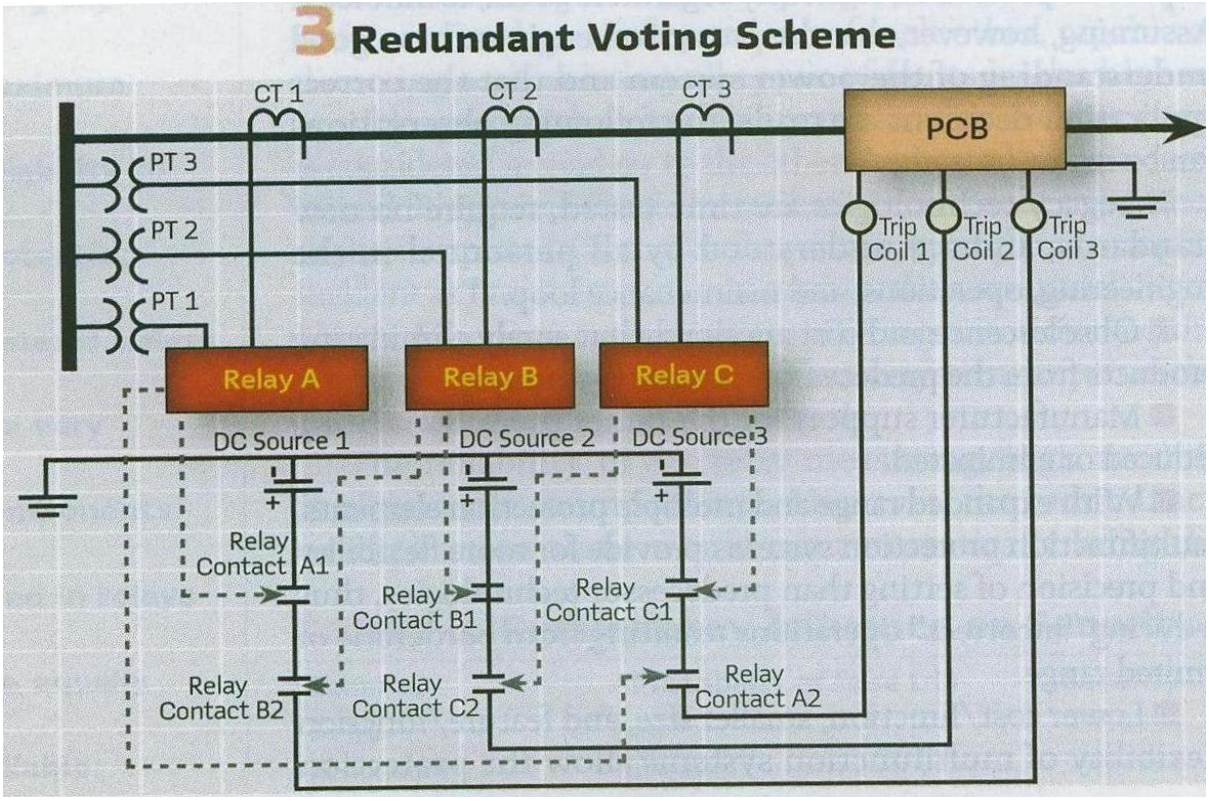
۱-) معمولا از سه عدد رله که ساخت شرکتهای متفاوت می باشند استفاده می گردد .

۲-) از جریان و ولتاژهای یکسان که از منابع جداگانه گرفته شده اند استفاده می شود .

۳-) در صورت استفاده از سه عدد رله ، حداقل باید دو عدد از رله ها فرمان تریپ صادر کرده باشند تا فرمان تریپ اصلی صادر شود .

معمولا از این سیستم در مواردی استفاده می شود که نیاز به درجه بالایی از اطمینان در عملکرد سیستم حفاظتی وجود داشته باشد . از این سیستم بیشتر در طرحهای خاص حفاظتی و در ولتاژهای EHV (Extra High Voltage)، یا در سیستمهایی که عملکرد اشتباه سیستم حفاظتی در آنها باعث از دست رفتن پایداری شبکه می گردد ، استفاده می شود . شکل زیر (شکل ۳) نشان دهنده یک نمونه از سیستم حفاظتی کامل رای گیری می باشد :

آدرس: شیراز خیابان مشیر نو _ صندوق پستی: ۱۱۹۵-۷۳۱۳۶۵ _ کد پستی: ۱۴۷۱۵-۷۱۷۳۶ تلفن: ۴-۲۳۰۸۷۵۲-۰۷۱۱
فاکس: ۲۳۰۸۷۵۵-۰۷۱۱ Web: www.fpmc.co.ir E-mail: info@fmpc.co.ir



(شکل ۳)

همانطور که ملاحظه میگردد ، در این سیستم هر رله به منبع ولتاژ و جریان مخصوص به خود متصل شده است . مدار تریپ نیز شامل سه منبع تغذیه جداگانه می باشد که بر مبنای شمای ۲ از ۳ به کنتاکتهای تریپ متصل گردیده است .

در این سیستم ، در صورتی که یکی از رله ها به دلیل عدم عملکرد صحیح CT یا PT یا حتی وجود اشکال در لاجیک رله ، عملکرد صحیح نداشته باشد ، رله دوم اجازه قطع بریکر به صورت اشتباه را نخواهد داد .

ملاحظات حفاظت پشتیبان :

مهمترین نکته در طراحی سیستمهای حفاظتی انعطاف پذیری آنهاست . این بدین معنیست که سیستم حفاظتی باید به صورت بهینه ارتباط بین هزینه ، قابلیت اطمینان و امنیت در شبکه را در نظر گرفته باشد . همچنین حذف یا عدم عملکرد صحیح هر یک از اجزا باید کمترین اختلال در سیستم را به وجود آورد .

آدرس: شیراز خیابان مشیر نو _ صندوق پستی: ۱۱۹۵-۷۳۱۳۶۵ _ کد پستی: ۱۴۷۱۵-۷۱۷۳۶ تلفن: ۴-۲۳۰۸۷۵۲-۰۷۱۱
فاکس: ۲۳۰۸۷۵۵-۰۷۱۱ Web: www.fpmc.co.ir E-mail: info@fmpc.co.ir

ملاحظات اقتصادی :

یکی از مهمترین عوامل در انتخاب سطح حفاظت پشتیبان در سیستمهای حفاظتی ، هزینه می باشد . هدف اصلی ما رسیدن به طرحی است که در آن بهینه ترین سیستم حفاظتی در ازای هزینه قابل قبول به دست آید .

معمولا مقدار هزینه انجام شده در سیستم حفاظتی ، متناسب با میزان بار شبکه و همچنین اهمیت بار مذکور می باشد .

با توجه به اینکه میزان بار هر شبکه متناسب با مقدار ولتاژ استفاده شده در آن شبکه می باشد ، میتوان گفت که با افزایش میزان ولتاژ ، بایستی از سطح بالاتری از حفاظت پشتیبان نیز استفاده نمود . البته باید در نظر داشت که این قانون همیشه برقرار نمی باشد . به عنوان مثال ممکن است مصرف کننده صنعتی بزرگی که با ولتاژ پایین تری تغذیه می گردد نیز به منظور رسیدن به سطح بالاتری از قابلیت اطمینان تقاضای نصب حفاظتهای پشتیبان داشته باشد .

باید توجه داشت که به غیر از موارد استثنا که نمونه ای از آن ذکر شد ، استفاده از حفاظتهای پشتیبان به جای حفاظتهای ساده ، هزینه های زیاد بی موردی به سیستم تحمیل خواهد نمود . در این موارد می توان به راحتی از حفاظتهای ساده استفاده کرده و نتیجه مطلوب را به دست آورد .

مدت زمان خاموشی :

خاموشیها به دو نوع تقسیم می شوند : ۱) با برنامه ریزی قبلی ۲)اجباری و بدون برنامه ریزی قبلی

خاموشیهای با برنامه ریزی قبلی معمولا به منظور انجام تعمیرات اعمال می گردد و به دلیل برنامه ریزی قبلی ، کلیه تمهیدات به منظور کاهش اثرات سوء آن بر روی سیستم از قبل اندیشیده می شود . اما خاموشیهای اجباری و بدون برنامه ریزی قبلی معمولا به دلیل بروز خطا در شبکه رخ داده و اثرات سوء بر عملکرد شبکه داشته و طبیعتا مورد دلخواه ما نخواهد بود . باید تلاش نمود تا خاموشیهای بدون برنامه ریزی که عملکرد شبکه را تحت تاثیر قرار میدهد را به حداقل میزان ممکن کاهش داد در غیر اینصورت ممکن است با جریمه های نقدی و عدم رضایت مشتری و همچنین بروز مشکلات عمده در صنایع مختلف مواجه شویم .

آدرس: شیراز خیابان مشیر نو _ صندوق پستی: ۱۱۹۵-۷۳۱۳۶۵ _ کد پستی: ۱۴۷۱۵-۷۱۷۳۶ تلفن: ۴-۲۳۰۸۷۵۲-۰۷۱۱
فاکس: ۲۳۰۸۷۵۵-۰۷۱۱ Web: www.fpmc.co.ir E-mail: info@fmpc.co.ir

به همین جهت مدیران منابع سعی در کاهش میزان تاثیر این خاموشیها بر روی سیستم با استفاده از سیستمهای پشتیبان دارند . این سیستمهای پشتیبان شامل : تغذیه های متعدد به یک ایستگاه ، استفاده از دو یا چند حفاظت به صورت اصلی و پشتیبان یا طراحی شبکه به صورتی که بتواند در مواقع مختلف به صورت انعطاف پذیر عمل نماید ، می باشد .

مدیران منابع همچنین باید موارد مربوط به نگهداری شبکه را در نظر داشته باشند . بدین منظور باید استفاده از سیستمهای پشتیبان به منظور کاهش زمان خاموشی را مد نظر داشته باشند . به عنوان مثال در هنگامی که نیاز به سرویس قسمتی از سیستم حفاظتی می باشد ، باید حفاظت پشتیبان جایگزین آن شود تا در طول مدت زمان سرویس ، نیاز به قطع قسمتی از شبکه نداشته باشیم .

مدت زمان بازیابی :

در صورتی که بخشی از حفاظت به دلیل تعمیرات یا اشکال از سرویس خارج شود ، قابلیت اعتماد سیستم تحت حفاظت ، به مدت زمان بازگشت بخش مذکور به سیستم بستگی خواهد داشت . در صورتی که حتی در هنگام خارج بودن بخش مذکور از سیستم حفاظتی نیاز به درجه خاصی از قابلیت اعتماد در سیستم وجود داشته باشد ، بایستی از حفاظتهای پشتیبان بیشتری استفاده نمود تا در طول مدت خارج بودن قسمت مذکور ، سطح قابلیت اعتماد سیستم در سطح قبلی حفظ شود .

در دسترس بودن :

دردسترس بودن و به تبع آن قابلیت اعتماد سیستم حفاظتی ، تحت تاثیر مدت زمان لازم جهت تعمیر قطعه معیوب می باشد . در سیستمهای بسیار حساس و مهم ممکن است از سه سیستم حفاظتی (یک اصلی و دو پشتیبان) استفاده شود اما در حالت عادی معمولا از دو سیستم حفاظتی (یک اصلی و یک پشتیبان) استفاده می شود .

در کاربردهایی که قابلیت اعتماد مساله بسیار مهمی نباشد (مانند فیدرهای خروجی) فقط از یک سیستم حفاظتی استفاده می شود .

آدرس: شیراز خیابان مشیر نو _ صندوق پستی: ۱۱۹۵-۷۳۱۳۶۵ _ کد پستی: ۱۴۷۱۵-۷۱۷۳۶ تلفن: ۴-۲۳۰۸۷۵۲-۰۷۱۱
فاکس: ۲۳۰۸۷۵۵-۰۷۱۱ Web: www.fpmc.co.ir E-mail: info@fmpc.co.ir

توجه داشته باشید که حتی در صورت استفاده از حفاظت پشتیبان ، نقاط مشترکی در هر دوحفاظت با یکدیگر وجود دارند که ممکن است به طور همزمان معیوب شده و عملکرد سیستم را مختل کنند . به عنوان مثال وقتی هر دو حفاظت به یک بوبین بریکر فرمان قطع صادر می نمایند یا در صورت استفاده از یک مجموعه باطری تغذیه ، در صورت معیوب شدن قسمتهای مشترک ، کل عملکرد سیستم حفاظتی تحت تاثیر قرار گرفته و اشتباه خواهد بود .

مدت زمان در دسترس بودن یک قطعه با استفاده از فرمول زیر تعریف می شود :

MTBF : Mean Time Between Failure

MTTR : Mean Time To Repair

همانطور که ملاحظه می شود ، استفاده از حفاظت پشتیبان نقش مهمی در افزایش سطح اعتماد کل شبکه ایفا خواهد نمود .

سخت افزار مورد نیاز جهت داشتن حفاظت پشتیبان کامل :

در صورتی که نیاز به داشتن حفاظت پشتیبان کامل داشته باشیم ، باید از وسایل اندازه گیری و تشخیص جداگانه ، تریپ کویل های جداگانه و همچنین رله های حفاظتی و باطری های جداگانه استفاده نمود . موارد زیر نیز باید بدین منظور مورد توجه قرار گیرد :

- ترانسهای جریان جداگانه برای هر یک از واحدهای حفاظتی
- ترانسهای ولتاژ جداگانه یا حداقل یک ترانس ولتاژ با چندین خروجی
- هر سیستم حفاظتی در پانل های جداگانه قرار گرفته باشد یا در صورت قرار داشتن در یک پانل به خوبی از یکدیگر جدا شده باشند
- در نظر گرفتن باطری های کاملا جداگانه و مستقل
- مسیر عبور کابلها تا حد امکان از یکدیگر جدا شده باشند
- استفاده از دو بوبین قطع در بریکرها
- استفاده از دو خط مخابراتی جهت سیستم تله پروتکشن و Transfer Trip

آدرس: شیراز خیابان مشیر نو _ صندوق پستی: ۱۱۹۵-۷۳۱۳۶۵ _ کد پستی: ۱۴۷۱۵-۷۱۷۳۶ تلفن: ۴-۲۳۰۸۷۵۲-۰۷۱۱
فاکس: ۲۳۰۸۷۵۵-۰۷۱۱ Web: www.fpmc.co.ir E-mail: info@fmpc.co.ir

سیستم حفاظتی A , B :

سیستمهای حفاظتی اصلی و پشتیبان به صورت گروه A و گروه B طراحی و اجرا می شوند . به منظور دستیابی به یک حفاظت پشتیبان کامل ، باید واحدهای اندازه گیری و تصمیم گیرنده (Logic) هر دو سیستم به صورت کامل از یکدیگر مجزا و مستقل بوده و هر یک به صورت جداگانه قادر به تشخیص و رفع کلیه خطاهای به وجود آمده در شبکه با حداکثر سرعت و با قابلیت اطمینان و امنیت بالا باشند . در این حالت ، هر یک از گروههای حفاظتی برای گروه دیگر به صورت پشتیبان محسوب شده و عمل خواهد نمود . سیستم A , B باید به صورت فیزیکی نیز از یکدیگر تفکیک شده و مجزا باشند تا در صورت بروز حوادث فیزیکی مانند آتش سوزی ، فقط یک واحد تحت تاثیر قرار گرفته و واحد دیگر بتواند به کار عادی خود ادامه دهد . برخی از شرکتهای برق منطقه ای شمال آمریکا یکی از معیارهای استاندارد خود در مورد سیستمهای قدرت بزرگ را ، جدا بودن فیزیکی سیستم حفاظت شبکه قرار داده اند .

توجه داشته باشید که قابل اطمینان بودن واحد های اندازه گیری و همچنین لاجیک رله های حفاظتی از اهمیت بسیار ویژه ای برخوردار است . دلیل این امر آنست که تا زمانی که واحد های استفاده شده در رله های حفاظتی قابل اطمینان نباشند ، استفاده از حفاظت پشتیبان به تنهایی نمی تواند قابلیت اطمینان کل سیستم را افزایش دهد . پس بایستی کلیه قطعات استفاده شده در رله های حفاظتی – علی الخصوص قطعاتی که در رله های جدید میکروپروسسوری استفاده می شود – در شرایط عملی به صورت کامل تست شده یا دارای تاییدیه از مراکز معتبر تست باشند .

برخی از شرکتهای بزرگ تامین کننده نیرو ، به دلیل احتمال بروز خطاهای مشترک در رله های یکسان ، استانداردهای خاصی در مورد عدم استفاده از یک نوع رله در هر دو سیستم اصلی و پشتیبان دارند . دلیل این امر آنست که در صورت وجود اشکال در طراحی اولیه قسمتی از یک رله ، این اشکال در تمام رله های مشابه وجود داشته و در هنگام بروز خطا ممکن است این اشکال در هر دو رله باعث بروز اشکال مشترکی در تشخیص خطا و در نتیجه عملکرد غلط هر دو سیستم اصلی و پشتیبان به صورت همزمان گردد .

نکته دیگری که باید مورد توجه قرار گیرد مربوط به لاجیک رله می باشد . بایستی لاجیک تریپ هر حفاظت (شامل لاجیک عملکرد و تریپ) به واحد اندازه گیری همان حفاظت مربوط بوده و حفاظتهای اصلی و پشتیبان دارای لاجیکهای جداگانه و واحد های اندازه گیری جداگانه مرتبط با لاجیک خود باشند . به

آدرس: شیراز خیابان مشیر نو _ صندوق پستی: ۱۱۹۵-۷۳۱۳۶۵ _ کد پستی: ۱۴۷۱۵-۷۱۷۳۶ تلفن: ۴-۲۳۰۸۷۵۲-۰۷۱۱
Web: www.fpmc.co.ir E-mail: info@fmpc.co.ir فاکس: ۲۳۰۸۷۵۵-۰۷۱۱

عبارت دیگر ، نباید در دو حفاظت اصلی و پشتیبان از یک واحد اندازه گیری و دولاجیک مرتبط به این یک واحد استفاده نمود .

جداسازی فیزیکی :

یکی از جهات استفاده از سیستمهای پشتیبان ، جدا سازی فیزیکی قطعات اصلی و پشتیبان از لحاظ محل قرار گرفتن فیزیکی از یکدیگر می باشد . در این حالت ، در صورت بروز حوادث فیزیکی مانند آتش سوزی و غیره ، هر دو سیستم اصلی و پشتیبان به صورت همزمان آسیب نخواهند دید . البته واضح است که در این زمینه محدودیتهایی نیز وجود دارد . به عنوان مثال : ۱-تمام تجهیزات در نهایت در یک ایستگاه برق نصب می شوند . ۲-تمام ترانسهای جریان بر روی یک کلید نصب می شوند یا در اطراف یک بوشینگ نصب می گردند و ... . حتی با در نظر گرفتن محدودیتها و مشکلات اینچنینی می توان به حد قابل قبولی از جداسازی فیزیکی دست یافت . بدین منظور می توان به عنوان مثال سیستمهای حفاظتی اصلی و پشتیبان را در دو پانل جداگانه نصب نمود ، ولتاژهای تغذیه AC و DC را از پانل های جداگانه تامین نموده و کابل ارتباطی تغذیه اصلی و پشتیبان را از هم تفکیک نمود ، کابلهای ارتباطی بین محوطه و اتاق فرمان را از مسیرهای جداگانه عبور داد .

لازم به ذکر است که جدا سازی فیزیکی در ایستگاههایی که در مرحله طراحی یا اجرا می باشند بسیار کم هزینه تر از ایستگاههای قدیمی است . با این وجود ، در ایستگاههای قدیمی که در حال بازسازی می باشند نیز می توان این جدا سازی را در حد امکان انجام داده و از مزایای آن بهره برد .

گوناگونی :

با استفاده از رله های گوناگون در سیستم ، می توان از اشکالات مشابه پیش آمده در حفاظتهای اصلی و پشتیبان جلوگیری نمود .

اصول عملکرد متفاوت :

در سیستمهای الکتریکی ، به منظور پوشش طیف وسیعی از خطاهای شبکه ، از حفاظتهای گوناگونی استفاده می شود . توجه داشته باشید که در این حالت باید از روشهای متفاوت حفاظتی که مکمل یکدیگر

آدرس: شیراز خیابان مشیر نو _ صندوق پستی: ۱۱۹۵-۷۳۱۳۶۵ _ کد پستی: ۱۴۷۱۵-۷۱۷۳۶ تلفن: ۴-۲۳۰۸۷۵۲-۰۷۱۱
فاکس: ۰۷۱۱-۲۳۰۸۷۵۵ Web: www.fpmc.co.ir E-mail: info@fmpc.co.ir

باشند جهت دستیابی به نتیجه فوق استفاده نمود . به عنوان مثال ، به منظور حفاظت از یک خط انتقال ، به طور همزمان از رله دیفرانسیل طولی و رله دیستانس (به همراه Schemeهای تله پروتکشن) استفاده می شود . همانطور که ملاحظه می شود ، در مثال فوق ، در صورت بروز اشکال در ترانسهای ولتاژ ، حفاظت دیفرانسیل طولی به دلیل مستقل بودن از ولتاژ ، بدون مواجه شدن با اشکال به کار خود ادامه میدهد . همچنین رله دیستانس در صورت قطع خطوط ارتباطی مخابراتی – که منجر به از کار افتادن حفاظت دیفرانسیل طولی می گردد – بدون مشکل به کار خود ادامه خواهد داد . به منظور دستیابی به شرایط فوق می توان از رله های جداگانه استفاده نموده یا اینکه با توجه به چند کاره بودن رله های نیومریک ، از واحدهای مختلف تعبیه شده در این نوع تجهیزات استفاده نمود . همانطور که ملاحظه می گردد ، یکی از روشهای دستیابی به حفاظت پشتیبان ، استفاده از حفاظتهای گوناگون بر روی یک تجهیز است .

استفاده از تجهیزات حفاظتی با مارکهای مختلف :

همانطور که قبلا نیز گفته شد ، مزیت استفاده از مارکهای مختلف رله اینست که در صورت عملکرد نامناسب رله ای با یک مارک مشخص در هنگام خطا به دلیل وجود یک اشکال خاص در طراحی و ساخت آن ، رله دیگر که در کارخانه دیگری طراحی و تولید شده در هنگام بروز خطا عملکرد صحیح خواهد داشت. به عبارت دیگر ، رله ها با مارکهای متفاوت اشکالات ساختاری یکدیگر را پوشش خواهند داد . می توان گفت ، سازندگان مختلف رله از آلگوریتمهای متفاوتی جهت تشیص خطا استفاده می نمایند که این امر باعث می شود در صورتی که یکی از رله ها به دلیل آلگوریتم خاص خود قادر به تشخیص نوع خاصی از خطا نباشد ، رله دیگر بتواند آن خطا را تشخیص داده و برطرف نماید .

نکته : در حال حاضر استفاده از رله های مختلف از یک مارک رایج تر از استفاده از مارکهای مختلف رله در سیستم حفاظتی می باشد . دلیل این امر آنست که با استفاده از این روش هزینه های مرتبط مانند آموزش پرسنل و غیره کاهش یافته و همچنین مشکلاتی مانند کار با چندین کارخانه سازنده و نمایندگی فروش نیز مرتفع خواهد گردید .

ادامه دارد ...

رضا حکمتی

منبع : مجله PAC World

آدرس: شیراز خیابان مشیر نو _ صندوق پستی: ۱۱۹۵-۷۳۱۳۶۵ _ کد پستی: ۱۴۷۱۵-۷۱۷۳۶ تلفن: ۴-۲۳۰۸۷۵۲-۰۷۱۱
فاکس: ۲۳۰۸۷۵۵-۰۷۱۱ Web: www.fpmc.co.ir E-mail: info@fmpc.co.ir