تعیین فواصل زمانی تست و نحوه تنظیم استراتژیهای تعمیراتی تجهیزات حفاظتی از نوع خطای پنهان

لیلا جلیلی [1] مسعود صادقی خمامی [2] محمود فتوحی فیروز آبادی[3]

1-معاونت بهره برداری -شرکت توزیع نیروی برق تهران بزرگ

2-معاونت هماهنگی توزیع- توانیر

3-دانشکده برق- دانشگاه صنعتی شریف

کلمات کلیدی: نت (تعمیرات و نگهداری)،تجهیزات حفاظتی،پیامد خطای پنهان، فعالیت جستجوی شکست، تعیین فاصله زمانی میان فعالیتهای تعمیراتی

چکیده:

اثرات خطاهای موجود در تجهیزات شبکه میتواند به دو صورت آشکار و پنهان نمود یابد. در این میان، اثرات خطاهای پنهان با تجهیزات حفاظتی مرتبط بوده و میتواند پیامدهای متفاوتی همچون خاموشیهای کلی و جزئی را در پی داشته باشد. از اینرو به منظور جلوگیری از وقوع چنین پیامدهایی ، شرکتهای برق اقدام به تستهای بازرسی دوره ای در تجهیزات حفاظتی با کمی تفاوت نسبت به سایر تجهیزات که دارای خطاهای از نوع آشکار میباشند، می نمایند. در حالیکه تعیین نوع و زمان تست به عوامل متعددی وابسته میباشد و در کشور ایران اغلب بر اساس دستورالعمل های رایج بهره برداری صورت میپذیرد که با توجه به شرایط عملی و اجرایی موجود در سیستم توزیع ، قابل پیاده سازی به صورت موثر نمی باشد. در این مقاله نوعی الگوریتم تنظیم استراتژیهای تعمیراتی تجهیزات حفاظتی به صورت الگوریتمی ارائه میگردد که منطبق بر شرایط واقعی موجود در شبکه های برق، علی الخصوص، توزیع است. سپس با معرفی مدل هورتون، تعیین فاصله زمانی میان فعالیتهای تعمیراتی صورت میپذیرد. این مدل با استفاده از دو پارامتر دسترس پذیری (Availability) و قابلیت اطمینان به محاسبه این زمان میپردازد.

مقدمه:

استمرار برق رسانی به مشترکین یکی از اهداف اصلی سیستم قدرت است لذا سیستم قدرت باید قابلیت اطمینان و پیوستگی انرژی را حفظ نماید. تجهیزات حفاظتی در این استمرار نقش موثری را ایفا می کنند. از زمانی که یک تجهیز حفاظتی نصب میشود احتمال خراب شدن آن وجود دارد و با گذشت زمان این احتمال بیشتر میگردد. از مشکلات کار با سیستم های حفاظتی این است که بندرت نیاز به عملکرد داشته باشند.این در حالی است که در صورت بروز ، این خرابی باقی خواهد ماند و در موقع ضرورت عملکرد نداشته و منجر به حادثه یا افزایش خسارت گردد که این موضوع همان اثرات خطای پنهان است که در ادامه شرح داده خواهد شد. برای رفع این عیب تجهیزات حفاظتی باید با استفاده از یک استراتژی مناسب تعمیراتی و در فواصل زمانی مناسب تست گردیده تا از صحت عملکرد آنها اطمینان حاصل گردد.

روش های برای تعیین نوع و فاصله زمانی تست برای تجهیزات مختلف حفاظتی وجود داشته و امروزه به صورت روتین در شبکه های توزیع مورد استفاده قرار میگردد که با توجه به شرایط عملی و اجرایی موجود در سیستم توزیع ، قابل پیاده سازی به طور موثر و اثر بخش نبوده و سبب گردیده تا در مواقعی، سیستم نتواند در شرایط بحرانی و بروز حادثه واکنش مناسبی از خود ارائه نموده و سیستم دچار خاموشی های حتی با وسعت بالا میگردد. لذا در این مقاله سعی شده است تا در ابتدا انواع استراتژیهای نگهداری و تعمیرات ، هفت سئوال اساسی RCM و تعاریف مربوط به خطاهای پنهان و آشکار مطرح گردد و سپس به تنظیم فعالیتهای تعمیراتی تجهیزات حفاظتی با تاکید بر فعالیت جستجوی شکست بپردازد و با تعیین فواصل زمانی انجام این فعالیت، تصمیم گیری نهایی پروسه RCM را صورت دهد و در پایان الگوریتم ارائه شده بر روی یک سیستم نمونه اجرا گردد.

1-انواع استراتژیهای تعمیراتی

هدف و تلاش عمده مهندسان نت اجرای یک استراتژی نت است که قابلیت دسترسی و بازده یک تجهیز را به حداکثر برساند، زوال و خرابی یک تجهیز را کنترل نموده، یک عملیات ایمن و درست با محیط را ایجاد و هزینه کل عملیات را حداقل کند. این هدف با قبول یک رویکرد سازمان یافته در مطالعه خرابی تجهیز و طراحی استراتژی بهینه بازرسی و نت بدست خواهد آمد. تکنیک های مدیریت نت دچار تغییر شکل و دگرگونی عمده در فرآیند شده اند. به طوری که از تمرکز بر تعمیرات اساسی دوره ای به استفاده از نظارت بر حسب شرایط CBM، RCM و کارشناسی سیستم ها تغییر پیدا کرده است. استراتژیهای تعمیراتی به 3 دسته زیر با زیر مجموعه های مربوط تقسیم میگردد:

1-فعالیتهای پیش اقدام: Corrective, TBM,CBM Maintenance

2-اقدامات پیش فرض : Failure _Finding, Redesign, Run To Failure

3-مجموعه ای از فعالیتهای 1 و 2 با در نظر داشتن هزینه و افزایش قابلیت اطمینان سیستم، تشکیل دهنده RCM میگردد.

آنچه در مواجه با RCM مهم است پاسخگویی به 7 سئوال زیر است که در تنظیم فعالیتهای تعمیراتی دارد.

1)**کارکردها** و **استانداردهای عملکرد** مربوطه تجهیز در **شرایط عملیاتی** موجود چیست؟

2) به چه صورتهای ممکن است تجهیز از انجام کارکردهایش باز ایستد؟ (تعیین شکست های کارکردی)

3) چه چیزی باعث وقوع هر کدام از شکست های (خرابی های) کارکردی می شود؟(تعیین حالات شکست)

4) در زمان رخداد هر شکست چه اتفاقاتی روی میدهد؟(تعیین اثرات شکست)

5) هر شکست از چه نظرهایی اهمیت دارد؟ (تعیین پیامد شکست)

6) برای پیش بینی یا پیش گیری از هر شکستی چه میتوان انجام داد؟(تعیین PM و فعالیتهای پیش اقدام مناسب)

7) اگر نتوان فعالیت پیش اقدام مناسبی پیدا کرد، چه باید کرد؟(اقدامات پیش فرض: شامل جستجوی شکست و بازطراحی)

عبارتهای کلیدی در پرسشهای فوق:

- کارکرد
- استاندارد
- شرایط
- شکست کارکردی
- حالات شکست
- اثرات شکست
- پیامدهای شکست

نظر به اینکه رویکرد این مقاله بررسی شکست های پنهان که مختص تجهیزات حفاظتی است لازم دانسته شد دو عبارت اثرات و پیامدهای شکست شرح داده شود.

اثرات شکست : این اثرات شرح میدهند که در زمان وقوع یک حالت شکست چه اتفاقاتی رخ میدهند. اثرات شکست باید به گونه ای تشریح شوند که مجریان تعمیرات قادر به تصمیم گیری درباره آشکار بودن یا آشکار نبودن شکست در شرایط عادی باشند. این موضوع آنان را در تعیین نوع نعمیرات یاری خواهد نمود که به کدامیک از استراتژیهای نیاز می باشد.

پیامدهای شکست:

- پیامدهای شکست پنهان :

شکستهای پنهان دارای اثرات مستقیم نمی باشند, ولی ممکن است که شبکه های برق را با شکست های چندگانه دارای پیامدهای خطرناک و اغلب فاجعه بار روبرو کنند(اکثر اینگونه شکستها مربوط به تجهیزات حفاظتی هستند که حالت شکست ایمن(Fail Safe) ندارند)

- پیامدهای شکست آشکار:

- پیامدهای ایمنی و محیط زیستی
- پیامدهای عملیاتی(Network Performance)
- پیامدهای غیر عملیاتی(Financial)

لازم به ذکر است که یک خطای پنهان، پس از آشکار سازی تمامی پیامدهای آشکار را شامل خواهد شد.

2-کارکرد تجهیزات حفاظتی:

با پیچیده تر شدن تجهیزات، حالت های احتمالی شکست نیز به صورت لگاریتمی افزایش می یابند. این موضوع باعث رشدی پیوسته در انواع و شدت پیامدها شده است. در تلاش برای جلوگیری (و یا حداقل کاهش) از این پیامدها، استفاده از تجهیزات حفاظتی خودکار به طور روزافزون، افزایش یافته است.

هدف از این تجهیزات محافظت کردن از افراد، تجهیزات و سیستم و گاهی تمامی این موارد در برابر شکست است. وجود محاقظت یعنی بتوان از سخت گیری کمتری برای نگهداری و تعمیرات کارکرد تحت محافظت نسبت به حالت عدم وجود محافظت استفاده نمود.

پس هر تجهیز محافظ در حقیقت بخشی از یک سیستم با دو بخش است:

- ابزار محافظت کننده
- کارکرد تحت محافظت

با توجه به پیامدهای شکست پنهان وآشکار، تجهیزات حفاظت با دو ویژگی مطرح میگردند:

تجهیزات حفاظتی دارای ویژگی شکست ایمن

اصطلاح ایمن به مفهوم این است که شکست تجهیز در شرایط کاری عادی خود به خود برای کاربران مشهود است. یک تجهیز دارای خصوصیت شکست ایمن, تجهیزی است که شکست آن در شرایط عادی عملیات برای کاربران آشکار باشد.

در یک سیستم با تجهیز حفاظتی با خصوصیت شکست ایمن، در هر دوره امکان سه نوع وضعیت زیر وجود دارد:

1- زمانیکه هیچ کدام از تجهیزات(حفاظتی و تحت حفاظت) خراب نشوند. در این حالت تمامی شرایط عادی است.

2- وضعیتی که کارکرد تحت حفاظت پیش از تجهیز حفاظتی دچار شکست شود. در این وضعیت تجهیز حفاظتی کارکرد مورد نظر خود را انجام میدهد، و بر اساس طبیعت این محافظت، پیامدهای شکست کارکرد تحت حفاظت از بین رفته یا کاهش می یابند.

3- وضعیتی که تجهیز حفاظتی پیش از کارکرد تحت حفاظت دچار شکست شود. این وضعیت نیز مشهود خواهد بود چون در غیر اینصورت دیگر نمی توان مطابق تعریف بالا ابزاری را دارای شکست ایمن نامید. اگر روش مناسبی اتخاذ شود، احتمال شکست تجهیز تحت محافظت در زمان خرابی تجهیز حفاظتی را میتوان با متوقف کردن کارکرد تحت حفاظت یا با استفاده از روش محافظتی دیگری در زمان تصحیح مشکل تجهیز حفاظتی تقریباً از بین برد.

تجهیزات حفاظتی که دارای شکست ایمن نیستند

در یک سیستم با تجهیزات حفاظتی بدون ویژگی شکست ایمن، اگر تجهیزات دچار شکست شده باشد و قادر به انجام کارکرد مورد انتظار نباشد تحت شرایط عادی آشکار نخواهد بود. این موضوع در هر دوره فرضی، احتمال چهار وضعیت از نظر شکست را به وجود می آورد که دو حالت آن مشابه موارد تجهیز حفاظتی با شکست ایمن هستند این چهار حالت در جدول زیر مشخص گردیده است.

جدول 1 -چهار حالت تجهیزات حفاظتی غیر ایمن

شرایط	وضعیت تجهیز حفاظتی	وضعیت کارکرد تحت حفاظت
عادی	سالم	سالم
ظاهراً عادی	خراب	سالم
بازگشت به شرایط عادی با عملکرد تجهیز حفاظتی	سالم	خراب
غیر عادی و غیر قابل کنترل (شکست چندگانه)	خراب	خراب

چهارمین وضعیت ممکن، میتواند شکست تجهیز حفاظتی و سپس شکست کارکرد تحت حفاظت در همان زمانی که ابزار محافظ خراب است، باشد. این وضعیت با عنوان شکست چندگانه شناخته میشوند.(این وضعیت یک احتمال واقعی است چرا که شکست تجهیز حفاظتی آشکار نبوده و در نتیجه هیچ کس از نیاز به اصلاح یا جایگزین کردن آن برای جلوگیری از شکست چندگانه با خبر نیست)

از بحث فوق میتوان نتیجه گرفت که کارکردهای پنهان را میتوان با پرسش زیر شناسایی نمود:

" آیا از دست دادن کارکرد به وسیله این حالت شکست در شرایط عادی "خود به خود" برای کاربر آشکار است؟"

اگر پاسخ به این سئوال منفی باشد، حالت شکست مورد نظر از نوع پنهان و اگر مثبت باشد حالت شکست از نوع آشکار است. توجه به این نکته ضروری است که در این خصوص ، عبارت خود به خود نشان دهنده آن است هیچ چیز دیگری خراب نشود. همچنین در این نقطه از بررسی ها فرض میشود که هنوز تلاشی برای کنترل وضعیت کارکردهای پنهان صورت نمی گیرد. چرا که چنین کنترل هایی در واقع نوعی از نگهداری و تعمیرات زمان بندی شده به حساب آمده و تمام هدف این بررسی ها، تحلیل ضرورت انجام چنین اقداماتی است.

هدف یک برنامه نگهداری و تعمیرات برای یک کارکرد پنهان، جلوگیری یا حداقل کاهش احتمال شکست های چندگانه مربوطه است.

دسترس پذیری مورد نیاز به کارکردهای پنهان:

احتمال وقوع شکست چندگانه در هر دوره زمانی توسط احتمال شکست کارکرد تحت حفاظت در حالی که در همان دوره تجهیز حفاظتی هم خراب شده باشد تعیین میشود این احتمال را میتوان به روش زیر محاسبه کرد:

احتمال شکست چندگانه = احتمال شکست کارکرد تحت حفاظت × در دسترس نبودن ابزار محافظ (1)

در عمل، احتمالی که برای شکست چندگانه قابل تحمل، ارزیابی میشود به پیامدهای شکست وابسته است. در اغلب موارد این ارزیابی باید توسط کاربران تجهیز انجام شود. این پیامد از یک سیستم به سیستم دیگر ممکن است تفاوت های چشم گیری داشته باشد .

3-ارائه الگوریتم تنظیم فعالیتهای تعمیراتی

در سیستمی که از تجهیز حفاظتی استفاده میشود که دارای خاصیت شکست ایمن نمی باشند، احتمال وقوع شکست چندگانه را به یکی از صورت های زیر میتوان کاهش داد:

جلوگیری از شکست کارکرد تحت حفاظت

ملاحظه شد که بخشی از یک شکست چندگانه وابسته به میزان شکست کارکرد تحت حفاظت است. مقدار این پارامتر را میتوان به وسیله ارتقای عملیات نگهداری و تعمیرات تجهیز تحت حفاظت، و یا تغییر در طراحی (به عنوان آخرین چاره) کاهش داد.

جلوگیری از شکست پنهان

برای جلوگیری از یک شکست چندگانه باید سعی کرد که از عدم قرار گرفتن کارکرد پنهان در وضعیت شکست در زمان شکست کارکرد تحت حفاظت اطمینان حاصل کرد. برای یک شکست پنهان، انجام یک فعالیت پیش اقدام فقط زمانی به صرفه است که دسترس پذیری مورد نیاز جهت کاهش احتمال شکست چندگانه تا حد قابل تحملی را تامین نماید.پس اگر نتوان روش مناسبی برای جلوگیری از وقوع شکست پنهان پیدا کرد باید در جهت یافتن روشی برای ارتقاء دسترس پذیری کارکرد پنهان کوشید.

جستجوی شکست پنهان

اگر امکان پیدا کردن یک روش مناسب برای جلوگیری از شکست پنهان وجود نداشته باشد. فرصت جهت کاهش ریسک چندگانه به وسیله کنترل کارکرد پنهان به صورت دوره ای جهت اطمینان از سلامت آن وجود داشته باشد. اگر این کنترل (که فعالیت جستجوی شکست نامیده میشود) در فواصل زمانی مناسب انجام شود و در صورت کشف مشکلات، به سرعت در جهت رفع آن اقدام گردد، امکان حفظ سطوح بالایی از دسترس پذیری وجود خواهد داشت.

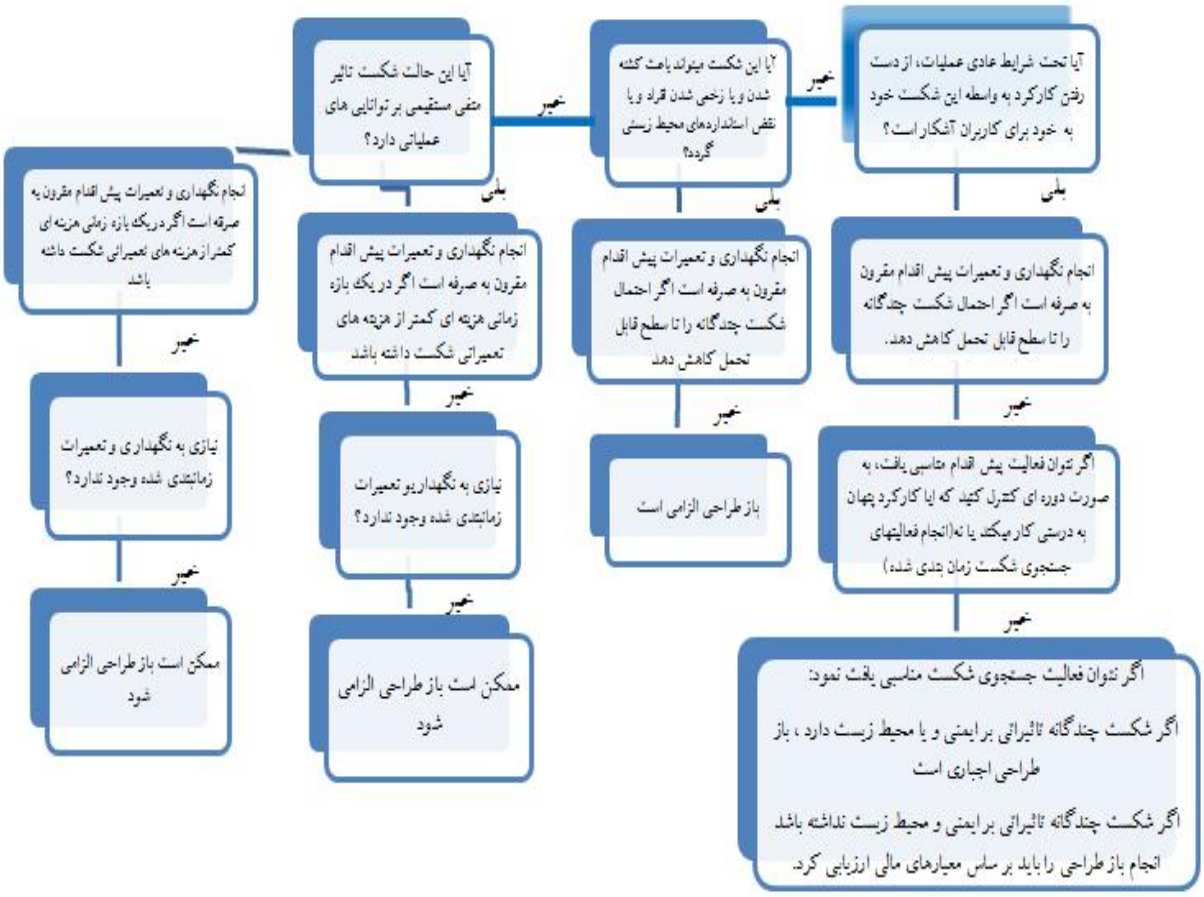
تعریف فعالیتهای زمان بندی شده جستجوی شکست (Detective) در ادامه آمده است.

انجام اصلاحات بر روی تجهیز

در تعداد اندکی از موارد ممکن است نتوان فعالیتی روتین یافت که بتواند سطح قابل قبولی از دسترس پذیری را حفظ نماید یا انجام فعالیت مورد نظر با فرکانس مناسب غیر عملی باشد. اما برای کاهش ریسک شکست چندگانه به میزان قابل تحمل باید کاری انجام داد، پس در این موارد معمولاً بازگشت به میزنقشه کشی و توجه به ایجاد تغییر در طراحی ضروری است.

هریک از روش های فوق میتواند جهت تعمیرات و نگهداری تجهیزات حفاظتی انتخاب کرد. در ذیل الگوریتمی ارائه گردیده است که روش انتخاب استراتژیهای تعمیراتی در هر دو حالت خطای پنهان و آشکار نشان میدهد. ملاحظه میشود در ابتدا سعی برآن است تا با استفاده از روشهای نت پیش اقدام همچون CBM و یا TBM و ترکیبی از آنها از وقوع خطا جلوگیری نمود اما در صورتیکه نتوان چنین فعالیتی را یافت و یا انجام چنین فعالیتی نتواند با توجه به هزینه در پی داشته، ریسک خطای مورد نظر را تا حد قابل قبولی کاهش دهد از اقدام فعالیت جستجوی شکست یا همان Detective بهره گرفته میشود. و پس از آن نیز با توجه به پیامدهای پیش رو از بازطراحی میتوان استفاده نمود. آنچنان که در ابتدای مقاله نیز به آن اشاره گردید فعالیتهای تست دوره ای که هم اکنون انجام میگردد چندان مثمر ثمر نبوده است و دلیل آن وجود تعداد بی شمار این تجهیزات در شبکه و عدم وجود شرایط عملی و اجرایی به منظور پیاده سازی کامل چنین روشهایی است و در نتیجه در بسیاری از این تجهیزات خطای پنهان شناسایی نگردیده و منجر به وقایع حادثه ساز همچون

شکل1 -فرآیند تصمیم گیری در خصوص نوع استراتژی تعمیراتی



خاموشی های طولانی مدت و در برخی موارد نیز پیامدهای ایمنی و عملیاتی و مالی میگردد. از آنجا که فعالیتهای پیش اقدام به موجب هزینه های بالا فقط در شرایط خاص صورت میپذیرد .

لذا با توجه به ویژگیهای فعالیت جستجوی شکست میتوان از آن به منظور تست های دوره ای تمامی تجهیزات حفاظتی استفاده نموده و در صورتیکه برای تعداد محدودی ازتجهیزات حفاظتی این فعالیت عملیاتی نباشد، با توجه به اهمیت آن تجهیز، عملیات نگهداری حذف و یا از سایر پیشنهادات RCM همچون اقدامات نت پیشگیرانه و یا تغییر نوع طراحی استفاده میگردد. این تصمیم گیری با توجه به فاصله زمانی میان فعالیت جستجوی شکست صورت میپذیرد که در ادامه شرح داده شده است.

4-فعالیت جستجوی شکست (detective):

بیشتر آنچه تا امروز درباره موضوع استراتژی نگهداری و تعمیرات نوشته شده است درباره سه نوع از نگهداری و تعمیرات پیشگویانه، پیشگیرانه و اصلاحی است. فعالیتهای پیشگویانه شامل بازرسی برای کشف وقوع شکست هستند. نگهداری و تعمیرات پیشگیرانه به معنی تعمیر اساسی یا تعویض قطعات در فواصل زمانی مشخص است. نگهداری و تعمیرات اصلاحی عبارت است از تعمیرو اصلاح وضعیت چه در زمانی که یک شکست در راه است و چه پس از وقوع شکست. فعالیتهای که فقط به منظور کنترل وضعیت سالم یا خراب بودن سیستم یا قطعه ای در همان لحظه به کار میروند را اصطلاحاً

فعالیتهای جستجوی شکست می نامند. جستجوی شکست تنها در مورد شکست های پنهان و آشکار نشده به کار میرود و شکست های پنهان نیز فقط بر روی تجهیزات حفاظتی تاثیر گذار است .اگرچه در مواقعی نگهداری و تعمیرات پیش اقدام مناسب نیستند، ولی هنوز انجام فعالیتی برای کاهش احتمال وقوع شکستهای چندگانه تا یک سطح قابل قبول الزامی است. جستجوی شکست زمان بندی شده شامل کنترل کردن کارکرد پنهان در فواصل منظم برای روشن شدن کارکرد یا عدم کارکرد آن است. از آنجا که فعالیتهای جستجوی شکست به کنترل آن چه که تجهیز دقیقاً باید انجام بدهد میپردازد و نه به خود تجهیز، به نام کنترل های کارکردی نیز شناخته میشود.

5-تعیین فواصل زمانی فعالیتهای جستجوی شکست (Failure Finding Interval : FFI):

یکی از جنبه های اساسی فعالیت جستجوی شکست، تعیین فاصله زمانی میان فعالیتهای کشف شکست می باشد. برای تعیین فواصل فعالیتهای جستجوی شکست از دو پارامتر دسترس پذیری و قابلیت اطمینان استفاده میگردد.

اگر از FFI به عنوان مخفف فاصله جستجوی شکست و از M به جای MTBF (میانگین زمان میان شکستها به عنوان یک شاخص قابلیت اطمینان) استفاده شود در اینصورت با در دست داشتن میزان دسترس پذیری(Availability) میتوان معادله زیر را نوشت:

$$FFI = 2(1 - A)\, M \qquad (۲)$$

بطوریکه:

A = Availability

M = MTBF

FFI = Failure Finding Interval

این رابطه به مدل موبری یا هورتون (Horton) مشهور است. به منظور درک نکته کلیدی ارتباط میان فواصل کنترل، دسترس پذیری مطلوب و MTBF و فارغ از فرمولهای ریاضی میتوان به جدول زیر مراجعه نمود.

جدول2– ارتباط دسترس پذیری و FFI

دسترس پذیری مورد نیاز برای کارکرد پنهان	%99,99	%99,95	%99,9	%99,5	%0,99	%98	%95
فاصله زمانی جستجوی شکست (به عنوان درصدی از MTBF)	%0,02	%0,1	%0,2	%1	%2	%4	%10

دسترس پذیری مورد نیاز:

با روشن شدن رابطه میان دسترس پذیری، قابلیت اطمینان و فواصل جستجوی شکست، موضوع مهم نحوه تصمیم گیری در خصوص دسترس پذیری مورد نیاز است.

در بخش دوم همین مقاله اشاره گردید که

احتمال شکست چندگانه = احتمال شکست کارکرد تحت حفاظت × در دسترس نبودن ابزار محافظ (1)

پس 3 مرحله زیر بایستی با توجه به رابطه فوق صورت پذیرد:

1-سازمان اعلام نماید برای چه احتمالی از وقوع شکست چندگانه(اگر تجهیز حفاظتی نتواند واکنش مقتضی نشان دهد) آماده است.

2-کارکرد تحت حفاظت در دوره مورد نظر با چه احتمالی ممکن است دچار خرابی گردد(نرخ خرابی تجهیز مورد حفاظت)

3- در انتها با استفاده ا ز رابطه (1) ، تعیین دسترس پذیری مورد نیاز برای تجهیزات حفاظتی جهت کاهش احتمال شکست چندگانه تا سطح مطلوب

علاوه بر 3 مرحله فوق جهت تعیین دسترس پذیری به منظور تعیین FFI لازم است تا MTBF، مدت زمان متوسط بین شکست تجهیزات حفاظتی نیز تعیین گردد. برای تعیین این شاخص نیز از اطلاعات گذشته تجهیزات و نظرات خبرگان و مجریان با سابقه تعمیرات استفاده میگردد.

با توجه به 3 مرحله فوق و رابطه 2 ،میتوان مدل هورتون را با استفاده از احتمالات یاد شده جایگزین نمود.

$P_{inc} \le P_{max}$

$P_{inc} = P_{ted} \times (1 - A) = P_{ted} \times FFI/(2M)$

$P_{ted} \times FFI/(2M) \le P_{max}$

$$FFI \le \frac{2MP\max}{Pted} \qquad (3)$$

احتمال کنونی شکست چندگانه P_{inc}= ماکزیمم احتمال قابل تحمل شکست چندگانه با P_{max} = نظر کارفرما (احتمال مورد نظر برای آینده سیستم با وجود تعمیرات)

باید در نظر داشت که در صورت تعمیرات میزان خواسته کاربر سیستم از تجهیزات و شبکه بالاتر رفته و یا حداقل نبایستی کاهش یابد. به همین دلیل از رابطه $P_{inc} \le P_{max}$ استفاده گردیده است .

این موضوع را در خصوص دسترس پذیری نیز صادق است رابطه دسترس پذیری بدون در نظر داشتن تعمیرات پیشگیرانه و با در نظر داشتن آن متفاوت بوده و در ذیل آمده است.

A_i=MTTF / (MTTF+MTTR)

A_O=MTTM / (MTTM+M+MTW)

MTTF=Mean Time to Failure

MTTR=Mean Time to Repair

MTTM= Mean Time to Maintenance

MTW=Mean Time Waste

(زمان هدر رفته برای تامین منابع تعمیراتی)

M=Mean Maintenance Time

(زمان مورد نظر برای انجام تعمیرات)

اگر اطلاعات دقیقی درباره احتمال شکست کارکرد تحت حفاظت و مدت زمان متوسط شکست کارکرد پنهان در دست باشند، محاسبات را با سرعت بیشتری میتوان انجام داد. اما اگر این اطلاعات در دسترس نباشد (که معمولاً نیست)، باید مقدار این پارامترها را در شرایط عملیات مربوطه تخمین زد. در موارد کمی ممکن است بتوان اطلاعات از این منابع بدست آورد:

- سازنده تجهیزات
- بانک های اطلاعاتی تجاری
- سایر کاربران تجهیزات مشابه

در بسیاری مواقع تخمین ها باید بر اساس دانش و تجربه افرادی که راجع به تجهیزات از همه آگاه تر هستند انجام شود. در بیش تر مواقع این افراد همان اپراتورها و استادکاران نگهداری و تعمیرات هستند.

اگر سوابق اطلاعاتی کافی در دسترس نباشد(که معمولاً نیست)، برای شروع چاره ای جز حدس زدن MTBF وجود ندارد. اما در این مورد نیز اطلاعاتی که بدست می آیند و ثبت میشوند، باید برای تایید اعتبار تصمیمات اولیه بررسی شوند.

سایر روش های محاسبه فواصل شکست:

انواع روش های تعیین فواصل شکست به هیچ وجه محدود به نمونه های که ذکر شد نیست. انواع روشهای دیگری نیز توسط متخصصین RCM ابداع و بکار گرفته شده اند که میتوان به نمونه های زیر اشاره کرد:

- سیستم رای گیری
- سیستم های چندگانه مستقل و تکراری
- به دست آوردن فواصل بهینه از نظر هزینه (وقتی شکست تاثیری بر ایمنی و محیط زیست نداشته باشد)

عملی بودن فواصل فعالیت:

روش هایی که تاکنون درباره محاسبه فواصل جستجوی شکست ذکر شده اند، گاهی فواصل بسیار کوتاه یا بسیار طولانی را نتیجه میدهند. در برخی موارد این فواصل بیش از حد کوتاه باشند، برای مثال میتوان به فعالیتهای جستجوی شکستی اشاره نمود که هر چند روز یک بار نیاز به توقف سیستم اصلی را ایجاد نماید.

فعالیت ممکن است درباره مواردی عادت ایجاد نموده و حساسیت ها را از بین ببرد، مثلاً آژیر خطری که هر روز به صورت آزمایشی به صدا در آید.

در این نمونه فعالیتهای پیشنهادی رد می شود، و به مرحله بعدی RCM موکول میگردد.

گاهی این فواصل زمانی بسیار طولانی بوده و حتی گاهی در حدود چند سال می باشد. در این موارد بدیهی است نیازی به نگرانی درباره عدم انجام فعالیت وجود ندارد. در این نمونه ها برای فعالیت پیشنهادی باید چنین شرحی را در نظر گرفت که " وضعیت ریسک یا قابلیت اطمینان به طوری است که به انجام فعالیت جستجوی شکست نیازی نیست"

در موارد بسیار اندکی، فاصله انجام فعالیتی از بازه زمانی که سیستم خودش را کنترل میکند هم طولانی تر میشود که منطقی به نظر نمی رسد. در این موارد پاسخ به سئوال عملی بودن یا نبودن فعالیت در بازه زمانی مورد نظر منفی است.

5-اجرای فعالیت جستجوی شکست در یک سیستم نمونه:

اجرای این نمونه برای رله های پرایمری بخشی از شبکه توزیع به انجام رسیده است به این منظور اطلاعات گذشته تجهیزات در حدود 3 سال گذشته جمع آوری و اطلاعات و تجارب خبرگان شبکه نیز گرد آوری گردید.در این اطلاعات میزان خرابی ها و فاصله زمانی خرابیها هر یک از رله ها مشخص گردید و سپس MTBFمیانگین مشخص گردید اطلاعات 5 رله پرایمری در 3 سال گذشته در جدول ذیل آمده است .

جدول 3 - اطلاعات سالهای گذشته رله های پرایمری

	سال 87	سال88	سال 89
A	OK	FAIL	OK
B	OK	OK	FAIL
C	FAIL	OK	OK
D	FAIL	OK	OK
E	OK	OK	FAIL

عمر کاری کل رله های این 5 پست معادل 5*3=15 سال است که در مجموع 5 خرابی را به دنبال داشته است این خرابیها میتواند در بازه های زمانی متفاوت از یک سال صورت پذیرفته باشد برای مثال یک خرابی میتواند یک روز پس از بازدید سالیانه یا حتی یک روز قبل از بازدید سالیانه صورت پذیرفته باشد. ولی به طور میانگین فاصله زمانی خرابیها 3سال (MTBF=15/5) در نظر گرفته میشود. با توجه به موقعیت سیستم تحت مطالعه میزان دسترس پذیری هریک از رله ها معین و سپس FFI آن تعیین گردید که در جدول زیر مشاهده میگردد.

جدول 4 -نتایج محاسبات شبکه نمونه

	Availability	FFI (روز)	RCM پیشنهادی	NET پیشین
A	%99,5	10	باز طراحی	1ساله
B	%98	44	فرآیند CBM یا TBM	1ساله
C	%0,90	219	FF	1ساله
D	%95	109	FF	1ساله
E	%85	328	FF	1ساله

در خصوص عملی بودن فاصله فعالیت محاسبه شده در جدول فوق مشاهده میگردد که برخی بسیار کوتاه است و در زمانهای بسیار نزدیک بایستی تست گردد لذا با توجه به این مقادیر RCM موارد دیگری را پیشنهاد می نماید زیرا در این فعالیت جستجوی شکست نمی تواند به طور موثری، مفید واقع گردد. لذا در مورد اول پیشنهاد گردید به منظور افزایش دسترسی و قابلیت اطمینان مور نظر باز طراحی و یا تغییر در نوع حفاظت صورت پذیرد و در مورد دوم نیز استفاده از سایر فرآیندهای تعمیراتی همچون CBM و یا TBM پیشنهاد میگردد که آنهم بایستی از نظر هزینه مقرون به صرفه باشد و با توجه به معیارهای حال حاضر شرکتهای توزیع تغییر نوع حفاظت و باز طراحی مقرون به صرفه تر خواهد بود.

نتیجه گیری :

در این مقاله به بررسی تجهیزات حفاظتی که دارای نوعی از خطای پنهان هستنند پرداخته شد و این ویژگی شرح و سپس با توجه به آن، فرآیندهای استراتژی تعمیراتی این نوع از تجهیزات تنظیم گردید و از آنجا که اجرای فعالیتهای پیشگیرانه همچون CBM و TBM نمی تواند به طور موثری به جهت وجود برخی از شرایط نامناسب عملی و اجرایی همچون هزینه های گزاف پیاده سازی گردد، لذا پیشنهاد گردید از ابتدا فعالیت جستجوی خطا برای تجهیزات حفاظتی صورت پذیرد و با استفاده از مدل هورتون فواصل تست و بازرسی تعیین گردد و در صورتیکه این میزان با لحاظ نمودن دسترس پذیری و قابلیت اطمینان بسیار زیاد و یا بسیار کم باشد طوریکه نتوان این فعالیت را عملی نمود، از سایر پیشنهادات RCM بهره گرفته میشود.

مراجع :

1-"Reliability-Centered Maintenance,2ed",1997,John Moubray

۲-"تعیین فاصله زمانی بهینه تستهای نگهداری دوره ای سیستم های حفاظتی پستهای فوق توزیع و انتقال"، 25 کنفرانس بین المللی، محمد هادی زارع

3-"Application of Reliability Centered maintenance to Optimize Operation and Maintenance in Nuclear Power Plants", International Atomic Energy Agency, may2007

4-"cost based risk analysis to indentify inspection and restoration intervals of hidden failures subject to aging", Alireza Ahmadi, IEEE transaction on Reliability, VOL 60, March 2011

5-"The easy way to understand Maintenance", 2nd Edition, 2007, Jan Frånlund, Swedish Maintenance Society, UTEK

6-" Developing Performance Indicators for Managing Maintenance", Terry Wireman, Industrial Press Inc., 2005

7-"Maintenance, Replacement and Reliability", A.K.S.Jardine, Pitman Publishing, 1973