دانشگاه صنعتی امیرکبیر
قطب علمی قدرت

اولین کنفرانس تخصصی حفاظت و کنترل سیستمهای قدرت
the 1st Power System Protection & Control conference PSPC
Dec 20, 21th 2006
۲۹ و ۳۰ آذر ۸۵

انجمن مهندسین برق و الکترونیک ایران
شاخه ی تهران

تعیین بازه زمانی بهینه تست‌های دوره‌ای و خود بازبینی در تجهیزات حفاظتی با استفاده از یک مدل قابلیت اطمینان

علی سعیدیان
استادیار دانشکده مهندسی - دانشگاه شهید چمران اهواز
a_saidian2000@yahoo.com

مالک قنواتی
کارشناسی ارشد برق قدرت - دانشگاه شهید چمران اهواز
malekghanavati@yahoo.com

چکیده :

قابلیت اطمینان یک رله حفاظتی می‌تواند بوسیلهٔ مراقبت‌های دوره‌ای و یا بوسیلهٔ گنجاندن یک سیستم ناظر داخلی و نیز پایش آن در طول عمر کارکرد، بهبود بخشیده شود. با توجه به خصوصی سازی و تجدید ساختار در صنعت برق، اهمیت به دو مقوله "کیفیت" و "قابلیت اطمینان" در بازار رقابتی برق ضروری است و در رضایت مندی طرف‌های ذی نفع به خصوص مشترکین و مصرف‌کنندگان نقش اساسی را ایفا می‌کنند. در این مقاله ضمن ارائه روشهای دقیق محاسبات قابلیت اطمینان تجهیزات حفاظتی، عوامل متنوع و شاخص‌های مؤثر در قابلیت اطمینان آنها به ازای خطاهای مختلف، مورد تجزیه و تحلیل قرار می‌گیرد. برای این منظور یک سیستم تست اجرا شده در شرکت مناطق نفتخیز جنوب با مشخصات مناسب و کاربردی شبیه‌سازی شده و تحلیل های لازم برروی آن انجام شده است که می‌تواند برای بررسی این ویژگی‌ها استفاده شود.

واژه‌های کلیدی : قابلیت اطمینان - عملکرد نابجا - عدم عملکرد- قابلیت اتکا - خود بازبینی

۱- مقدمه :

بحث قابلیت اطمینان در سیستم‌های حفاظتی با سایر قسمتهای شبکه قدرت متفاوت است. دلیل این اختلاف را می‌بایست در نحوه عملکرد سیستم‌های حفاظتی و انواع خطاهائی که بر آنها مترتب است، جستجو نمود. سیستم حفاظتی شبکه‌های قدرت نقش اساسی در ایمنی، پایداری و قابلیت اطمینان سیستم دارد، سرعت بالا، حساسیت مناسب، دقت کافی، عملکرد بموقع و قابل اطمینان سیستم‌های حفاظتی همیشه جزء عوامل اصلی ارزیابی آنها بوده است. نیازهای شبکه گاه بالاتر از توانائیهای تکنیکی بکار رفته در ساخت و طراحی این سیستم‌ها می‌باشد، به همین دلیل ترکیبهای نسبتاً پیچیده‌ای از سیستم‌های حفاظتی مختلف جهت نیل به خواسته‌های شبکه معرفی شده‌اند، که هر یک از این ترکیبها خصوصیات تکنیکی خاص خود را دارند و از طرف دیگر، هر یک هزینه‌های ساخت و بهره‌برداری خاص خود را نیز دارا می‌باشد.

دو نوع خطای اولیه یک رله، عدم عملکرد[1] و عملکرد نابجا[2] می‌باشند. اقدامات قابل توجهی به منظور بررسی کردن ظواهر مختلف قابلیت اطمینان سیستم‌های حفاظتی انجام شده است. مرجع [11] ، روشی را برای محاسبه احتمال خطای رله حفاظتی معرفی می‌کند. یک شاخص قابلیت اطمینان که با عنوان «احتمال ندیده شدن» در مراجع [1,3] به صورت احتمال اینکه رله برای پاسخ دادن، در زمان عملکرد دچار اشکال شود، ارائه شده است. روش پیشنهاد شده در مرجع [12]، در مرجع [10] با مفهوم عدم دسترسی به سیستم حفاظتی، بهبود و گسترش داده شده است. رله‌های دیجیتالی مدرن معمولاً بوسیلهٔ قابلیت خود بازبینی[3] و کنترل کنندگی[4] تجهیز می‌شوند[4]. مرجع [13] یک مدل مارکوف (Markov) را برای پیش بینی کردن بازهٔ زمانی بهینه تست دوره ای[5] رله‌های حفاظتی با قابلیت خود بازبینی ، توضیح می‌دهد.

1- Fail to Operate
2- Mal Operation
3 - Self Checking
4 - Watchdog
5- Routine Test

۲ - ارزیابی قابلیت اطمینان

قابلیت اطمینان یک محصول عبارتست از کیفیت آن محصول در طول عمر کاری خود. در بحث قابلیت اطمینان سیستم‌های حفاظتی می‌بایست این سیستم‌ها را به شکل مجزا از سایر تجهیزات شبکه‌های قدرت مورد تجزیه و تحلیل قرار داد زیرا این سیستم‌ها خود از اجزای متعددی تشکیل شده‌اند و با این سبک تجزیه و تحلیل می‌توان حساسیت سیستم‌های حفاظتی مختلف را نیز مطالعه کنیم. سیستم‌های حفاظتی به سه طریق می‌توانند خارج از محدوده کار خود خطا کنند.

۲-۱- عملکرد نابجا(Maloperation) : زمانی که خطائی در شبکه رخ نداده است سیستم حفاظتی بی‌جهت با عملکرد نابجا خود باعث قطع جریان برق می‌گردد. این نوع خطا عمدتاً به علت وجود یک سیگنال غیر واقعی در سیستم حفاظتی رخ می‌دهد که نهایتا باعث قطع بی‌مورد کلید می‌شود. این نوع خطا در سیستم حفاظتی از نوع خود آشکار ساز است زیرا پس از بروز به علت قطع بی‌مورد کلید، وجود خود را اعلام می‌کند[15].

۲-۲- عدم عملکرد(Fail To Operate) : زمانی که خطائی در شبکه رخ داده باشد و سیستم حفاظتی نسبت به این خطا از خود عکس العملی را نشان ندهد از آنجائی که سیستم‌های حفاظتی در شبکه‌های قدرت جزء تجهیزات ساکت می‌باشند (یعنی در حالت عادی کار سیستم هیچ عکس العملی از خود نشان نمی‌دهند مگر در صورت بروز خطا با قطع بخشی از شبکه وظیفه خود را انجام دهند). بنابراین هر گونه خطائی در این سیستم آشکار نخواهد شد مگر آنکه پس از بروز خطا در شبکه سیستم حفاظت به غلط نسبت به آن عمل نکند. به‌همین دلیل این نوع خطاهای سیستم حفاظتی از نوع خودآشکار ساز نمی‌باشد.

2-3- عملکرد نادرست (False Operation) : زمانی که خطائی در شبکه رخ داده باشد و سیستم حفاظتی نسبت به این خطا از خود عکس العمل مناسب را نشان ندهد (به عنوان مثال در زمان نامناسب اقدام به قطع مدار بکند) این نوع خطا را می‌توان در ارزیابی از همان نوع قبلی به حساب آوریم. با توجه به تقسیم‌بندی‌های فوق‌الذکر قابلیت اطمینان سیستم حفاظتی به دو بخش عمده تقسیم می‌گردد: قابلیت اتکا و ایمنی

۲-۳-۱- قابلیت اتکا[6]: عبارتست از حصول اطمینان از عملکرد صحیح سیستم حفاظتی به‌هنگام بروز خطا در شبکه، که در اصطلاح به آن قطع موضعی و صحیح می‌گویند.

۲-۳-۲- ایمنی[7]: عبارتست از حصول اطمینان از عدم عملکرد بی‌مورد و نابجای سیستم حفاظتی، مگر در مواقعی که در شبکه خطایی رخ داده باشد.

۳- قابلیت دسترسی[8] :

این عامل عبارتست از نسبت طول عمر مفید کاری یک دستگاه که عملکرد صحیحی دارد به کل طول عمر همان دستگاه. بنابراین قابلیت دسترسی برابر کل طول عمر منهای زمان از دست رفته بعلت خرابی، تعمیر، سرویس و... می‌باشد.

طول عمر یک دستگاه لزوما برابر با زمان مفید کاری همین دستگاه نیست و بسیاری از دستگاهها دارای زمان مفید کاری کمتری نسبت به طول عمر خود می‌باشند. قابلیت‌اطمینان سیستم مقدار خاصی است که بستگی به زمان دارد و با گذشت زمان احتمال خرابی و عیب بالا می‌رود و به شکل تابعی نمائی از زمان است.

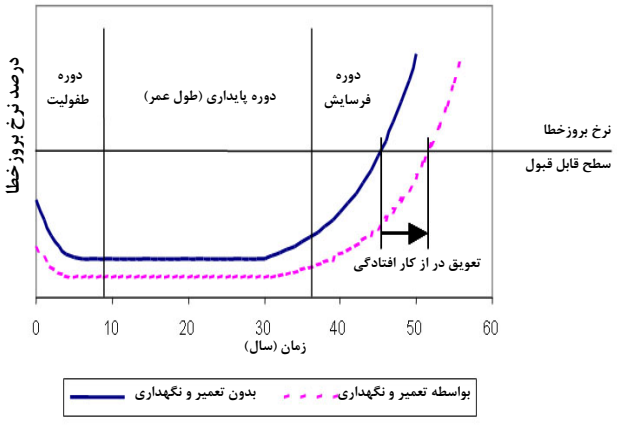
$$R = e^{-\lambda t} \qquad (۱)$$

که در این رابطه R قابلیت اطمینان و λ نرخ خطاست. مقدار λ می‌تواند متغیر باشد ولیکن در مورد اکثر تجهیزات به شکل تجربی ثابت شده است، ابتدا در زمان راه‌اندازی مقدار بالائی است و به مرور کاهش پیدا می‌کند و در طی یک مدت بخصوص این مقدار ثابت باقی می‌ماند و پس از طی این دوره دوباره افزایش پیدا می‌کند. مدت زمانی را که λ ثابت است را از این پس عمر مفید می‌نامیم و تمام بررسیها را در این زمان انجام می‌دهیم. درانتهای عمر مفید جهت جلوگیری از افزایش λ می‌توان با اعمال تعمیر یا سرویس مجدد، λ را به مقدار ثابت خود برگرداند (شکل ۱) و بدین ترتیب

---

6 – Dependability
7- Security
8 - Availability

طول عمر مفید افزایش پیدا می‌کند[13] البته لازم به تذکر است که در اینجا آزمایش، تعمیر یا سرویس بدون خطا در نظر گرفته شده است.



شکل (۱) افزایش منحنی طول عمر مفید و قابلیت دسترسی بدلیل کاهش زمان تعمیرات دوره‌ای

در نهایت مقدار λ در تمام محاسبات ثابت در نظر گرفته می‌شود و از آنجا که مقدار R با زمان تغییر پیدا می‌کند در بررسیهای زمانی از عواملی چون قابلیت دسترسی A و یا عدم قابلیت دسترسی U [9]، استفاده می‌کنند.

اگر فاصله بین دو آزمایش، تعمیر یا سرویس را Tc بگیریم آنگاه خواهیم داشت :

$$U = \frac{1}{Tc}\int_0^{Tc}\left(1 - e^{-\lambda t}\right)dt = 1 - \frac{1}{\lambda Tc}\left(1 - e^{-\lambda t}\right) \qquad (۲)$$

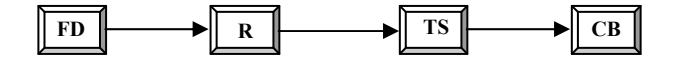
و با فرض $\lambda Tc << 1$ خواهیم داشت :

$$U = \frac{\lambda Tc}{2} \qquad (۳)$$

همانطور که از رابطه (۳) مشخص است با کاهش زمان Tc مقدار عدم قابلیت دسترسی کم می‌شود.

٤ - روش‌های ارزیابی و مدلسازی سیستم :

سیستم‌های حفاظتی ترکیبی از تجهیزات مختلف می‌باشند که هر یک وظیفه خاصی را به عهده دارند در بسیاری از موارد عملکرد یکی از این تجهیزات بستگی به عملکرد تجهیزات قبلی در طی یک سلسله عملیات پی‌درپی دارد و بخاطر این ویژگی خاص سیستم‌های حفاظتی، روش‌های ارزیابی قابلیت اطمینان در آنها از روش‌های مرسوم درشبکه‌های قدرت متفاوت است، که به آنها اشاره گردید. (شکل ۲)



شکل (۲) بلوک دیاگرام تجهیزات حفاظتی

FD : واحد تشخیص دهنده خطا که خود شامل قسمتهای متعددی است از قبیل ترانسهای اندازه‌گیری (مانند ترانس جریان و ترانس ولتاژ خازنی) همچنین مقایسه کننده‌های اولیه را نیز شامل می‌گردد.

R : واحد رله و یا تصمیم‌گیر که عمل تشخیص خطا به عهده این واحد است و مغز متفکر سیستم حفاظتی است که خود می‌تواند شامل مدار تغذیه، مدارهای پروسه تشخیص خطا، مدارهای عمل کننده، مدارهای پایدارکننده و غیره باشد. البته در یک سیستم حفاظتی ممکن است ترکیبی از رله‌های مختلف وجود داشته باشد که در اینجا برای سادگی همه را در یک بلوک قرار می‌دهیم.

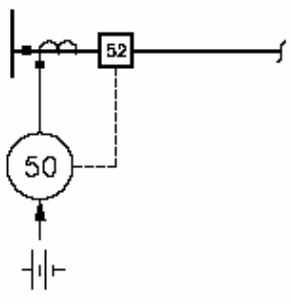
T.S : این واحد شامل منابع تغذیه مربوط به مدار تریپ (که شامل Trip coil و سیم کشی‌های مربوطه است) و غیره می‌باشد.

C.B (مدار شکن) : این قسمت از سیستم حفاظتی تفاوت ماهوی با سایر قسمتها دارد بدین جهت که کلید قسمت محرک و عمل کننده زنجیره حفاظتی بوده و خود هیچگونه تصمیمی نمی‌گیرد، لیکن اجرا کننده دستورات سیستم حفاظتی است و حاصل کار آن قطع قسمتی ازمدار شبکه است.

۵- بررسی آلترناتیو های حفاظتی مختلف :

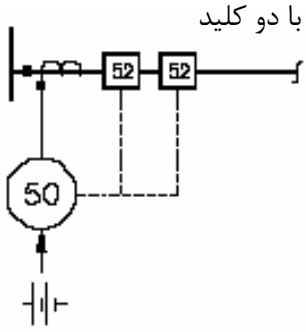
جهت ارزیابی قابلیت اطمینان تجهیزات حفاظتی، سناریوهای زیر را می‌توان مد نظر داشت شامل :

۱) سیستم ساده تکی

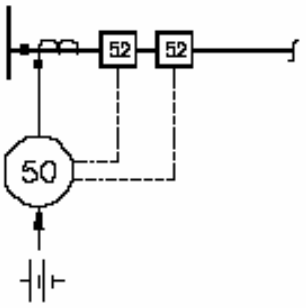


9 - Unavailability

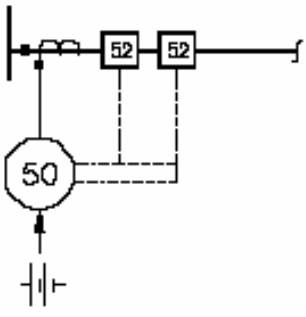
۲) سیستم ساده تکی با دو کلید



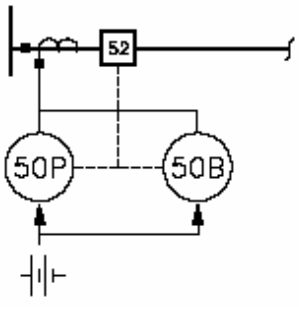
۳) سیستم ساده تکی با دو کلید و مدار تریپ جداگانه برای هر کلید



٤) سیستم ساده تکی با دو کلید و مدار تریپ مشترک بین دو کلید

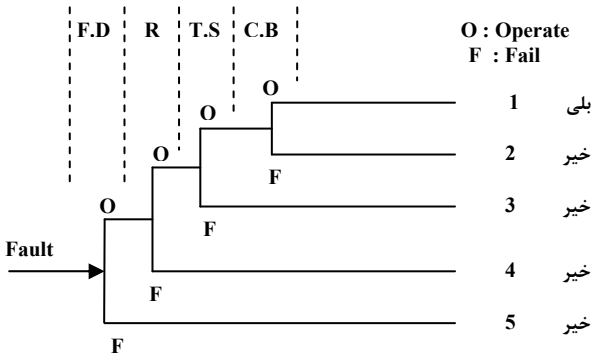


۵) سیستم مضاعف (حفاظت دوبل) و یک کلید



٦ - ارزیابی و مدلسازی سیستم تست :

در شکل (**۳**) درخت وقایع سیستم تست از نوع ساده تکی اجرا شده در صنعت نفت جنوب را می بینیم، مجموعا پنج حالت پیش آمده است که هر یک احتمال خاص خود را داراست . در بین این پنج حالت فقط حالت یک عملکرد مطلوب سیستم حفاظتی را نشان می‌دهد و چهار حالت بعدی همگی حالات خطا می‌باشند. مطابق اطلاعات سازنده هر یک از اجزاء سیستم حفاظتی دارای نرخ خطای 0.02 خطا در سال باشند آنگاه برای هر یک از این اجزاء مقدار ضریب عدم قابلیت دسترسی U از رابطه (**۲**) و یا (**۳**) قابل محاسبه است.



شکل (**۳**) درخت وقایع سیستم تست از نوع ساده تکی اجرا شده در صنعت نفت جنوب

اگر فاصله بین دو آزمایش متوالی را به ترتیب سه ماه، شش ماه و یک سال بگیریم مقدار عدم دسترسی برای هر یک از اجزاء سیستم حفاظتی به ترتیب برابر 0.0025 ، 0.005 و 0.01 خواهد شد. حال جهت ارزیابی قابلیت اطمینان مجموعه سیستم حفاظتی با استفاده از درخت وقایع احتمال حالت های مختلف را محاسبه می کنیم که نتیجه آن جدول (**۱**) می باشد .

حالت	دوازده ماه	شش ماه	سه ماه	نرخ خطا
5	0.01	0.005	0.0025	0.02
4	0.0099	0.004975	0.002493	0.02
3	0.009801	0.004950	0.002487	0.02
2	0.009705	0.004925	0.002481	0.02
fail to operate	0.039407	0.019850	0.009962	0.02
Reliability (1)	0.960592	0.980149	0.990037	0.02

جدول (**۱**) ارزیابی قابلیت اطمینان سیستم تست از نوع ساده تکی با فواصل تعمیر مختلف

جهت ارزیابی عملکرد نابجای سیستم حفاظتی دقیقا مشابه حالت قبل و با استفاده از اطلاعات موجود و درخت وقایع ترسیم شده در شکل (**۳**) عمل می نمائیم، ولیکن نکته اضافی در این است که سیگنال ناخواسته در کجای زنجیره حفاظتی بوجود آمده است اگر در FD بوجود آید آنگاه چهار حالت اول و اگر اشکال در R باشد تنها سه حالت اول درخت وقایع مد نظر خواهند بود و اگر در TS بوجود آید فقط دو حالت اول در نظر گرفته می شود .

در(جدول **۲**) احتمال هر یک از این حالات مشخص شده است. در تمام این سه حالت فقط یک حالت خطاست زیرا تنها در این حالت است که کلید به اشتباه باز می شود. حال هر یک از این احتمالات می بایست در مقدار احتمال بوجود آمدن سیگنال خطا در واحد مربوطه ضرب گردد (مطابق اطلاعات ثبت شده برای هر سه مورد FD و R و TS این احتمال برابر0.001 در سال می باشد) و احتمال بوجود آمدن سیگنال خطا در هر یک از این سه واحد مستقل از دیگری است.

حالت	دوازده ماه	شش ماه	سه ماه	نرخ خطا
Error in FD	0.970592	0.985149	0.992537	0.001
error in R	0.980492	0.990124	0.995031	0.001
error in TS	0.990294	0.995074	0.997518	0.001
mal operation	0.002941	0.002970	0.002985	0.001

جدول (**۲**) نتایج عملکرد نابجا سیستم حفاظتی از نوع ساده تکی با فواصل تعمیر مختلف

۶-۱- نتایج بکارگیری آلترناتیوهای حفاظتی در سیستم تست معرفی شده :

	ساده تکی		
	دوازده ماه	شش ماه	سه ماه
Fail to operate	0.03915030	0.01978547	0.00994610
mal operation	0.00294137	0.00297034	0.00298508
Reliability	0.96084969	0.98021452	0.99005389

جدول (**۳**) ارزیابی قابلیت اطمینان سیستم تست ساده تکی

	ساده تکی با دو کلید		
	دوازده ماه	شش ماه	سه ماه
Fail to operate	0.02970199	0.01492524	0.00748128
mal operation	0.00291226	0.00295557	0.00297764
Reliability	0.97029801	0.98507475	0.99251871

جدول (**٤**) ارزیابی قابلیت اطمینان سیستم تست ساده تکی با دو کلید

	ساده با دو کلید و مدار تریپ جداگانه		
	دوازده ماه	شش ماه	سه ماه
Fail to operate	0.01970395	0.00992549	0.00498131
mal operation	0.00288255	0.00294064	0.0029701
Reliability	0.98029604	0.99007450	0.99501868

جدول (**۵**) ارزیابی قابلیت اطمینان سیستم تست ساده با دو کلید و مدار تریپ جداگانه

	ساده با دو کلید و مدار تریپ مشترک		
	دوازده ماه	شش ماه	سه ماه
Fail to operate	0.01990000	0.00997500	0.00499375
mal operation	0.00289251	0.00294565	0.00297265
Reliability	0.98010000	0.99002500	0.99500625

جدول (**٦**) ارزیابی قابلیت اطمینان سیستم تست ساده با دو کلید و مدار تریپ مشترک

	سیستم دوبل		
	دوازده ماه	شش ماه	سه ماه
Fail to operate	0.00992549	0.00498131	0.00249532
mal operation	0.00294069	0.00297017	0.00298504
Reliability	0.99007450	0.99501868	0.99750467

جدول (**۷**) ارزیابی قابلیت اطمینان سیستم تست از نوع مضاعف

با مقایسه جدول های (**۳**) تا (**۷**) مشاهده می شود که استفاده از سیستم های دوبل (مضاعف) باعث کاهش خطای سیستم حفاظتی تا حد $\left(\frac{1}{4}\right)$ شده و راهی جهت افزایش قابلیت اطمینان می‌باشد. برای بهینه سازی قابلیت اطمینان سیستم حفاظتی دوبله نمودن کلید قدرت بسیار گران است لذا استفاده از رله بسیار منطقی است. یکی از راهکار های مناسب دوبله نمودن تریپ کویل[10] کلید می باشد، دوبله نمودن منبع تغذیه برای هر کدام از تریپ کویل ها نیز شیوه ای مناسب است.

۷- افزایش قابلیت اطمینان تجهیزات حفاظتی :

جهت افزایش قابلیت اطمینان سیستم های حفاظتی روشهای متعددی تا کنون پیشنهاد و اجرا شده اند. این روشها در مورد رله‌های استاتیکی، رله‌های جدید دیجیتالی یا میکروپروسسوری بیشتر مطرح شده اند زیرا در این نوع رله ها اجرای این روشها به مراتب آسانتر گشته است .

۷-۱- بازبینی مستمر :[11]

یکی از روشهای تشخیص عیب در قسمتهای سیستم حفاظتی ، بازبینی آنهاست. وجود ارتباطات و اتصالات متعدد رله با منابع تغذیه DC ، ترانسهای جریان و ولتاژ، مدارهای تریپ کلید و غیره با توجه به ماهیت سری

10 - Trip Coil
11- Continous Supervision

سیستم حفاظتی احتمال خطای سیستم مجموع را افزایش می دهد. بنابراین بازبینی هر یک از این مدارها می تواند وجود عیب در آنها، قبل از اینکه خطائی در شبکه پیش آید و سیستم حفاظتی نسبت به آن عمل نکند، را مشخص نماید و با انجام تعمیر مناسب سیستم حفاظتی را به حالت سالم خود برگردانیم. امروزه بازبینی مستمر مدارهای تغذیه DC ، مدارهای تریپ کلید، مدار ثانویه ترانسهای ولتاژ و ترانسهای جریان در پستهای فشار قوی از ضروریات است. هر چند که وجود چنین مدارهای بازبینی کمک زیادی به افزایش قابلیت اطمینان سیستم حفاظتی می کند، ولیکن به دلیل پیچیدگی عمل قسمتهای مختلف سیستم حفاظتی، این مدارها قابل به تشخیص عیب در تمام حالات کاری سیستم حفاظتی نیستند و از طرفی مدارهای بازبینی نیز خود دچار عملکرد خطادار می شوند. بنابراین نمی توان تمام اعتماد را بر روی این مدارها پایه ریزی نمود .

مدارهای بازبینی نه تنها برای سیستم های ساده حفاظتی (تکی) مفید می باشند بلکه در مورد سیستم های مضاعف نیز ضروری می باشند، زیرا در غیر این صورت در اثر وجود خطا در یکی از قسمتهای سیستم حفاظتی، عملاً سیستم حفاظتی مضاعف تبدیل به سیستم حفاظتی تکی می گردد. در رله های استاتیکی و دیجیتالی (میکروپروسوری) امکان افزودن مدارهای بازبینی مستمر به مراتب آسانتر از مدار رله های الکترومکانیکی است .

۷-۲- بازرسی و آزمایش دوره‌ای :

در قسمت‌های قبل دیدیم که انجام آزمایشات دوره ای می‌تواند قابلیت اطمینان را در محدوده بخصوصی نگهدارد. طبیعی است که زمان بین دو آزمایش متوالی می بایست از طول عمر مفید سیستم حفاظتی کوتاهتر باشد و هر چه این زمان کاهش یابد احتمال خطا (عمل نکردن سیستم حفاظتی در هنگام خطا) در سیستم حفاظتی کاهش خواهد یافت. از طرف دیگر هر یک از این آزمایشات زمانبر و دارای هزینه است و در حین آزمایش عملاً سیستم حفاظتی خارج از مدار خواهد بود بنابراین این آزمایشها نمی توانند در فواصل زمانی کوتاه انجام گردند و معمولترین پریود آزمایش دوره ای رله ها شش ماه و یا یکسال می باشد. متاسفانه اهمیت این موضوع در برخی سیستم ها چندان جا افتاده نیست و در اکثر موارد مسئولین ضرورتی بر انجام این کار نمی بینند. که نتیجه آن واضح است « مواجهه با سیستم های حفاظتی پیچیده و غامض و در عین حال عدم اعتماد و اطمینان به عملکرد صحیح آن » .

با انجام چنین آزمایشهائی ، محدودیتهای ذکر شده در حالت بازبینی مستمر از بین می رود و عملاً نقاط ضعف آنرا هم خواهد پوشاند. وضعیت سیستم حفاظتی در طی آزمایش نیز به دقت بررسی می گردد و در نتیجه با اتکا به این اطلاعات می توان محاسبات دقیقتری را در مورد قابلیت اطمینان سیستم حفاظتی انجام دهیم .

امروزه با رله های جدید استاتیکی و دیجیتالی امکان آزمایش خودکار رله های حفاظتی تا حدی به وجود آمده است، در این حالت سیستم "آزمایش خودکار" می تواند هم به شکل دستی و یا در زمانهای بخصوص به شکل خودکار رله را تحت آزمایش قرار دهد و در صورت وجود عیب، آنرا اعلام کند. آزمایش رله می بایست زمانیکه خطایی در شبکه بروز می کند قطع گردد و رله کار عادی خود را انجام دهد. همین نکته باعث پیچیده تر شدن مدار آزمایش خودکار می گردد که هزینه ها را نیز بالا خواهد برد البته در مورد رله های دیجیتالی این مشکل کمتر به چشم می خورد زیرا فقط با افزودن نرم افزار مربوطه این امکان را در رله بوجود می آورند .

۸- نتیجه گیری :

در این مقاله ضمن ارائه تکنیکهای پیشنهادی جهت محاسبه شاخص قابلیت اطمینان تجهیزات حفاظتی به ازای انواع خطاهای آنها، ارزیابی سیستمهای مختلف حفاظتی از ساده‌ترین نوع آنها تا پیچیده‌ترین شکل‌شان مطرح شدند و همانطور که مشاهده شد استفاده از سیستم‌های حفاظتی مضاعف[12] و پیچیده همیشه جوابگوی نیازهای ما نخواهد بود. اگر با استفاده از چنین سیستمهائی بعنوان مثال قابلیت اتکا افزایش یابد چه بسا که ایمنی همان سیستم شدیداً کاهش یابد و بالعکس.

12- Redundant

لذا راه حل منطقی شناخت تجهیزات بطور کامل از نقطه نظر نوع خطا، قابلیت اطمینان ازیکسو ، و از طرف دیگر شناخت کامل بخشی از شبکه که قرار است حفاظت شود، از نقطه نظر اهمیت ، سرعت و نوع خطا می‌باشد. برای بهینه سازی سیستم‌های حفاظتی، متناسب با این اطلاعات و آمار خطاها، تصمیم به انتخاب ادوات حفاظتی گرفته شود و در عمل نیز ضمن آزمایش دوره‌ای تجهیزات حفاظتی می‌توان بر خلاف تجربیات فعلی، از یک سیستم حفاظتی منظم، قابل اطمینان و ایمن برخوردار بود.

مراجع :

[1] Xingbin Yu & Chanan Singh.” A Practical Approach for Integrated Power System Vulnerability Analysis With Protection Failures “ IEEE TRANSACTIONS ON POWER SYSTEMS, VOL. 19, NO. 4, NOVEMBER 2004

[2] Nagaraj Balijepalli & Subrahmanyam S. Venkata. “ Modeling and Analysis of Distribution Reliability Indices “ IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 19, NO. 4, OCTOBER 2004

[3] Xingbin Yu & Chanan Singh.” Integrated Power System Vulnerability Analysis Considering Protection Failures “ IEEE TRANS , 2003 , PP. 706 - 711

[4] Roy Billinton & M. Fotuhi-Firuzabad & T. S. Sidhu “ Determination of the Optimum outine Test and Self-Checking Intervals in Protective Relaying Using a Reliability Model “IEEE TRANS. ON POWER SYSTEMS, VOL. 17, NO. 3, AUGUST 2002

[5] Gerald F. Johnson “ Reliability Considerations of Multifunction Protection “ IEEE TRANS. ON INDUSTRY APPLICATIONS, VOL. 38, NO. 6, NOVEMBER / DECEMBER 2002

[6] L. Rafael Castro Ferreira & Peter A. Crossley & Ronald N. Allan & John Downes “ The Impact of Functional Integration on the Reliability of Substation Protection and Control Systems “ IEEE TRANS. ON POWER DELIVERY, VOL. 16, NO. 1, JANUARY 2001

[7] Hongye Wang & James S. Thorp “ Optimal Locations for Protection System Enhancement: A Simulation of Cascading Outages “IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 16, NO. 4, OCTOBER 2001

[8] J S Pugh & L R Castro Ferreira & P A Crossley & R N Allan & J Goody & J Dowries & M Burt. “ THE RELIABILITY OF PROTECTION AND CONTROL SYSTEMS FOR TRANSMISSION FEEDERS “ Developments in Power System Protection, 25-27th March 1997, Conference Publication No. 434, IEE, 1997

[9] P. M. Anderson and S. K. Agarwal, “ An improved model for protective system reliability,” IEEE Trans. Rel., vol. 41, pp. 422–426, Sept. 1992.

[10] IEEE Working Group D5 of the Line Protection Subcommittee, Power System Relaying Committee, “Proposed statistical performance measures for microprocessor-based transmission-line protective relays—Part I: Explanation of the statistics,” IEEE Trans. Power Delivery, vol. 12, pp. 134–143, Jan. 1997.

[11] J. D. Grimes, “On determining the reliability of protective relay systems,” IEEE Trans. Rel., vol. R-19, pp. 82–85, Aug. 1970.

[12] C. Singh and A. D. Patton, “Protection system reliability modeling: Unreadiness probability and mean duration of undetected faults,” IEEE Trans. Rel., vol. R-29, pp. 339–340, Oct. 1980.

[13] J. J. Kumm, M. S.Weber, D. Hou, and E. O. Schweitzer, “Predicting the optimum routine test interval for protective relays,” IEEE Trans. Power Delivery, vol. 10, pp. 659–665, Apr. 1995.

[14] P. M. Anderson, G. M. Chintaluri, S. M. Maghbuhat, and R. F. Ghajar, “An improved reliability model for redundant protective systems—Markov models,” IEEE Trans. Power Syst., vol. 12, pp. 573–578, May 1997.

[15] D. C. Elizondo, J. de la Ree, A. G. Phadke, and S. Horowitz, “Hidden failures in protection systems and their impact on wide-area disturbances,” in Proc. IEEE Winter Power Meeting, vol. 2, 2001, pp. 710–714.

[16] A. G. Phadke and J. S. Thorp, “Expose hidden failures to prevent cascading outages in power systems,” IEEE Comput. Applicat. Power, vol. 9, pp. 20–23, July 1996. Annu. Western Protective Relay Conf., Oct. 18–20, 1994, pp. 1–14.