

روشی جدید برای بهبود و ارتقاء تجهیزات حفاظتی با استفاده از یک مدل قابلیت اطمینان

مالک قنواتی

کارشناس ارشد رله های حفاظتی

شرکت بهره برداری نفت و گاز مارون ، ایران

ghanavati3.m@nisoc.ir

علی سعیدیان

استادیار دانشکده مهندسی

دانشگاه شهید چمران اهواز ، ایران

a_saidian@scu.ac.ir

واژه های کلیدی: قابلیت اطمینان - عملکرد نابجا - عدم عملکرد- قابلیت اتکا - خود بازیینی

۱- مقدمه :

چکیده

بحث قابلیت اطمینان در سیستم های حفاظتی با سایر قسمتهای شبکه قدرت متفاوت است. دلیل این اختلاف را می بایست در نحوه عملکرد سیستم های حفاظتی و انواع خطاهائی که بر آنها مترتب است، جستجو نمود. سیستم حفاظتی شبکه های قدرت نقش اساسی در امنیت، پایداری و قابلیت اطمینان سیستم دارد، عوامل اصلی ارزیابی قابلیت اطمینان سیستم های حفاظتی شامل سرعت بالا، حساسیت مناسب، دقت کافی، عملکرد بموقع است. نیازهای شبکه گاه بالاتر از توانائیهای تکنیکی بکار رفته در ساخت و طراحی این تجهیزات می باشد، به همین دلیل ترکیبهای نسبتاً پیچیده ای از سیستم های حفاظتی مختلف جهت نیل به خواسته های شبکه معرفی شده اند، که هر یک از این ترکیبها خصوصیات تکنیکی خاص خود را دارند و از طرف دیگر، هر یک هزینه های ساخت و بهره برداری خاص خود را نیز دارا می باشد [1,3].

بوسیله مراقبت های دوره ای و یا بوسیله گنجانیدن یک سیستم ناظر داخلی و نیز پایش آن در طول عمر کارکرد، قابلیت اطمینان یک رله حفاظتی می تواند بهبود بخشیده شود. اهمیت به دو مقوله "قابلیت اطمینان" و "کیفیت" در بازار رقابتی برق با توجه به خصوصی سازی و تجدید ساختار در صنعت برق ضروری است و در رضایت مندی طرف های ذی نفع به خصوص مشترکین و مصرف کنندگان نقش اساسی را ایفا می کنند. در این مقاله ضمن ارائه روشهای دقیق محاسبات قابلیت اطمینان تجهیزات حفاظتی، عوامل متنوع و شاخص های مؤثر در قابلیت اطمینان آنها به ازای خطاهای مختلف، مورد تجزیه و تحلیل قرار می گیرد. برای این منظور یک سیستم تست در شرکت ملی مناطق نفتخیز جنوب (NISOC) با مشخصات مناسب و کاربردی اجرا، شبیه سازی و تحلیل های لازم بر روی آن انجام شده است که می تواند برای بررسی این ویژگی ها مورد استفاده قرار گیرد.

بیست و چهارمین کنفرانس بین‌المللی برق

حفاظتی رخ می‌دهد که نهایتاً 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 [19].

۲-۲- عدم عملکرد (Fail To Operate): زمانی که خطائی در شبکه رخ داده باشد و سیستم حفاظتی نسبت به این خطا از خود عکس‌العملی را نشان ندهد از آنجائی که سیستم‌های حفاظتی در شبکه‌های قدرت جزء تجهیزات ساکت می‌باشند (یعنی در حالت عادی کار سیستم هیچ عکس‌العملی 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.

۲-۳- عملکرد نادرست (False Operation): زمانی که خطائی در شبکه رخ داده باشد و سیستم حفاظتی نسبت به این خطا از خود عکس‌العمل 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 آورد. با توجه به تقسیم‌بندی‌های فوق‌الذکر قابلیت اطمینان سیستم حفاظتی به دو بخش عمده تقسیم می‌گردد: قابلیت اتکا و امنیت

۲-۳-۱- قابلیت اتکا^۶: 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- امنیت^۷: عبارتست از حصول اطمینان از عدم عملکرد بی‌مورد و نابجای سیستم حفاظتی، مگر در مواقعی که در شبکه خطایی رخ داده باشد.

دو نوع خطای اولیه یک رله، عدم عملکرد^۱ و عملکرد نابجا^۲ می‌باشند. اقدامات قابل توجهی به منظور بررسی کردن ظواهر مختلف قابلیت اطمینان سیستم‌های حفاظتی انجام شده است. مرجع [15]، روشی را برای محاسبه احتمال خطای رله حفاظتی معرفی می‌کند. یک شاخص قابلیت اطمینان که با عنوان «احتمال ندیده شدن» در مراجع [5,7] به صورت احتمال اینکه رله برای پاسخ دادن، در زمان عملکرد دچار اشکال شود، ارائه شده است. روش پیشنهاد شده در مرجع [16]، در مرجع [14] با مفهوم عدم دسترسی به سیستم حفاظتی، بهبود و گسترش داده شده است. رله‌های دیجیتال مدرن معمولاً بوسیله قابلیت خود بازمی‌یابی^۳ و کنترل کنندگی^۴ تجهیز می‌شوند [8]. مرجع [17] یک مدل مارکوف (Markov) را برای پیش بینی کردن بازه زمانی بهینه تست دوره ای^۵ رله‌های حفاظتی با قابلیت خود بازمی‌یابی، توضیح می‌دهد.

۲- ارزیابی قابلیت اطمینان

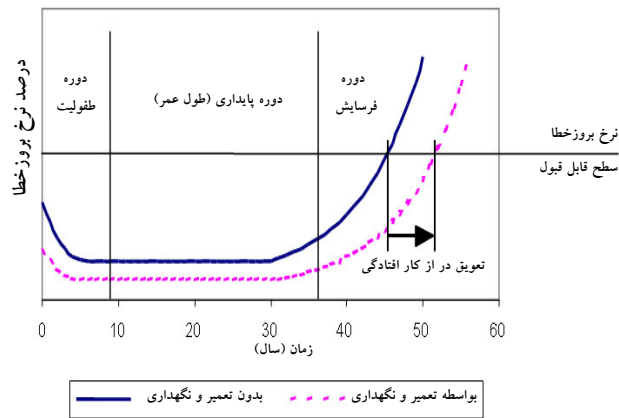
کیفیت هر محصول در طول عمر کاری خود با قابلیت اطمینان بیان می‌شود. در بحث قابلیت اطمینان سیستم‌های حفاظتی می‌بایست این سیستم‌ها را به شکل مجزا از سایر تجهیزات شبکه‌های قدرت مورد تجزیه و تحلیل قرار داد زیرا این سیستم‌ها خود از اجزای متعددی تشکیل شده‌اند و با این سبک تجزیه و تحلیل می‌توان حساسیت سیستم‌های 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

- ۱- Fail to Operate
- ۲- Mal Operation
- ۳- Self Checking
- ۴ - Watchdog
- ۵- Routine Test

۶ - Dependability
۷- Security

بیست و چهارمین کنفرانس بین‌المللی برق



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

۳- قابلیت دسترسی^۱:

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 غیره می‌باشد.

طول عمر یک دستگاه لزوماً برابر با زمان مفید کاری همین دستگاه نیست و بسیاری از دستگاهها دارای زمان مفید کاری کمتری نسبت به طول عمر خود می‌باشند. قابلیت اطمینان 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.

$$R = e^{-\lambda t} \quad (1)$$

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 طول عمر مفید افزایش پیدا می‌کند [17] البته لازم به تذکر است که در اینجا آزمایش، تعمیر یا سرویس بدون خطا در نظر گرفته شده است.

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^۲، استفاده می‌کنند.

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

$$U = \frac{1}{Tc} \int_0^{Tc} (1 - e^{-\lambda t}) dt = 1 - \frac{1}{\lambda Tc} (1 - e^{-\lambda Tc}) \quad (2)$$

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

$$U = \frac{\lambda Tc}{2} \quad (3)$$

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

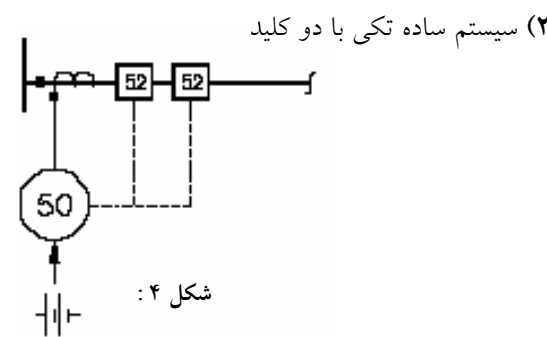
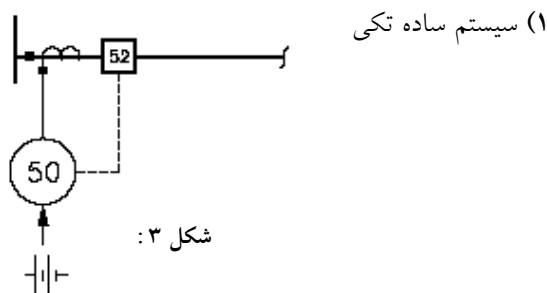
۴- روش‌های ارزیابی و مدلسازی سیستم:

سیستم‌های حفاظتی ترکیبی از تجهیزات مختلف می‌باشند که هر یک وظیفه خاصی را به عهده دارند در بسیاری از

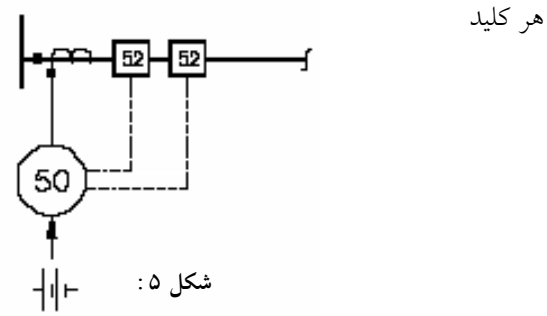
بیست و چهارمین کنفرانس بین‌المللی برق

۵- بررسی آلترناتیوهای حفاظتی مختلف :

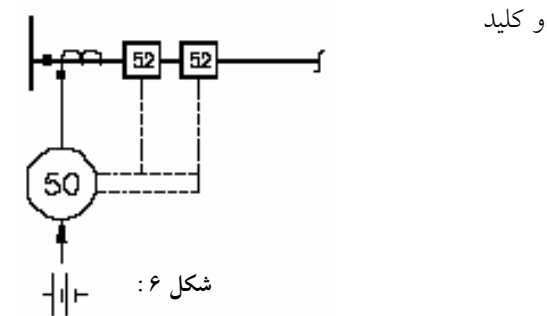
جهت ارزیابی قابلیت اطمینان تجهیزات حفاظتی، سناریوهای زیر را می‌توان مد نظر داشت شامل :



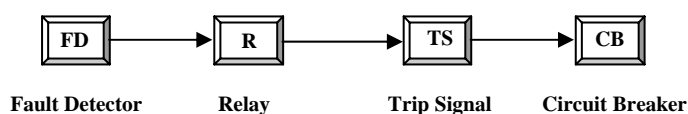
(۳) سیستم ساده تکی با دو کلید و مدار تریپ جداگانه برای هر کلید



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



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 در شبکه‌های 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 مقایسه‌کننده‌های اولیه را نیز شامل می‌گردد.

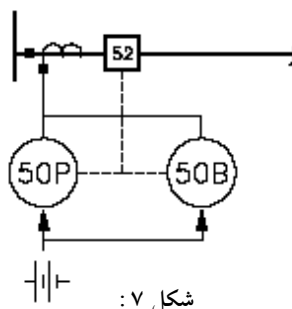
R : واحد رله و یا تصمیم‌گیر که عمل تشخیص خطا به عهده این واحد است و مغز متفکر سیستم حفاظتی است که خود می‌تواند شامل مدار تغذیه، مدارهای پروسه تشخیص خطا، مدارهای عمل‌کننده، مدارهای پایدارکننده و غیره باشد. البته در یک سیستم حفاظتی ممکن است ترکیبی از رله‌های مختلف وجود داشته باشد که در اینجا برای سادگی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

T.S : این واحد شامل منابع تغذیه مربوط به مدار تریپ (که شامل Trip coil و سیم‌کشی‌های 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 عمل‌کننده زنجیره حفاظتی بوده و خود هیچگونه تصمیمی نمی‌گیرد، لیکن اجراکننده دستورات سیستم حفاظتی است و حاصل کار آن قطع قسمتی از مدار شبکه است.

بیست و چهارمین کنفرانس بین‌المللی برق

(۵) سیستم مضاعف (حفاظت دوپل) و یک کلید



وقایع سیستم تست از نوع ساده تکی اجرا شده در شرکت ملی مناطق نفتخیز جنوب را می بینیم، جهت بررسی قابلیت اطمینان زنجیره حفاظتی مجموعاً 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 می دهد و چهار حالت بعدی همگی حالات خطا می باشند. مطابق اطلاعات سازنده هر یک از اجزاء سیستم حفاظتی دارای نرخ خطای 0.02 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.

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.

۶ - ارزیابی و مدل سازی سیستم تست NISOC:

شکل (۸) سیستم حفاظتی تست شده در شرکت ملی مناطق نفتخیز جنوب را نشان می دهد که دیمانند خود را از شبکه انتقال وزارت نیرو از طریق دو فیدر ورودی با سطح ولتاژ ۳۳ کیلوولت دریافت و توسط خطوط انتقال به واحدهای بهره برداری نفت و نمکزدایی نفت و تقویت فشارگاز مارون ارسال می گردد و هر یک از این فیدرها توسط سه عدد رله اضافه جریان و یک عدد رله اتصال زمین ساخت GEC حفاظت می شوند، که در شکل (۹) درخت

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 دقیقاً مشابه حالت قبل و با استفاده از اطلاعات موجود و درخت وقایع ترسیم شده در شکل (۳) عمل می نمایم، 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 برابر 0.001 در سال می باشد) و احتمال بوجود آمدن سیگنال خطا در هر یک از این سه واحد مستقل از دیگری است.

بیست و چهارمین کنفرانس بین‌المللی برق

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

۱-۶- نتایج بکارگیری آلترناتیوهای حفاظتی در سیستم

تست معرفی شده:

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

جدول ۳: ارزیابی قابلیت اطمینان سیستم تست ساده تکی

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

جدول ۴: ارزیابی قابلیت اطمینان سیستم تست ساده تکی با دو کلید

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

جدول ۵: ارزیابی قابلیت اطمینان سیستم تست ساده با دو کلید و مدار تریپ جداگانه

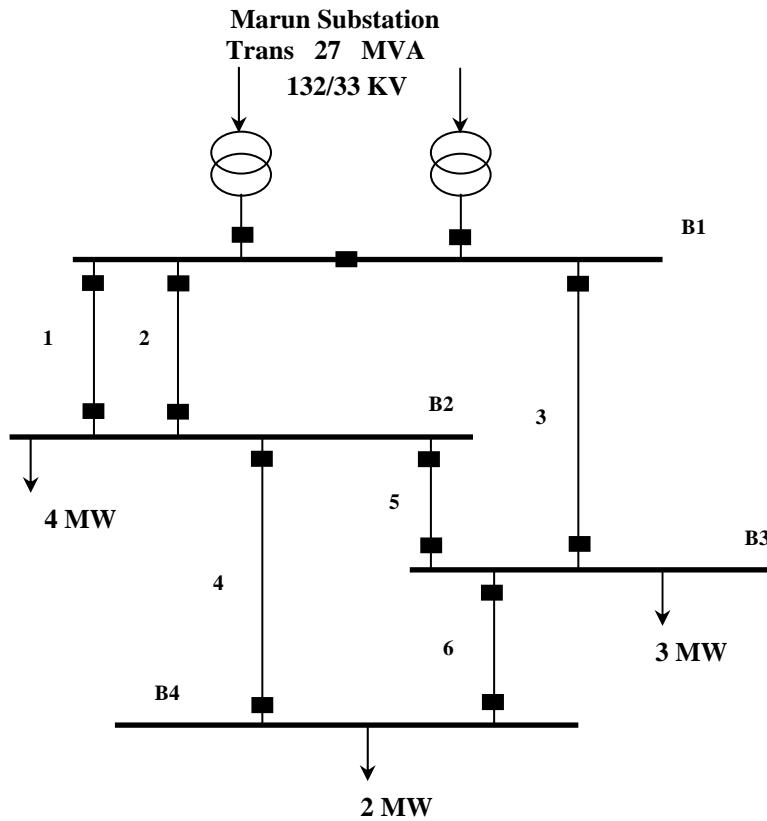
	ساده با دو کلید و مدار تریپ مشترک		
	سه ماه	شش ماه	دوازده ماه
Fail to operate	0.00499375	0.00997500	0.01990000
mal operation	0.00297265	0.00294565	0.00289251
Reliability	0.99500625	0.99002500	0.98010000

جدول ۶: ارزیابی قابلیت اطمینان سیستم تست ساده با دو کلید و مدار تریپ مشترک

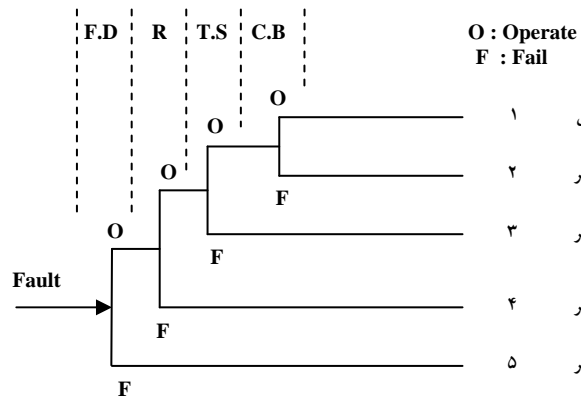
بیست و چهارمین کنفرانس بین‌المللی برق

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

جدول ۷: ارزیابی قابلیت اطمینان سیستم تست از نوع مضاعف

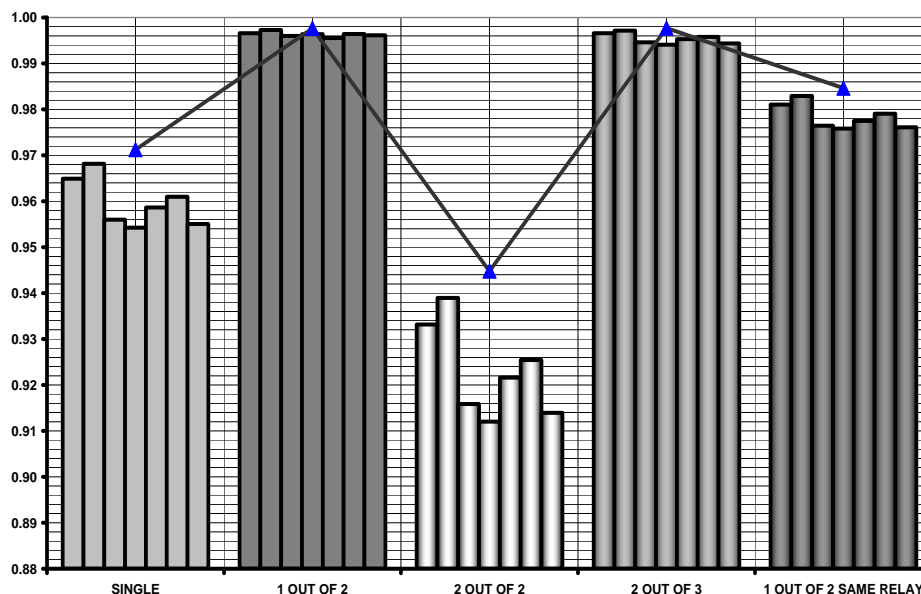


شکل ۸: سیستم تست معرفی شده در شرکت مناطق نفت خیز جنوب



شکل ۹: درخت وقایع سیستم تست از نوع ساده تکی اجرا شده در صنعت نفت جنوب

بیست و چهارمین کنفرانس بین‌المللی برق



شکل ۱۰: نمودار محاسبات قابلیت اطمینان سیستم تست به ازای حالت‌های مختلف

مشخص می‌شود استفاده از سیستم‌های دوبل (مضاعف) باعث کاهش خطای سیستم حفاظتی تا حد $\left(\frac{1}{4}\right)$ شده و راهی جهت افزایش قابلیت اطمینان می‌باشد. برای بهینه‌سازی قابلیت اطمینان سیستم حفاظتی دوبله نمودن کلید قدرت بسیار گران است لذا استفاده از رله بسیار منطقی است. یکی از راهکارهای مناسب دوبله نمودن تریپ کویل^۱ کلید می‌باشد، دوبله نمودن منبع تغذیه برای هر کدام از تریپ کویل‌ها نیز شیوه‌ای مناسب است.

۷- افزایش قابلیت اطمینان تجهیزات حفاظتی :

جهت افزایش قابلیت اطمینان سیستم‌های حفاظتی روش‌های متعددی تا کنون پیشنهاد و اجرا شده‌اند. این روش‌ها در مورد رله‌های استاتیکی، رله‌های جدید دیجیتالی یا میکروپروسسوری بیشتر مطرح شده‌اند زیرا در این نوع رله‌ها اجرای این روش‌ها به مراتب آسانتر گشته است.

با مقایسه جدول نتایج (۳) تا (۷) و همچنین شکل (۱۰) مشاهده می‌شود هر چقدر بازه زمانی تست تجهیزات حفاظتی کوتاه‌تر شود مطابق رابطه (۲)، مقدار شاخص عدم دسترسی آن کمتر شده، که این موضوع باعث افزایش قابلیت اطمینان آن تجهیز شده و در نهایت شاخص قابلیت اطمینان کل سیستم افزایش می‌یابد. ولی می‌بایست هزینه‌ای که از بابت تست تجهیزات حفاظتی تحمیل می‌شود به گونه‌ای باشد که صرفه اقتصادی طرح را نیز به همراه داشته باشد. طی مطالعاتی که در این رابطه صورت گرفته و از جدول نتایج سیستم تست مشهود است بازه زمانی بهینه برای تست تجهیزات حفاظتی، دوره شش ماهه می‌باشد که در این حالت هم سیستم از قابلیت اطمینان خوبی برخوردار است و هم مسئله اقتصادی طرح نیز توجیه‌پذیر است. خاطر نشان می‌سازد برنامه ریزی عملیاتی جهت انجام این روش بدین صورت بوده که تست دوره‌ای و تست کالیبراسیون در پیوندهای سالانه ولی با فاصله زمانی شش ماه از یکدیگر انجام پذیرد. همچنین از جدول نتایج سیستم تست

۱-۷- بازبینی مستمر^۱:

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 سیستم حفاظتی احتمال خطای سیستم مجموع را افزایش می‌دهد. بنابراین بازبینی هر یک از این مدارها می‌تواند 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 می‌کند، 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 خطا دار می‌شوند. بنابراین نمی‌توان تمام اعتماد را بر روی این مدارها پایه ریزی نمود.

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

۲-۷- بازرسی و آزمایش دوره‌ای :

در قسمت‌های قبل دیدیم که انجام آزمایشات دوره‌ای می‌تواند قابلیت اطمینان را در محدوده بخصوصی نگهدارد. طبیعی است که زمان بین دو آزمایش متوالی می‌بایست 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 نمی‌توانند در فواصل زمانی کوتاه انجام گردند و معمولترین پیروی آزمایش دوره‌ای رله‌ها شش ماه و یا یکسال می‌باشد. متأسفانه اهمیت این موضوع در برخی سیستم‌ها چندان جا افتاده نیست و در اکثر موارد مسئولین ضرورتی بر انجام این کار نمی‌بینند. که نتیجه آن واضح است «مواجهه با سیستم‌های حفاظتی پیچیده و غامض و در عین حال عدم اعتماد و اطمینان به عملکرد صحیح آن».

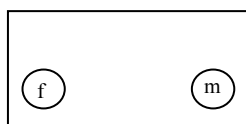
با انجام چنین آزمایشهایی، محدودیتهای ذکر شده در حالت بازبینی مستمر از بین می‌رود و عملاً نقاط ضعف آنها هم خواهد پوشانند. وضعیت سیستم حفاظتی در طی آزمایش نیز به دقت بررسی می‌گردد و در نتیجه با اتکا به این اطلاعات می‌توان محاسبات دقیقتری را در مورد قابلیت اطمینان سیستم حفاظتی انجام دهیم.

امروزه با رله‌های جدید استاتیکی و دیجیتالی امکان آزمایش خودکار رله‌های حفاظتی تا حدی به وجود آمده است، در این حالت سیستم "آزمایش خودکار" می‌تواند هم به شکل دستی و یا در زمانهای بخصوص به شکل خودکار رله را تحت آزمایش قرار دهد و در صورت وجود عیب، آنها اعلام کند. آزمایش رله می‌بایست زمانیکه خطایی در شبکه بروز می‌کند قطع گردد و رله

بیست و چهارمین کنفرانس بین‌المللی برق

نشان دهنده عملکرد نابجا (m) و عدم عملکرد (f) می‌باشد. دایره کوچک نشان دهنده حالت بهتری از ایمنی و اتکا است.

(۱) مدل تک حفاظتی :

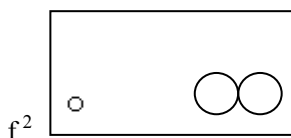


شکل (۱۱)

$$D = 1 - f$$

$$S = 1 - m$$

(۲) مدل یک از دو :

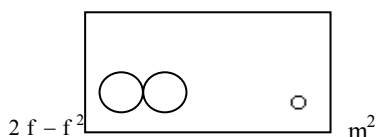


شکل (۱۲)

$$D = 1 - f^2$$

$$S = 1 - (2m - m^2)$$

(۳) مدل دو از دو :

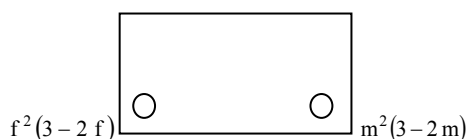


شکل (۱۳)

$$D = 1 - (2f - f^2)$$

$$S = 1 - m^2$$

(۴) مدل دو از سه :

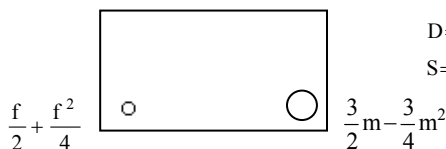


شکل (۱۴)

$$D = 1 - f^2(3 - 2f)$$

$$S = 1 - m^2(3 - 2m)$$

(۵) مدل یک از دو با دو رله مشابه :



شکل (۱۵)

$$D = 1 - 0.5f - 0.25f^2$$

$$S = 1 - 1.5m + 0.75m^2$$

کار عادی خود را انجام دهد. همین نکته باعث پیچیده تر شدن مدار آزمایش خودکار می‌گردد که هزینه‌ها را نیز بالا خواهد برد البته در مورد رله‌های دیجیتالی این مشکل کمتر به چشم می‌خورد زیرا فقط با افزودن نرم افزار مربوطه این امکان را در رله بوجود می‌آورند.

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^۱ و پیچیده همیشه جوابگوی نیازهای ما نخواهد بود. اگر با استفاده از چنین سیستمهایی بعنوان مثال قابلیت اتکا افزایش یابد چه بسا که ایمنی همان سیستم شدیداً کاهش یابد و بالعکس.

لذا راه حل منطقی شناخت تجهیزات بطور کامل از نقطه نظر نوع خطا، قابلیت اطمینان از یکسو، 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 در یک بازه زمانی بهینه می‌توان بر خلاف تجربیات فعلی، از یک سیستم حفاظتی منظم، قابل اطمینان و ایمن برخوردار بود.

۹- پیوست :

در ادامه مدل‌های مختلف قابلیت اتکا و ایمنی سیستم‌های حفاظتی بررسی می‌شود دایره‌های درون مربع

- [12] P. M. Anderson and S. K. Agarwal, "An improved model for protective system reliability," IEEE Trans. Rel., vol. 41, pp. 422-426, Sept. 1992.
- [13] 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.
- [14] J. D. Grimes, "On determining the reliability of protective relay systems," IEEE Trans. Rel., vol. R-19, pp. 82-85, Aug. 1970.
- [15] 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.
- [16] 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.
- [17] 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.
- [18] 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.
- [1] Ioannis S. Baxevas and Dimitris P. Labridis, "Implementing Multiagent Systems Technology for Power Distribution Network Control and Protection Management" IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 22, NO. 1, JANUARY 2007
- [2] Aleksandar Pregelj and Miroslav Begovic and Ajeet Rohatgi "Recloser Allocation for Improved Reliability of DG-Enhanced Distribution Networks" IEEE TRANSACTIONS ON POWER SYSTEMS, VOL. 21, NO. 3, AUGUST 2006
- [3] M. Nordman and M. Lehtonen, "An agent concept for managing electrical distribution networks," IEEE Trans. Power Del., vol. 20, no. 2, pp. 696-703, Apr. 2005.
- [4] P. A. A. F. Wouters, P. C. J. M. vanderWielen, J. Veen, P. Wagenaars, and E. F. Steennis, "Effect of cable load impedance on coupling schemes for MV power line communication," IEEE Trans. Power Del., vol. 20, no. 2, pt. 1, pp. 638-645, Apr. 2005.
- [5] 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
- [6] Nagaraj Balijepalli & Subrahmanyam S. Venkata. " Modeling and Analysis of Distribution Reliability Indices " IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 19, NO. 4, OCTOBER 2004
- [7] Xingbin Yu & Chanan Singh." Integrated Power System Vulnerability Analysis Considering Protection Failures " IEEE TRANS , 2003 , PP. 706 - 711
- [8] Roy Billinton & M. Fotuhi-Firuzabad & T. S. Sidhu " Determination of the Optimum outline Test and Self-Checking Intervals in Protective Relaying Using a Reliability Model "IEEE TRANS. ON POWER SYSTEMS, VOL. 17, NO. 3, AUGUST 2002
- [9] Gerald F. Johnson " Reliability Considerations of Multifunction Protection " IEEE TRANS. ON INDUSTRY APPLICATIONS, VOL. 38, NO. 6, NOVEMBER / DECEMBER 2002
- [10] 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
- [11] 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