TEEGES

Technovations in Electrical Engineering & Green Energy System

Research Article (2022) 1(1):36-62

یک روش هوشمند مبتنی بر سیستم چندعاملی به منظور حفاظت از شبکه‌های توزیع

An Intelligent Multi-Agent Based Approach for Protecting Distribution Networks

Danial Alibeigi[1], *M.Sc*, Ehsan Abbaspour[1], *M.Sc*, Bahador Fani[1,2], *Associate Professor*, Haidar Samet[3], *Professor*

[1] *Department of Electrical Engineering, Najafabad Branch, Islamic Azad University, Najafabad, Iran*
[2] *Smart Microgrid Research Center, Najafabad Branch, Islamic Azad University, Najafabad, Iran*
[3] *Department of Electrical Engineering, Shiraz University, Shiraz, Iran*

Abstract:

Nowadays, the presence of distributed generations has made traditional networks into dynamic state. Current flow fluctuation, increment of fault current and as a result loss of coordination and also error in relays operation in safe sections in the network have been among the problems due to using these generations. Finding solution for these problems has always been challenging over the years. The purpose of this paper is to suggest a new solution in the study of protection system operation in electrical energy networks by using intelligent electronic equipment with communication protocols at the level of distribution networks. In recent years, telecommunications platform and intelligent equipment usage has provided a platform that has been able to show its effectiveness against network sudden changes. Multi-Agent system is the name of this communication platform that has been able to pioneer the beginning of a fundamental change in the design of protection systems in electrical energy networks by using a new scheme. These systems have shown that they have not been without problems and in some cases have caused problems for the network. In the proposed approach, the multilayer structure of the multi-agent system will be broken and the surfaces will be independent of each other. Unlike the typical multi-agent system protection method, protection settings at the moment of fault are not calculated for the entire network. This problem, which has not been seen in previous methods, also removes a large load density from the central unit and increases the operating speed and reliability of the protection system.

Keywords: Intelligent Protection, Distribution Network, Distributed Generation, Multi-Agent System

Received: 1 March 2022
Revised: 10 May 2022
Accepted: 7 June 2022
Corresponding Author: Dr. Haidar Samet, samet@shirazu.ac.ir
DOI: http://dx.doi.org/10.30486/teeges.2022.691104

فناوری‌های نوین در مهندسی برق و سیستم انرژی سبز

TEEGES

مقاله پژوهشی

یک روش هوشمند مبتنی بر سیستم چندعاملی به منظور حفاظت از شبکه‌های توزیع

دانیال علی بیگی[۱]، *کارشناسی ارشد*، احسان عباسپور[۱]، *کارشناسی ارشد*، بهادر فانی[۱و۲]، *دانشیار*،
حیدر صامت[۳]، *استاد*

۱- دانشکده مهندسی برق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران
۲- مرکز تحقیقات ریزشبکه های هوشمند، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران
۳- دانشکده مهندسی برق، دانشگاه شیراز، شیراز، ایران

چکیده: امروزه حضور منابع تولید پراکنده این شبکه‌ها را به حالت پویا تبدیل کرده‌است. تغییر حرکت جریان، افزایش میزان جریان خطا و به دنبال آن از دست رفتن هماهنگی و همچنین اشتباه در عملکرد رله‌های نواحی سالم در شبکه از جمله مشکلات استفاده از این منابع بوده است. پیدا کردن راه حل برای رفع این دسته از مشکلات در طول سالیان متوالی، همواره چالش برانگیز بوده است. هدف این مقاله ارائه یک راه حل جدید در بررسی عملکرد سیستم حفاظت شبکه‌های انرژی الکتریکی به کمک تجهیزات هوشمند الکترونیکی و با استفاده از پروتکلهای ارتباطی موجود در سطح شبکه‌های توزیع می‌باشد. در سالهای اخیر استفاده از بستر مخابراتی و بکارگیری تجهیزات هوشمند بستری را فراهم کرده که توانسته است کارآمدی خود را در برابر تغییرات ناگهانی شبکه نشان دهد. سیستم چندعاملی، نام این بستر ارتباطی می‌باشد که توانسته است با طرحی نو، پیشگام در شروع یک تحول بنیادی در طراحی سیستمهای حفاظتی شبکه‌های انرژی الکتریکی باشد. این سیستم‌ها نشان داده‌اند که بدون مشکل نیز نبوده و در مواردی شبکه را با مشکلاتی مواجه کرده‌اند. در طرح پیشنهادی ساختار چندلایه سیستم چندعاملی شکسته شده و سطوح از وابستگی یکدیگر خارج خواهند شد. بر خلاف روش حفاظتی سیستم چندعاملی که در گذشته وجود داشته است، تنظیمات حفاظتی در لحظه خطا برای تمام شبکه محاسبه نمی‌گردد. این مسئله که در روش‌های قبلی دیده نشده چگالی بار زیادی را هم از روی واحد مرکزی برداشته و سرعت عملکرد و قابلیت اطمینان در عملکرد سیستم حفاظت را بالا می‌برد.

واژه‌های کلیدی: حفاظت هوشمند، شبکه توزیع، تولید پراکنده، سیستم چندعاملی

تاریخ ارسال مقاله: ۱۴۰۰/۱۲/۱۰
تاریخ بازنگری مقاله: ۱۴۰۱/۰۲/۲۰
تاریخ پذیرش مقاله: ۱۴۰۱/۰۳/۱۷
نویسنده‌ی مسئول: دکتر حیدر صامت، samet@shirazu.ac.ir
DOI: http://dx.doi.org/10.30486/teeges.2022.691104

۱- مقدمه

با توجه به محدودیت در استفاده از سوخت‌های فسیلی که مشکلات زیست محیطی زیادی نیز به همراه دارد، استفاده از منابع تولید پراکنده مبحثی است که روز به روز به اهمیت آن افزوده می‌شود. منابع تولید پراکنده به صورت صفحات خورشیدی، توربینهای بادی، موتورهای دیزلی و یا پیلهای سوختی و غیره مورد استفاده قرار می‌گیرند و لازم به ذکر است که اتصال برخی از این منابع مثل صفحات خورشیدی به شبکه‌ی توزیع به کمک اینورتر انجام می‌شود. اتصال منابع تولید پراکنده به سیستم توزیع، موجب بروز تغییرات در ساختار شبکه‌ی توزیع می‌شود. این تغییرات می‌توانند برای سیستم توزیع مفید بوده و یا باعث بروز مشکلاتی شوند [۱و ۲]. با حضور منابع پراکنده، سطح جریان اتصال کوتاه تا حدی زیاد می‌شود که منجر به ایجاد ناهماهنگی در عملکرد رله‌های موجود در سیستم می‌شود. رله‌های موجود در شبکه، بسته به میزان سطح جریان اتصال کوتاه شبکه تنظیم شده‌اند که افزایش ناگهانی جریان عبوری از خط باعث از بین رفتن هماهنگی میان آنها و در نتیجه باعث بی برق شدن نواحی وسیعی در شبکه‌ی توزیع می‌شود [۳و ۴].

طرح‌های گوناگونی برای بهبود عملکرد سیستم حفاظتی شبکه‌های توزیع در حضور منابع تولید پراکنده وجود دارند. طرح پیشنهاد شده در [۵و ۶]، مربوط به زمان جداسازی منابع تولید پراکنده می‌باشد. بعد از وقوع خطا، بهترین زمان برای جداسازی این منابع، قبل از شروع عملکرد تجهیزات حفاظتی می‌باشد اما به دلیل آن که تأمین بارها از اولویت بیشتری برخوردار بوده، این طرح قابل اجرا نمی‌باشد. طرح معرفی شده در [۷] شامل تقسیم بندی سیستم توزیع به نواحی مجزا می‌باشد که در آن رله‌ها توسط یک رله‌ی اصلی کنترل می‌شوند. جداسازی ناحیه‌ی خطا دیده توسط عملکرد رله‌ی مناسب انجام می‌شود. نقطه‌ی ضعف این طرح، هزینه‌ی بالای آن در مسافت‌های طولانی می‌باشد. در روش حفاظتی پیشنهاد شده در [۸-۱۱]، با توجه به تغییرات وارد شده به شبکه، تجهیزات حفاظتی با استفاده از الگوریتم برنامه نویسی شده در حفاظت شبکه شرکت می‌کنند. برای به کار گیری این طرح لازم است که تمامی تغییرات شبکه، پیش بینی شده و برای هر تغییر، یک دسته از تنظیمات در رله‌ها اعمال شود. مقاله [۱۲] مربوط به قرار دادن رله‌های دیستانس بر روی فیدر می‌باشد. هدف از انجام این کار، بالا بردن امنیت در عملکرد فیوز و همچنین حفاظات شبکه در حضور منابع تولید پراکنده می‌باشد. مقالات [۱۳-۱۵] مربوط به پیدا کردن آستانه‌ی مناسب ضریب نفوذ منابع تولید پراکنده می‌باشد. این طرح، حالت‌های مختلفی که باعث برهم زدن هماهنگی تجهیزات می‌شوند را بررسی می‌کند. روش ارائه شده در [۱۶] مربوط به طرحی مبتنی بر تغییر منحنی مشخصه‌ی ریکلوزرها می‌باشد. در این طرح، هدف اصلی حفظ هماهنگی میان ریکلوزرها و فیوزهای شبکه در حضور منابع پراکنده می‌باشد. برای تحقق این هدف، استفاده از یک بستر ارتباطی جهت برقراری ارتباط بین این تجهیزات پیشنهاد شده‌است. [۱۷] روش حفاظت مبتنی بر ارتباط هوشمند را پیشنهاد می‌دهد که بر اساس حفاظت چند منظوره است. در روش‌های [۱۸و ۱۹] جهت کاهش اثر منابع تولید پراکنده بر روی اضافه جریان تولید شده، از تجهیزاتی استفاده شده تا جریان خطا را محدود کنند. این طرح به خاطر هزینه‌ی ساخت بالایی که دارد از اولویت کمتری برخوردار می‌باشد. با توجه به مشکلات گفته شده در مورد عملی نشدن طرح‌های پیشنهادی، ارائه‌ی طرحی که مشکلات ذکر شده را رفع کند و در کنار آن دارای قابلیت اجرا شدن در شرایط مختلف بهره برداری شبکه باشد، مبحثی مهم بوده که در سال‌های اخیر مورد توجه می‌باشد ولی با پیشرفت تجهیزات هوشمند، مشکلات مربوط به اجرا شدن این طرح رفع شده‌است.

یکی از طرح‌های ارائه شده بر اساس ساختار سیستم چندعاملی می‌باشد. اساس عملکرد این طرح، تبادل اطلاعات مربوط منابع تولید پراکنده، آرایش شبکه و تجهیزات حفاظتی می‌باشد. یک عامل در واقع یک تجهیز الکترونیکی می‌باشد که اطلاعات مربوط به تجهیزات شبکه‌ی توزیع را گردآوری کرده، بر روی آن فرآیند محاسباتی انجام داده، جهت دریافت و ارسال سیگنال با دیگر عوامل ارتباط برقرار می‌کند و به صورت مستقل وظایف خود را انجام می‌دهد. منظور از این که عامل‌ها به صورت مستقل وظایف خود را انجام می‌دهد آن است که این عامل‌ها می‌توانند بدون نیاز به تجهیزات اضافه تصمیم گیری کرده و به تنهایی اطلاعات را دریافت و ارسال کنند. عامل‌ها به صورت سخت افزاری بوده و به تجهیزات الکترونیکی هوشمند متصل می‌شوند و برای انجام وظایف خود نیازمند یک زیرساخت و پروتکل ارتباطی می‌باشند [۲۰]. در مقالات [۲۱-۲۵] نویسندگان از سیستم چندعاملی استفاده کرده‌اند. در طرح پیشنهاد شده از انتخاب تجهیزات حفاظتی شبکه به عنوان عامل‌های طرح سیستم چندعاملی، مشکلات مربوط به هماهنگی تجهیزات حفاظتی را برطرف می‌کنند. هنگامی که شبکه‌ی قدرت دچار تغییر می‌شود، اطلاعات مربوطه از طرف عامل‌های مرتبط با رخداد به سیستم مرکزی ارسال می‌شود. سیستم مرکزی اطلاعات را پردازش کرده و سپس دستورات جدید را به تجهیزات موجود در سطح‌های پایین ارسال می‌کند. عامل‌ها

فرمان‌ها را دریافت کرده و تغییرات لازم را در شبکه اعمال می‌کنند. شرط تصمیم‌گیری عامل‌ها داشتن ارتباط با یک دیگر است، زیرا تصمیم گیری و اجرای آن نیازمند داشتن آگاهی از وضعیت شبکه است و تنها با برقراری ارتباط می‌توان از وضعیت شبکه آگاهی داشت. با توجه به نکات ذکر شده، می‌توان اذعان داشت که در ساختار چندعاملی، عامل‌ها در تمام سطوح دارای ۳ وظیفه‌ی اساسی می‌باشند، انتقال اطلاعات (دریافت و ارسال)، پردازش اطلاعات و تصمیم گیری به صورت مستقل و اجرای فرمان دریافت شده از سیستم مرکزی[۲۶-۲۹]. استفاده از ساختارهای چندعاملی مشکلاتی را در پی دارد که اگر در زمان مناسب رفع نشوند، صدمات جبران ناپذیری به تجهیزات موجود در شبکه وارد می‌کنند. فرآیند تشخیص رویداد و ارسال تنظیمات مناسب به رله‌ها برای پردازشگر مرکزی بسیار زمان بر است که به دنبال آن مرکز کنترل نمی‌تواند از عملکرد غیر ضروری رله‌ها جلوگیری کند. همچنی زمان فرآیند به روز رسانی رله‌ها بر اساس تغییر رخ داده در شبکه به قدری زیاد می‌باشد که اگر خطایی حین بروز رسانی رخ دهد، امکان دارد شبکه با آسیب جدی مواجه شود. برای رفع این مشکل لازم است یک رله‌ی پشتیبان در مکان هر رله قرار داده شده تا از افزایش تعداد رخدادهای شبکه و خسارات احتمالی جلوگیری شود. همچنین در شبکه‌های بزرگ، با افزایش تعداد رویدادها، اطلاعات انتقالی رشد چشمگیری خواهند داشت و طبیعتا وظایف پردازشگر مرکزی افزایش می‌یابد. این تراکمِ وظایف، خطر عملکرد اشتباه پردازشگر مرکزی را افزایش می‌دهد.

با توجه به مشکلات ذکر شده در خصوص استفاده از ساختار چندعاملی، طرح پیشنهاد شده نگرانی‌های ساختار چندعاملی را که شامل حفظ هماهنگی تجهیزات حفاظتی در حضور منابع تولید پراکنده است را کاهش می‌دهد و همچنین عدم عملکرد مناسب سیستم حفاظتی بواسطه‌ی نیاز به پردازشگر مرکزی را بر طرف می‌نماید. در طرح پیشنهادی این مقاله ساختار چندلایه سیستم چندعاملی شکسته شده و سطوح از وابستگی یکدیگر خارج خواهند شد. به عبارت دیگر وظایفی برای هر سطح مشخص می‌شود که باعث می‌شود سرعت عملکرد را افزایش داده بطوریکه در زمان خطا وابستگی به حداقل رسیده و در برخی موارد حتی حذف شود. از جمله موارد دیگری که لازم است تا به آن اشاره نمود استفاده از ناحیه بندی است که در این ساختار پیاده سازی می‌شود. بر خلاف روش حفاظتی سیستم چندعاملی که در گذشته وجود داشته است، تنظیمات حفاظتی در لحظه خطا برای تمام شبکه محاسبه نمی‌گردد. این مسئله که در روش‌های قبلی دیده نشده چگالی بار زیادی را هم از روی واحد مرکزی بر می‌دارد و هم سرعت عملکرد و قابلیت اطمینان در عملکرد سیستم حفاظت را بالا می‌برد. همچنین در این روش به کمک توابع پیاده سازی شده سعی می‌شود تا بتوان بدون در نظر داشتن ظرفیت و مکان قرار گیری منابع و یا اتصال و یا عدم اتصال آنها و بدون محدود کردن ظرفیت آنها، همواره هماهنگی حفاظتی را حفظ نماییم.

بخش بندی مقاله بدین صورت است که در بخش دوم مشکلات حفاظتی ناشی از حضور منابع تولید نشان داده می‌شود و در بخش بعد تجهیزات هوشمند، مفهموم عامل و جایگاه قرارگیری آنها در شبکه تشریح می‌شود. در بخش چهارم استراتژی هوشمند سازی حفاظت شبکه‌ی توزیع به کمک سیستم چندعاملی معرفی می‌شود. در این فصل الگوریتم حفاظتی پیشنهادی به منظور برقراری هماهنگی حفاظتی و همچنین جلوگیری از عملکرد اشتباه سیستم حفاظتی در شرایط تغییر جهت جریان و همچنین تغییر سطح جریان اتصال کوتاه ارائه می‌شود و در انتهای این فصل به منظور بررسی ارزیابی و تصدیق درستی روش ارائه شده، شبیه سازی بر روی یک شبکه آزمایشی صورت می‌گیرد و در نهایت در بخش ششم از مطالب بررسی شده در مقاله نتیجه گیری به عمل می‌آید.

۲- منابع تولید پراکنده و اثر گذاری آنها بر روی رله‌های جریان زیاد

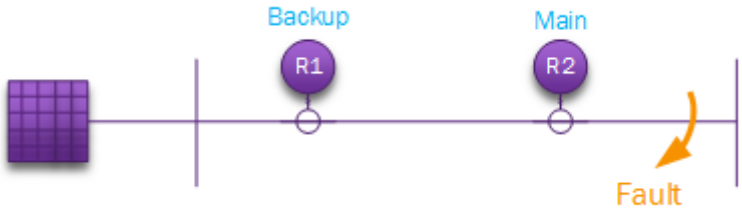
عملکرد رله‌های اضافه بر اساس میزان جریان عبوری از آنها می‌باشد. رله‌های جریان زیاد به کمک ترانسفورماتور جریان میزان جریان عبوری از شبکه را در اندازه کوچکتری دریافت می‌کنند. هر رله جریان زیاد برای عملکرد خود به سه پارامتر جریان خطا، جریان تحریک و ضریب تنظیم زمانی و ثابت¬های مربوط به نوع منحنی مشخصه آن بستگی دارد. این مقادیر مشخص کننده زمان عملکرد یک رله می‌باشد. رابطه (۲-۱) زمان عملکرد رله مشخص می‌شود[۳۰]:

$$t = \frac{A}{\left(\frac{I_F}{I_{Pickup}}\right)^n - 1} \times TMS \qquad (۱)$$

در رابطه (۱) پارامترهای A وn مقادیر ثابت این رابطه می‌باشند. TMS و I_{pickup} مقادیر می‌باشند که بر اساس اطلاعات شبکه و مکان قرارگیری رله‌ها مشخص می‌شوند. I_F نیز جریان خطای اتصال کوتاه شبکه می‌باشد که در زمان وقوع خطا بر روی رله‌ها مشاهده می‌باشد.

I_{pickup} رله جریانی است که در آن خطا تشخیص داده می‌شود. این مقدار به گونه ای تعیین می‌شود که رله جریان بار را جریان خطا تشخیص نداده و همچنین بتواند حداقل جریان اتصال کوتاه شبکه که در فواصل دورتر از رله رخ می‌دهد را تشخیص دهد. ضریب تنظیم زمانی یک پارامتر مهم برای حفظ هماهنگی عملکردی در رله‌ها می‌باشد.

رله‌ها در زمان وقوع خطا لازم است تا با توجه به مکان نقطه خطا، هماهنگی خود را با رله‌های همسایه حفظ نمایند. به این معنا که برای خطای پایین دست دو رله در ابتدا لازم است تا پایین دست ترین رله نزدیک به رله عمل نماید و سپس با حاشیه زمانی مناسب نزدیک ترین حفاظت بالادست رله عمل نماید.



شکل (۱): بررسی هماهنگی رله‌های اصلی و پشتیبان

در شکل (۱) خطای رخ داده در پایین دست دو رله R1 و R2 موجب تحریک دو رله می‌گردد. رله R2 با توجه به نزدیکی به نقطه خطا لازم است تا به عنوان رله اصلی عمل نماید. رله R1 در این حالت نقش پشتیبان این رله را خواهد داشت. با توجه به استاندارد IEC شرایط هماهنگی برای دو رله، حاشیه زمانی عملکرد ۳۰۰ میلی ثانیه می‌باشد. به بیان کاملتر جهت برقراری هماهنگی حفاظتی لازم است تا شرط رابطه (۲) برقرار گردد:

$$t_{R1} - t_{R2} \geq 300\ (ms) \qquad (۲)$$

برای این منظور لازم است تا TMS رله R1 محاسبه گردد:

$$\frac{A_{R1}}{\left(\frac{I_F}{I_{R1}}\right)^{n_{R1}}-1} \times TMS_{R1} - \frac{A_{R2}}{\left(\frac{I_F}{I_{R2}}\right)^{n_{R2}}-1} \times TMS_{R2} \geq 300\ (ms) \qquad (۳)$$

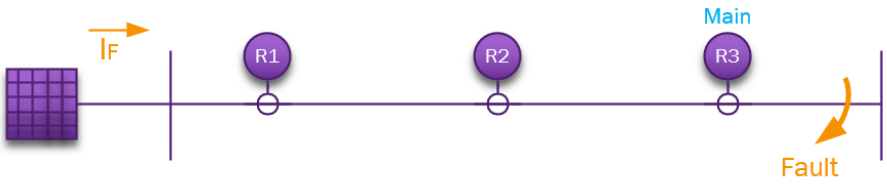
$$\frac{A_{R1}}{\left(\frac{I_F}{I_{R1}}\right)^{n_{R1}}-1} \times TMS_{R1} \geq 300\ (ms) + \frac{A_{R2}}{\left(\frac{I_F}{I_{R2}}\right)^{n_{R2}}-1} \times TMS_{R2} \qquad (۴)$$

مقدار عبارت $\frac{A_{R1}}{\left(\frac{I_F}{I_{R1}}\right)^{n_{R1}}-1}$ همواره بزرگتر از صفر می‌باشد، در نتیجه خواهیم داشت:

$$TMS_{R1} \geq \frac{\left(\frac{I_F}{I_{R1}}\right)^{n_{R1}}-1}{A_{R1}} \times 300\ (ms) + \frac{\left(\frac{I_F}{I_{R1}}\right)^{n_{R1}}-1}{A_{R1}} \times \frac{A_{R2}}{\left(\frac{I_F}{I_{R2}}\right)^{n_{R2}}-1} \times TMS_{R2} \qquad (۵)$$

مقدار TMS_{R1} با توجه به رابطه (۵) باید شرط لازم را برقرار نماید. با محاسبه این رابطه برای جریان خطای ماکزیم شبکه می‌توان مقدار TMS_{R1} را محاسبه نمود.

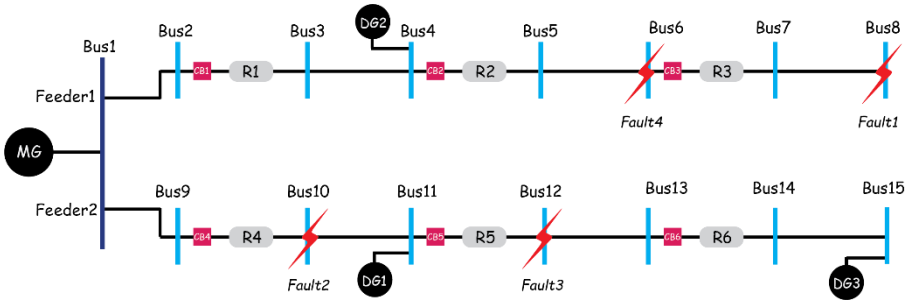
اولویت عملکرد رله‌های جریان زیاد در زمان خطا بسیار مهم می‌باشد. یک رله جریان زیاد باید به گونه ای تنظیم شده باشد که در زمان خطا عملکردی سریعتر و یا همزمان با رله اصلی نداشته باشد[۳۱]. به عنوان مثال در شکل (۲) مشاهده می‌شود که برای خطای اتفاق افتاده در پایین دست رله R3، ترتیب عملکرد رله‌ها باید اینگونه باشد: اولویت اول؛ رله R3، اولویت دوم؛ رله R2 و الویت سوم؛ رله R1. حال در صورت تنظیمات اشتباه بر روی رله R3، ممکن است تا رله R2 سریعتر عمل کند. این مشکل به میزان جریان IF بستگی بسیاری دارد. هرچه میزان جریان خطا بزرگتر باشد، امکان وقوع این مشکل افزایش می‌یابد. در حالت بعد ممکن است میزان جریان خطایی که از روی رله عبور می‌کند به قدری نباشد که رله تحریک شود. همانطور که اشاره شد رله جریان زیاد برای عملکرد خود نیاز دارد تا جریان عبوری از آن، بزرگتر از مقدار I_{pickup} تنظیم شده بر روی آن باشد. در این شرایط در صورتی که جریان IF بسته به مکان خطا و نوع آن کمتر از مقدار جریان تحریک رله‌ها باشد، می‌توان گفت که رله نمی تواند خطا را تشخیص دهد.



شکل (۲): بررسی اولویت عملکرد رله‌های جریان زیاد

۲-۱- بررسی چالش‌های حفاظتی در حضور منابع تولید پراکنده

میزان تاثیر گذاری منابع تولید پراکنده به جریان خطای تزریقی آنها بستگی دارد. وقوع خطا بر روی شبکه اصلی و بالا بودن سطح جریان تزریق شده از این شبکه‌ها می‌تواند میزان تاثیر گذاری آنها را بالا ببرد. در تکمیل این بررسی باید گفت، بالابردن سطح جریان اتصال کوتاه شبکه می‌تواند موجب به هم ریختگی و عملکرد اشتباه سیستم حفاظت شبکه گردد. حفاظت‌های پشتیبان هماهنگی خود را با حفاظت اصلی ناحیه دیگر از دست می‌دهند و همچنین حفاظت‌های نواحی دیگر سریعتر از رله‌های بخش خطا دیده عمل می‌کنند. در بررسی این موضوع، منابع تولید پراکنده به شبکه تست شکل (۳) متصل شده‌است. در این حالت تمام منابع تولید انرژی شبکه می‌توانند از جهات مختلف در مقدار جریان اتصال کوتاه شبکه تاثیر گذار باشند. خطای Fault2 در ناحیه حفاظتی رله R4 اتفاق افتاده است. برخلاف حالتهای قبل مشاهده می‌شود که به علت جریان ایجاد شده توسط منابع تولید پراکنده، رله‌های R1 بر روی فیدر اول و رله‌های R5 و R6 بر روی فیدر دوم نیز جریان خطا را مشاهده می‌کنند. در این شرایط لازم است تا خطا از هر دو سمت شبکه برطرف گردد. در نتیجه عملکرد رله R4 و رله R5 در این طرح حفاظتی نسبت به دو رله دیگر اولویت خواهد داشت.

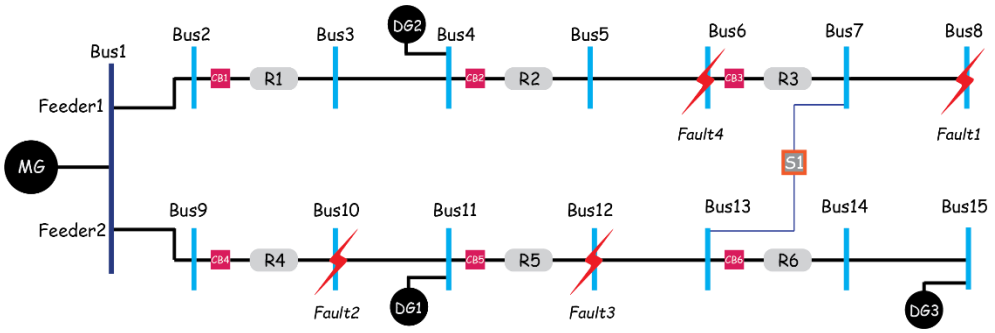


شکل (۳): اتصال منابع تولید پراکنده در شبکه تست مورد آزمایش

۲-۲- بررسی چالش‌های حفاظتی در حضور منابع تولید پراکنده

یکی از سیساست گذاری‌های مربوط به تأمین بار شبکه، امکان تغییر ساختار شبکه بوسیله کلیدهای مانور می‌باشد. در این حالت شبکه می‌تواند از مسیرهای مختلفی بارهای بخش‌های مختلف را تأمین نماید. این مسئله به خودی خود تا زمانی که خطایی بر روی شبکه رخ ندهد مشکل ایجاد نخواهد کرد. در این حالت شبکه با دو چالش اساسی مواجه می‌باشد. اولین چالش در زمان جلوگیری از عملکرد اشتباه رله‌های حفاظتی نواحی سالم به جهت مشاهده جریان برگشتی می‌باشد و چالش دوم در زمان عملکرد یکی از رله‌های خطا خواهد بود که موجب تغییر مسیر جریان و عبور مقدار جریان زیاد از مسیرهای منتهی شده به نقطه خطا می‌شود. شکل (۴) به بررسی چالش حفاظتی در زمان اتصال کلید S1 می‌پردازد. زمانی که خطای Fault4 بر روی شبکه اتفاق افتد، با توجه به محل وقوع خطا مشاهده می‌شود که دو رله R2 و R3 منتهی به نقطه خطا می‌باشند. با توجه به اتصال دو فیدر به یکدیگر، جریان خطا بر روی رله R3 و R6 با یکدیگر برابر می‌باشد. همچنین جریان خطایی از سمت شبکه و و DG1 بر روی رله R5 جاری خواهد شد. در این شرایط امکان عملکرد سریعتر هریک از دو رله R5 نسبت به رله R3 وجود دارد. از طرف دیگر با فرض اینکه حفاظت R2 خطا را در زمان مناسبی تشخیص دهد و در سریعترین زمان ممکن به درستی عمل نماید، جریان خطا شبکه بطور کامل از فیدر دوم به نقطه خطا تزریق خواهد شد. با

توجه به افزایش میزان جریان خطای عبور کرده از شبکه این امکان وجود دارد که حفاظت‌های R1، R4 و R5 در مسیر عبور جریان خطا، به اشتباه عمل نمایند.



شکل (۴): بررسی چالش حفاظتی در زمان مانور شبکه تست مورد آزمایش

۳- بررسی عملکرد سیستم حفاظتی در شبکه‌های هوشمند

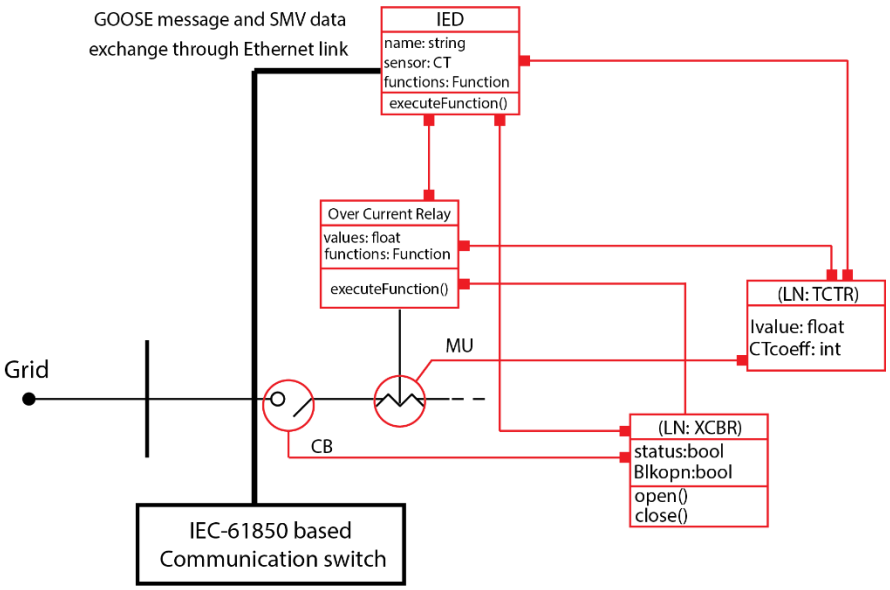
پیشرفت تکنولوژی در طراحی سخت‌افزار رله و توسعه پروتکل‌های ارتباطی به ظهور نسل جدیدی از وسایل الکترونیکی هوشمند منجر شده‌است. یک راه موثر برای استفاده از این ابزارها و دستیابی به یک طرح انتقال خودکار استفاده از یک مکانیزم پیام‌رسانی منعطف، قابل اطمینان و با سرعت بالا می‌باشد. IEC61850 یک دسته از پروتکل‌های ارتباطی است که از یک اتصال اترنت به عنوان واسطه ارتباط بین رله‌های حفاظتی استفاده می‌کند. در صنعت برق یکی از جدیدترین استانداردهایی که برای ارتباط با این ویژگی تدوین شده‌استاندارد IEC61850 می‌باشد. در این پروتکل مانیتور کردن همزمان دستگاه‌ها و همچنین مدیریت شبکه با مجموعه ای از قابلیت‌های مختلف از یک مرکز کنترل ممکن می‌گردد. همچنین این استاندارد، توانایی انطباق با تغییرات سریع، حفاظت، ارتباط و کنترل ایستگاه‌های برق را دارد. IEC61850 از پروتکل‌های MMS[۱]، GOOSE[۲] وSMV[۳] استفاده می‌کند[۳۲]. این پروتکل‌ها ارتباط را بروی شبکه TCP/IP با سرعت زیاد برقرار می‌نمایند. به عنوان مثال پروتکل GOOSE یک مکانیزم سریع و قابل اعتماد از انتقال داده‌ها بر روی ایستگاه‌های شبکه می‌باشد. قبل از انتقال داده، هر گره با این پروتکل وضعیت خود را برای دیگر گره‌ها ی موجود ارسال می‌کند. در ادامه توضیحات مربوط به چارچوب استاندارد IEC61850، زمان است که نحوه مدل سازی ساختار ارتباطی و عملیاتی در این استاندارد چگونه انجام می‌شود. یک تجهیز هوشمند بر اساس این استاندارد با انتساب به یک تجهیز فیزیکی آغاز می‌شود. به عنوان مثال تجهیز الکترونیکی هوشمند رله، مشخص می‌کند که تجهیز فیزیکی منتخب، ماهیت حفاظتی دارد. این تجهیز هوشمند بر روی شبکه ارتباطی قرار گرفته و در دسترس قرار می‌گیرد.

۳-۱- طرح حفاظتی بر مبنای استاندراد IEC61850

در ادامه فرآیند مدل‌سازی، قابلیت‌هایی مانند عملکرد کنترلی، انداره گیری تحت عنوان گره منطقی تشکیل می‌شوند. یک گره منطقی به داده‌ها و فرمان‌های مشخصی اشاره دارد که هرکدام به بخشی از تجهیز فیزیکی مرتبط می‌شود. این گره‌های منطقی با توجه به عملکردشان، نام‌های مشخصی را خواهند داشت. در بررسی یک دستگاه منطقی نسبت داده شده به یک رله جریان زیاد، بر طبق این استاندارد، ۵ نوع گره منطقی تعریف می‌شود. PTOC گره منطقی مربوط به رله جریان زیاد می‌باشد. این گره منطقی وظایف مربوط به یک رله مانند تنظیمات و صدور فرمان به کلید و دریافت اطلاعات جریان را شامل می‌شود. TCTR گره منطقی مربوط به ترانس جریان می‌باشد که اطلاعات جریان شبکه را مدل می‌کند. گره منطقی دیگر، MMXU بوده که مربوط به تجهیزات اندازه‌گیری می‌باشد و با گره منطقی TCTR در ارتباط می‌باشد. XCBR گره منطقی مربوط به انتقال فرمان به کلید قدرت می‌باشد و این گره مستقیما با گره CSWI که مدیریت کننده اطلاعات مربوط به فرمان ارسال شده به کلید قدرت می‌باشد. هر کدام از گره‌های منطقی بیان شده دارای مشخصات و ویژگی‌های مشخصی برای خود می‌باشند.

در شکل (۵)، یک مدل تک خطی برای نمایش مدل سازی استاندارد IEC61850 نمایش داده شده‌است. در این شکل که بخشی از شبکه می‌باشد، IED که یک رله جریان زیاد می‌باشد، به کمک یک سوییچ IEC61850 به شبکه متصل شده‌است. IED از یک رشته به عنوان نام استفاده می‌کند. MU واحد اندازه‌گیری می‌باشد، که اطلاعات خود را برای گره منطقی TCTR و PTOC ارسال می‌کند.

TCTR دو مقدار را در بر می‌گیرد. مقدار جریان که از واحد mu دریافت کرده و نسبت تبدیل CT که عددی صحیح می‌باشد. این مقادیر در IED توسط بخش sensor دریافت می‌شود. IED به کمک این اطلاعات توابع برنامه ریزی بر روی خود را اجرا می‌کند. بخش executeFunction جهت اجرای فرمان‌های لازم می‌باشد. این فرمان‌ها شامل ارسال درخواست به کلید و یا ارسال سیگنالهای عملیاتی به سایر رله‌ها می‌باشد. گره منطقی PTOC که بر حسب توابع عملیاتی رله جریان زیاد عمل می‌نماید به گره‌های منطقی XCBR و TCTR متصل می‌باشد. این گره منطقی مقادیر جریان را از TCTR دریافت می‌کند، گرچه در شرایط عادی به CT نیز متصل می‌باشد. تابع عملکردی این گره منطقی نیز بر اساس تنظیمات رله مطابق با رابطه عملکرد زمانی رله فرمان کلید را صادر می‌کند. گره منطقی XCBR وضعیت کلید را بر اساس یک مقدار "0" و "1" بررسی می‌کند و همچنین قادر است تا با ارسال درخواست قفل مانع از عملکرد حفاظت‌ها شود. این گره منطقی رابطه مستقیمی با کلید قدرت موجود بر روی شبکه داشته و وضعیت آن را بررسی می‌کند.



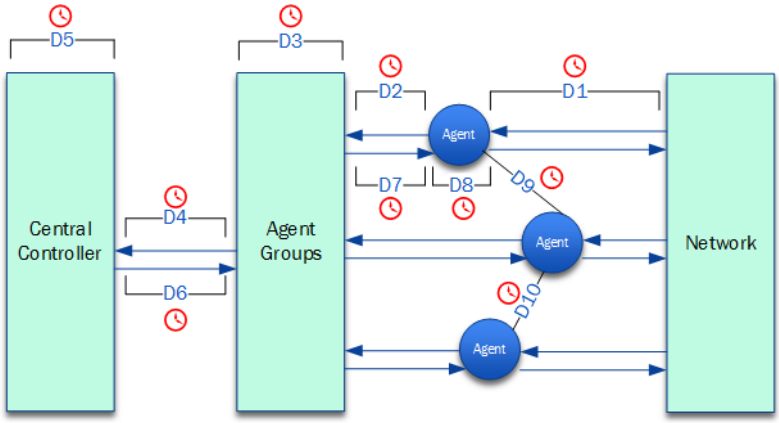
شکل(۵): گره‌های منطقی و ساختار آن بر روی حفاظت جریان زیاد

۳-۲- معرفی سیستم چندعاملی

مدیریت بهتر و سهولت در دسترسی پذیری به تجهیزات شبکه نیازمند تغییر در طراحی آن می‌باشد. افزایش تعداد نیروی کار و همچنین استفاده از سیستم‌های مدیریتی و محاسباتی بر روی شبکه توانسته تا حدودی این نیاز را برطرف سازد. اما همواره نیاز بود تا این مسئله به شیوه‌ای مناسب تغییرات تدریجی را بر روی خود مشاهده کند. در علوم کامپیوتری به منظور سهولت در مدیریت شبکه و همچنین جداسازی قسمت‌های شبکه از یکدیگر برای افزایش کارایی شبکه، چالشی ایجاد شد تا بر اساس آن بتوان اطلاعات نقاط مختلف را بر اساس ناحیه آنها در اختیار گرفت و متناسب با هر ناحیه تصمیم گیری مشخصی داشت. علاوه بر این با توجه به اینکه در بعضی موارد نیاز بود تا تجهیزات شبکه بتوانند خود تغییرات را دریافت و بر روی خود اعمال نمایند، یک مفهوم جدید ارائه داده شد[۳۳]. واژه "عامل" مفهومی بود که بدین منظور تعریف شده‌است. در واقع عامل‌ها تمام فعالیت‌های شبکه را به صورت خود مختار مشاهده کرده و گزارش می‌دهند، علاوه بر این وظیفه دارند تا عملکرد خود نسبت به آن را نیز گزارش دهند. این طراحی در ساختار مدیریتی بسیار استفاده می‌گردد و حتی توانسته تا قابلیت اطمینان شبکه را ارتقاء دهد و نگرانی‌های توسعه شبکه را کاهش دهد.

با تعریف شدن عامل و مشخص شدن کارایی آنها، سیستم شبکه‌های برق نیز استفاده از چنین ساختار را در طراحی شبکه بررسی و پیشنهاد نموده‌اند. عامل‌ها مجموعه ای از تجهیزات سخت افزاری و نرم ا فزاری تعریف می‌شوند که بصورت کاملا پویا می‌توانند درون یک ناحیه که با آن ارتباط دارند، بصورت مستقل و یا تحت هدایت یک واحد دیگر تصمیم گیری نموده و بر روی آن تاثیر گذارند. یک تجهیز الکترونیکی هوشمند به عنوان میزبان این عامل‌ها برگزیده می‌شوند. ارتباط میان تجهیزات الکترونیکی بر مبنای پروتکل ارتباطی IEC61850 عمل می‌باشد.

با کنار هم قرار گرفتن مجموعه ای از این عامل‌ها، ساختار توسعه یافته است و نیاز به مدیریت خواهد داشت. در این صورت هر دسته از عامل‌ها در دسته‌های مختلفی قرار گرفته و مدیریت می‌شوند. علاوه بر این یک ساختار چندلایه ای را نیاز خواهیم داشت که وظایف هر لایه مشخص گردد. لایه اول به عامل‌های فیزیکی اختصاص داده شود و در لایه‌های بالاتر با استفاده از اطلاعات بدست آمده، آنها مدیریت شوند. در این حالت این لایه‌های بالاتر هستند که نقش مدیریتی را ایفا کرده و هماهنگی ساختار را فراهم می‌کنند. این ساختار به هم پیوسته که از تعداد زیادی عامل تشکیل شده‌است را سیستم چندعاملی می‌نامند. سیستم‌های چندعاملی ساختارهای هوشمندی را تشکیل خواهند داد که می‌توانند برای اهداف مختلفی برنامه ریزی شوند. این ساختارها با توجه به نوع برنامه ریزی و مدیریتشان می‌توانند در دو حالت متمرکز و غیر متمرکز فعالیت نمایند. امروزه طراحی زیرساخت‌های غیرمتمرکز، توسعه بهتری یافته است، علت آن بالارفتن حساسیت سیستم‌ها بوده است. برای نمونه در سیستم‌های حفاظتی که بحث مورد نظر این مقاله می‌باشد، استفاده از ساختار چندعاملی متمرکز نمی تواند تا در شرایطی پیچیده که زمان مسئله مهمی می‌باشد، نقش موثری داشته باشد.



شکل(۶): تأخیرهای زمانی در سیستم چندعاملی سنتی

با توجه به اینکه طرحهای حفاظتی وقتی نیازمند دریافت تنظیمات جدید متناسب با شرایط شبکه می‌باشند، در ساختار چندعاملی این مسئله می‌تواند تا حدی قابل نگران کننده باشد، علت وجود تأخیرهای زیاد و زمان بر روی شبکه می‌باشد. تنظیمات حفاظتی متناسب با تغییرات شبکه می‌باشند، پس در صورت وقوع تغییرات زیاد در شبکه، شامل تغییرات جریان در زمان حضور منابع تولید پراکنده تجدید پذیر که تولید آنها متناسب با تغییرات شرایط آب و هوایی می‌باشد، این موضوع اهمیت پیدا خواهد کرد. در شکل (۶) زمان‌های تأخیر به ۱۰ بخش تقسیم بندی شده‌اند:

D1: اولین تأخیر در زمان دریافت و خوانش اطلاعات شبکه بر روی بستر مخابراتی و تجهیزات اندازه‌گیری می‌باشد.

D2: پس از دریافت اطلاعات توسط عامل‌ها، صحت دریافت صحیح اطلاعات چک شده و به گروه عاملی ارسال می‌شود. گروه عاملی شامل عامل‌هایی هستند که وظیفه مدیریت اطلاعات دریافتی از عامل‌های پایین دستی خود را دارند.

D3: سومین تأخیر مربوط به پردازش اطلاعات دریافتی توسط گروه‌های عاملی هر دسته عامل می‌باشد، با توجه به اینکه ممکن است این عامل‌ها نقش‌های متفاوتی را در شبکه داشته باشند، بنابراین زمانی برای پردازش اطلاعات هر دسته و فرستنده آنها سپری می‌شود.

D4: ارسال اطلاعات برای واحد مرکزی چهارمین تأخیر در فرآیند حفاظتی ساختار چندعاملی متمرکز می‌باشد. گروه‌های عاملی وظیفه دارند تا اطلاعات خود را به درستی و با مشخصات مربوط به هر عامل به واحد مرکزی انتقال دهند.

D5: در این مرحله که می‌تواند بیشترین تأخیر زمانی را داشته باشد، اطلاعات دریافت شده توسط واحد مرکزی مورد پردازش قرار می‌گیرد. پس از پردازش لازم است تا تنظیمات جدید محاسبه شوند. در این حالت یک جدول جستجو وجود دارد که در آن واحد مرکزی تنظیمات مناسب را ثبت و ذخیره می‌کند.

D6: با محاسبه تنظیمات جدید، واحد مرکزی این اطلاعات را با توجه به عامل مورد نظر مشخص کرده و برای گروهای عامل ارسال می‌کند.

D7: این مدت زمان برای دسته بندی کردن اطلاعات و ارسال مجدد آن برای عامل‌های مشخص می‌باشد. گروه‌های عاملی تنظیمات دریافتی از واحد مرکزی را برای عامل‌های متناظر با آنها ارسال می‌کنند.
D8: پس از دریافت تنظیمات جدید، لازم است تا این تنظیمات بر روی عامل‌ها قرار گرفته و مجددا در دسترس قرار گیرند. این مدت زمان هم می‌تواند با توجه به نوع رله‌ها، زمان قابل توجهی را داشته باشد.
D9 و D10: بعد از بروزرسانی تنظیمات، عامل‌ها مدت زمانی را برای چک کردن هماهنگی میان خود و سایر عامل‌ها صرف می‌کنند تا درستی عملکردشان در شرایط جدید را بررسی کنند.

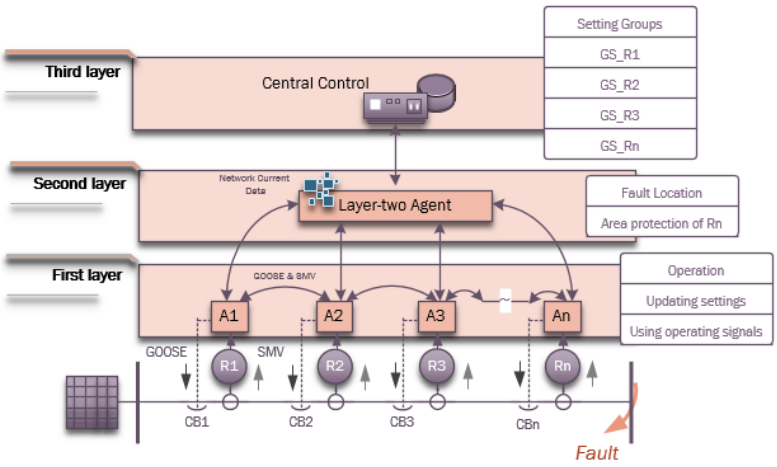
با توجه به تأخیرهای زمانی ذکر شده، برای قرار گرفتن یک عامل در شرایط جدید لازم است تا مدت زمان $\sum_{i=1}^{10} D_i$ سپری شود. این زمان به خودی خود در زمانی که شرایط شبکه در وضعیت نرمال قرار دارد مشکل ساز نخواهد بود، اما مشکل در زمانی آشکار می‌شود که خطایی بر روی شبکه اتفاق افتد و بصورت همزمان با آن شبکه دچار تغییرات گردد. در این زمان است که این سیستم با مشکل مواجه می‌شود. شبکه قدرت در جریان‌های بالا عملکرد سریعی خواهند داشت بنابراین وجود این حجم از تأخیر در شبکه می‌تواند منجر به بروز مشکل در عملکرد سیستم حفاظتی گردد.
با وجود این دسته از مشکلات در روش‌های متمرکز، روش‌های غیر متمرکز نیز مبتنی بر این ساختار پیشنهاد شده‌اند. روش‌های پیشنهاد شده با استفاده از امکانات پروتکل GOOSE در همان سطح عامل‌ها سعی نمودند تا مشکل سیستم‌های حفاظتی را در زمان خطا بدون وابستگی به واحد پردازش مرکزی حل نمایند. در این روش‌ها که صرفا جهت رفع خطا در زمان مناسب معرفی شدند، پیش از بروزرسانی تنظیمات حفاظتی، خطا به درستی رفع می‌گردد. این روش‌ها با توجه به ارسال درخواست سیگنالهای GOOSE در شبکه و انتشار آنها به عامل‌های مختلف، از عملکرد سایر عامل‌های شبکه جلوگیری می‌نمایند. بنابراین طرحی نیاز داریم تا بر اساس آن بتوانیم علاوه بر ساده سازی ساختار و کاهش وابستگی به واحد مرکزی، شبکه را از تغییراتی گسترده آزاد سازیم.

٤- هوشمند سازی طرح حفاظتی بر مبنای تغییر ساختار سیستمهای چندعاملی

به طور کلی در طرح پیشنهادی ساختار چندلایه سیستم چندعاملی شکسته شده و سطوح از وابستگی یکدیگر خارج خواهند شد. به عبارت دیگر وظایفی برای هر سطح مشخص می‌شود که باعث می‌شود سرعت عملکرد را افزایش داده بطوریکه در زمان خطا وابستگی به حداقل رسیده و در برخی موارد حتی حذف شود. از جمله موارد دیگری که لازم است تا به آن اشاره نمود استفاده از ناحیه بندی است که در این ساختار پیاده سازی می‌شود. بر خلاف روش حفاظتی سیستم چندعاملی که در گذشته وجود داشته است، تنظیمات حفاظتی در لحظه خطا برای تمام شبکه محاسبه نمی گردد. این مسئله که در روش‌های قبلی دیده نشده چگالی بار زیادی را هم از روی واحد مرکزی برداشته و سرعت عملکرد و قابلیت اطمینان در عملکرد سیستم حفاظت را بالا می‌برد. علاوه بر آن، در این روش به کمک توابع پیاده سازی شده سعی می‌شود تا صرف نظر از ظرفیت، مکان قرار گیری و محدود کردن ظرفیت منابع، همواره هماهنگی حفاظتی را کنترل نماییم.

٤-١- بررسی سیستم چندعاملی پیشنهادی

شکل (۷) معماری حفاظتی در طرح پیشنهادی را نمایش می‌دهد. در سطح اول عامل‌هایی قرار گرفته‌اند که با توجه به نقش آنها، به عنوان عامل رله شناخته می‌شوند. این عامل‌ها که از نوع حفاظت جریان زیاد می‌باشند، مدیریت وظایف یک رله را خواهند داشت. نوع ارتباط ایجاد شده بر اساس پروتکل IEC61850 بوده و تحت آن فرمان‌های لازم بر روی پروتکل GOOSE و اطلاعات شبکه بر روی پروتکل SMV انتقال داده می‌شوند. عامل‌ها به صورت نقطه به نقطه با یکدیگر در ارتباط بوده و هر کدام تحت فرمان لایه دوم می‌باشند. کلیدهای قدرت شبکه تحت فرمان عملکرد عامل‌ها خواهند بود و این وظیفه توسط پروتکل GOOSE محقق می‌گردد. اطلاعات جریان شبکه که توسط ترانس جریان اندازه‌گیری می‌شود توسط پروتکل SMV دریافت و جمع آوری می‌شود.



شکل(۷): معماری حفاظتی پیشنهادی در ساختار چندعاملی

٤-۲- بررسی ساختار عامل‌های رله در لایه اول

در اولین لایه که شامل عامل‌های رله می‌شود، هر عامل رله از چهار بخش تشکیل می‌گردد. شکل(۸) ساختمان یک عامل رله را نشان می‌دهد. در شکل دو عامل A1 و A2 که با یکدیگر در ارتباط می‌باشند، قادرند تا با یکدیگر داده اشتراک گذاری کنند. هر عامل رله که از نظر فیزیکی بر روی یک تجهیز الکترونیکی هوشمند قرار گرفته است، شامل بخش‌های Setting، Data، Status و Operation می‌باشد.

Setting: این قسمت مربوط دربرگیرنده اطلاعات مربوط به عملکرد معمول یک رله می‌باشد. اطلاعاتی مانند ماکزیمم جریان خطا، جریان تحریک رله و ضریب تنظیم زمانی رله. این سه پارامتری است که رله برای عملکرد خود نیاز داشته و با توجه به تغییرات شبکه تغییر می‌کند. اطلاعات این بخش همواره در لایه‌های مختلف به اشتراک گذاشته شده و قابل مشاهده می‌باشد. این بخش تنها قسمتی است که تحت عملکرد لایه سوم بوده و تغییر می‌کند. انتخاب این مقادیر در شرایط ابتدایی متناسب با محاسبات اتصال کوتاه و جریان بار شبکه می‌باشد، که در این ساختار به کمک واحد پردازش مرکزی محاسبه می‌شود.

Data: مقادیر جریان عبوری و وضعیت سیگنال ارسال شده به کلید قدرت، اطلاعاتی هستند که در این بخش قرار داده می‌شوند. با توجه به اینکه تغییرات جریان تنها پارامتری است که حفاظت‌های جریان زیاد بر اساس آن عمل می‌کنند، داده‌های مربوط به این بخش به منظور بررسی وضعیت و نحوه عملکرد یک رله استفاده می‌شوند. اطلاعات این بخش بر روی پروتکل IEC61850 و توسط دو گره منطقی TCTR و XCBR داده گزاری خواهند شد.

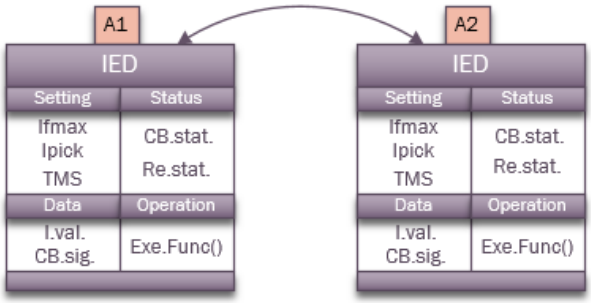
Status: در این قسمت وضعیت عملکرد یک رله از نظر عملکرد کلید و سلامت رله، مورد بررسی قرار می‌گیرد. با توجه به اهمیت عملکرد صحیح در زمان مناسب و اطمینان از وضعیت حضور و یا عدم حضور رله در طرح حفاظتی و همچنین اطمینان از عملکرد صحیح کلید، این بخش اختصاص داده شده تا تمام ساختار از عملکرد هر عامل مطلع شوند.

Operation: در این بخش که منتهی به اجرای فرمان توسط رله می‌باشد، با توجه به برنامه ریزی که بر روی رله صورت گرفته است، توابع و فرمان‌های لازم اجرا می‌شوند.

٤-۳- بررسی ساختار لایه دوم سیستم چندعاملی پیشنهادی

همانطور که ذکر شد در طرح پیشنهادی لایه دوم وظیفه بررسی ناحیه وقوع خطا را خواهد داشت. به بیان کاملتر این لایه وظیفه دارد تا ناحیه حفاظتی که خطا در آن رخ داده تشخیص داده و حفاظت متناظر با آن خطا را مشخص کند. شکل (۹) به بررسی عملکرد این لایه می‌پردازد. با توجه به شکل در لایه دوم جدولی تشکیل می‌شود که از سه بخش تشکیل می‌شود. در بخش Agent، نام تمامی عامل‌های متصل شده به شبکه ثبت می‌گردد. برخلاف ساختار مرسوم، اطلاعات هر فیدر به صورت جداگانه به همراه نام عامل‌های آن ذخیره می‌شود. اطلاعات ثبت شده به صورت تفکیک شده در این جدول کمک خواهد کرد تا بتوان سیستم حفاظت شبکه را سریعتر و بهتر مدیریت نمود.

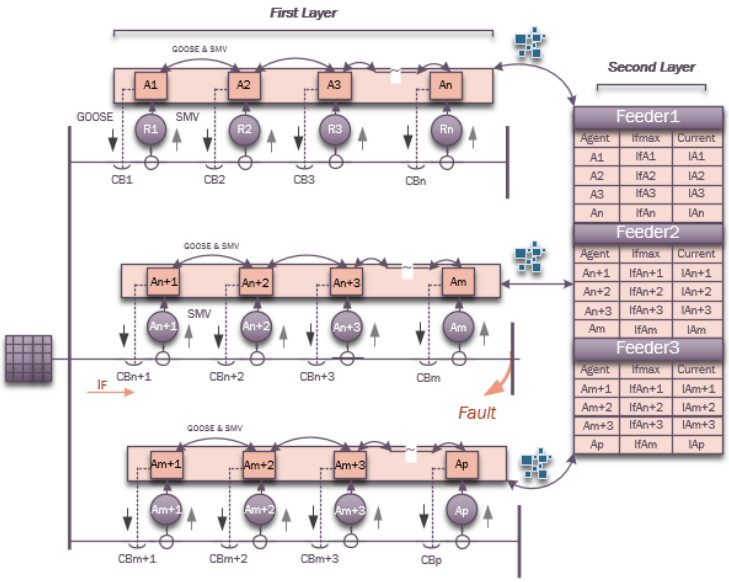
در بخش Ifmax، اطلاعات مربوط به تنظیمات هر عامل رله در لایه اول که در بخش Setting ثبت شده‌است ذخیره می‌شود. در واقع، در صورت تغییر این مقدار که در زمان تغییر تنظیمات حفاظتی انجام می‌شود، عامل‌های رله به لایه دوم اطلاع خواهند داد. در لایه دوم نیز با مقایسه مقدار جدید با مقدار ثبت شده، در صورت تفاوت، مقدار جدید را ثبت می‌کند. این اطلاعات بصورت IfAi ذخیره می‌شود که در آن i به شماره عامل اشاره دارد.



شکل(۸): ساختمان عامل رله در طرح حفاظت پیشنهادی

در بخش مربوط به Current، اطلاعات مربوط به جریان عبوری از عامل‌های رله ثبت می‌شود. این اطلاعات که توسط عامل‌های رله از لایه اول گرفته می‌شود، توسط پروتکل SMV از بخش Data توسط مقدار .I.val دریافت می‌گردد. این اطلاعات بصورت IAi برای هر عامل ذخیره می‌شود که در آن i به شماره عامل مورد نظر می‌باشد.

برای مشخص شدن چگونگی قرار گرفتن اطلاعات و نمایش آن در لایه دوم، فرض کنیم خطایی در ناحیه حفاظت رله Am اتفاق افتاده باشد. در این شرایط تنها فیدر دوم جریان خطا را بر روی خود مشاهده می‌کند. همانطور که از شکل (۹) مشخص است، به علت عدم حضور منابع تولید پراکنده عامل‌های موجود بر روی فیدرهای اول و سوم جریانی را مشاهده نکرده و نقشی در طرح حفاظتی نخواهند داشت. اما عامل‌های رله‌ای که جریان خطای Ifmax متفاوتی دارند، در مقدار جریان عبوری از خود در زمان خطا، مقدار جریان خطای برابر را که مقدار آن IF می‌باشد، بر روی خود مشاهده می‌کنند. نکته ای که در اینجا حائز اهمیت می‌باشد، مقدار جریان خطای IF می‌باشد که با توجه به اینکه در شرایط عدم حضور منابع تولید پراکنده و همچنین عدم تغیر ساختار شبکه می‌باشد، می‌بایست به یکی از مقادیر جدول Ifmax نزدیک باشد، زیرا میزان جریان Ifmax در شرایطی بر روی لایه دوم ثبت شده‌است که رله‌ها در وضعیت ابتدایی شبکه می‌باشند. در بررسی الگوریتم حفاظتی در نظر گرفته شده نشان خواهیم داد که این موضوع چگونه در تشخیص وضعیت خطا و ناحیه وقوع آن می‌تواند تاثیر گذار باشد.



شکل(۹): ساختار لایه دوم سیستم چندعاملی پیشنهادی

٤-٤- بروزرسانی تنظیمات رله پشتیبان در لایه سوم طرح حفاظت پیشنهادی

برای بررسی عملکرد لایه سوم در طرح پیشنهادی به بررسی عملکرد آن در شرایط خطا در شکل (۱۰) می‌پردازیم. در ابتدا ساختار لایه سوم را بررسی می‌کنیم.

طرح حفاظتی در لایه سوم از پنج مرحله تشکیل شده‌است:

مرحله اول) در این مرحله تمامی اطلاعات جریان و وضعیت کلیدهای شبکه که توسط عامل‌ها گزارش شده بررسی می‌شود.

مرحله دوم) وضعیت خطا که توسط لایه دوم مشخص شده‌است، به این لایه گزارش داده می‌شود.

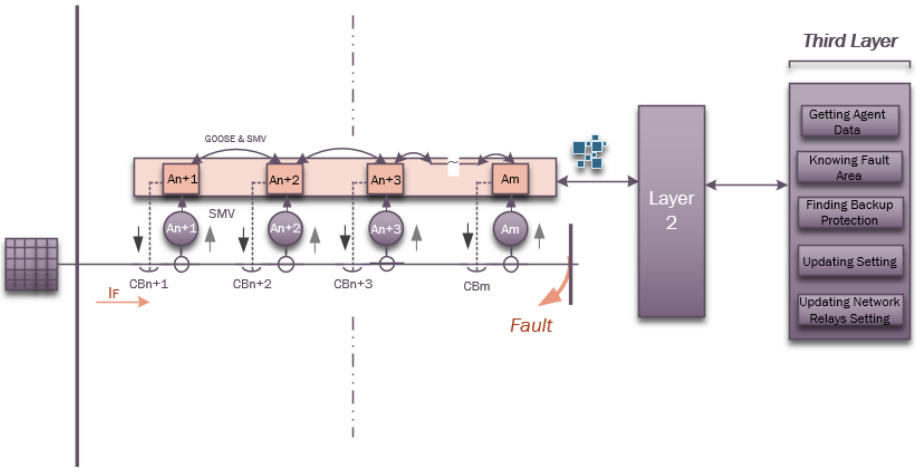
مرحله سوم) با مشخص شدن ناحیه خطا، حفاظت اصلی و پشتیبان تشخیص داده می‌شود.

مرحله چهارم) با تشخیص رله پشتیبان، تنظیمات جدید محاسبه شده و برای آ ارسال می‌شود

مرحله پنجم) پس از ارسال تنظیمات برای رله پشتیبان، تنظیمات جدید برای همه رله‌های شبکه محاسبه شده و برای آنها ارسال می‌گردد.

در زمان وقوع خطا در ناحیه حفاظتی رله Rm، لایه دوم مکان خطا را تشخیص می‌دهد و به لایه سوم گزارش می‌دهد. اطلاعات جریان عبوری از رله‌ها که برابر مقدار IF می‌باشد به لایه سوم گزارش داده می‌شود. در این شرایط رله Rm و رله Rm-1 به ترتیب به عنوان حفاظت اصلی و پشتیبان تشخیص داده می‌شوند. در مرحله بعد با توجه به اینکه عملکرد اشتباه می‌تواند تا بر اساس تغییرات شبکه بر روی رله پشتیبان اتفاق افتد، تنظیمات جدید در ابتدا برای رله Rm-1 ارسال شده تا هماهنگی حفاظتی برای رله‌ها برقرار شود و سپس تنظیمات جدید برای کل شبکه محاسبه می‌شود.

در ساختار چندعاملی پیشنهادی به بررسی نحوه عملکرد هر لایه پرداخته شد و مشخص شد که هر لایه چه وظایفی را در لایه خود و نسبت به لایه‌های دیگر بر عهده دارد. همانطور که مشخص می‌باشد ساختار چندلایه پیشنهادی وظایف همسو با وظایف سیستم چندعاملی مرسوم دارد، اما تفاوت آن در نحوه اجرای آن می‌باشد. به عبارت دیگر ساختار مرسوم تمام وظایف را بطور کامل و همزمان در اختیار لایه سوم قرار داده است، در صورتی که در ساختار پیشنهادی، این وظایف نه تنها در سطوح مختلف پخش شده‌است، بلکه عملکرد آن نیز بهمبود داده شده‌است. بررسی‌های انجام شده در مورد نحوه ارتباط و کنترل و مدیریت وظایف بوده است، در ادامه قصد داریم تا طرح حفاظتی پیشنهادی را به همراه الگوریتم حفاظتی بررسی نماییم.

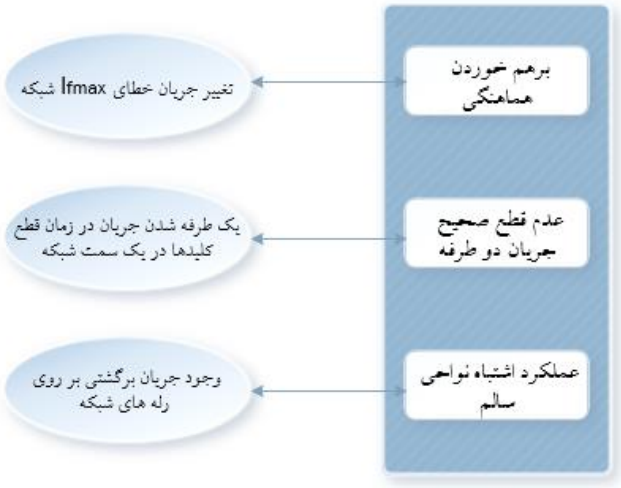


شکل(۱۰): عملکرد لایه سوم در طرح حفاظت پیشنهادی

٤-٥- بررسی الگوریتم حفاظتی سه لایه در طرح پیشنهادی

در الگوریتم حفاظتی پیشنهادی در این مقاله ما به دنبال اهداف مختلفی هستیم که بتوانیم به کمک این ساختار مشکلات حفاظتی را برطرف نماییم. در شکل (۱۱) این مشکلات به همراه علت به وجود آمدن آنها نمایش داده شده‌است. با توجه به شکل سه دسته مشکل وجود دارد که منجر می‌شود تا عملکرد یک سیستم حفاظتی با چالش‌هایی مواجه گردد. بر هم خوردن هماهنگی که ناشی از تغییرات جریان خطای Ifmax می‌باشد که می‌تواند بر اثر حضور منابع تولید پراکنده و یا تغییر توپولوژی شبکه باشد. در دومین چالش حفاظتی مشکل در زمان وقوع خطا در ناحیه ما بین دو یا چند رله است که در صورتی که یکی از آنها درست عمل کند، در صورتی که مسیر

برگشتی به نقطه خطا وجود داشته باشد، مسیر جدید جریان رله‌های موجود در مسیر خطا را تحریک کرده و موجب عملکرد اشتباه آنها می‌شود. در سومین چالش حفاظتی، امکان عملکرد اشتباه فیدرهای سالم در زمان وقوع خطا به علت وجود جریان برگشتی ناشی از حضور منابع تولید پراکنده بر روی شبکه می‌باشد. طرح حفاظتی پیشنهادی این مقاله در ابتدا هریک از شرایط فوق را تشخیص داده و سپس متناسب با آن طرح حفاظتی خود را پیش می‌گیرد.



شکل(۱۱): علل و مشکلات سیستم حفاظت شبکه

شکل (۱۲) نحوه شمارکت طرح حفاظتی پیشنهادی را در هریک از چالش‌های در حال وقوع نمایش می‌دهد. در ابتدا لازم است تا اطلاعات جریان شبکه در سطح دوم در زمان خطا بررسی گردد. در این زمان سه حالت برای شبکه وجود داردکه لازم است تشخیص داده شوند:

- تشخیص چالش اول:

در این حالت در ابتدا وضعیت جریان خطای عبوری از رله‌ها ثبت شده و با مقدار IFmax مقایسه می‌شود. در این شرایط شبکه در وضعیتی قرار دارد که تنها لازم است تا هماهنگی میان رله‌های اصلی و پشتیبان حفظ گردد. در این شرایط لایه دوم در طی گام‌های زیر عمل می‌کند:

گام اول: اطلاعات جریان هر فیدر دریافت می‌شود.

گام دوم: فیدری که بیشترین جریان خطا بر روی آن جاری شده تشخیص داده می‌شود

گام سوم: در این زمان پیامی برای جلوگیری از عملکرد اشتباه سایر فیدرها ارسال می‌شود.

گام چهارم: بررسی نقض شدن میزان جریان IFmax ثبت شده برای هر عامل. در این حالت با توجه به اینکه اطلاعات بیشترین جریان خطا برای هر عامل ثبت شده‌است، بررسی می‌شود جریان کدام ناحیه حفاظتی از مقدار مشخص شده قبلی آن فراتر رفته است.

گام پنجم: در این حالت انتهایی ترین رله موجود در فیدر که در آن جریان خطا از میزان ماکزیم ثبت شده فراتر رفته است، به عنوان رله اصلی شناخته شده و حفاظت همسایه آن، به عنوان پشتیبان معرفی می‌شود.

گام ششم: با توجه به اینکه رله اصلی با توجه به افزایش میزان جریان خطا در زمان مناسبی عمل می‌کند، در نتیجه تنها لازم است تا وضعیت کلید در عامل رله پشتیبان مدیریت شود.

در این نتیجه در حالت عملکردی که منجر به عملکرد اشتباه رله پشتیبان می‌شود، جلوگیری به عمل می‌آید.

- تشخیص چالش دوم:

تشخیص این حالت کمی متفاوت تر از چالش اول می‌باشد، علت آن وجود تعداد بیشتری حفاظت‌های محدود شده به نقطه خطا و همچنین وجود تعداد بیشتری حفاظت پشتیبان می‌باشد. شکل (۱۳) روش عملکرد در تشخیص این حالت را نشان می‌دهد. در مرحله اول، اطلاعات جریان فیدرها لازم است تا جمع آوری شوند. با فرض وجود تعداد k فیدر، اطلاعات جریان فیدرها شروع به دریافت می‌شوند. در ابتدا i=1 شروع شده و اولین فیدر وارد مرحله بررسی قرار می‌گیرد. در این حالت شبکه در وضعیتی قرار دارد که جریان از دو سمت

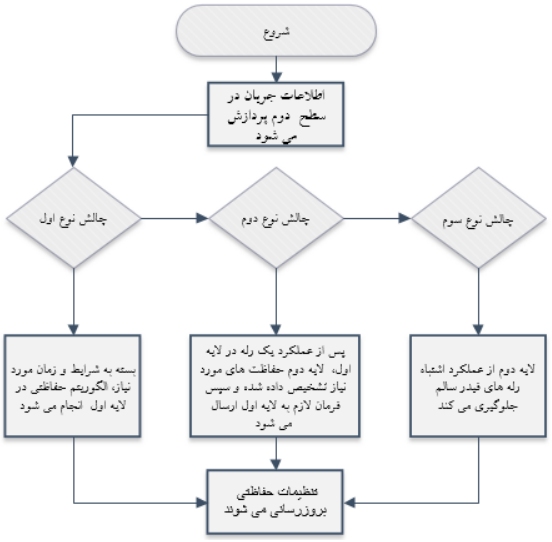
یا چند سمت به صورت همزمان وارد نقطه خطا می‌شود. که در این میان ممکن است بر روی هر فیدر لازم باشد تعداد دو رله عمل نمایند.

در لایه دوم جهت تشخیص این وضعیت نیاز دارد تا بر روی هر فیدر تغییرات جریان خطا را بررسی نماید. در این حالت تغییرات جریان بصورتی می‌باشد که بر اساس آن فیدر به دو بخش تقسیم بندی می‌شود. شکل (۱۴) بخشی از شبکه را در این وضعیت نمایش می‌دهد. به عنوان مثال خطایی در بخشی از قیدر اصلی اتفاق افتاده است. در این حالت جریان عبوری از هریک از رله‌ها با توجه به مکان قرارگیری منابع PV متفاوت می‌باشد. برای سه رله R1، R2 و R3 خواهیم داشت:

$$I_{R1}=I_{MG}+I_{PV1} \quad (۶)$$

$$I_{R2}=I_{MG}+I_{PV1}+I_{PV2} \quad (۷)$$

$$I_{R3}=I_{MG}+I_{PV1}+I_{PV2} \quad (۸)$$



شکل(۱۲): نحوه عملکرد الگوریتمهای حفاظتی در چالش‌های شبکه

بر روی همین فیدر در بخشی دیگر فیدر به ترتیب بر روی سه رله R4، R5 و R6 میزان جریان شبکه اصلی مشاهده نشده و به صورت زیر می‌باشد:

$$I_{R4}=I_{PV3}+I_{PV4}+I_{PV5} \quad (۹)$$

$$I_{R5}=I_{PV4}+I_{PV5} \quad (۱۰)$$

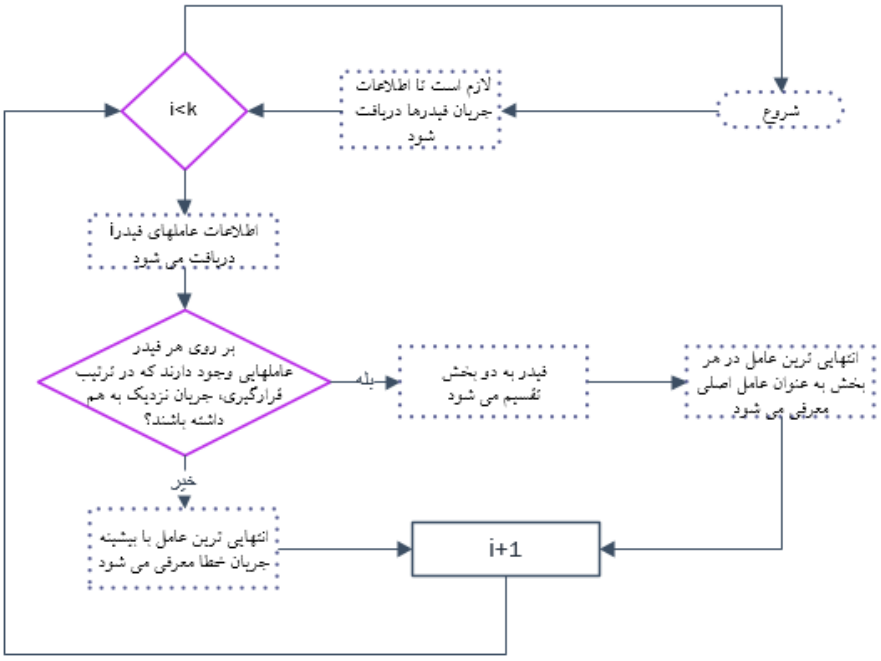
$$I_{R6}=I_{PV5} \quad (۱۱)$$

در این حالت که بر روی یک فیدر جریان خطا از دو نقطه وارد می‌گردد، لازم است تا بتوان ناحیه وقوع این خطا را تشخیص داد. در این حالت در لایه دوم از عملکرد اولین رله بر روی این فیدر وضعیت را مشخص می‌کند. لایه دوم مقدار CB.Sig را از رله دریافت می‌کند. بر روی فیدر اصلی سه رله R1، R2 و R3 به نحوی تنظیم شده‌اند که برای بیشترین جریان خطا در ابتدا رله R3 عمل می‌کند. این جریان برابر مقدار ثبت شده IFA3 می‌باشد. با توجه به اینکه برای وقوع این جریان خطا در ابتدا این رله عمل می‌نماید، رله R3 به عنوان اولین رله ای است که در ترتیب رله‌های قرار گرفته در یک مسیر به خطا نزدیکتر می‌باشد، در نتیجه لازم است تا عمل نماید. در این حالت فیدر از این قسمت به دو بخش تقسیم شده و در طرف دیگر رله R4 به با بیشترین جریان خطای عبوری رله نزدیک به نقطه خطا می‌باشد.

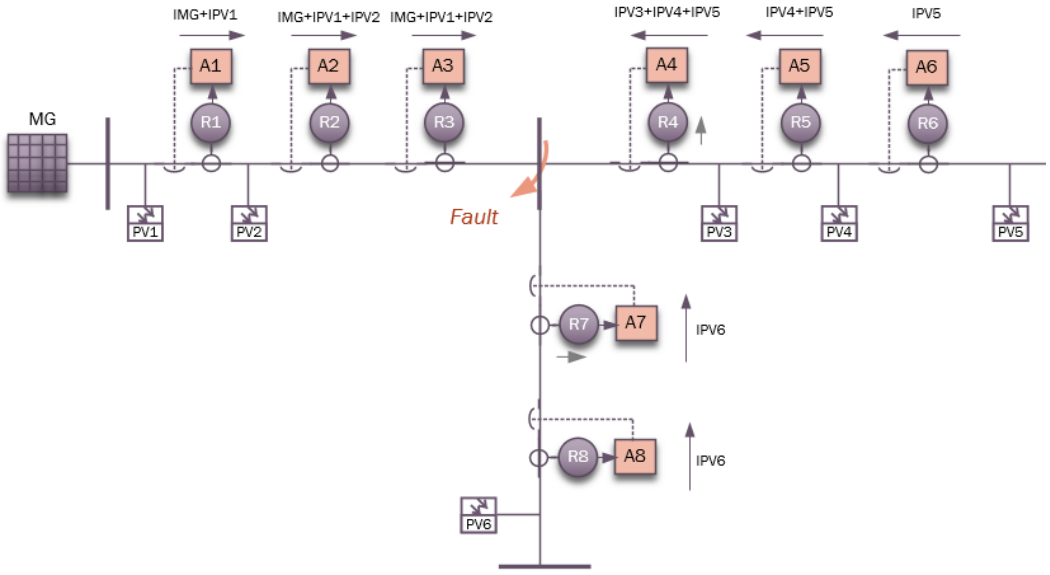
بر روی فیدر جانبی با حضور دو رله R7 و R8 هر دو رله جریان خطای مشابه:

$$I_{R8}=I_{PV7}=I_{PV6} \quad (۱۲)$$

را بر روی خود مشاهده می‌کنند. در این مرحله با توجه به مکان خطا برای دو رله R3 و R4، با در نظر داشتن اینکه مکان رله R7 در همسایگی این دو رله قرار دارد، این رله به عنوان حفاظت اصلی تشخیص داده می‌شود. در تمامی حالت‌های بررسی شده، در صورتی که به هر دلیلی در بخش Status رله سیگنال مبنی بر عدم سلامت رله و یا عدم عملکرد صحیح کلید قدرت مشاهده شود، با توجه به اینکه نقش‌ها در لایه دوم مشخص شده‌اند، حفاظت‌های پشتیبان آماده عملکرد می‌باشند. در این حالت حفاظت‌های اصلی با ارسال سیگنال درخواست قطع عملکرد حفاظتی را به رله پشتیبان گزارش می‌دهند.



شکل(۱۳): الگوریتم حفاظتی پیشنهادی در چالش نوع دوم

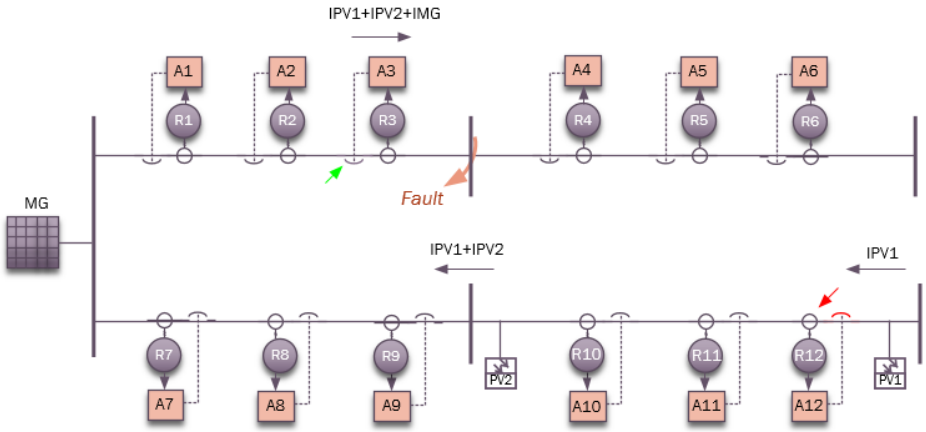


شکل(۱۴): تقسیم سازی فیدر شبکه در چالش حفاظتی نوع دوم

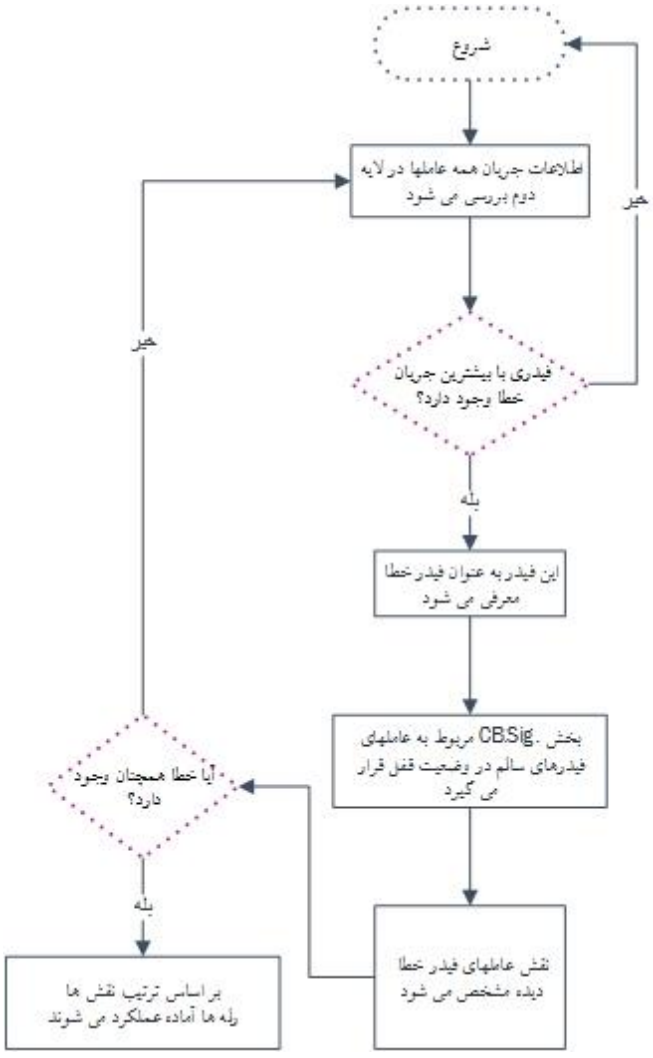
- تشخیص چالش سوم:

در زمانی که جریان خطای شبکه یک مسیر حلقه را برای رسیدن به نقطه خطا طی می‌کند، شرایط به سمتی می‌رود که ممکن است قسمت‌های زیادی از شبکه دچار قطعی اشتباه بر روی قسمت‌های سالم شود. شکل (۱۵) را به بررسی رفتار و نحوه تشخیص این چالش می‌پردازد. در صورتی که بر روی فیدری میزان جریان خطای اتصال کوتاه بالا باشد، در زمان وجود جریان برگشتی می‌تواند برای حفاظت‌های آن فیدر مشکل ایجاد نماید. علت آن عملکرد سریع حفاظت‌های آن نواحی می‌باشد. در شکل (۱۵) با وقوع خطا در ناحیه

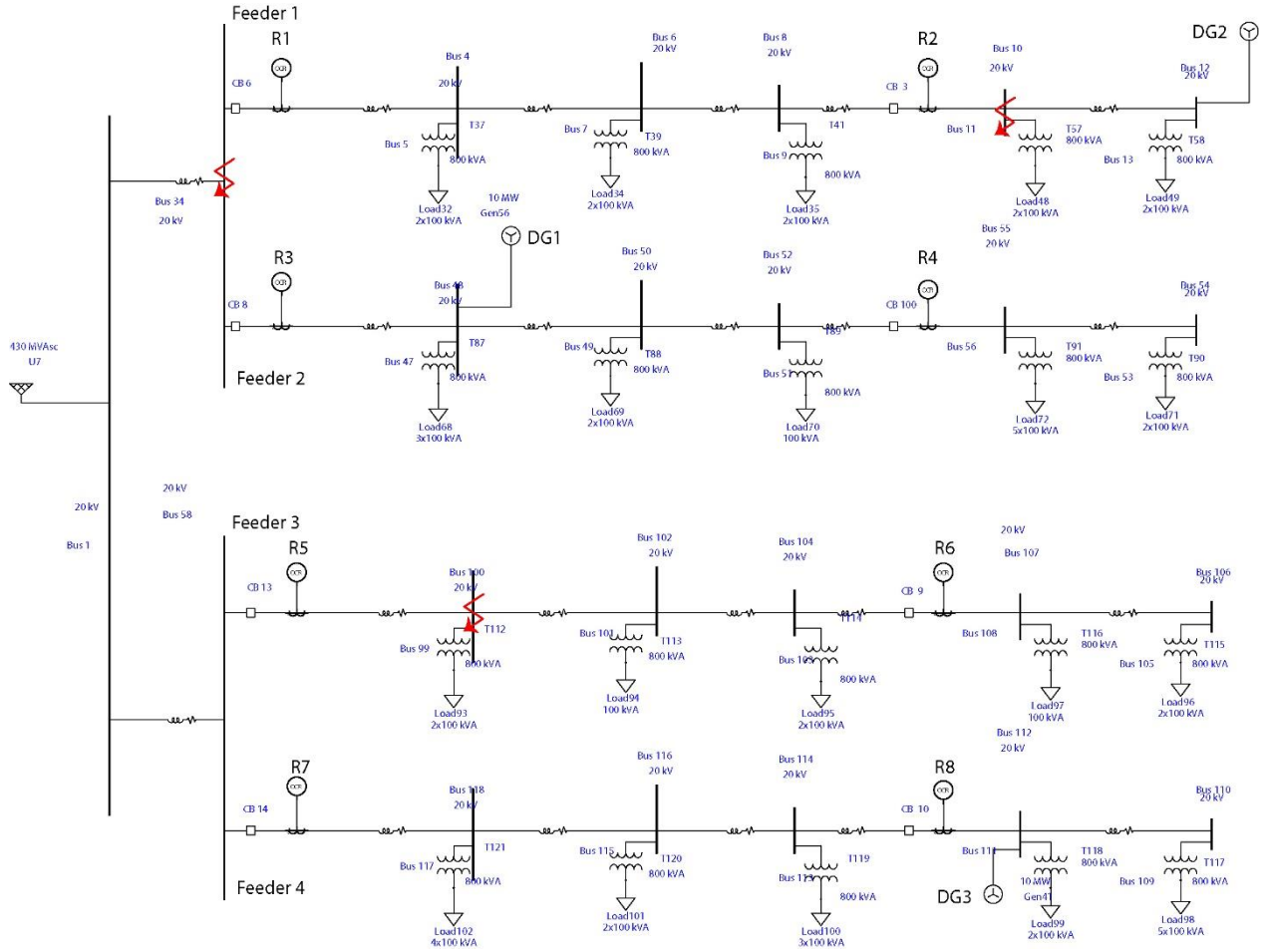
حفاظتی رله R3، سه جریان خطای متفاوت بر روی شبکه جاری می‌شود. مقدار جریان خطای IPV1 که از رله R12 عبور می‌کند، مقدار جریان IPV1+IPV2 عبوری از رله R9 و مقدار جریان IPV1+IPV2+IMG که از رله R3 عبور می‌کند. در این حالت لازم است تا وضعیت این رله‌ها نسبت به خطا مشخص شوند. زیرا درصورت عدم مدیریت عملکرد، در ابتدا رله‌های R12 و R9 فیدر سالم را بی‌برق خواهند کرد.



شکل(۱۵): بررسی چالش حفاظتی نوع سوم



شکل(۱۶): الگوریتم حفاظتی پیشنهادی در چالش نوع سوم

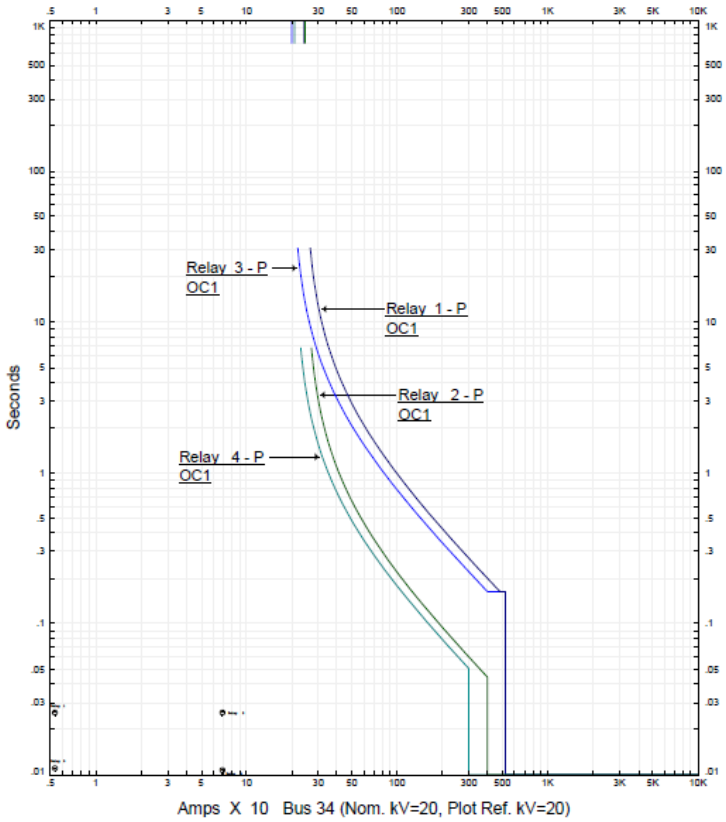


شکل(۱۷): شبکه شبیه سازی شده در نرم افزار ETAP

جدول(۱): اطلاعات مربوط به جریان هماهنگی رله‌های اصلی و پشتیبان

رله‌ها	مقدار جریان خطا	زمان عملکرد
R1,R2	2140	395,88
R3,R4	1620	436,100
R5,R6	2500	397,85
R7,R8	1480	538,144

در شکل (۱۶) مشاهده میکنیم که فرآیند نقش پذیری در این حالت چگونه صورت می‌پذیرد. اطلاعات جریان که بر روی پروتکل SMV به سطح دوم ارسال شده‌اند، مورد بررسی قرار می‌گیرند. در ادامه لایه دوم بررسی می‌کند که آیا فیدری با بیشترین جریان خطا بر روی شبکه قابل شناسایی است یا خیر. در صورت وجود این فیدر به عنوان نزدیکترین فیدر به محل خطا معرفی خواهد شد. به منظور جلوگیری از عملکرد اشتباه فیدرهای دیگر در این لحظه بخش Sig.CB عامل‌های رله فیدر سالم در وضعیت قفل قرار می‌گیرند. در ادامه بر روی فیدر خطا حفاظت‌های اصلی و پشتیبان توسط لایه دوم مشخص می‌شود. سپس بررسی می‌گردد که آیا خطا برطرف شده‌است و یا خیر. درصورتی که خطا برطرف شده باشد و وضعیت جریان فیدرها به شرایط جریان نرمال شبکه رسیده باشد، عامل‌های سایر فیدرها به وضعیت عادی خود بازمیگردند. در صورتی که خطا همچنان بر روی شبکه وجود داشته باشد لازم است تا بر اساس ترتیب نقشهای مشخص شده بر روی فیدر خطا، عامل‌ها عمل نمایند.



شکل(۱۸): مشخصه حفاظتی بر روی فیدر اول و دوم

۵- شبیه سازی

به منظور بررسی عملکرد روش پیشنهاد شده در این مقاله، شبکه شبیه سازی شده در نرم افزار ETAP در شکل (۱۷) نمایش داده شده‌است. شبکه از ۴ فیدر تشکیل شده‌است. بر روی فیدر اول دو رله R1 و R2، بر روی فیدر دوم دو رله R3 و R4، بر روی فیدر سوم دو رله R5 و R6 و بر روی فیدر چهارم دو رله R7 و R8 قرار گرفته‌اند. منحنی حفاظتی بر روی چهار فیدر به ترتیب در شکل‌های (۱۸) و (۱۹) قابل مشاهده می‌باشد. اطلاعات مربوط به جریان هماهنگی رله‌های اصلی و پشتیبان در جدول (۱) نمایش داده شده‌است.

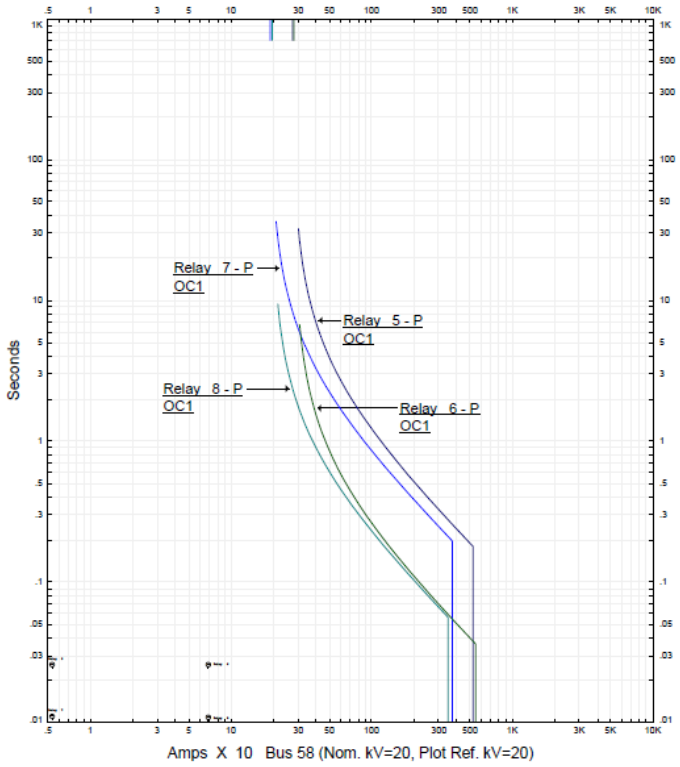
این اطلاعات مربوط به سیستم حفاظتی و درزمان عدم حضور منابع تولید پراکنده می‌باشد. در ادامه قصد داریم تا چالش‌های بررسی شده در قسمت قبل را مورد بررسی قرار دهیم.

بررسی چالش اول:

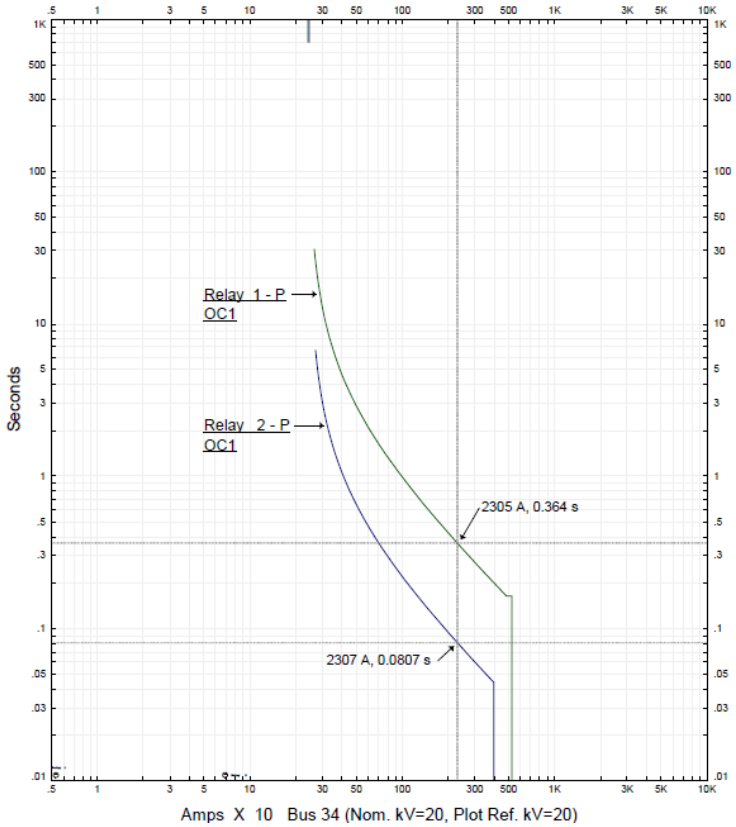
فرض کنیم تنها منبع تولید پراکنده DG1 به شبکه متصل می‌باشد. در این حالت خطایی در ناحیه حفاظتی رله R2 اتفاق می‌افتد. شکل (۲۰)، وضعیت عملکرد دو رله R1 و R2 را نمایش می‌دهد. با توجه به شکل میزان جریان عبوری از دو رله افزایش یافته است که منجر به کاهش زمان عملکرد هر دو رله شده و حاشیه هماهنگی ۳۰۰ میلی ثانیه را نقض کرده است. با توجه به الگوریتم پیشنهاد شده، در ابتدا لازم است تا جریان فیدرها با مقدار IFmax ثبت شده مقایسه گردد. در این حالت اطلاعات جریان هر فیدر دریافت می‌شود. جدول (۲) این اطلاعات را نمایش می‌دهد. با توجه به جدول مشخص است که جریان بر روی فیدر اول مقدار ثبت شده را نقض کرده است.

جدول(۲): اطلاعات مربوط به جریان رله‌ها در چالش اول

R1	R2	R3	R4	R5	R6	R7	R8
2310	2310	477	-	-	-	-	-

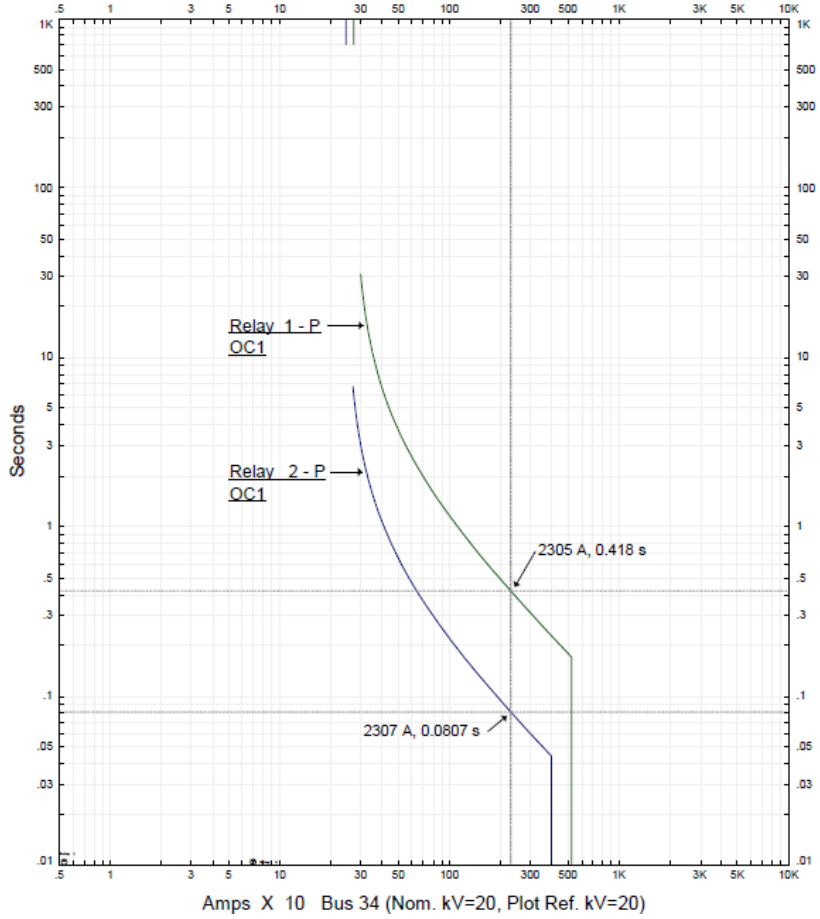


شکل(۱۹): مشخصه حفاظتی بر روی فیدر سوم و چهارم



شکل(۲۰): وضعیت عملکرد دو رله R1 و R2 در بررسی چالش اول

با توجه به اطلاعات فیدر شماره ۱، فیدری است که بیشترین جریان خطا از روی آن عبور می‌کند. در این حالت فیدرهای شماره ۳،۲و ۴ پیامی را جهت جلوگیری از عملکردشان دریافت می‌کنند. در ادامه با توجه به اینکه بر روی فیدر اول دو رله با بیشینه جریان خطای مشابه وجود دارند انتهایی ترین رله یعنی رله R2 به عنوان حفاظت اصلی معرفی شده و رله R1 به عنوان پشتیبان آن می‌باشد. با توجه به اینکه در این حالت حفاظت اصلی در زمان مناسبی عمل خواهد کرد، رله پشتیان آماده به عملکرد می‌باشد. در ادامه نیز فرمان برای بروزرسانی تنظیم حفاظت R1 ارسال شده و این رله تنظیمات خود را بروزرسانی می‌کند. شکل (۲۱) وضعیت این دو رله را پس از دریافت تنظیمات جدید نشان می‌دهد.



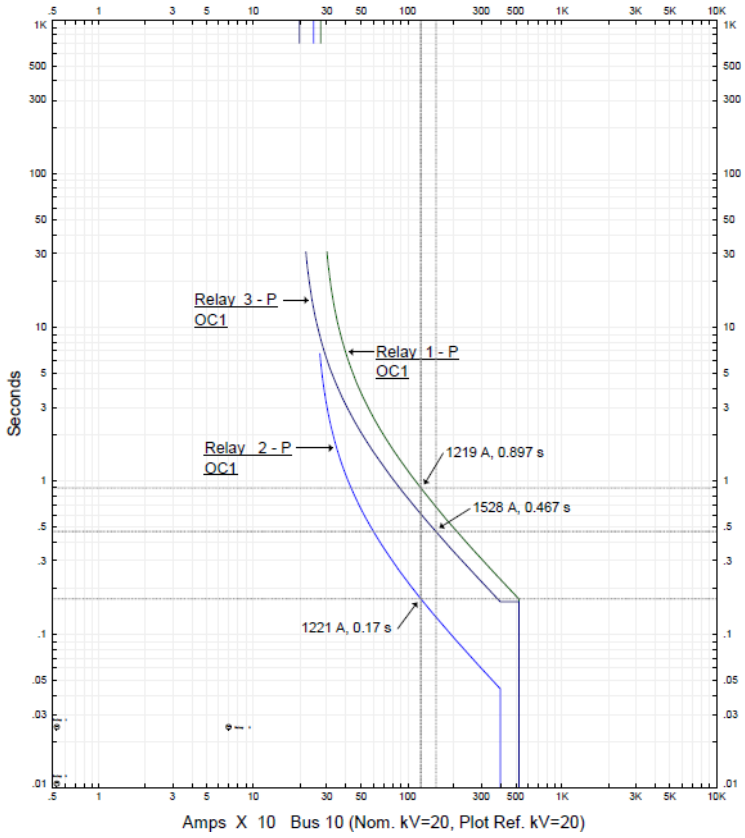
شکل(۲۱): بروزرسانی تنظیمات رله R1 در بررسی چالش اول

با توجه به شکل مشخص است که رله R1 در جایگاه حفاظت پشتیان با دریافت تنظیمات جدید در وضعیت مناسبی قرار گرفته است. در شرایط قبلی میزان زمان عملکرد این رله ۳۶۴ میلی ثانیه بوده است که در شرایط جدید به مقدار ۴۱۸ میلی ثانیه افزایش یافته است.

بررسی چالش دوم:

DG2 را به شبکه متصل می‌نماییم. خطایی بر روی فیدر وروی دو فیدر اول و دوم ما بین رله R1 و R3 اتفاق می‌افتد. وضعیت عملکرد سیستم حفاظتی در شکل (۲۲) نمایش داده شده‌است. با توجه به شکل مشخص است که رله R2 عملکرد سریعتری داشته است که با توجه به مکان قرارگیری آن و همچنین وجود رله R1 عملکرد اشتباهی داشته است. جریان عبوری از سه رله به ترتیب برابر ۱۲۲۰، ۱۲۲۰ و ۱۵۳۰ آمپر می‌باشد.

راهکار پیشنهادی در این مقاله به منظور جلوگیری از وقوع این حالت عملکرد به این صورت می‌باشد که در ابتدا اطلاعات جریان فیدرها که در جدول (۳) آمده است به لایه دوم ارسال می‌شود.



شکل(۲۲): وضعیت عملکرد رله‌های R1 ، R2 و R3 در بررسی چالش دوم

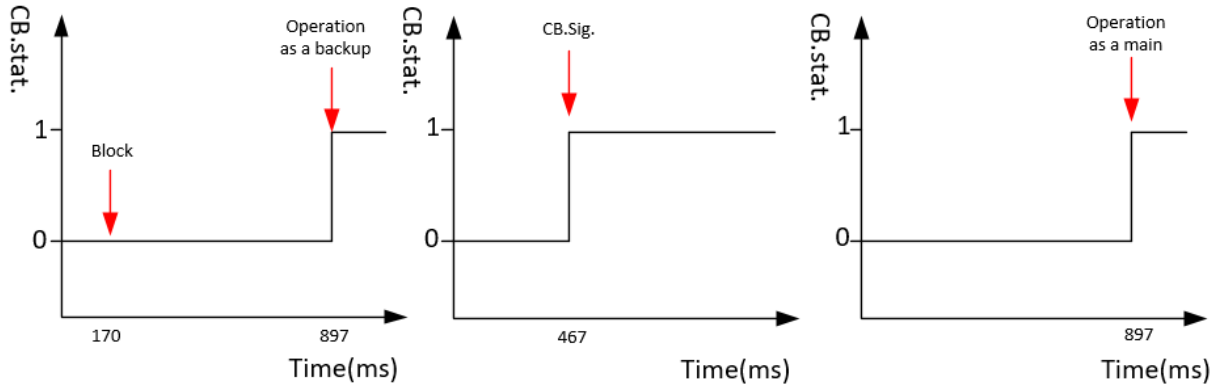
جدول(۳): اطلاعات مربوط به جریان رله‌ها در چالش دوم

R1	R2	R3	R4	R5	R6	R7	R8
1220	1220	1530	-	-	-	-	-

در مرحله اول، اطلاعات جریان فیدرها مطابق با جدول (۳) جمع آوری می‌شود. با توجه به وجود تعداد ۴ فیدر، اطلاعات جیران فیدرها توسط لایه دوم دریافت می‌شوند. در ابتدا اولین فیدر وارد مرحله بررسی قرار می‌گیرد. در این حالت شبکه در وضعیتی قرار دارد که جریان از دو سمت به طور همزان وارد نقطه خطا می‌شوند. در این حالت نیاز است تا بر روی هر فیدر که لازم باشد تعداد دو رله عمل نماید.

در لایه دوم جهت تشخیص این وضعیت نیاز دارد تا بر روی هر فیدر تغییرات جریان خطا را بررسی نماید. با دریافت اطلاعات کامل عامل‌های فیدرها، بر روی فیدر اول عامل‌هایی وجود دارند که در ترتیب قرارگیری، جریان مشابه به هم دارند. در این حالت تغییرات جریان بصورتی می‌باشد که بر اساس آن فیدر به دو بخش تقسیم بندی می‌شود.

عامل‌های R1 و R2 به عنوان دو عامل با جریان مشابه می‌باشند که بر اساس اطلاعات جریان، رله R1 به عنوان حفاظت اصلی معرفی می‌شود. به همین ترتیب بر روی فیدر دوم رله R3 به عنوان حفاظت اصلی معرفی می‌شود. با توجه به جریان خطا بر روی رله R3، مقدار CB.Sig توسط لایه دوم دریافت می‌شود. در این قسمت فیدرهای منتهی به خطا به دو بخش تقسیم می‌شود. با توجه به اطلاعات جریان بدست آمده دو رله R1 و R3 به عنوان حفاظت‌های اصلی تقسیم بندی می‌شود. در صورتی که به هر دلیلی در بخش Status رله سیگنال مبنی بر عدم سلامت رله و یا عدم عملکرد صحیح کلید قدرت مشاهده شود، با توجه به اینکه نقش‌ها در لایه دوم مشخص شده‌اند، حفاظت‌های پشتیبان آماده عملکرد می‌باشند. در این حالت حفاظت‌های اصلی با ارسال سیگنال درخواست قطع عملکرد حفاظتی را به رله پشتیبان گزارش می‌دهند. در این وضعیت رله R1 در صورت عدم عملکرد در زمان مناسب با ارسال سیگنال رله R2 را در وضعیت آماده عملکرد قرار می‌دهد. این در حالی است که رله R4 با توجه به اینکه جریانی بر روی خود مشاهده می‌کند، نقش حفاظت پشتیبان را نخواهد داشت. شکل (۲۳) وضعیت ارسال فرمان میان رله‌ها را در استاندارد IEC61850 نمایش می‌دهد.



شکل(۲۳): ارسال فرمان میان رله‌ها در چالش دوم

بررسی چالش سوم:

DG3 در ناحیه حفاظتی رله R8 به شبکه متصل می‌گردد. در شرایطی که خطایی در ناحیه حفاظتی رله R5 اتفاق افتد، جریان خطای عبوری از رله‌های شبکه بصورت جدول (۴) تشکیل می‌گردد.

جدول(۴): اطلاعات مربوط به جریان رله‌ها در چالش سوم

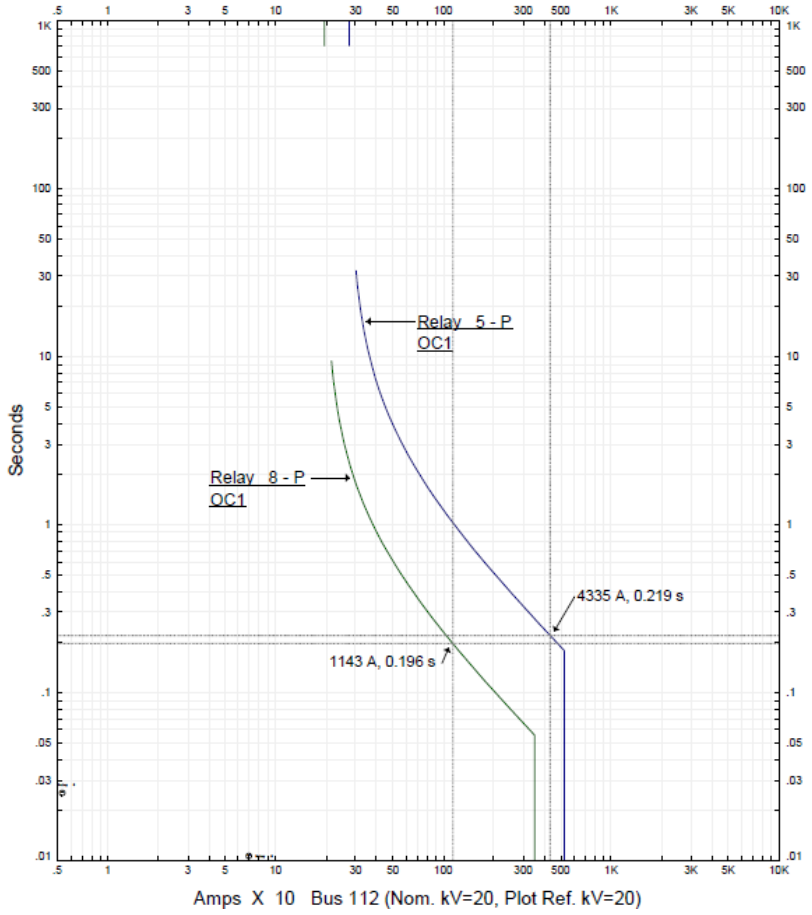
R1	R2	R3	R4	R5	R6	R7	R8
227	227	283	-	4300	-	1140	1140

با توجه به جدول مشخص است که جریان عبوری از هریک از فیدرها به چه صورت درحال تغییر می‌باشد. در این وضعیت از سه رله R5، R7 و R8 به ترتیب جریان ۴۳۰۰، ۱۱۴۰ و ۱۱۴۰ عبور می‌کند. شکل (۲۴) عملکرد دو رله R5 و R8 را برای این خطا نمایش می‌دهد. با توجه به شکل مشخص است که رله R5 که نقش حفاظت اصلی را داشته است در زمان ۲۱۹ میلی ثانیه خطا را تشخیص داده است در حالی که رله R8 در زمان ۱۹۶ میلی ثانیه عمل خواهد کرد.

با توجه به بررسی چالش سوم، در صورتی که بر روی فیدری میزان جریان خطای اتصال کوتاه بالا باشد، در زمان وجود جریان برگشتی می‌تواند برای حفاظت‌های آن فیدر مشکل ایجاد نماید. علت آن عملکرد سریع حفاظت‌های آن نواحی می‌باشد که همانطور که مشاهده کردیم به علت جاری شدن جریان خطای بالا توسط DG3 بر روی رله R8 این اتفاق رخ داده است. در این حالت لازم است تا وضعیت رله‌ها نسبت به خطا مشخص شوند. زیرا درصورت عدم مدیریت عملکرد، در ابتدا رله‌های R8 فیدر سالم را بی برق خواهند کرد.

طبق طرح پیشنهادی بررسی می‌کنیم که فرآیند نقش پذیری در این حالت چگونه صورت می‌پذیرد. اطلاعات جدول(۶) که بر روی پروتکل SMV به سطح دوم ارسال شده‌اند، مورد بررسی قرار می‌گیرند. در ادامه لایه دوم بررسی می‌کند که آیا فیدری با بیشترین جریان خطا بر روی شبکه قابل شناسایی است یا خیر. با توجه به اطلاعات جریان فیدر سوم بیشترین جریان خطا را بر روی خود مشاهده می‌کند. در نتیجه این فیدر به عنوان فیدر نزدیک به نقطه خطا معرفی خواهد شد. به منظور جلوگیری از عملکرد اشتباه فیدرهای دیگر در این لحظه، بخش .CB.Sig رله R8 در وضعیت قفل قرار می‌گیرد. در ادامه بر روی فیدر خطا حفاظت‌های اصلی و پشتیبان توسط لایه دوم مشخص می‌شود. دراین حالت با توجه به اینکه بر روی فیدر سوم تنها رله R5 خطا را مشاهده می‌کند به عنوان رله اصلی معرفی شده و رله‌های R7، R1 و R3 نیز به عنوان حفاظت‌های پشتیبان معرفی خواهند شد. پس از مشخص شدن نقش‌ها، رله R5 فرمان قطع را صادر می‌کند. در ادامه بررسی می‌گردد که آیا خطا برطرف شده‌است و یا خیر. درصورتی که خطا برطرف شده باشد و وضعیت جریان فیدرها به شرایط جریان نرمال شبکه رسیده باشد، سایر فیدرها به وضعیت عادی خود بازمی‌گردند. در صورتی که خطا همچنان بر روی شبکه وجود داشته باشد لازم است تا بر اساس ترتیب نقشهای مشخص شده، رله‌ها عمل نمایند.

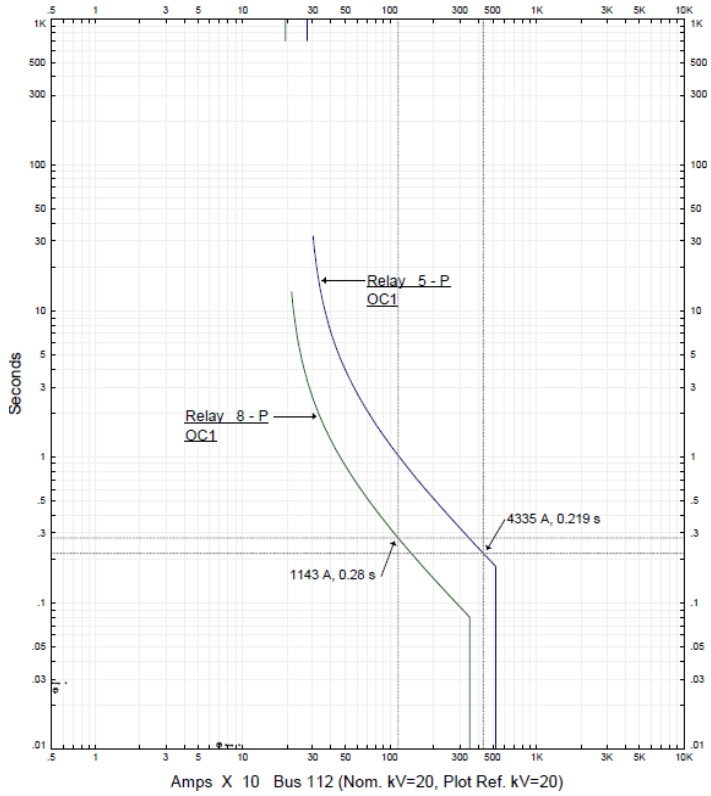
پس از رفع شدن خطا، زمان بروزرسانی تنظیمات حفاظتی می‌باشد که توسط سطح سوم انجام می‌گیرد. شکل (۲۵) وضعیت عملکرد دو رله R5 و R8 را پس از دریافت تنظیمات جدید نشان می‌دهند. همانطور که مشخص می‌باشد رله R5 در شرایط جدید در زمان ۲۱۹ میلی ثانیه و رله R8 در زمان ۲۶۰ میلی ثانیه برای این محدوده جریان خطا عمل می‌کنند. مشخص است که رله R5 عملکرد سریعتری داشته و از عملکرد اشتباه رله R8 جلوگیری کرده است.



شکل(۲۴): وضعیت عملکرد دو رله R5 و R8 در بررسی چالش سوم

٦- نتیجه‌گیری

عامل‌ها مجموعه‌ای از تجهیزات سخت‌افزاری و نرم افزاری می‌باشند که بصورت کاملا پویا می‌توانند درون یک ناحیه، که با آن ارتباط دارند، بصورت مستقل و یا تحت هدایت یک واحد دیگر تصمیم گیری نموده و بر روی آن تاثیر گذارند. یک تجهیز الکترونیکی هوشمند به عنوان میزبان این عامل‌ها انتخاب می‌شود. ارتباط میان تجهیزات الکترونیکی بر مبنای پروتکل ارتباطی IEC61850 عمل می‌باشد. روش پیشنهادی با بهره‌گیری از استاندارد IEC61850 و دو پروتکل GOOSE و SMV در تبادل اطلاعات وضعیتی و مقادیر اندازه‌گیری شده، توانست ساختار سنتی در الگوریتم حفاظتی مرسوم در سیستم‌های چندعاملی را بهبود بخشد. به منظور این کار، در ساختار حفاظتی چندلایه وظایف سطوح مدیریتی را معطوف به بروزرسانی خطا کرده و شرایط مانند تشخیص وضعیت شبکه و انتخاب نحوه عملکرد حفاظت‌ها را در سطوح پایین تر انجام می‌دهد. در نتیجه در هر لایه نقش‌هایی مشخص گردید و برای عملکرد هر نقش الگوریتم مشخصی ارائه شد. در نهایت طرح پیشنهادی بر روی یک شبکه آزمایشی مورد بررسی قرار گرفت که نتایج برآمده از طرح پیشنهادی، صحت عملکرد آن را نشان داده است.



شکل(۲۵): بروزرسانی تنظیمات دو رله R5 و R8 در بررسی چالش سوم

مراجع

[1] H. Yazdanpanahi, Y. W. Li and W. Xu, "A New Control Strategy to Mitigate the Impact of Inverter-Based DGs on Protection System," in *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1427-1436, Sept. 2012, doi: 10.1109/TSG.2012.2184309.

[2] K. A. Wheeler, M. Elsamahy and S. O. Faried, "A Novel Reclosing Scheme for Mitigation of Distributed Generation Effects on Overcurrent Protection," in *IEEE Transactions on Power Delivery*, vol. 33, no. 2, pp. 981-991, April 2018, doi: 10.1109/TPWRD.2017.2743693.

[3] R. A. Walling, R. Saint, R. C. Dugan, J. Burke and L. A. Kojovic, "Summary of Distributed Resources Impact on Power Delivery Systems," in *IEEE Transactions on Power Delivery*, vol. 23, no. 3, pp. 1636-1644, July 2008, doi: 10.1109/TPWRD.2007.909115.

[4] N. Rajaei, M. H. Ahmed, M. M. A. Salama and R. K. Varma, "Fault Current Management Using Inverter-Based Distributed Generators in Smart Grids," in *IEEE Transactions on Smart Grid*, vol. 5, no. 5, pp. 2183-2193, Sept. 2014, doi: 10.1109/TSG.2014.2327167.

[5] C. Prapanukool and S. Chaitusaney, "An appropriate disconnecting time of distributed generation by optimal protection setting and transformer connection type," *2012 9th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, Phetchaburi, 2012, pp. 1-4, doi: 10.1109/ECTICon.2012.6254264.

[6] J. K. Tailor and A. H. Osman, "Restoration of fuse-recloser coordination in distribution system with high DG penetration," *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, Pittsburgh, PA, 2008, pp. 1-8, doi: 10.1109/PES.2008.4596422.

[7] S. M. Brahma and A. A. Girgis, "Development of adaptive protection scheme for distribution systems with high penetration of distributed generation," in *IEEE Transactions on Power Delivery*, vol. 19, no. 1, pp. 56-63, Jan. 2004, doi: 10.1109/TPWRD.2003.820204.

[8] F. Coffele, C. Booth and A. Dyśko, "An Adaptive Overcurrent Protection Scheme for Distribution Networks," in *IEEE Transactions on Power Delivery*, vol. 30, no. 2, pp. 561-568, April 2015, doi: 10.1109/TPWRD.2013.2294879.

[9] H. F. Habib, M. E. Hariri, A. Elsayed and O. Mohammed, "Utilization of supercapacitors in adaptive protection applications for resiliency against communication failures: A size and cost optimization case study," *2017 IEEE Industry Applications Society Annual Meeting*, Cincinnati, OH, 2017, pp. 1-8, doi: 10.1109/IAS.2017.8101884.

[10] M. Singh, T. Vishnuvardhan and S. G. Srivani, "Adaptive protection coordination scheme for power networks under penetration of distributed energy resources," in *IET Generation, Transmission & Distribution*, vol. 10, no. 15, pp. 3919-3929, 17 11 2016, doi: 10.1049/iet-gtd.2016.0614.

[11] H. Wan, K. K. Li and K. P. Wong, "An Adaptive Multiagent Approach to Protection Relay Coordination With Distributed Generators in Industrial Power Distribution System," in *IEEE Transactions on Industry Applications*, vol. 46, no. 5, pp. 2118-2124, Sept.-Oct. 2010, doi: 10.1109/TIA.2010.2059492.

[12] D. Uthitsunthorn and T. Kulworawanichpong, "Distance protection of a renewable energy plant in electric power distribution systems*," 2010 International Conference on Power System Technology*, Hangzhou, 2010, pp. 1-6., doi: 10.1109/POWERCON.2010.5666058.

[13] S. Chaitusaney and A. Yokoyama, "Prevention of Reliability Degradation from Recloser–Fuse Miscoordination Due To Distributed Generation," in *IEEE Transactions on Power Delivery*, vol. 23, no. 4, pp. 2545-2554, Oct. 2008, doi: 10.1109/TPWRD.2007.915899.

[14] T. Saksornchi and B. Eua-arporn, "Determination of allowable capacity of distributed generation with protection coordination", Eng, J, Vol 13 No 3, Nov 3, 2009, doi: 10.4186/ej.2009.13.3.29.

[15] J. Chen, R. Fan, X. Duan and J. Cao, "Penetration level optimization for DG considering reliable action of relay protection device constrains," *2009 International Conference on Sustainable Power Generation and Supply*, Nanjing, 2009, pp. 1-5, doi: 10.1109/SUPERGEN.2009.5348221.

[16] S. M. Brahma and A. A. Girgis, "Microprocessor-based reclosing to coordinate fuse and recloser in a system with high penetration of distributed generation*," 2002 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No.02CH37309)*, New York, NY, USA, 2002, pp. 453-458 vol.1, doi: 10.1109/PESW.2002.985041.

[17] I. Xyngi and M. Popov, "An Intelligent Algorithm for the Protection of Smart Power Systems," in *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1541-1548, Sept. 2013, doi: 10.1109/TSG.2013.2244621.

[18] A. Agheli, H. A. Abyaneh, R. M. Chabanloo and H. H. Dezaki, "Reducing the impact of DG in distribution networks protection using fault current limiters," *2010 4th International Power Engineering and Optimization Conference (PEOCO)*, Shah Alam, 2010, pp. 298-303, doi: 10.1109/PEOCO.2010.5559205.

[19] W. El-Khattam and T. S. Sidhu, "Restoration of Directional Overcurrent Relay Coordination in Distributed Generation Systems Utilizing Fault Current Limiter," in *IEEE Transactions on Power Delivery*, vol. 23, no. 2, pp. 576-585, April 2008, doi: 10.1109/TPWRD.2008.915778.

[20] Hongxia Zhan *et al*., "Relay protection coordination integrated optimal placement and sizing of distributed generation sources in distribution networks," *2016 IEEE Power and Energy Society General Meeting (PESGM)*, Boston, MA, 2016, pp. 1-1, doi: 10.1109/PESGM.2016.7741277.

[21] C. Su, Z. Liu, Z. Chen and Y. Hu, "An adaptive control strategy of converter based DG to maintain protection coordination in distribution system," *IEEE PES Innovative Smart Grid Technologies, Europe*, Istanbul, 2014, pp. 1-6, doi: 10.1109/ISGTEurope.2014.7028900.

[22] Z. Liu, C. Su, H. K. Høidalen and Z. Chen, "A Multiagent System-Based Protection and Control Scheme for Distribution System with Distributed-Generation Integration," in *IEEE Transactions on Power Delivery*, vol. 32, no. 1, pp. 536-545, Feb. 2017, doi: 10.1109/TPWRD.2016.2585579.

[23] P. Mahat, Z. Chen, B. Bak-Jensen and C. L. Bak, "A Simple Adaptive Overcurrent Protection of Distribution Systems with Distributed Generation," in *IEEE Transactions on Smart Grid*, vol. 2, no. 3, pp. 428-437, Sept. 2011, doi: 10.1109/TSG.2011.2149550.

[24] M. Singh, T. Vishnuvardhan and S. G. Srivani, "Adaptive protection coordination scheme for power networks under penetration of distributed energy resources," in *IET Generation, Transmission & Distribution*, vol. 10, no. 15, pp. 3919-3929, 17 11 2016, doi: 10.1049/iet-gtd.2016.0614.

[25] H. F. Habib, T. Youssef, M. H. Cintuglu and O. A. Mohammed, "Multi-Agent-Based Technique for Fault Location, Isolation, and Service Restoration," in *IEEE Transactions on Industry Applications*, vol. 53, no. 3, pp. 1841-1851, May-June 2017, doi: 10.1109/TIA.2017.2671427.

[26] A. Manickam, S. Kamalasadan, D. Edwards and S. Simmons, “A Novel Self-Evolving Intelligent Multiagent Framework for Power System Control and Protection,” in *IEEE Systems Journal*, vol. 8, no. 4, pp. 1086-1095, Dec. 2014, doi: 10.1109/JSYST.2013.2269731.

[27] M. Pipattanasomporn, H. Feroze and S. Rahman, “Multi-agent systems in a distributed smart grid: Design and implementation,” *2009 IEEE/PES Power Systems Conference and Exposition*, Seattle, WA, 2009, pp. 1-8, doi: 10.1109/PSCE.2009.4840087.

[28] H. Wan, K. K. Li and K. P. Wong, “Multi-agent application of substation protection coordination with distributed generators,” *2005 International Conference on Future Power Systems*, Amsterdam, 2005, pp. 6 pp.-6, doi: 10.1109/FPS.2005.204251.

[29] Z. Liu and H. K. Høidalen, “A simple multi agent system based adaptive relay setting strategy for distribution system with wind generation integration,” *13th International Conference on Development in Power System Protection 2016 (DPSP)*, Edinburgh, 2016, pp. 1-6, doi: 10.1049/cp.2016.0025.

[30] IEC standard for single input energizing quantity measuring relays with dependent or independent time, IEC standard 60255 (2009).

[31] K. Kauhaniemi and L. Kumpulainen, “Impact of distributed generation on the protection of distribution networks,” 2004 *Eighth IEE Int. Conf. Develop. Power Syst. Protect.*, 2004, pp. 315-318 Vol.1, doi: 10.1049/cp:20040126.

[32] G. Zhabelova and V. Vyatkin, “Multiagent Smart Grid Automation Architecture Based on IEC 61850/61499 Intelligent Logical Nodes,” *IEEE Trans. Ind. Elect.*, vol. 59, no. 5, pp. 2351-2362, May 2012, doi: 10.1109/TIE.2011.2167891.

[33] W. X. Sheng, X. S. Yang, “Multi-Agent system applied in electric power system”, Beijing: *China Electrical Power*, pp.18.

زیرنویس‌ها

[1]Manufacturing Message Specification
[2]Generic Object Oriented System Event
[3]Sampled Measure Values