Computational Intelligence in Electrical Engineering
Vol. 14, No. 2, 2023
Research Paper

Intelligent Protection Scheme of Electrical Energy Distribution Systems in the presence of Distributed Generation Sources using Agent-Based Distributed Controller

Majid Rostamnia [1,2], Bahador Fani [1,2], Majid Moazzami [1,2], Mohamad Sadegh Rostamnia[1,2]

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

Abstract:
The ever-increasing of renewable distributed generation sources in distribution networks, as well as increasing network size, have faced agent-based protection schemes with a heavy communicational load. Accordingly, despite the fast and reliable nature of multi-agent systems, they have the possibility of improper performance, especially in centralized protection systems. This paper presents an intelligent self-healing method that has the ability to replace common multi-agent systems during fault conditions. Therefore, protection tasks are performed in a single control level, without dependence on higher communicational levels, to clear the fault. Decentralized operation of this structure is provided by using intelligent electronic devices and distributed communications. In this way, the proposed scheme is described with high-speed peer-to-peer communication capability using the IEC-61850 GOOSE protocol. Then, a penetration-free algorithm, without the help of a central controller, is provided by using GOOSE message capabilities, to prevent any electricity interruption due to insufficient protection settings. Finally, by planning different scenarios and simulating a practical distribution network via ETAP software, the accuracy of the proposed algorithm has been proven.

Keywords: Over Current Protection, Intelligent Electronic Device, Multi-Agent System, IEC-61850.

https://doi.org/10.22108/ISEE.2022.135103.1582

مقاله پژوهشی

طرح هوشمند حفاظت از سیستم‌های توزیع انرژی الکتریکی در حضور منابع تولید پراکنده با استفاده از کنترل‌کنندهٔ توزیع‌شده مبتنی بر عامل

مجید رستم نیا[۳،۱]، بهادر فانی*[۳،۲]، مجید معظمی[۳،۲]، محمدصادق رستم نیا[۳،۱]

۱- کارشناسی ارشد، دانشکده مهندسی برق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران
majidrostamnia1@gmail.com, msadegh.rostamnia@gmail.com

۲- دانشیار، دانشکده مهندسی برق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران
b.fani@pel.iaun.ac.ir, m_moazzami@pel.iaun.ac.ir

۳- مرکز تحقیقات ریزشبکه های هوشمند، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

چکیده: افزایش روزافزون منابع تولید پراکنده تجدیدپذیر در شبکه‌های توزیع و نیز افزایش سایز شبکه، طرح‌های حفاظت مبتنی بر عامل را با یک بار ارتباطی سنگین روبه‌رو کرده است. بر این اساس، با وجود ماهیت سریع و مطمئن سیستم‌های چندعاملی، احتمال عملکرد نامناسب را به‌خصوص در سیستم‌های حفاظتی متمرکز به دنبال دارند. در این مقاله، روش خودترمیمی هوشمند ارائه شده است؛ روشی که قابلیت جایگزین طرح‌های مبتنی بر سیستم‌های چندعاملی معمول را در شرایط خطا دارد. به این ترتیب، وظایف حفاظتی در یک تک‌سطح کنترل، بدون وابستگی به سطوح مخابراتی بالاتر، به‌منظور رفع خطا انجام می‌شوند. عملکرد غیرمتمرکز این ساختار با استفاده از دستگاههای الکترونیکی هوشمند و مخابرات توزیع‌شده ارائه می‌شود. به این ترتیب، طرح پیشنهادی با قابلیت ارتباط نقطه‌به‌نقطه سرعت بالا با استفاده از پروتکل IEC-61850 GOOSE بیان می‌شود. سپس یک الگوریتم مستقل از نفوذ، بدون کمک کنترل‌کنندهٔ مرکزی با استفاده از قابلیت‌های پیام GOOSE ارائه شده است تا از هرگونه وقفه برق ناشی از عدم کفایت تنظیمات حفاظتی جلوگیری کند. درنهایت، با طرح سناریوهای مختلف و شبیه‌سازی یک شبکه توزیع عملی با نرم‌افزار ETAP، صحت عملکرد الگوریتم پیشنهادی اثبات شده است.

واژه‌های کلیدی: حفاظت جریان زیاد، دستگاه الکترونیکی هوشمند، سیستم چندعاملی، IEC-61850.

۱- مقدمه

باوجود مزایای مسلم منابع تولید پراکنده (DG)[۱] نصب‌شده در شبکه توزیع (DN)[۲]، وجود این منابع چالش‌های جدیدی را دربارهٔ سیستم حفاظتی شبکه به وجود می‌آورند. ازجمله این چالش‌ها ناتوانی در تشخیص خطا، از دست رفتن هماهنگی میان دستگاههای حفاظتی و عملکرد اشتباه سیستم حفاظتی هستند [۱-۳]. این چالش‌ها عمدتاً ناشی از تغییر سطح جریان‌های اتصال کوتاه و همچنین، تغییر جهت جریان‌ها در انشعابات شبکه به‌دلیل حضور DGها هستند [۴-۶].

در سال‌های اخیر تحقیقات گسترده‌ای به‌منظور کاهش تأثیرات عدم قطعیت DGها بر سیستم حفاظتی صورت

[۱] تاریخ ارسال مقاله: ۱۴۰۱/۰۶/۲۱
تاریخ پذیرش مقاله: ۱۴۰۱/۰۸/۲۸
نام نویسندهٔ مسئول: بهادر فانی
نشانی نویسندهٔ مسئول: ایران، نجف آباد، دانشگاه آزاد اسلامی، واحد نجف آباد، دانشکده مهندسی برق

گرفته و تکنیک‌های مختلفی ارائه شده است. ازجمله این روش‌ها محدودکردن درصد نفوذ DGها [۷و۸]، استفاده از محدودکننده‌های جریان خطا [۹و۱۰] (FCL)[۳]، خروج سریع DGها در لحظه خطا [۱۱و۱۲]، اصلاح سیستم حفاظتی [۱۳-۱۵] و استفاده از طرح‌های حفاظت تطبیقی[۴] (APS) [۱۶-۱۹] هستند.

اگرچه روش‌های مذکور مشکلات حفاظتی را به‌طور مؤثری کاهش می‌دهند، همچنان شامل اشکالاتی هستند. ازجمله این اشکالات، از دست دادن مزایای واحدهای DG در حالت نرمال شبکه با توجه به اهمیت تأمین بارها، افزایش احتمال آسیب به واحدهای DG، هزینه‌بر بودن و پیچیدگی طرح حفاظتی با افزایش تعداد منابع تجدیدپذیر و همچنین نیاز به ساختار ارتباطی و وجود یک کنترل‌کننده پردازشی سرعت بالا هستند.

چنین اشکالاتی با توجه به پیشرفت‌های جدید در فناوری، تأثیرات مهمی بر جهت‌گیری تحقیقات علمی در حل مسائل فوق خواهند داشت. بر این اساس، دانشمندان از میان روش‌های فوق، توجه بیشتری به APS به دلیل ظهور و گسترش سریع سیستم‌های حفاظت هوشمند مبتنی بر عامل داشته‌اند. به عبارت دیگر، با توجه به ماهیت مستقل، تعاملی و فعال سیستم‌های چندعاملی[۵] (MAS) استفاده از این تکنولوژی هوشمند، به‌منظور حفاظت از DNها در حضور DGهای مختلف و سایر مشکلات احتمالی به‌شدت استقبال شده است [۲۰-۲۲]. به‌منظور بیان جزئیات بیشتر، در یک MAS هر عامل به‌عنوان یک عملگر هوشمند در همکاری با عامل‌های دیگر در یک بستر مخابراتی به‌منظور حل مشکلات حفاظتی در نظر گرفته می‌شود. بر این اساس، از مسائل مهم در این سیستم، ارتباط فردی هر عامل با دیگر عامل‌ها و درک وضعیت آنها است. منظور از وضعیت، به معنی آگاهی از سالم‌بودن یا نبودن عامل، حضور در شبکه و اطلاعات مشاهده‌شده توسط آن است. درخور ذکر است عامل حالت‌های محیطی که مشاهده می‌کند را درک می‌کند و اگر هر تغییری در چنین حالت‌هایی تشخیص دهد، در زمان و شیوه از پیش تعیین شده مخصوص پاسخ می‌دهد.

در بیشتر APSهای مبتنی بر MAS، عامل‌های گوناگونی مانند دستگاههای حفاظتی، کلیدها، DGها، بارها و غیره می‌توانند در طرح‌های حفاظتی شرکت کنند [۲۳و۲۴]. برای نمونه، چنانچه رویدادی در شبکه رخ دهد، عامل‌ها پس از شناسایی تغییرات و جمع‌آوری اطلاعات، داده‌ها را به کنترل‌کننده مرکزی انتقال می‌دهند. پس از پردازش اطلاعات توسط واحد مرکزی، تصمیم مناسب با توجه به شرایط جدید به لایه‌های زیرین فرستاده می‌شود. در این روش، عامل‌های مربوطه، اقدامات و تغییرات لازم را انجام می‌دهند. بر این اساس، با توجه به عملکرد تقریباً مشابه طرح‌های ارائه‌شده در [۲۵-۲۸]، به دلیل استفاده از MAS، چهار اشکال مهم را به‌ویژه با اتصال DGهای تجدیدپذیر به شبکه‌های کاربردی بزرگ‌تر و نیز وابستگی به نفوذ DGها به‌دنبال دارند که عبارت‌اند از:

- وجود یک کنترل‌کننده مرکزی قدرتمند و وابستگی همه‌جانبه به آن: در سیستم‌های عملی بزرگ، با افزایش تعداد عامل‌ها و تولیدات تجدیدپذیر، وظایف واحد مرکزی در صورت افزایش تعداد رویدادهای شبکه به‌طور درخور توجهی افزایش پیدا خواهد کرد؛ از این رو افزایش فشار، افزایش خطر خرابی کنترل‌کننده مرکزی را به دنبال دارد که باعث نقص در طرح حفاظت کلی می‌شود.
- زمان‌بر بودن پردازش و انتقال اطلاعات بین سطوح مختلف: با رخداد خطا در شبکه، اطلاعات باید جمع‌آوری، ارزیابی و پردازش شوند تا دستورات مناسب به عامل‌های اجرایی فرستاده شود. این فرآیندهای پردازشی و ارتباطی، زمان‌بر است و احتمال ناکارایی این روش‌ها را افزایش می‌دهد.
- بار اطلاعاتی سنگین بر شبکه مخابراتی: در این طرح‌ها از شبکه مخابراتی به سمت بالا و به سمت پایین به ترتیب برای اطلاعات جمع‌آوری‌شده توسط عامل‌ها و ارسال دستورات مناسب به عامل‌های مربوطه استفاده می‌شود. شایان ذکر است افزایش روزافزون اندازه سیستم و عدم قطعیت DGهای تجدیدپذیر باعث می‌شود بار سنگین بر سیستم مخابراتی مشکل‌ساز شود.
- الزام استفاده از رله جایگزین به دلیل به‌روزرسانی طولانی‌مدت تنظیمات رله: معمولاً پس از یک رویداد شبکه، کنترل‌کننده مرکزی تنظیمات جدیدی را برای رله‌های مربوطه بارگذاری می‌کند که این فرآیند برای رله‌ها چند ثانیه طول می‌کشد. برخلاف احتمال کم آن، چنانچه خطایی به‌طور ناگهانی طی فرآیند به‌روزرسانی رخ دهد، باید یک

رله جایگزین برای مقابله با رخداد احتمالی وجود داشته باشد [۲۵]. با توجه به اینکه نفوذ متغیر با زمان DGهای تجدیدپذیر تعداد رویدادهای شبکه را به‌طور چشمگیری افزایش می‌دهند، احتمال رخداد خطا طی فرآیند به‌روزرسانی رله افزایش می‌یابد و طراحان ناچار به استفاده از رله جایگزین‌اند.

مشکلات بیان‌شده عملکرد سیستم حفاظت را به‌طور مستقیم تهدید می‌کنند. باوجود طرح‌های مستقل از نفوذ DG با استفاده از روش‌های غیرمتمرکز ارائه‌شده در [۲۹-۳۱]، این مقاله حفاظت DN را با استفاده از دستگاههای الکترونیکی هوشمند[۶](IED) و مخابرات توزیع‌شده به‌منظور غلبه بر مشکلات ساختارهای متمرکز سیستم‌های حفاظتی ارائه می‌دهد. در این طرح، یک ساختار غیرمتمرکز به‌منظور جایگزین MAS معمول در شرایط خطا پیشنهاد شده است که ابتدا خطا را به‌سرعت رفع و هماهنگی را حفظ می‌کند. سپس با توجه به ساختار جدید و گروه تنظیمات از پیش تعریف شده، تنظیمات IEDها را به‌روزرسانی می‌کند. به عبارت دیگر، در ساختار پیشنهادی وظایف کنترل و حفاظت، بدون کمک‌های کنترل‌کننده مرکزی پیشنهاد می‌شود. همچنین، این روش وظایف اساسی سیستم حفاظتی را بدون نیاز به انجام کارهای زمان‌بر یا استفاده از رله‌های جایگزین انجام می‌دهد. ازجمله ویژگی‌های برجسته طرح پیشنهادی، عملکرد خودترمیمی سیستم حفاظت با یک روش غیرمتمرکز هوشمند است که به کاهش بار ارتباطی منجر می‌شود و نیز ارائه یک الگوریتم مستقل از نفوذ با توجه به عدم قطعیت DGهای تجدیدپذیر.

در ادامه مقاله، بخش (۲) ساختار متداول سیستم حفاظت مبتنی بر MAS را مرور و احتمال عملکرد نامناسب سیستم را به علت افزایش تعداد ارتباطات در این ساختار شرح می‌دهد. سپس مشخصات یک راه‌حل مناسب ارائه می‌شود که به‌عنوان پایه‌های اساسی الگوریتم حفاظت پیشنهادی در بخش (۳) استفاده می‌شود. بخش (٤) روش پیشنهادی را ازطریق شبیه‌سازی یک سیستم تست عملی تأیید می‌کند. درنهایت، بخش (۵) نتیجه‌گیری مقاله را ارائه می‌دهد.

۲- ساختار کلی سیستم حفاظت مبتنی بر MAS

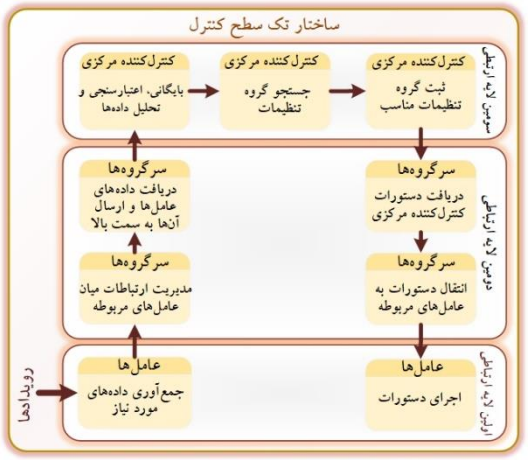
در این بخش، ابتدا به‌طور خلاصه ساختار ارتباطی و کنترل طرح‌های حفاظت مبتنی بر MAS معمول، بررسی و سپس مشکل افزایش تعداد ارتباطات همراه با راه‌حل‌های پیشنهادی مطرح می‌شود.

۲-۱- لایه‌های ارتباطی طرح حفاظت مبتنی بر MAS

با توجه به شکل (۱)، ساختار ارتباطی یک MAS نوعی معمولاً به‌واسطهٔ سه لایه اجرا می‌شود [۲۵]. نخستین لایه به عامل‌های توزیع‌شده اشاره دارد. عامل یک بخش روی تجهیز الکترونیکی هوشمند است. این بخش به‌صورت نرم‌افزاری یا سخت‌افزاری است و می‌تواند با قرارگیری در شبکه، رویدادها را تشخیص دهد. یک عامل با قرارگیری در شبکه می‌تواند نسبت به تغییرات محیط واکنش نشان دهد. هر عامل براساس یک تابع اجرایی و یک پروتکل ارتباطی (به‌طور مثال، IEC-61850) امکان پردازش و تبادل اطلاعات را میسر می‌سازد؛ بنابراین، مطابق با مشخصات فنی دستگاههای مختلف سیستم، عامل‌های توزیع‌شده در سیستم حفاظتی مبتنی بر MAS می‌توانند رله‌ها، DGها، کلیدها، بارها و غیره در نظر گرفته شوند [۳۳و۳۲].

دومین لایه ارتباط میان عامل‌های لایه اول را با استفاده از سرگروههای در نظر گرفته شده مربوط به هر گروه از عامل‌های با توابع یکسان مدیریت می‌کند که شامل گروه عامل رله[۷](RAG)، گروه عامل DG، گروه عامل کلید[۸](BAG) و گروه عامل بار است [۲۵]. به عبارت دیگر، این سرگروهها، لایه دوم ساختار ارتباطی MAS را تشکیل می‌دهند.

سومین لایه، کنترل‌کننده مرکزی شناخته می‌شود که وظیفه جمع‌آوری اطلاعات شبکه، شناسایی پیشامدهای جدید و ارسال اطلاعات و دستورات لازم به تجهیزات را به عهده دارد.



شکل (۱): ساختار تک‌سطح کنترل طرح حفاظت مبتنی بر MAS معمول

۲-۲- سطوح کنترل طرح حفاظت مبتنی بر MAS

توابع کنترلی شبکه معمولاً دارای چندین سطح کنترل هستند که پایین‌ترین (اولین) سطح بلافاصله وظایف اساسی را انجام می‌دهد؛ در حالی که سطوح بالاتر به‌تدریج وظایف سطوح پایین‌تر را با تنظیم نقاط کار مربوط به آنها تصحیح می‌کنند. با وجود این، براساس دانش نویسندگان، باوجود سایر کنترل‌کننده‌های سیستم قدرت، هیچ طبقه‌بندی سلسله‌مراتبی پذیرفته‌شده کلی برای وظایف سیستم حفاظت وجود ندارد. این امر به این دلیل است که تقریباً بیشتر محققان برای طرح‌های حفاظتی، جز رفع خطا و حفظ هماهنگی رله‌ها هیچ انتظار دیگری ندارند؛ از این رو، هیچ‌کسی تمایل ندارد صرفاً این یک وظیفه را در چندین سطح کنترل تقسیم کند؛ با این حال سیستم‌های حفاظت سنتی دو سطح کنترل دارند که به شرح زیر است:

- سطح کنترل اول (پاکسازی خطا و حفظ هماهنگی): رله‌های سنتی معمولاً از برخی منحنی مشخصه‌های از پیش تعریف شده به‌منظور پاکسازی خطا و هماهنگ‌شدن با سایر رله‌ها (ظرف چند صد میلی‌ثانیه) استفاده می‌کنند.
- سطح کنترل دوم (به‌روزرسانی تنظیمات رله): اپراتورها با رویدادهای رایج شبکه، منحنی‌ها را به‌صورت دستی به‌منظور عملکرد صحیح حفاظت شبکه (ظرف چند دقیقه تا چند ساعت) اصلاح می‌کنند.

قابلیت سرعت بالای ساختارهای مبتنی بر ارتباطات مدرن، محققان را مایل به ترکیب هر دو این سطوح کنترل در یک تک‌سطح کنترل می‌کند. در چنین ساختاری – که در شکل (۱) نشان داده شده است – هم برای وظایف سطح کنترل اول و هم وظایف سطح کنترل دوم، داده در میان سه لایه ارتباطی منتقل خواهد شد؛ یعنی عامل‌ها (لایه اول) اطلاعات را به سمت بالا به سرگروه (لایه دوم) و سپس به سیستم مرکزی (لایه سوم) منتقل می‌کنند. در ادامه داده در سیستم مرکزی، پردازش و هر تصمیمی که گرفته شود، به لایه دوم منتقل خواهد شد. سرانجام، سرگروهها اطلاعات را به عامل‌های مربوطه برای اقدامات لازم یا هر تغییری در شبکه تحویل می‌دهند.

به این ترتیب کنترل‌کننده مرکزی، هوشمندانه بهترین تصمیمات را با توجه به دانش گسترده دربارهٔ سیستم انتخاب می‌کند. با وجود این، اگر تعداد ارتباطات مذکور افزایش یابد، به زمان‌بندی نامناسب ارتباطی و کاهش قابلیت اطمینان سیستم منجر می‌شود؛ از این رو، طرح حفاظت ممکن است در انجام وظایف هر دو سطح کنترل اول و دوم ناموفق باشد. در چنین شرایطی سؤال اصلی این است که چه چیزی باعث افزایش تعداد ارتباطات می‌شود، که از مهم‌ترین آنها به دو مورد زیر اشاره می‌شود:

- افزایش سایز شبکه: با افزایش تعداد عامل‌ها، ارتباطات ایجادشده میان عامل‌ها و لایه‌های مخابراتی به میزان چشمگیری نسبت به عامل‌های قبلی بیشتر می‌شود. بر این اساس، شبکه‌های بزرگ‌تر که تعداد بیشتری عامل دارند، به نسبت تعداد بیشتری از ارتباطات را تجربه می‌کنند.
- عدم قطعیت DGهای تجدیدپذیر: با هر گونه تغییر در نفوذ DGها، اطلاعات باید به‌منظور تصحیح تنظیمات رله‌ها در میان زیرساخت‌های سه لایه ارتباطی منتقل شود؛ بنابراین، نفوذ متغیر با زمان DGها به دلیل ماهیت پیش‌بینی‌ناپذیری این منابع باعث افزایش چشمگیر تعداد ارتباطات در سیستم‌های حفاظت می‌شود.

در ساختار MAS بررسی‌شده، با توجه به استفاده از تجهیزات هوشمند، شبکه ارتباطی میان عامل‌ها بسیار حائز اهمیت است. به این ترتیب در زیر بخش بعد، ویژگی‌ها و قابلیت‌های پروتکل ارتباطی (IEC-61850)[۹] بیان می‌شوند.

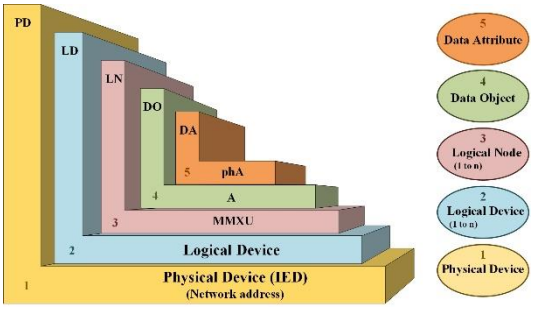
۲-۳- استاندارد IEC-61850

IEC-61850 پروتکل اختصاصی سیستم اتوماسیون پست است که هدف اصلی آن، تبادل اطلاعات میان IEDها از سازندگان مختلف است. این استاندارد بین‌المللی چهارچوب ارتباطی و اشتراک‌گذاری اطلاعات را در حالی فراهم می‌کند که بهره‌برداری سیستم‌های قدرت درحال انتقال از یک ساختار کنترل متمرکز به برخی قابلیت‌های نامتمرکز است [۳۴]. همچنین، براساس ترکیب مدل‌سازی شئ استاندارد با بلوک‌های توابع اجرایی امکان استفاده از سیستم‌های چندعاملی در سیستم‌های قدرت و کاربردهای اتوماسیون را میسر می‌سازد [۳۶و۳۵].

IEC-61850 توابعی مربوط به تجهیزات کنترل، حفاظت، نظارت و ثبت را در پست تعریف می‌کند. این توابع می‌توانند در یک تجهیز فیزیکی (PD)[10] به‌طور مثال، یک IED اجرا شوند یا بین چندین دستگاه با استفاده از رابط ارتباطات توزیع شوند. هر تابع به زیرتابع و عناصر کاربردی تقسیم‌پذیر است. عناصر کاربردی کوچک‌ترین بخش یک تابع هستند که می‌توانند اطلاعات را تبادل کنند. این عناصر اساسی در IEC-61850 گره منطقی (LN)[11] نامیده می‌شوند. LNها درحقیقت شئ‌هایی تعریف‌شده در متن مدل شئ‌گرا استاندارد هستند [۳۷].

هر LN شامل تعدادی شئ داده (DO)[12] است که هرکدام متعلق به یک کلاس معمول داده است؛ به‌طور مثال، رله اضافه جریان با گره منطقی (PTOC)[13] مدل شده که شامل DOهای TmASt برای مشخصات منحنی فعال، StrVal برای مقدار شروع، TmMult برای ضریب تنظیم زمانی و غیره است [۳۹و۳۸]. گره منطقی PTOC زمانی که جریان متناوب ورودی از یک مقدار از پیش تعیین شده فراتر می‌رود، عمل می‌کند که در آن جریان ورودی و زمان عملکرد، در یک بخش چشمگیری از محدوده عملکرد به‌طور معکوس رابطه دارند. DOهای Str و Op به‌ترتیب بیان‌کنندهٔ شروع و عمل کردن هستند که در بخش شبیه‌سازی به آنها پرداخته شده است.

شکل (۲) ساختار سلسله‌مراتبی داده در IEC-61850 را نشان می‌دهد. PD اولین قدم برای مدلسازی داده در IEC-61850 است. PD دستگاهی است که از یک یا چند پردازشگر ساخته شده است که توانایی تبادل داده و انجام پردازش روی آنها را دارد. درخور ذکر است هر PD می‌تواند میزبان چندین LN بسته به عملکرد آن باشد. این LNها در تجهیزات منطقی (LD)[14] دسته‌بندی می‌شوند که در متن PD به‌منظور اهداف ارتباطی تعریف شده‌اند. DOها نیز از گروهی از داده‌های پیوستی (DA)[15] ساخته شده‌اند. این داده‌ها براساس کاربرد خاص خود گروه‌بندی می‌شوند؛ به‌طور مثال، برخی از آنها نشان‌دهندهٔ حالات LN هستند؛ در حالی که برخی دیگر به‌منظور پیکربندی یا اندازه‌گیری استفاده می‌شوند.



شکل (۲): ساختار سلسله‌مراتبی در IEC-61850 [۳۷]

گره منطقی توصیف اندازه‌گیری در یک سیستم سه فاز، MMXU نامیده می‌شود که شامل چندین داده است. به‌طور مثال، A، W و VAr به‌ترتیب نماینده اندازه‌گیری جریان، توان اکتیو و راکتیو هستند. همچنین، phsA،phsB، phsC و neut داده‌هایی هستند که یک اندازه‌گیری مشخص، مربوط به فاز اول، دوم، سوم و خنثی را توصیف می‌کنند. کلید نیز با گره منطقی XCBR مدل شده است. Pos بیان‌کنندهٔ وضعیت کلید است و stVal مقدار حالت آن را مشخص می‌کند.

سیستم‌های حفاظتی غیر ارتباطی متداول معمولاً وظایف سطح کنترل اول را به‌صورت محلی با استفاده از رله‌های مبتنی بر منحنی سنتی انجام می‌دهند. به همین ترتیب در ساختارهای ارتباطی اگرچه امکان دارد، لازم نیست از هر سه لایه ارتباطی برای انجام این نوع وظایف استفاده شود؛ از این رو، وظایف سطح کنترل اول به‌طور مجزا می‌توانند با استفاده از قابلیت‌های پروتکل ارتباطی و یک الگوریتم مناسب با اولین لایه ارتباطی به انجام برسند. الگوریتم مدنظر

باید دو ویژگی زیر را به‌منظور تضمین عملکرد مطمئن وظایف سطح کنترل اول داشته باشد:

- مستقل از نفوذبودن: اگر طرح به سطح نفوذ DG وابسته باشد، باید پس از هر تغییر نفوذ به‌روزرسانی شود؛ در حالی که اگر مستقل از نفوذ باشد، می‌تواند از سیستم در هر سطح نفوذ واحدهای DG تجدیدپذیر محافظت کند. به عبارت دیگر، با توجه به عدم قطعیت واحدهای DG تجدیدپذیر، ویژگی اصلی یک طرح کارآمد اجتناب از استفاده از سطوح ارتباطی بالاتر به‌منظور مستقل از نفوذبودن است.
- استفاده از حداقل تعداد عامل: اگرچه طرح در لایه ارتباطی اول اجرا می‌شود، در صورت استفاده از عامل کمتر، مطمئناً بیشتر در برابر مشکلات بار ارتباطی مصون خواهد بود؛ بنابراین، طرح باید با حداقل تعداد عامل انجام شود؛ اما این سؤال مهم مطرح می‌شود که کدام مجموعه منحصربه‌فرد از عامل‌ها توانایی عمل موفقیت‌آمیز و نیز مقرون به‌صرفه را به‌عنوان یک طرح حفاظت کنترل سطح اول دارا هستند. در میان انواع مختلف عامل‌ها، با توجه به وظایف حیاتی رله‌ها در طرح‌های حفاظتی، آنها تنها تجهیزاتی هستند که این قابلیت را دارند. در غیر این صورت، هر نوع عامل دیگر علاوه بر خود، لزوماً باید از رله‌ها برای محافظت کامل از شبکه استفاده کند. بر این اساس، در این طرح IEDها که مسئول انجام وظایف حیاتی حفاظت‌اند، عامل در نظر گرفته می‌شوند.

۳- الگوریتم حفاظتی پیشنهادی

در روش پیشنهادی، IEDها به کمک توابع حفاظتی و LNهای مربوطه که پروتکل IEC-61850 ارائه می‌دهد، در شبکه پیاده‌سازی می‌شوند تا مشکلات موجود در سیستم‌های چندعاملی معمول را کاهش دهند و بهبود ببخشند. به این ترتیب روش حفاظتی پیشنهادی با ارائه یک ساختار غیرمتمرکز مبتنی بر عامل با عدم وابستگی به سطوح مخابراتی بالاتر و درنتیجه، حذف کنترل‌کننده مرکزی، افزایش قابلیت اطمینان سیستم را به دنبال دارد. در این بخش ابتدا لازم است قابلیت‌های پیام‌های GOOSE استفاده‌شده در طرح، به‌منظور انجام وظایف اینترلاک معرفی شوند. سپس بیان خواهد شد چگونه این قابلیت‌ها به نویسندگان در ارائه یک الگوریتم مستقل از نفوذ و حداقل عامل کمک کرده است.

۳-۱- سرویس‌ها و قابلیت‌های پیام GOOSE

رویداد عمومی شئ‌گرا پست [۱۶](GOOSE) یکی از پروتکل‌های متداول اجراشده بر IEC-61850 است که ارتباطات نقطه به نقطه سریع و قابل اطمینان را میان دستگاهها فراهم می‌آورد. مطابق با این پروتکل، یک دستگاه می‌تواند سایر دستگاهها را با یک تأخیر ٤ میلی‌ثانیه به‌روزرسانی کند [٤١و٤٠].

پیام GOOSE می‌تواند در یک برنامه جامع که از سیستم در هر سطح نفوذ تجدیدپذیر محافظت می‌کند، استفاده کند. بدین منظور که قابلیت‌های آن توانایی تجهیز سیستم به یک الگوریتم مستقل از نفوذ DGهای استفاده‌شده در شبکه را دارند. این قابلیت‌ها و سرویس‌ها به‌منظور هماهنگ‌کردن IEDها با یکدیگر به شرح زیر بیان می‌شوند:

- پیام GOOSE lockout: در صورت رخداد خطا، نزدیک‌ترین IED به خطا می‌تواند «پیام GOOSE lockout» را به هر IED بالادست یا پایین‌دست به‌منظور آگاه‌کردن دیگر عامل‌ها دربارهٔ پیکاپ IED اصلی ارسال کند. در این روش از هر گونه همکاری غیرضروری دیگر عامل‌ها جلوگیری می‌شود. به عبارت دیگر، هر عامل با استفاده از «پیام GOOSE lockout» از عملکرد عامل یا عامل‌های پشتیبان خود ازطریق مسدودسازی فرمان بازشدن کلید مربوطه آنها جلوگیری می‌کند.
- پیام GOOSE Reset: اگر IED اصلی در رفع خطا ناموفق باشد، انتظار می‌رود عامل پشتیبان در سریع‌ترین زمان ممکن این کار را انجام دهد. بر این اساس از «پیام GOOSE Reset» برای آزادکردن عامل پشتیبان از حالت قفل استفاده می‌شود.
- پیام GOOSE Request: در صورت عدم موفقیت رله اصلی «پیام GOOSE Request» باعث می‌شود عامل پشتیبان بلافاصله برای رفع خطا بدون هیچ تأخیر هماهنگی اقدام کند.

• پیام GOOSE Adaptive Reconfiguration: زمانی که حالت کلیدIED تغییر می‌کند، عملگر کنترلی مربوطه از IED فعال می‌شود و با انتشار «پیام GOOSE Adaptive Reconfiguration» برای سایر IEDها، گروه تنظیمات فعال آنها را به گروه تنظیمات از پیش تعریف شده بعدی، با توجه به شرایط جدید تغییر می‌دهد.

همان‌طور که در بخش دوم ذکر شد عامل‌های سطوح بالاتر از تمام زیرساخت‌های ارتباطی برای شناسایی وضعیت جدید شبکه و اعمال تنظیمات مناسب به رله‌ها استفاده می‌کنند. با استفاده از چنین راهبردی، در صورت رخداد خطا، عامل‌های سطوح بالاتر باید تنظیمات مناسب برای رله‌ها را قبلاً به‌روزرسانی کرده باشند تا خطا را با موفقیت رفع کنند؛ اما اگر خطای ناگهانی هم‌زمان با تغییر نفوذ رخ دهد، تنظیمات جاری رله‌ها نمی‌توانند لزوماً مشکل را حل کنند. در چنین وضعیتی، الگوریتم پیشنهادی با استفاده از سرویس‌های پیام GOOSE مطابق با منطق‌های تعریف‌شده آنها، کاملاً مستقل از نفوذ DGها با موفقیت عمل می‌کند. به عبارت دیگر، تغییرات نفوذ، صحت پیام‌های «GOOSE lockout، Reset و Request» را تغییر نمی‌دهد. به این ترتیب، استفاده از الگوریتم پیشنهادی که در زیربخش بعدی بیان می‌شود، راه‌حلی توانا به‌منظور عملکرد مطمئن سیستم حفاظت در برابر هر سطح نفوذی، بدون مواجه با مسئله کندی سطوح کنترل بالاتر خواهد بود.

۳-۲- الگوریتم تک‌سطح کنترل پیشنهادی

فلوچارت رسم‌شده در شکل (۳) نشان می‌دهد چطور الگوریتم پیشنهادی توابع سطح کنترل اول و دوم را در یک تک‌سطح کنترل بدون استفاده از لایه‌های ارتباطی بالاتر با استفاده از حداقل تعداد عامل اجرا می‌کند. این فرآیند به‌صورت زیر شروع و گام‌به‌گام ادامه می‌یابد:

• IEDها که عامل‌ها در نظر گرفته شده‌اند، با توجه به ارتباطی که روی بستر مخابراتی با یکدیگر برقرار می‌کنند، پیوسته با هم در ارتباط‌اند و تغییرات جریان خود را به یکدیگر گزارش می‌دهند.

• IEDها نسبت به جریان عبوری از خود، با توجه به تنظیمات مشخص‌شده برای آنها در شرایط طبیعی شبکه، حساسیت نشان می‌دهند. بر این اساس، توابع حفاظتی IEDها جریان خطا را در صورت عبور جریانی بیشتر از آستانه تحریک‌شان تشخیص خواهند داد.

• عامل‌ها حفاظت‌های اصلی و پشتیبان را با توجه به مکان خطا و جهت IEDها در تشخیص دادن یا ندادن جریان خطا مشخص می‌کنند.

• وضعیت هماهنگی IEDهای اصلی و پشتیبان، براساس منحنی مشخصه IEDها با توجه به سطح جریان خطا، با عامل‌ها مشخص می‌شود. در صورت نبود هماهنگی، الگوریتم کمکی پیشنهادی فراخوانده می‌شود.

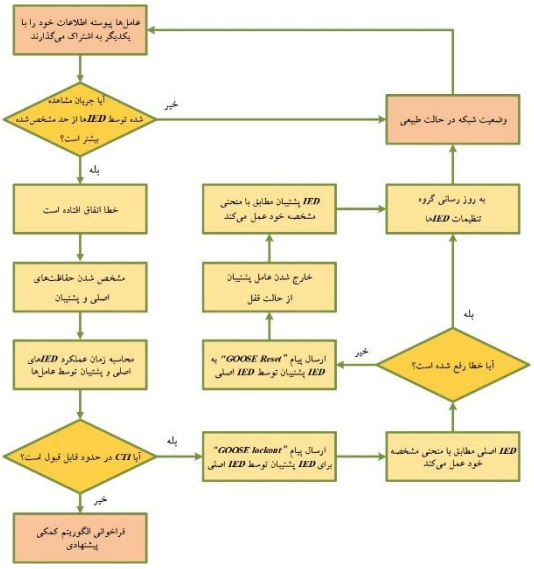
• در صورت حفظ هماهنگی، IED اصلی پیام «GOOSE lockout» را برای IED پشتیبان، منتشر و براساس زمان عملکرد خود با توجه به منحنی مشخصه عمل می‌کند.

• در صورت ناتوان‌بودن IED اصلی در رفع خطا، پیام «GOOSE Reset» را به IED پشتیبان ارسال می‌کند. به این ترتیب، IED پشتیبان با دریافت این پیام از حالت قفل خارج می‌شود.

• IED پشتیبان که در یک وضعیت هماهنگ با IED اصلی قرار دارد، مطابق با منحنی مشخصه و زمان عملکرد خود جداسازی ناحیه خطا دیده را انجام می‌دهد.

در لحظه جداسازی خطا، با بازشدن کلید مربوطه IED پیام «GOOSE Adaptive Reconfiguration» برای سایر IEDها ارسال و تنظیمات آنها براساس گروه تنظیمات از پیش تعریف شده به‌روزرسانی می‌شود. به این ترتیب شبکه در حالت طبیعی قرار می‌گیرد.

شایان ذکر است تنظیمات پیکاپ جریان زیاد این IEDها نیز ازطریق یک تحلیل حفاظتی براساس منحنی مشخصه رله که دارای دو بخش معکوس و آنی است، محاسبه و در تنظیمات فعال آنها جایگذاری می‌شود.



شکل (۳): فلوچارت الگوریتم حفاظتی پیشنهادی

به دنبال رخداد خطا، زمانی که تابع حفاظتی جهتی یا غیرجهتی (LN PTOC/PDOC) از IED اصلی، اضافه جریان را تشخیص دهد، عملگر Str.general آن فعال می‌شود، تایمر داخلی IED شروع می‌شود و پیام « GOOSE lockout» را به عملگر BlkOpn از IED پشتیبان ارسال می‌کند تا آن را فعال و فرمان بازشدن کلید مربوطه دستگاه را مسدود کند. در ادامه، وقتی تایمر IED اصلی پس از تأخیر در نظر گرفته شده به اتمام رسید، عملگر Op.general فعال و قطع انجام می‌شود. درخور ذکر است این تأخیر عامل با توجه به منحنی مشخصه و میزان جریان خطا تنظیم می‌شود. در صورتی که IED اصلی در رفع خطا ناموفق باشد، عامل این دستگاه پیام «GOOSE Reset» را به IED پشتیبان به‌منظور رهایی از حالت قفل ارسال می‌کند. با توجه به هماهنگ‌بودن IEDها، دستگاه پشتیبان براساس زمان عملکرد خود با توجه به منحنی مشخصه، اقدام به رفع خطا می‌کند.

به‌منظور بیان جزئیات بیشتر، زمان عملکرد IED مطابق رابطه (۱) محاسبه می‌شود:

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

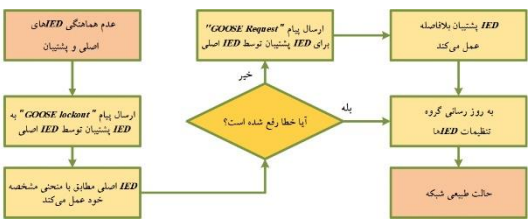
که I_F جریان خطا، I_p جریان پیکاپ و TMS ضریب تنظیم زمانی را بیان می‌کنند. A و B نیز بسته به نوع منحنی مشخصه تعیین می‌شوند. مطابق با این پارامترها، هماهنگی عامل‌های اصلی و پشتیبان مطابق معادله زیر انجام می‌شود:

$$\frac{A_1 . TMS_1}{(m_1)^{B_1} - 1} - \frac{A_2 . TMS_2}{(m_2)^{B_2} - 1} \geq \Delta T \qquad (۲)$$

که m نسب جریان خطا به جریان پیکاپ را بیان می‌کند و ΔT به زمان در نظر گرفته شده برای IEDها اشاره می‌کند که یک فاصله زمانی هماهنگی (CTI)[۱۷] مناسب (۴۰۰ تا ۳۰۰ میلی‌ثانیه) [۴۲] را داشته باشند.

مطابق با این معادلات، زمانی که عامل‌ها در حال انتقال داده به یکدیگرند، مقدار ΔT را بررسی می‌کنند. اگر این مقدار در حدود یک CTI استاندارد باشد، نشان از هماهنگ‌بودن حفاظت‌های اصلی و پشتیبان است و IEDها مطابق با زمان محاسبه‌شدهٔ عامل‌ها براساس رابطه (۱) عمل می‌کنند. در غیر این صورت، هماهنگی میان IEDهای اصلی و پشتیبان وجود ندارد که می‌تواند به معنی تغییر نفوذ واحدهای DG قلمداد شود. بر این اساس، الگوریتم کمکی پیشنهادی شکل (۴) به‌منظور عملکرد مستقل از نفوذ سیستم حفاظت به شرح زیر انجام می‌شود:

- IED اصلی پیام «GOOSE lockout» را به IED پشتیبان ارسال می‌کند.
- IED اصلی با توجه به میزان جریان خطا عبوری از آن، براساس زمان عملکرد محاسبه‌شده از منحنی مشخصه خود عمل می‌کند.
- اگر خطا با موفقیت برطرف نشده باشد، IED اصلی پیام «GOOSE Request» را برای IED پشتیبان به‌منظور پاکسازی فوری خطا ارسال می‌کند.
- پس از رفع خطا و تغییر وضعیت کلید، عملگر Pos.stVal از IED، فعال و تنظیمات IEDها به‌روزرسانی می‌شود. به این ترتیب، شبکه در حالت طبیعی قرار می‌گیرد.

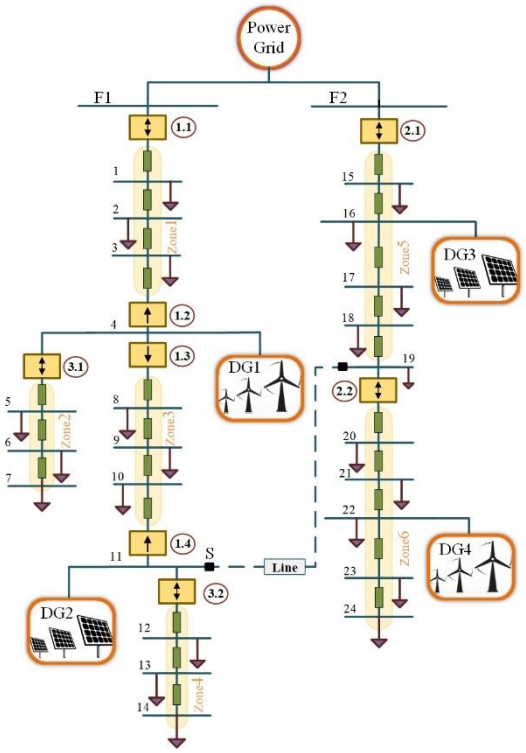


شکل (٤): فلوچارت الگوریتم کمکی پیشنهادی

شایان ذکر است تغییر سطح نفوذ DGها یا هرگونه عملکرد غیرمنتظره سایر تجهیزات، قادر به تغییر منطق هر یک از پیام‌های GOOSE ارسالی و دریافتی میان عامل‌ها در هر مرحله از اجرای الگوریتم و حتی سرعت انتقال دستورات نیست؛ از این رو، الگوریتم ارائه‌شده امکان پیاده‌سازی در هر شبکه‌ای را با افزایش قابلیت اطمینان سیستم دارا است.

٤- نتایج شبیه‌سازی

به‌منظور تعیین کارایی طرح پیشنهادی، شبکه رسم‌شده در شکل (۵) با نرم‌افزار *ETAP* ارزیابی می‌شود. همان‌طور که نشان داده شده است دو فیدر با نام‌های *F1* و *F2* به یک پست ٦٣/٢٠ کیلو ولت برای تأمین بارهای مربوطه متصل شده‌اند. همه بارهای متصل‌شده به فیدرها نیز با دو ترانسفورماتور ٢٠/٠/٤ کیلو ولت تغذیه می‌شوند. در این مطالعه، *DG*های تجدیدپذیر شامل واحدهای بادی و خورشیدی هستند که روی فیدر *F1* یا *F2* نصب شده‌اند. *DG1* و *DG4* بادی، *MVA* ۱۰ را فراهم می‌کنند که به‌ترتیب به باس‌های ٤ و ٢٢ متصل شده‌اند. همچنین، *DG2* و *DG3* دو سیستم خورشیدی *MVA* ۵ هستند که به باس‌های ١١ و ١٦ متصل شده‌اند. علاوه بر این، زمان مورد نیاز برای انتقال یک سیگنال، عملکرد کلید قدرت و اجرای توابع و پردازش داده در *IED*ها به‌ترتیب ٤، ۵۰ میلی‌ثانیه و ۵۰ میکروثانیه (که نادیده گرفته شده) در نظر گرفته شده‌اند *[۲۵]*.



شکل (۵): دیاگرام تک‌خطی شبکهٔ مطالعه‌شده

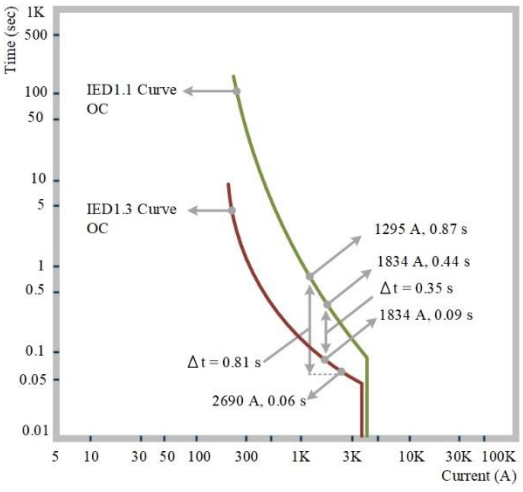
با توجه به شکل (۵)، در بین شش ناحیه شبکه مطالعه‌شده، ناحیه ٤ و ٦ با توجه به برخی ضروریات عملکردی، دارای بحرانی‌ترین بارها هستند. بر این اساس، طراح دو فیدر *F1* و *F2* را (با کلید*S*) به گونه‌ای متصل کرده است که بارهای موجود در هر دو ناحیه بتوانند با هر یک از ناحیه‌های ۳ یا ۵ تغذیه شوند؛ البته برای اجرای این طرح در یک فیدر شعاعی، یک اینترلاک میان *IED*ها به‌منظور بررسی وضعیت کلیدها برقرار است. چنانچه هر دو فیدر *F1* و *F2* در مدار باشند، دیگر امکان بسته‌بودن *S* و تغییر آرایش شبکه به حلقوی وجود ندارد. اگر *S* بسته شده باشد، یکی از کلیدهای مربوط به *IED1.1* یا *IED2.1* باز می‌شوند. برای محافظت از این شبکه شش *IED* روی فیدر *F1* و دو *IED* روی فیدر *F2* وجود دارند. *IED1.2*، *IED1.3* و *IED1.4* به‌عنوان *IED*های جهتی (که جریان خطا را تنها در جهت مشخص‌شده رؤیت می‌کنند) انتخاب شده‌اند. سایر *IED*های موجود غیرجهتی در نظر گرفته شده‌اند. همچنین، *IED3.1* و *IED3.2* دستگاههای حفاظتی فیدر بار در نظر گرفته شدند؛ به این منظور که با تعریف و در نظر گرفتن یک تأخیر زمانی بسیار کوتاه برای این

*IED*ها، پس وقوع خطا در هر نقطه از پایین‌دست آنها، در کمترین زمان ممکن عمل خواهند کرد. این تأخیر به‌طور نمونه ۲۰ میلی‌ثانیه در نظر گرفته شده است. با توجه به وضعیت کلیدها، سه سناریو ازنظر حفاظتی رخ می‌دهد که در این بخش، طرح پیشنهادی با توجه به سناریوهای مختلف در برابر تغییرات نفوذ *DG*ها بررسی می‌شود.

٤-١- سناریو اول (*S* باز است و دو فیدر *F1* و *F2* در مدارند)

زمانی که *S* باز است، فیدرهای *F1* و *F2* و حفاظت‌های مربوطه آنها به‌طور مستقل عمل خواهند کرد؛ بنابراین، روی فیدر *F1*، *IED1.1* پشتیبان *IED1.3* و *IED1.4* پشتیبان *IED1.2* به‌طور هماهنگ‌اند. به‌طور مشابه *IED2.1* پشتیبان *IED2.2* روی فیدر *F2* است.

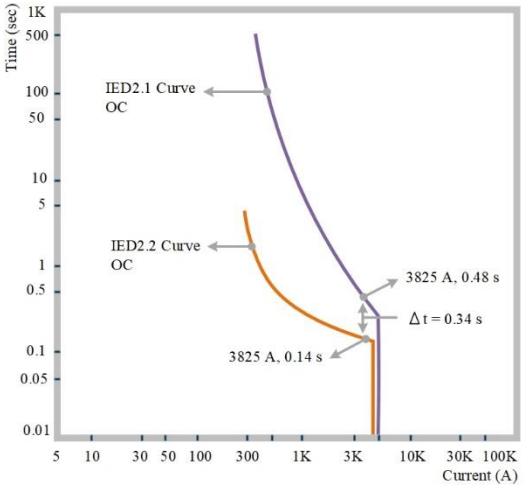
به‌منظور بررسی اینکه چطور تغییرات نفوذ بر طرح حفاظتی تأثیر می‌گذارند، ابتدا فرض می‌شود هیچ *DG* در شبکه برای حفاظت فیدر *F1* وجود ندارد. *IED1.1* با مشخصه «به‌شدت معکوس» و *IED1.3* با مشخصه «خیلی معکوس» تجهیز شده‌اند. حداقل جریان خطا بر فیدر *F1*، ۱۳۱٦ آمپر است؛ در حالی که *IED1.3* ماکزیمم جریان خطا ۱۸۳٤ را رؤیت می‌کند. با توجه به اینکه *IED1.1* پشتیبان *IED1.3* است، باید به‌طور صحیح در محدوده *[*۱۳۱٦-۱۸۳٤*]* آمپر عمل کند. شکل (٦) هماهنگی انجام‌شده میان این *IED*ها را نشان می‌دهد.



شکل (٦): طرح هماهنگی میان *IED1.1* و *IED1.3*

برای سناریو اول روی فیدر *F1*

در این وضعیت با روشی مشابه، *IED2.1* و *IED2.2* فیدر *F2* را به‌ترتیب با مشخصه‌های «به‌شدت معکوس» و «معکوس» حفاظت می‌کنند. در این فیدر انتظار می‌رود *IED2.1*، *IED2.2* را با توجه به محدوده جریان خطا *[*۱٦۹٤-۳۸۲۵*]* پشتیبانی کند. شکل (۷) هماهنگی انجام‌شده در این فیدر را نشان می‌دهد

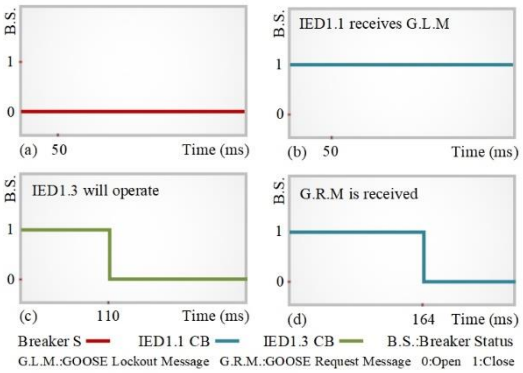


شکل (۷): طرح هماهنگی میان *IED2.1* و *IED2.2*

برای سناریو اول روی فیدر *F2*

هنگامی که *DG*ها تولید توان را آغاز می‌کنند، اندازه‌های جریان خطا و حتی جهت آن ممکن است در *F1* و *F2* تغییر کند. با وجود این، سیستم حفاظت باید به‌درستی برای سطوح نفوذ مختلف عمل کند؛ برای مثال، فرض کنید تنها *DG1* با تولید حداکثر توان خود به فیدر *F1* متصل شده باشد. با رخداد خطا بر بأس ۸، زمانی که توابع حفاظتی از *IED1.1* و *IED1.3* اضافه جریان را تشخیص دهند، تایمر داخلی آنها شروع می‌شود. با توجه به اینکه جریان‌های عبوری از *IED1.1* و *IED1.3* به‌ترتیب ۱۲۹۵ و ۲٦۹۰ آمپرند، عامل‌ها باید وضعیت هماهنگی خود را با این جریان‌ها بسنجند که متأسفانه *CTI* حاصل مناسب نیست؛ ازاین رو، *IED1.3* پیام «*GOOSE lockout*» را به *IED1.1* ارسال می‌کند. سپس *IED1.3* پس از اتمام تایمر خود (٦۰ میلی‌ثانیه)، عمل خواهد کرد. چنانچه خطا با موفقیت رفع شده باشد، وظیفه حیاتی انجام شده است. در

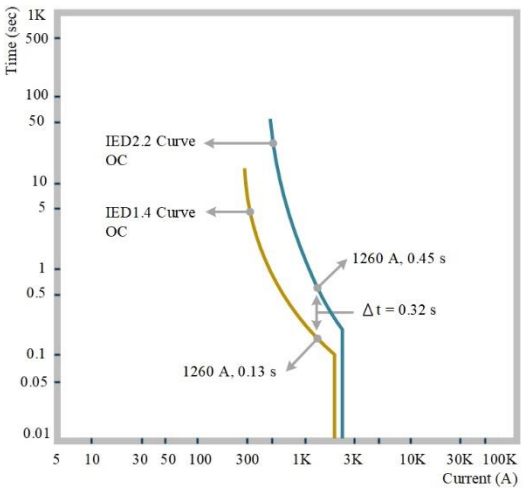
غیر این صورت پیام «*GOOSE Request*» را برای *IED1.1* ارسال می‌کند تا خطا را فوراً مانند یک رله آنی رفع کند. شکل (۸) زمان صرف‌شده برای این مرحله با توجه به زمان تریپ کلیدها را نشان می‌دهد.



شکل (۸): زمان قطع کلید باتوجه به رویه پیام *GOOSE* برای سناریو اول

٤-۲- سناریو دوم (*S* بسته است و فیدر *F2* از مدار خارج است)

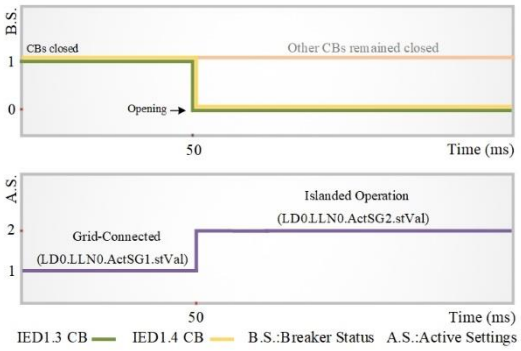
در این وضعیت *IED2.1* از سرویس خارج و حفاظت باید با سایر *IED*ها انجام شود. به این منظور، فرض وجود خطا بر بأس ۸ و حضور تنها *DG1* و *DG4* را با حداکثر توان در نظر بگیرید. پس از تشخیص اضافه جریان توسط توابع حفاظتی *IED*ها، عملگر *Str.general* آنها فعال، تایمر داخلی آنها شروع و حفاظت‌های اصلی و پشتیبان با عامل مشخص می‌شوند. شایان ذکر است با توجه به جریان‌های خطا، عملکرد *IED1.1* و *IED1.3* به‌طور مشابه با سناریو اول است. در این وضعیت *IED1.4* و *IED2.2* نیز به‌ترتیب با مشخصه‌های «بسیار معکوس» و «به‌شدت معکوس» با توجه به جریان خطای رؤیت‌شده (۱۲٦۰ آمپر) مطابق با شکل (۹) در یک وضعیت هماهنگ قرار دارند. بر این اساس، *IED1.4* پیام « *GOOSE lockout*» را برای عملگر *CTRL.XCBR.BlkOpn* از *IED2.2* به‌منظور جلوگیری از عملکرد پشتیبان آن ارسال می‌کند. سپس *IED1.4* با توجه به منحنی مشخصه، در زمان عملکرد خود (۱۳۰ میلی‌ثانیه) با فعال‌سازی عملگر *LD0.PDOC.Op.general* خود عمل می‌کند. در ادامه، چنانچه رفع خطا با موفقیت انجام نشده باشد، *IED1.4* با ارسال پیام «*GOOSE Reset*» به *IED2.2* آن را از حالت قفل خارج می‌کند. به این ترتیب، *IED2.2* با توجه به منحنی مشخصه پس از سپری‌شدن تأخیر ٤٥۰ میلی‌ثانیه، خطا را پاکسازی خواهد کرد.



شکل (۹): طرح هماهنگی میان *IED1.4* و *IED2.2* برای سناریو دوم روی فیدر *F1*

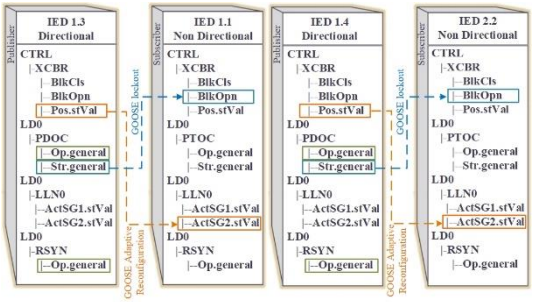
پس از عملکرد حفاظت‌های اصلی و جداسازی ناحیه خطادیده، شبکه به دو قسمت تقسیم می‌شود که بخش بالایی آن متصل به شبکه اصلی باقی می‌ماند و بخش پایین، در مد جزیره‌ای به عملکرد خود ادامه خواهد داد. به این ترتیب، با توجه به گروه تنظیمات از پیش تعریف شده برای *IED*ها، می‌توان تنظیمات آنها را برای ساختار جدید سیستم به‌روزرسانی کرد؛ به‌طور مثال، در این مورد خطا، *ActSG1* تنظیمات در حالت عملکرد شبکه متصل می‌شود و *ActSG2* تنظیمات پس از رفع این مورد، خطا را برای *IED*ها بیان می‌کند.

بر این اساس، در ابتدا تمام *IED*ها در تنظیمات گروه یک، *ActSG1* قرار دارند. به دنبال رخداد بر بأس ۸، مطابق با شکل (۱۰) زمانی که کلیدهای *IED1.3* و *IED1.4* باز می‌شوند، عملگر *CTRL.XCBR.Pos.stVal* از این *IED*ها فعال و پیام «*GOOSE Adaptive Reconfiguration*» را برای سایر *IED*ها منتشر می‌کنند تا تنظیمات فعال آنها را از *LD0.LLN0.ActSG1.stVal*به *LD0.LLN0.ActSG2.stVal* جایگزین کنند.



شکل (۱۰): وضعیت کلیدها و تنظیمات فعال دستگاهها

با توجه به الگوریتم حفاظتی بیان‌شده و عملگرهای فعال‌شده از *IED*ها در این نقطه خطا، شکل (۱۱) الگوی فرستنده/گیرنده و ارتباطات نقطه به نقطه میان *IED*ها را نشان می‌دهد.



شکل (۱۱): پیام‌های *GOOSE* ارسالی و دریافتی میان *IED*ها برای سناریو دوم، خطا بر بأس ۸

ناحیه خطادیده پس از رفع خطا، یکبار دیگر می‌تواند به شبکه اصلی متصل شود. این عمل توسط گره منطقی (*RSYN*)[۱۸] از *IED*ها اجراشدنی است. این گره منطقی، اختلاف ولتاژ، زاویه فاز و فرکانس قسمت جداشده را با شبکه اصلی بررسی می‌کند. بر این اساس، بستن کلید در صورتی مجاز است که این پارامترها در حدود تعیین‌شده باشند. به این ترتیب، با فعال‌شدن عملگر *LD0.RSYN.Op.general* از *IED*ها اتصال مجدد انجام می‌شود.

درخور ذکر است ساختار سیستم حفاظت به‌گونه‌ای طراحی شده است که مکان دقیق برخی نقاط خطا قابل شناسایی است. این قابلیت با توجه به جهت *IED*ها در رؤیت‌شدن یا نشدن خطا امکان‌پذیر است؛ به‌طور مثال، چنانچه *IED1.1* و *IED1.4* اضافه جریان خطا را رؤیت کند، در حالی که دو *IED1.2* و *IED1.3* هیچ اضافه جریانی را مشاهده نکنند، مکان دقیق خطا بأس ٤ شبکه شناسایی می‌شود. همچنین، در صورتی که *IED1.3* جریان خطا را رؤیت کند، در حالی که دو *IED1.4* و *IED3.2* هیچ اضافه جریانی را تشخیص ندهند، نقطه خطا دقیقاً روی بأس ۱۱ شبکه مکان‌یابی می‌شود.

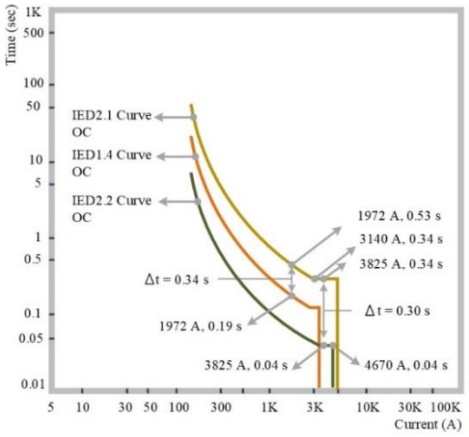
٤-۳- سناریو سوم (*S* بسته است و فیدر *F1* از مدار خارج است)

در این سناریو، کل حفاظت به تمام *IED*ها به‌جز *IED1.1* واگذار شده است. بر این اساس، *IED2.1* باید به‌طور صحیح هر دو *IED2.2* و *IED1.4* را برای داشتن یک هماهنگی مناسب روی هر دو فیدر پشتیبانی کند. در مقایسه با سناریو اول، *IED2.1* و *IED1.3* ناحیه‌های حفاظتی مختلفی دارند. بر این اساس، باید گروه تنظیمات مناسبی با توجه به این ساختار برای *IED*ها در نظر گرفته شود. این گروه تنظیمات می‌توانند علاوه بر اینکه از پیش تعریف شده باشند، از گروه تنظیمات سناریو اول گرفته شوند. به این منظور که عامل‌ها با در اختیار داشتن گروه تنظیمات سناریو اول، می‌توانند آنها را با توجه به شرایط موجود، اصلاح و استفاده کنند؛ البته در صورت ناکارایی تنظیمات و نبود هماهنگی، روش پیشنهادی همان‌طور که در سناریوی اول ذکر شد، باید استفاده شود. به این ترتیب، در این سناریو، ابتدا هماهنگی با اصلاح زمان عملکرد ازطریق تنظیمات، امتحان و سپس در صورت عدم موفقیت، الگوریتم پیشنهادی اجرا می‌شود.

ابتدا فرض می‌شود هیچ واحد *DG* در شبکه وجود ندارد. با توجه به اینکه حداکثر جریان خطا *IED2.2* برابر ۳۸۲۵ آمپر است، تنظیم قبلی *IED2.1* که در *[۱۶۹٤-۳۸۲۵]* تنظیم شده بود، مناسب برای پشتیبانی *IED2.2* نیست. همچنین، با توجه به اینکه *IED2.1* باید با *IED1.4* نیز هماهنگ شود، تنظیم جدید *IED2.1* باید پاسخگوی نیازهای هر دو ناحیه ٦ و ۳ باشد.

در چنین شرایطی متأسفانه با اصلاح *TMS* و I_{pickup} (رابطه۱) مشکل نبود هماهنگی به‌تنهایی حل نمی‌شود؛ یعنی

علاوه بر این پارامترها نوع منحنی مشخصه نیز باید تطبیق داده شود. بر این اساس، برای *IED2.2* منحنی مشخصه به «خیلی معکوس» تغییر یافته است؛ حال آنکه تنظیمات جدید برای *TMS* و I_{pickup} به‌ترتیب ۰/۰۵ ثانیه و ۱۶۳/۵ آمپر است. *IED1.4* نیز به‌طور مشابه یک مشخصه «بسیار معکوس» با ۰/۱۷ ثانیه و ۱۶۰ آمپر به‌ترتیب برای *TMS* و I_{pickup} دارد. با توجه به اینکه انتظار می‌رود *IED2.1*، هر دو *IED2.2* و *IED1.4* را پشتیبانی کند، باید در ۰/۰۵ ثانیه ۱۶۲/۵ آمپر و نیز یک منحنی مشخصه «طولانی معکوس» تنظیم شود. شکل (۱۲) هماهنگی میان این رله‌ها را برای مقادیر به‌روزشده در حداقل و حداکثر جریان خطا نشان می‌دهد.



شکل (۱۲) هماهنگی میان *IED2.1*، *IED2.2* و *IED1.4* برای سناریو سوم

با توجه به اینکه اصلاح تنظیمات توسط عامل، در شرایط نفوذ صفر انجام گرفته است، باید در برابر حداکثر نفوذ ارزیابی شود تا دریابیم آیا استفاده از گروه تنظیمات از پیش تعریف شده نیاز است یا خیر. به همین منظور، ابتدا فرض کنید *DG2* و *DG3* به شبکه متصل شده‌اند و به‌طور ناگهانی یک خطا در منطقه محافظت‌شده توسط *IED2.2* رخ داده است. در این شرایط، جریان عبوری از *IED2.2*، ۴۶۷۰ آمپر است؛ در حالی که *IED2.1*، ۳۱۴۰ آمپر را احساس می‌کند. به هر حال، با توجه به شکل (۱۲)، این میزان تغییر میان *IED* اصلی و پشتیبان هیچ ناهماهنگی ایجاد نمی‌کند.

به‌منظور بررسی دقیق‌تر سیستم حفاظت، *IED3.1* و *IED3.2* به‌ترتیب مسئول ناحیه‌های دوم و چهارم هستند. این *IED*ها به‌عنوان دستگاههای حفاظتی فیدر بار انتخاب شده‌اند و در لحظه خطا عملکرد مشابهی را خواهند داشت. بر این اساس، به‌محض تشخیص اضافه‌جریان در پایین‌دست خود، پیام «*GOOSE lockout*» را برای سایر*IED*ها منتشر می‌کنند و بعد از یک تأخیر بسیار کوتاه ثابت (۲۰ میلی‌ثانیه)، جداسازی را انجام می‌دهند. در این حالت، تغییر تنظیمات ضروری نیست و شبکه می‌تواند بدون هیچ بازپیکربندی به عملکرد خود ادامه دهد.

شایان ذکر است طرح‌های خودترمیمی در سیستم‌های توزیع، مکان‌یابی خطا، جداسازی و بازگردانی سرویس شناخته می‌شوند. همان‌طور که در سناریوهای مختلف نشان داده شد طرح پیشنهادی این مقاله نیز با ارائه یک عملکرد خودترمیمی هوشمند، وظایف حیاتی سیستم حفاظت را به‌درستی به نمایش می‌گذارد. به‌منظور بیان جزئیات بیشتر، ساختار سیستم حفاظت پیشنهادی به گونه‌ای طراحی شده است که در مقایسه با مرجع *[۲۵]*، علاوه بر نبود وابستگی به واحد کنترل مرکزی، مکان دقیق برخی نقاط خطا نیز قابل شناسایی است. این قابلیت با توجه به جهت *IED*ها در رؤیت‌داشتن یا نداشتن خطا امکان‌پذیر است؛ به‌طور مثال، چنانچه *IED1.1* و *IED1.4* اضافه‌جریان خطا را رؤیت کنند، در حالی که دو *IED1.2* و *IED1.3* هیچ اضافه‌جریانی را مشاهده نکنند، مکان دقیق خطا بأس ٤ شبکه شناسایی می‌شود. همچنین، در صورتی که *IED1.3* جریان خطا را رؤیت کند، در حالی که دو *IED1.4* و *IED3.2* هیچ اضافه‌جریانی را تشخیص ندهند، نقطه خطا دقیقاً روی بأس ۱۱ شبکه مکان‌یابی می‌شود. به این ترتیب، مطابق با منحنی مشخصه *IED*ها در سناریوهای مختلف، فرآیندهای حفاظتی با توابع حفاظتی و گرههای منطقی مربوطه در یک ساختار غیرمتمرکز مبتنی بر عامل به‌خوبی اجراشدنی است.

۵- نتیجه‌گیری

عدم قطعیت *DG*های تجدیدپذیر در شبکه‌های توزیع، باعث می‌شود ساختار *MAS* پس از هر تغییر سطح نفوذ، نسبت به آنها با تصحیح یا حداقل بررسی گروه تنظیمات

کنونی واکنش نشان دهد؛ درنتیجه، این ارتباطات بی‌شمار، احتمال خرابی یا تأخیر در برقراری ارتباطات را به دنبال دارند که بر وظایف حیاتی سیستم حفاظتی در رفع خطا و حفظ هماهنگی تأثیر می‌گذارند. بر این اساس، این مقاله یک ساختار غیرمتمرکز حفاظتی هوشمند را برای حل چنین مشکلی ارائه می‌دهد که سیستم حفاظت مبتنی بر *MAS* با آن روبه‌رو است؛ از این رو، ابتدا با بازبینی ساختار کنترل و ارتباطات *MAS* معمول، دقیقاً بیان می‌شود چطور *MAS* ممکن است در حفاظت از سیستم ناتوان باشد. سپس با توجه به ویژگی‌های یک راه‌حل مناسب، الگوریتمی برای حل مسئله با استفاده از حداقل تعداد عامل (*IED*ها) و قابلیت‌های استاندارد *IEC-61850* در یک تک‌سطح کنترل به‌منظور کاهش حجم ارتباطات پیشنهاد می‌شود. همچنین، به‌منظور تجهیز سیستم به یک الگوریتم مستقل از نفوذ *DG*، یک الگوریتم کمکی با استفاده از سرویس‌های پیام *GOOSE* ارائه شده است تا سیستم را در برابر هر رویداد پیش‌بینی‌ناپذیر، با کمترین تأخیر ممکن محافظت کند. با توجه به اهمیت رفع خطا و احتمال تأخیر ارتباطات در شبکه‌های توزیع با حضور تجدیدپذیرها، چنین الگوریتم کمکی سرعت بالا و کارآمدی، توانایی پوشش موفقیت‌آمیز هر سطح نفوذی را همراه با افزایش قابلیت اطمینان سیستم دارا است.

مراجع

[1] M. Meskin, A. Domijan and I. Grinberg, "Impact of distributed generation on the protection systems of distribution networks:analysis and remedies", *IET Generation, Transmission & Distribution*, Vol. 14, No. 24, pp. 5944-5960, Nov. 2020.

[2] K. A. Wheeler, M. Elsamahy and S. O. Faried, "A Novel Reclosing Scheme for Mitigation of Distributed Generation Effects on Overcurrent Protection", *IEEE Transactions on Power Delivery*, Vol. 33, No. 2, pp. 981-991, April 2018.

[3] S. R. Kafimousavi, B. Fani, and I. Sadeghkhani, "Optimal Determination of Photovoltaic Penetration Level Considering protection coordination", *IEEE Systems Journal*, Vol. 16, No. 2, pp. 2121-2124, June. 2022.

[4] S. P. S. Matos, M. C. Vargas, L. G. V. Fracalossi, L. F. Encarnacao and O. E. Batista, "Protection philosophy for distribution grids with high penetration of distributed generation", *Electric Power Systems Research*, Vol. 196, No. 4, July. 2021.

[5] S. Katyara, L. Staszewski, Z. Leonowicz, "protection coordination of Properly Sized and Placed Distributed Generations-Methods, Applications and Future Scope", *Energies*, Vol. 11, No. 10, pp. 1-22, Oct. 2018.

[6] N. bayati, F. Aghaee, and S. H. H. Sadeghi, "The Adaptive and Robust Power System Protection Schemes in the Presence of DGs", *International Journal of Renewable Energy Research*, Vol. 9, No. 2, June 2019.

[7] P. Singh and A. k. Pradhan, "A Local measurement based protection technique for distribution system with photovoltaic plans", *IET Renewable Power Generation*, Vol. 14, No. 6, pp. 996-1003, April 2020.

[8] J. Kim, S. M. Baek, and J. W. Park, "Allowable Capacity Estimation of DGs for High Renewable Penetration to Distribution System", *IEEE Industry Applications Society Annual Meeting (IAS)*, pp. 1-8, Sept. 2018.

[9] T. E. Sati and M. A. Azzouz, "An adaptive virtual impedance fault current limiter for optimal protection coordination of islanded microgrids", *IET Renewable Power Generation*, Vol. 16, No. 8, pp. 1719-1732, April. 2022.

[10] A. Heidary, H. Radmanesh, S. H. Naghibi and S. Samandarpour, "Distribution System Protection by Coordinated Fault Current Limiters", *IET Energy Systems Integration*, Vol. 2, No. 3, pp. 59-65, March. 2020.

[11] C. Prapanukool, and S. Chaitusaney, "An appropriate disconnecting time of distributed generation by optimal protection setting and transformer connection type", IEEE International Conferenceon Electrical Engineering/Electronics, Computer, *Telecommunications and Information Technology (ECTI-CON)*; pp. 1–4, May 2012.

[12] M. H. Sadeghi, A. Dastfan and Y. Damchi, "Optimal distributed generation penetration considering relay coordination and power quality requirements", *IET Generation, Transmission & Distribution*, Vol. 16, No. 2, pp. 2466-2475, April. 2022.

[13] A. Tjahjono, D. O. Anggriawan, A.K. Faizin, and A. Priyadi, "Adaptive modified firefly algorithm for optimal coordination of overcurrent relays", *IET Generation, Transmission & Distribution*, Vol. 11, pp. 2575-2585, July 2017.

[14] R. Azami, S. Esmaeilbeigi, M. Valizadeh and M. S. Javadi, "Novel intelligent multi-agent system for hybrid adaptive protection of microgrid", *Sustainable Energy Grids and Networks*, Vol. 30, No. 12, March. 2022.

[15] M. A. Ataei, M. Gitizadeh, M. Lehtonen and R. Razavi-far, "Multi-agent based protection scheme using current-only directional overcurrent relays for looped/meshed distribution systems", *IET Generation, Transmission & Distribution*, Vol. 16, No. 6, pp. 1567-1581, April. 2022.

[16] B. Fani, F. Hajimohammadi, M. Moazzami, and M. J. Morshed, "An adaptive current limiting strategy to prevent fuse-recloser miscoordination in PV-dominated distribution feeders", *Electric Power Systems Research*, Vol. 157, pp. 177-186,

"Modeling of a Centralized Microgrid Protection System and Distributed Energy Resources According to IEC 61850-7-420", *IEEE Transactions on Power Systems*, Vol. 27, No. 3, pp. 1560-1567, Aug. 2012.

[29] M. Hojjaty, B. Fani and I. Sadeghkhani, "Intelligent protection coordination restoration for active distribution networks", *IET Generation, Transmission & Distribution*, Vol. 16, No. 3, pp. 397-413, June. 2022.

[30] H. Bishe and B. Fani, "Local Penetration-Free Control Approach Against Numerous Changes in PV Generation Level in MAS-Based Protection Schemes", *IET Renewable Power Generation*, Vol. 13, No. 7, pp. 1197-1204, May 2019.

[31] E. Abbaspour, B. Fani, I. Sadeghkhani and H. H. Alhelou, "Multi-Agent System-Based Hierarchical Protection Scheme for Distribution Networks with High Penetration of Electronically-Coupled DG", *IEEE Access*, Vol. 9, pp. 102998-103018, July 2021.

[32] G. Zhabelova and V. Vyatkin, "Multiagent Smart Grid Automation Architecture Based on IEC 61850/61499 Intelligent Logical Nodes," *IEEE Transactions on Industrial Electronics*, Vol. 59, No. 5, pp. 2351-2362, May 2012.

[33] N. fawzy, H. Habib and O. A. Mohammad, "IEC 61850-Based Communication Networks of Distribution System against Cyber and Physical Failures", *World Electric Vehicle Journal*, Vol. 12, No. 3, Sept. 2021.

[34] M. H. Cintuglu, T. Ma and O.A. Mohammed, "Protection of autonomous microgrids using agent-based distributed communication", *IEEE Transactions on Power Delivery*, Vol. 32, No. 1, pp. 351-360, Feb. 2017.

[35] C. Zhang, M. Liu, Y. Gao and Y. li, "Modeling and fault diagnosis of distribution networks cyber physical system based on IEC61850", *Sustainable Energy Technologies and assessments*, Vol. 53, No. 6, Oct. 2022.

[36] A. A. d. Sotomayor, D. D. Giustina, G.Massa, A.Dedè, F. Ramos, and A. Barbato, "IEC 61850-based adaptive protection system for the MV distribution smart grid", *Sustainable Energy, Grids and Networks*, Vol. 15, pp. 26-33, Sept. 2018.

[37] G. Han, B. Xu, K. Fan and G. Lv, "An open communication architecture for distribution automation based on IEC 61850", *International Journal of Electrical Power & Energy Systems*, Vol. 54, pp. 315-324, Jan. 2014.

[38] Communication networks and systems for power utility automation–Part7–4: Basic communication structure – Compatible logical node classes and data object classes, *IEC61850, Int. Electrotech. Committee*, 2010.

[39] W. Ling, D. Liu, Y. Lu, P. Du and F. Pan, "IEC 61850 Model Expansion Toward Distributed Fault Localization, Isolation, and Supply Restoration", *IEEE Transactions on Power Delivery*, Vol. 29, No. 3, pp. 977-984, June 2014.

[40] S. Wang, F. Yang, X. Yan and T. Liu, "Analysis of GOOSE message and the engineering application for GOOSE message in the intelligent

April 2018.

[17] E. Abbaspour, B. Fani and A. Karami-Horestani, "Adaptive scheme protecting renewable dominated micro-grids against usual topology-change events", *IET Renewable Power Generation*, Vol. 15, No. 12, pp. 2686-2698, May. 2021.

[18] M. Y. Shih, A. Conde, Z. Leonowicz, and L. Martirano, "An Adaptive Overcurrent Coordination Scheme to Improve Relay Sensitivity and Overcome Drawbacks due to Distributed Generation in Smart Grids", *IEEE Transactions on Industry Applications*, Vol. 53, No. 6, pp.5217-5228, Dec. 2017.

[19] H. Bisheh, B. Fani, G. Shahgholian, I. Sadeghkhani and J. M. Guerrero, "An adaptive fuse-saving protection scheme for active distribution networks", *International Journal of Electrical Power & Energy Systems*, Vol. 14, Jan. 2023.

[20] M. S. Rahman, M. A. Mahmud, A. M. T. Oo and H. R. Pota, "Multi-Agent Approach for Enhancing Security of Protection Schemes in Cyber-Physical Energy Systems", *IEEE Transactions on Industrial Informatics*, Vol. 13, No. 3, pp. 436-447, April 2017.

[21] A. Al-Hinai and H. H. Alhelou, "A multi-agent system for distribution network restoration in future smart grids", *Energy Reports*, Vol. 7, pp. 8083-8090, Nov. 2021.

[22] H. F. Habib, T. Youssef, M. H. Cintuglu and O. A. Mohammed, "Multi-Agent-Based Technique for Fault Location, Isolation, and Service Restoration", *IEEE Transactions on Industry Applications*, Vol. 53, No. 3, pp. 1841-1851, May 2017.

[23] M. A. Ataei and M. Gitizadeh, "A distributed adaptive protection scheme based on multi-agent system for distribution networksin the presence of distributed generation", *IET Generation, Transmission & Distribution*, Vol. 16, No. 8, pp. 1521-1540, Nov. 2021.

[24] F. C. Sampaio, R. P. S. Leao, R. F. Sampaio, L. S. Melo and G. C. Barros, "A multi-agent-based integrated self-healing and adaptive protection system for power distribution systems with distributed generation", *Electric Power Systems Research*, Vol. 188, Nov. 2020.

[25] 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", *IEEE Transactions on Power Delivery*, Vol. 32, No. 1, pp. 536-545, Feb. 2017.

[26] F. B. Dos Reis, C. P. Pinto, F. S. Dos Reis, D. Issicaba and J. G. Rolim, "Multi-agent dual strategy based adaptive protection for microgrids", Sustainable Energy, *Grids and Networks*, Vol. 27, No. 6, Sept. 2021.

[27] H. Laaksonen, D. Ishchenko and A. Oudalov, "Adaptive Protection and Microgrid Control Design for Hailuoto Island", *IEEE Transactions on Smart Grid*, Vol. 5, No. 3, May. 2014.

[28] T. S. Ustun, C. Ozansoy and A. Zayegh,

substation", *The Journal of Engineering*, Vol. 2020, No. 6, pp. 207-212, June. 2020.

[41] R. Feizimirkhani, A. I. Bratcu and Y. Besanger, "Time-series Modeling of IEC 61850 GOOSE Communication Traffic between IEDs in Smart grids-a parametric analysis", *IFAC-PapersOnline*, Vol. 51, No. 28, pp. 444-449, Dec. 2018.

[42] S. D. Saldarriaga-Zuluaga, J. M. Lopez-Lezama and N. Munoz-Galeano, "Optimal coordination of over-current relays in microgrids considering multiple characteristic curves", *Alexandria Engineering Journal*, Vol. 60, No. 2, pp. 2093-2113, April 2021.

---

[1] Distributed Generation
[2] Distributed Network
[3] Fault Current Limiter
[4] Adaptive Protection Scheme
[5] Multi-Agent System
[6] Intelligent Electronic Device
[7] Relay Agent
[8] Breaker Agent
[9] International Electrotechnical Commission
[10] Physical Device
[11] Logical Node
[12] Data Object
[13] Protection Time Over Current
[14] Logical Device
[15] Data Attribute
[16] Generic Object Oriented Substation Event
[17] Coordination Time Interval
[18] Synchronism Check