TEEGES

# Technovations of Electrical Engineering in Green Energy System

Research Article (2023) 2(3):54-75

## Decentralized Agent-Based Protection Coordination for Distribution Networks with Renewable Distributed Generations using Intelligent Electronic Devices

Majid Rostamnia[1,2], *M.Sc*, Mohammad Sadegh Rostamnia[1,2], *M.Sc*, Ehsan Heydarian-Forushani[3], *Assistant Professor*, Seyed Fariborz Zarei[3], *Assistant Professor*, Seyed Hossein Hosseinian[4], *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 & Computer Engineering, Qom University of Technology, Qom, Iran*
[4] *Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran.*

## Abstract:

By increasing the penetration level of renewable distributed generations and increasing the size of the distribution networks, the more number of agent-based protection systems with its communication infrastruture will be used. Such systems play a vital role in the protection system to detect the faults and maintain the protection coordination. Despite the fast and reliable nature of multi-agent systems, there is a possibility of poor performance especially in protection coordination schemes with heavy communication load. For this purpose, this paper presents an intelligent self-healing method under fault conditions, which provides the protection coordination in a single control level without dependence on a higher communication level. The decentralized performance of the proposed scheme is expressed by using intelligent electronic devices and distributed communication. Accordingly, the coordination is done using the high-speed point-to-point communication capability of the IEC-61850 GOOSE protocol. Also, to avoid power outages due to the protection system malfunction, an algorithm independent of DG peneration and based on GOOSE message service mechanism is proposed, which does not need a central processor. Finally, the performance of the proposed algorithm is evaluated under different scenarios in a practical distribution network using ETAP software environment.

**Keywords:** Protection coordination, Multi-agent system, Intelligent electronic device, Distributed generation, IEC-61850.

**Received:** 30 March 2023
**Revised:** 17 May 2023
**Accepted:** 21 June 2023
**Corresponding Author:** Ehsan Heydarian-Forushani, heydarian@qut.ac.ir
DOI: 10.30486/TEEGES.2023.1986361.1072

فناوری‌های نوین در مهندسی برق و سیستم انرژی سبز

TEEGES

مقاله پژوهشی

# هماهنگی حفاظت غیرمتمرکز مبتنی بر عامل برای شبکه‌های توزیع در حضور منابع تولید پراکنده تجدیدپذیر با استفاده از دستگاه‌های الکترونیکی هوشمند

مجید رستم‌نیا[۱،۲]، *کارشناسی ارشد*، محمدصادق رستم‌نیا[۱،۲]، *کارشناسی ارشد*، احسان حیدریان فروشانی[۳]، *استادیار*، سید فریبرز زارعی[۳]، *استادیار*، سید حسین حسینیان[۴]، *استاد*

*۱- دانشکده مهندسی برق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران*

*۲- مرکز تحقیقات ریزشبکه‌های هوشمند، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران*

*۳- دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی قم، قم، ایران*

*۴- دانشکده مهندسی برق، دانشگاه صنعتی امیرکبیر، تهران، ایران*

**چکیده:** با افزایش روز افزون منابع تولید پراکنده تجدیدپذیر در شبکه‌های توزیع و نیز افزایش وسعت شبکه، تعداد ارتباطات مبتنی بر عامل در سیستم‌های حفاظت بطور چشمگیری افزایش خواهند یافت؛ که نقش حیاتی در سیستم حفاظتی به منظور تشخیص خطا و حفظ هماهنگی خواهند داشت. علیرغم ماهیت سریع و مطمئن سیستم‌های چندعاملی، احتمال عملکرد نامناسب به خصوص در طرح‌های هماهنگی حفاظتی متمرکز به دلیل وجود یک بار ارتباطی سنگین وجود دارد. به همین منظور این مقاله یک روش خود ترمیمی هوشمند را در شرایط خطا ارائه می‌دهد، که هماهنگی حفاظتی را در یک تک سطح کنترل و بدون وابستگی به سطوح مخابراتی بالاتر انجام می‌دهد. عملکرد غیرمتمرکز طرح پیشنهادی با استفاده از دستگاه‌های الکترونیکی هوشمند و مخابرات توزیع‌شده بیان می‌شود. بر این اساس، حفظ هماهنگی در این ساختار با استفاده از قابلیت ارتباط نقطه به نقطه سرعت بالا از پروتکل IEC-61850 GOOSE انجام خواهد شد. همچنین، به منظور جلوگیری از هرگونه قطع برق ناشی از تنظیمات حفاظتی نامناسب، یک الگوریتم مستقل از نفوذ DG، بدون کمک پردازشگر مرکزی و با استفاده از سرویس‌های پیام GOOSE ارائه شده است. در نهایت، صحت عملکرد الگوریتم پیشنهادی با طرح سناریوهای مختلف و شبیه‌سازی یک شبکه توزیع عملی توسط نرم افزار ETAP ارزیابی می‌شود.

**واژه‌های کلیدی:** هماهنگی حفاظتی، سیستم چند عاملی، دستگاه الکترونیکی هوشمند، تولید پراکنده، IEC-61850.

**تاریخ ارسال مقاله:** ۱۴۰۲/۰۱/۱۰

**تاریخ بازنگری مقاله:** ۱۴۰۲/۲/۲۷

**تاریخ پذیرش مقاله:** ۱۴۰۲/۳/۳۱

**نویسنده‌ی مسئول:** احسان حیدریان فروشانی، heydarian@qut.ac.ir

DOI: 10.30486/TEEGES.2023.1986361.1072

## ۱- مقدمه

حضور منابع تولید پراکنده [۱](DG) در شبکه توزیع [۲](DN)، علی‌رغم مزایای مسلم آن‌ها، چالش‌های جدیدی را پیرامون سیستم حفاظتی شبکه به همراه خواهند داشت. از مهم‌ترین این چالش‌ها می‌توان به ناتوانی در تشخیص خطا، از دست رفتن هماهنگی میان دستگاه‌های حفاظتی و عملکرد اشتباه سیستم حفاظتی اشاره نمود [۱,۲]. این چالش‌ها عمدتاً به دلیل تغییر سطح جریان‌های اتصال‌کوتاه و همچنین تغییر جهت جریان‌ها در انشعابات شبکه می‌باشند [۳,۴]. اخیراً تحقیقات گسترده‌ای به‌منظور کاهش تاثیرات عدم قطعیت DGها بر سیستم حفاظتی انجام گرفته و روش‌های مختلفی پیشنهاد شده است. از جمله این روش‌ها می‌توان به استفاده از محدودکننده‌های جریان خطا [۳](FCL) [۵-۷]، محدود کردن درصد نفوذ DGها [۸-۱۰]، خروج سریع DGها در لحظه خطا [۱۱-۱۳]، استفاده از طرح‌های حفاظت تطبیقی [۴](APS) [۱۴-۱۷] و اصلاح سیستم حفاظتی [۱۸-۲۰] اشاره نمود.

روش‌های بیان شده مشکلات حفاظتی را به‌طور مؤثری کاهش می‌دهند اما شامل اشکالاتی نیز هستند. از جمله این اشکالات می‌توان به عدم تعادل در تولید و مصرف، اختلال در فرکانس و نااپایداری ولتاژ، احتمال آسیب به واحدهای DG و کاهش مزایای آن‌ها در عملکرد عادی شبکه، پیچیدگی طرح حفاظت با افزایش منابع تجدیدپذیر، نیاز به زیرساخت‌های مخابراتی و عدم توجیه‌پذیری از لحاظ اقتصادی اشاره نمود. وجود چنین اشکالاتی با توجه به پیشرفت‌های قابل توجه در تکنولوژی، تاثیرات مهمی بر جهت‌گیری تحقیقات علمی در حل مسائل فوق دارند. 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 فناوری هوشمند، به‌منظور حفاظت از DNها در حضور DGهای مختلف و سایر مشکلات احتمالی به شدت مورد توجه قرار گرفته است [۲۱-۲۳].

در بیشتر طرح‌های حفاظت مبتنی بر MAS، عامل‌های مختلفی مانند DGها، دستگاه‌های حفاظتی، بارها، کلیدها وغیره می‌توانند در طرح‌های حفاظتی شرکت نمایند [۲۴-۲۶]. به این ترتیب چنانچه رویدادی در شبکه رخ دهد، عامل‌ها پس از شناسایی تغییرات و جمع‌آوری اطلاعات، داده‌ها را به پردازشگر مرکزی منتقل می‌کنند. پس از پردازش اطلاعات توسط واحد مرکزی، تصمیم مناسب با توجه به شرایط جدید به لایه‌های زیرین فرستاده خواهد شد [۲۷,۲۸]. بر اساس این روش، اقدامات و تغییرات لازم توسط عامل‌های مربوطه انجام می‌گیرد. این روش‌ها چهار اشکال مهم را مخصوصاً با اتصال DGهای تجدیدپذیر به شبکه‌های کاربردی بزرگ‌تر به‌دنبال دارند که عبارت‌اند از:

- حجم سنگین اطلاعات بر شبکه ارتباطی: در این نوع طرح‌ها از شبکه ارتباطی به سمت بالا و پایین به‌ترتیب برای اطلاعات جمع‌آوری شده توسط عامل‌ها و ارسال دستورات مناسب به عامل‌های مربوطه استفاده می‌شود. از اینرو افزایش روز افزون اندازه سیستم و عدم قطعیت DGهای تجدیدپذیر باعث می‌شود که بار سنگین اطلاعات بر سیستم ارتباطی مشکل‌ساز شود.
- زمان‌بر بودن پردازش و انتقال اطلاعات میان سطوح مختلف: با رخداد خطا در شبکه، اطلاعات باید جمع‌آوری، ارزیابی و پردازش شده تا دستورات مناسب به عامل‌های اجرایی فرستاده شود. این فرآیندهای پردازشی و ارتباطی زمان‌بر بوده و منجر به افزایش احتمال ناکارایی این روش‌ها می‌شوند.
- وابستگی زیاد به یک کنترل‌کننده مرکزی قدرتمند: به دلیل افزایش تعداد عامل‌ها و منابع تولید تجدیدپذیر در سیستم‌های عملی بزرگ، وظایف واحد مرکزی در صورت افزایش تعداد رویدادهای شبکه، به‌طور قابل توجهی افزایش پیدا می‌کند. بر این اساس افزایش فشار، افزایش خطر خرابی کنترل‌کننده مرکزی را به‌دنبال داشته که باعث نقص در طرح حفاظت کلی خواهد شد.
- ضرورت استفاده از رله جایگزین به دلیل به روز رسانی طولانی مدت تنظیمات رله: پس از یک رویداد شبکه، پردازشگر مرکزی تنظیمات جدید را برای رله‌های مربوطه بارگذاری می‌کند که معمولاً این فرآیند برای رله‌ها چند ثانیه زمان می‌برد. علی‌رغم احتمال کم آن، چنانچه خطای غیرمنتظره‌ای طی فرآیند به روز رسانی روی دهد، یک رله جایگزین باید برای مقابله با رویداد احتمالی در نظر گرفته شود [۲۸]. با توجه به این‌که عدم قطعیت DGهای تجدیدپذیر تعداد رویدادهای سیستم را به طور قابل توجهی افزایش می‌دهند، احتمال رویداد خطا طی فرآیند به‌روز رسانی رله افزایش می‌یابد و طراحان مجبور به بهره‌برداری از رله جایگزین می‌شوند.

مشکلات مذکور عملکرد سیستم حفاظت را به‌طور مستقیم مورد تهدید قرار داده و کاهش قابلیت اطمینان سیستم را به‌دنبال دارند. از اینرو، این مقاله یک روش هماهنگی سیستم حفاظت DN را با بهره‌گیری از دستگاه‌های الکترونیکی هوشمند[۶](IED) و مخابرات توزیع‌شده به‌منظور غلبه بر مشکلات ساختارهای متمرکز سیستم‌های حفاظتی بیان می‌کند. در این طرح، یک ساختار غیرمتمرکز به‌منظور جایگزین MAS معمول در شرایط خطا ارائه شده است که ابتدا خطا را به سرعت پاکسازی و هماهنگی را حفظ می‌نماید. سپس با توجه به ساختار جدید و گروه تنظیمات از پیش تعریف شده، تنظیمات IEDها را به روز رسانی می‌کند. به عبارت دیگر در این ساختار وظایف هماهنگی حفاظتی، بدون کمک‌های پردازشگر مرکزی انجام می‌گیرد. همچنین در این روش وظایف اساسی سیستم حفاظت بدون نیاز به انجام فرآیندهای زمان‌بر یا استفاده از رله‌های جایگزین پیشنهاد می‌شود. از جمله ویژگی‌های برجسته طرح ارائه شده می‌توان به عملکرد خود ترمیمی سیستم حفاظت با یک روش غیرمتمرکز هوشمند در یک تک سطح کنترل که منجر به کاهش بار ارتباطی می‌شود اشاره نمود. علاوه بر آن، با توجه به عدم قطعیت DGهای تجدیدپذیر، یک الگوریتم کمکی عملکرد مستقل از نفوذ سیستم را به نمایش می‌گذارد.

در ادامه مقاله، ساختار کلی سیستم حفاظت مبتنی بر MAS در بخش (۲) مرور و احتمال شکست یا تاخیر در عملکرد سیستم، به علت افزایش تعداد ارتباطات در این ساختار شرح داده می‌شود. سپس ویژگی‌های یک راه حل مناسب بیان می‌شود که به عنوان پایه‌های اساسی الگوریتم حفاظت پیشنهادی در بخش (۳) مورد استفاده قرار خواهد گرفت. بخش (۴) طرح پیشنهادی را با کمک شبیه‌سازی یک سیستم عملی در نرم‌افزار ETAP ارزیابی و تایید می‌کند. درنهایت، نتیجه‌گیری مقاله در بخش (۵) ارائه می‌شود.

## ۲- ساختار متداول سیستم‌های حفاظت مبتنی بر MAS

در این بخش، ابتدا ساختار ارتباطی و کنترل طرح‌های حفاظت مبتنی بر MAS متداول مورد بررسی قرار می‌گیرد و سپس مشکل افزایش تعداد ارتباطات مطرح و راه حل‌های پیشنهادی ارائه می‌گردد.

### ۲-۱- لایه‌های ارتباطی طرح حفاظت مبتنی بر MAS

ساختار ارتباطی یک MAS نوعی همانطور که در شکل (۱) نشان داده شده است، معمولاً از طریق سه لایه اجرا می‌شود [۲۸].

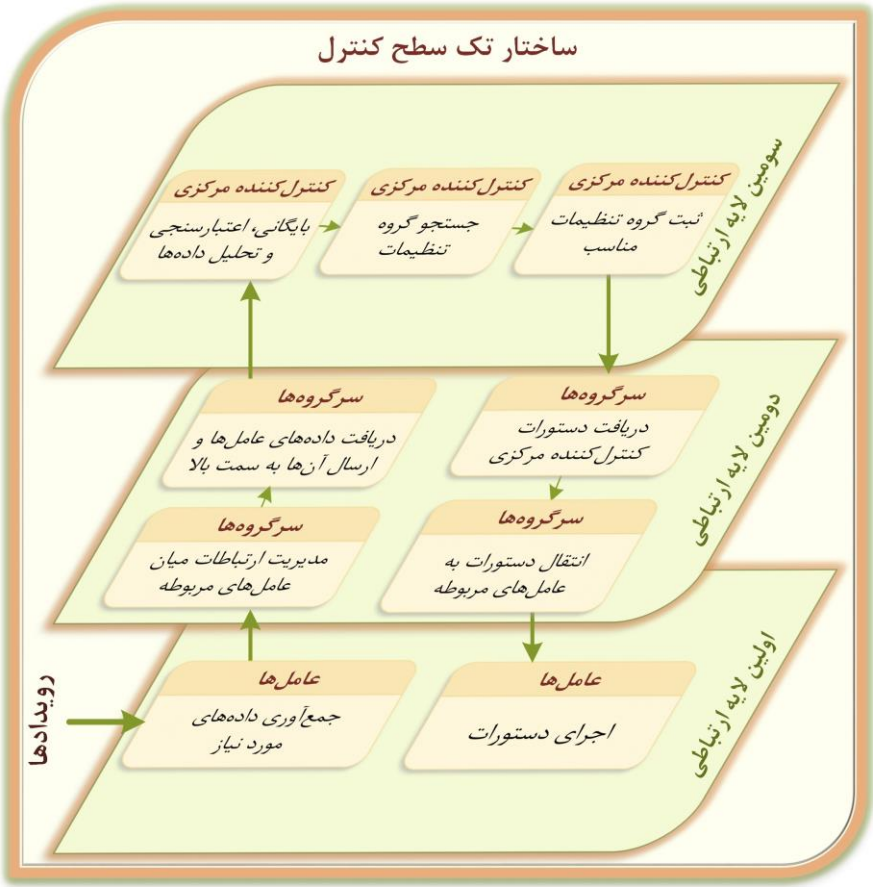
لایه اول شامل عامل‌های توزیع شده می‌باشد. به‌عنوان تعریف، یک عامل بخشی از یک IED است، سخت افزاری که محاسبه، ایجاد ارتباط و ارسال سیگنال را انجام می‌دهد. هر عامل بر اساس یک تابع اجرایی و یک پروتکل ارتباطی (به‌طور نمونه IEC-61850)، پردازش و تبادل اطلاعات را امکان پذیر می‌سازد. بنابراین مطابق با ویژگی‌های فنی دستگاه‌های مختلف سیستم، عامل‌های توزیع شده در سیستم حفاظت مبتنی بر MAS می‌توانند DGها، رله‌ها، بارها، کلیدها و غیره در نظر گرفته شوند [۳۰-۲۸].

لایه دوم ارتباط میان عامل‌های لایه اول را از طریق سرگروه‌های در نظر گرفته شده مربوط به هر گروه از عامل‌های با توابع یکسان مدیریت می‌نماید که شامل گروه عامل رله[۷](RAG)، گروه عامل DG، گروه عامل کلید[۸](BAG) و گروه عامل بار[۹](LAG) می‌باشد [۲۸]. به عبارت دیگر لایه دوم ساختار ارتباطی MAS را این سرگروه‌ها تشکیل می‌دهند.

لایه سوم نیز به عنوان کنترل‌کننده مرکزی در نظر گرفته می‌شود که مسئولیت جمع‌آوری اطلاعات شبکه، شناسایی رویدادهای جدید و ارسال اطلاعات و دستورات لازم به تجهیزات مربوطه را به عهده دارد.

### ۲-۲- سطوح کنترل طرح حفاظت مبتنی بر MAS

در یک شبکه معمولاً توابع کنترلی دارای چندین سطح کنترل می‌باشند که پایین‌ترین (اولین) سطح فوراً وظایف اساسی را انجام داده و سپس سطوح بالاتر به تدریج وظایف سطوح پایین‌تر را با تنظیم نقاط کار مربوط به آن‌ها تصحیح می‌نمایند. با این حال بر اساس دانش نویسندگان، برخلاف سایر کنترل‌کننده‌های سیستم قدرت، هیچ طبقه‌بندی سلسله مراتبی مورد قبول کلی برای وظایف سیستم حفاظت وجود ندارد. لازم به ذکر است که دلیل این امر این گونه بیان می‌شود که تقریباً اکثر پژوهشگران برای طرح‌های حفاظتی، جز پاکسازی خطا و حفظ هماهنگی رله‌ها هیچ انتظار دیگری نداشته و تمایل ندارند صرفاً این یک وظیفه را در چندین سطح کنترل تقسیم نمایند. با این وجود سیستم‌های حفاظت سنتی دارای دو سطح کنترل هستند که به شرح زیر می‌باشد:




**شکل (۱): ساختار تک سطح کنترل در حفاظت مبتنی بر MAS متداول**

- سطح کنترل اول (رفع خطا و حفظ هماهنگی): به طور معمول رله‌های سنتی با استفاده از برخی منحنی مشخصه‌های از پیش تعریف شده عملیات رفع خطا و برقراری هماهنگی با سایر رله‌ها (ظرف چند صد میلی‌ثانیه) به نمایش می‌گذارند.
- سطح کنترل دوم (به‌روز رسانی تنظیمات رله): اپراتورها پس از رخدادهای متداول شبکه، منحنی‌ها را به صورت دستی جهت عملکرد صحیح حفاظت شبکه (ظرف چند دقیقه تا چند ساعت) اصلاح می‌نمایند.

با توجه به سرعت بالای ساختارهای مبتنی بر ارتباطات مدرن، پژوهشگران مایل به ترکیب هر دو این سطوح کنترل در یک تک سطح کنترل می‌باشند. 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 گردش می‌کند. به این ترتیب عامل‌ها در لایه اول اطلاعات را به سمت بالا به سرگروه‌ها در لایه دوم و سپس به سیستم مرکزی در لایه سوم انتقال می‌دهند. در ادامه داده در سیستم مرکزی پردازش و هر تصمیمی که اتخاذ شود به لایه دوم منتقل می‌شود. سرانجام سرگروه‌ها اطلاعات را به عامل‌های مربوطه برای اقدامات لازم و یا هر تغییری که در شبکه باید انجام گیرد عرضه خواهند کرد.

به این ترتیب پردازشگر مرکزی هوشمندانه تصمیمات مناسب را با توجه به دانش گسترده درباره سیستم انتخاب می‌نماید. با این حال چنانچه تعداد ارتباطات مذکور افزایش یابد، منجر به زمان‌بندی نامناسب ارتباطی و کاهش قابلیت اطمینان سیستم خواهد شد. از اینرو احتمال ناتوانی طرح حفاظت در انجام وظایف هر دو سطح کنترل اول و دوم افزایش پیدا می‌کند. در چنین شرایطی سوال اصلی این است که "چه چیزی افزایش تعداد ارتباطات را به دنبال دارد؟" که دو مورد از مهم‌ترین آن‌ها به شرح زیر می‌باشد:

- افزایش سایز شبکه: هر چقدر تعداد عامل‌ها بیشتر شود، ارتباطات ایجاد شده میان عامل‌ها و لایه‌های مخابراتی به میزان چشمگیری نسبت به عامل‌های قبلی افزایش می‌یابد. از اینرو شبکه‌های کاربردی و بزرگتر که تعداد عامل بیشتری دارند، تعداد ارتباطات بیشتری را نیز تجربه خواهند کرد.

- سطح نفوذ متغیر DGهای تجدیدپذیر: پس از هر تغییر نفوذ DGها، اطلاعات باید به منظور اصلاح تنظیمات رله‌ها درمیان زیرساخت‌های سه لایه ارتباطی گردش نماید. بنابراین نفوذ متغیر با زمان DGهای تجدیدپذیر ناشی از ماهیت غیرقابل پیش‌بینی این منابع منجر به افزایش قابل توجه تعداد ارتباطات در سیستم‌های حفاظت خواهد شد.

با توجه به استفاده از تجهیزات هوشمند در ساختار MAS بررسی شده، شبکه ارتباطی میان عامل‌ها از اهمیت ویژه‌ای برخوردار است. به این ترتیب ویژگی‌ها و قابلیت‌های پروتکل ارتباطی IEC-61850[۱۰] در زیر بخش بعد شرح داده می‌شوند.

### ۲-۳- استاندارد بین‌المللی IEC-61850

IEC-61850 پروتکل اختصاصی سیستم اتوماسیون پست می‌باشد که هدف اصلی آن تبادل اطلاعات میان IEDها از سازندگان مختلف است. این استاندارد چهارچوب ارتباطی و اشتراک‌گذاری اطلاعات را با توجه به اینکه بهره‌برداری از سیستم‌های قدرت درحال گذر از یک ساختار کنترل متمرکز به برخی قابلیت‌های نامتمرکز می‌باشند، ارائه می‌دهد [۳۱]. لازم به ذکر است که بر اساس ترکیب مدل‌سازی شئ استاندارد با بلوک‌های توابع اجرایی نیز امکان استفاده از سیستم‌های چندعاملی در سیستم‌های قدرت و کاربردهای اتوماسیون را فراهم می‌کند [۳۲,۳۳].

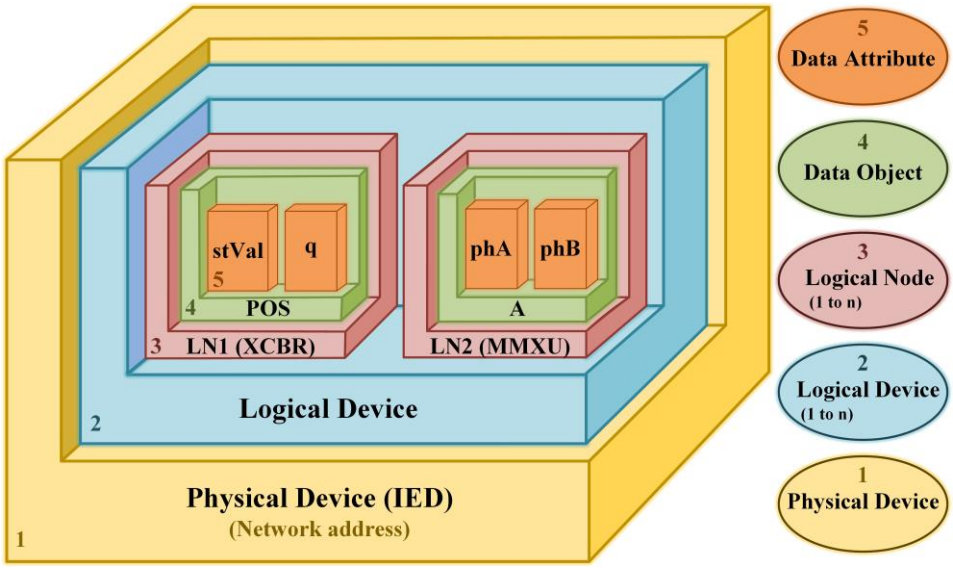
استاندارد IEC-61850 توابعی مربوط به تجهیزات کنترل، حفاظت، نظارت و ثبت را در پست تعریف می‌نماید که این توابع می‌توانند در یک تجهیز فیزیکی (PD)[۱۱] مثلاً یک IED اجرا و یا بین چندین دستگاه با استفاده از رابط ارتباطات توزیع شوند. لازم به ذکر است که هر تابع را می‌توان به زیر تابع و عناصر کاربردی تقسیم نمود. بر این اساس عناصر کاربردی کوچک‌ترین بخش یک تابع می‌باشند که می‌توانند اطلاعات را تبادل کنند. این عناصر اساسی در IEC-61850 گره منطقی (LN)[۱۲] نامیده می‌شوند [۳۴].

هر کدام از LNها شامل تعدادی شئ داده (DO)[۱۳] هستند که متعلق به یک کلاس معمول داده می‌باشند. مثلاً TCTR گره منطقی مربوط به ترانس جریان می‌باشد که اطلاعات جریان شبکه را مدل می‌کند. رله اضافه جریان نیز توسط گره منطقی (PTOC)[۱۴] مدل می‌شود که DOهای (TmASt)[۱۵] برای مشخصات منحنی فعال، (StrVal)[۱۶] برای مقدار شروع، (TmMult)[۱۷] برای ضریب تنظیم زمانی و غیره را دارا می‌باشد [۳۵,۳۶]. گره منطقی PTOC هنگامی‌که جریان متناوب ورودی از یک میزان از پیش مشخص شده بالاتر می‌رود، عمل خواهد کرد که در آن جریان ورودی و زمان عملکرد به‌طور معکوس رابطه دارند. DOهای Str و Op نیز به ترتیب نماینده شروع و عمل کردن هستند که در بخش شبیه‌سازی به آن‌ها خواهیم پرداخت.

ساختار سلسله مراتبی داده در IEC-61850 توسط شکل (۲) نشان داده شده است. PD به عنوان اولین گام برای مدلسازی داده در IEC-61850 در نظر گرفته می‌شود. PD دستگاهی است که از طریق یک یا چند پردازشگر ساخته می‌شود و قابلیت تبادل داده و انجام پردازش روی آن‌ها را فراهم می‌سازد. لازم به ذکر است که هر PD توانایی میزبانی از چندین LN را بسته به عملکرد آن دارد. این LNها در تجهیزات منطقی (LD)[۱۸]، که در متن PD جهت اهداف ارتباطی تعریف می‌شوند، طبقه‌بندی خواهند شد. همچنین در این ساختار DOها از گروهی از داده‌های پیوستی (DA)[۱۹] ساخته می‌شوند. این داده‌ها بر اساس کاربرد مخصوص خود گروه‌بندی می‌شوند. به طور نمونه بعضی از آن‌ها بیانگر حالات LN هستند در حالی که برخی دیگر به منظور پیکربندی و یا اندازه‌گیری به کارگیری می‌شوند.

LN توصیف اندازه‌گیری در یک سیستم سه فاز، MMXU نامیده می‌شود که دارای چندین داده است. به عنوان مثال W، VAr و A به‌ترتیب نشانگر اندازه‌گیری توان اکتیو ، راکتیو و جریان هستند. همچنین phsA، phsB، phsC و neut داده‌هایی می‌باشند که توصیف یک اندازه‌گیری مشخص، پیرامون فاز اول، دوم، سوم و خنثی را به عهده دارند. کلید نیز توسط گره منطقی (XCBR)[۲۰] مدل می‌شود که Pos نشان دهنده وضعیت کلید می‌باشد و (stVal)[۲۱] مقدار حالت آن را تعیین می‌نماید.

وظایف سطح کنترل اول در سیستم‌های حفاظتی غیر ارتباطی رایج، با استفاده از رله‌های مبتنی بر منحنی سنتی انجام می‌شوند. به همین ترتیب در ساختارهای ارتباطی نیز لازم نیست که حتماً از هر سه لایه ارتباطی برای انجام این نوع وظایف استفاده شود. از اینرو وظایف سطح کنترل اول می‌توانند با استفاده از قابلیت‌های پروتکل ارتباطی و یک الگوریتم مناسب از طریق اولین لایه ارتباطی به طور مجزا انجام گیرند. لازم به ذکر است که الگوریتم مورد نظر جهت تضمین عملکرد مطمئن وظایف سطح کنترل اول باید دو ویژگی زیر را دارا باشد:




**شکل (۲): ساختار سلسله مراتبی در استاندارد IEC-61850 [۳۴]**

- **مستقل از نفوذ بودن:** در صورت وابستگی طرح به سطح نفوذ DG، باید پس از هر تغییر نفوذ به روز رسانی تنظیمات سیستم حفاظت انجام شود. در حالی که اگر طرح مستقل از نفوذ DG باشد می‌تواند از شبکه در هر سطح نفوذ واحدهای تجدیدپذیر محافظت کند. به عبارت دیگر با توجه به عدم قطعیت واحدهای DG تجدیدپذیر، مشخصه اصلی یک طرح کارآمد و مؤثر اجتناب از به کارگیری سطوح ارتباطی بالاتر به منظور مستقل از نفوذ بودن طرح پیشنهادی می‌باشد.
- **بهره‌برداری از حداقل تعداد عامل:** با وجود اینکه طرح در لایه ارتباطی اول اجرا می‌شود اما در صورت استفاده از تعداد عامل کمتر، مسلماً بیشتر در برابر مشکلات بار ارتباطی محفوظ خواهد ماند. بر این اساس طرح ارائه شده باید با حداقل تعداد عامل انجام گیرد. با این حال سوال مهمی که مطرح می‌شود این است که کدام مجموعه منحصر به فرد از عامل‌ها توانایی عمل موفقیت‌آمیز و نیز مقرون به صرفه را به عنوان یک طرح حفاظت کنترل سطح اول دارا هستند؟ به عنوان جواب این گونه می‌توان بیان نمود که در میان انواع مختلف عامل‌ها، با توجه به وظایف حیاتی رله‌ها در طرح‌های حفاظتی، آن‌ها تنها تجهیزاتی می‌باشند که این قابلیت را دارا هستند. در غیر این صورت با در نظر گرفتن هر نوع عامل دیگر، لزوماً نیاز است که از رله‌ها برای محافظت کامل از شبکه استفاده شود. از اینرو در طرح ارائه شده IEDها که مسئولیت انجام وظایف حیاتی سیستم حفاظت را به عهده دارند به عنوان عامل درنظر گرفته می‌شوند.

## ۳- الگوریتم هماهنگی حفاظت پیشنهادی

در این طرح، IEDها با استفاده از توابع حفاظتی و LNهای مربوطه که توسط پروتکل IEC-61850 فراهم شده است، در شبکه پیاده‌سازی و اجرا می‌شوند تا مشکلات موجود در MAS معمول را کاهش و بهبود دهند. بنابراین رویکرد هماهنگی حفاظتی پیشنهادی با ارائه یک ساختار غیرمتمرکز مبتنی بر عامل ضمن عدم وابستگی به سطوح ارتباطی بالاتر و در نتیجه حذف کنترل‌کننده مرکزی، افزایش قابلیت اطمینان سیستم را به دنبال خواهد داشت. در این بخش ابتدا قابلیت‌های پیام‌های GOOSE مورد استفاده در طرح، به منظور انجام وظایف اینترلاک معرفی می‌شوند. و در ادامه بیان خواهد شد که چگونه این سرویس‌ها به نویسندگان در ارائه یک الگوریتم مستقل از نفوذ DG ضمن به کارگیری حداقل تعداد عامل کمک کرده است.

### ۳-۱- سرویس‌ها و قابلیت‌های پیام GOOSE

یکی از پروتکل‌های متداول اجرا شده بر IEC-61850، رویداد عمومی شئ گرا پست [۳۲](GOOSE) است که ارتباطات نقطه به نقطه سریع را همراه با قابلیت اطمینان بالا میان دستگاه‌ها فراهم می‌سازد. مطابق با این پروتکل، یک دستگاه قابلیت به روز رسانی سایر دستگاه‌ها را با یک تاخیر ۴ میلی‌ثانیه‌ای دارد [۳۷,۳۸].

پروتکل پیام GOOSE می‌تواند در یک برنامه جامع که از شبکه در هر سطح نفوذ منابع تجدیدپذیر محافظت می‌نماید، مورد استفاده قرار گیرد. به این معنی که قابلیت‌های آن قادر به تجهیز سیستم به یک الگوریتم مستقل از نفوذ DG می‌باشند. بهره‌گیری از این قابلیت‌ها و سرویس‌ها به منظور حفظ هماهنگی IEDها با یکدیگر مطابق با زیر شرح داده می‌شوند:

- **پیام GOOSE lockout**: با رویداد خطا، نزدیک‌ترین IED به خطا "پیام GOOSE lockout" را به هر IED بالادست یا پایین دست به منظور اطلاع رسانی به دیگر عامل‌ها درمورد جریان قطع IED اصلی ارسال می‌کند. بر این اساس از هر گونه همکاری غیر ضروری دیگر عامل‌ها جلوگیری خواهد شد. به عبارت دیگر در این روش، هر کدام از عامل‌ها می‌توانند با استفاده از "پیام GOOSE lockout" از عملکرد عامل یا عامل‌های پشتیبان خود به واسطه مسدودسازی فرمان باز شدن کلید مربوطه آن‌ها جلوگیری کنند.
- **پیام GOOSE Reset**: اگر IED اصلی نتواند خطا را با موفقیت رفع کند، انتظار می‌رود که عامل پشتیبان در سریع‌ترین زمان ممکن پاکسازی خطا را انجام نماید. به این ترتیب از "پیام GOOSE Reset" جهت آزاد سازی عامل پشتیبان از حالت قفل استفاده خواهد شد.
- **پیام GOOSE Request**: در صورت عملکرد ناموفق عامل اصلی، "پیام GOOSE Request" باعث می‌شود که IED پشتیبان فوراً برای پاکسازی خطا بدون هیچ تأخیر هماهنگی اقدام نماید.
- **پیام GOOSE Adaptive Reconfiguration**: هنگامی که وضعیت کلید IED تغییر نماید، عملگر کنترلی مربوطه از IED فعال می‌شود و با انتشار "پیام GOOSE Adaptive Reconfiguration" برای دیگر IEDها، گروه تنظیمات فعال آن‌ها را به گروه تنظیمات از پیش تعریف شده بعدی، بر اساس شرایط جدید تغییر خواهد داد.

الگوریتم ارائه شده در زیر بخش بعد، با بهره‌گیری از سرویس‌های پیام GOOSE مطابق با منطق‌های تعریف شده آن‌ها، کاملاً مستقل از نفوذ DGها عمل می‌نماید. به عبارت دیگر تغییر نفوذ واحدهای تجدیدپذیر، قادر به تغییر صحت پیام‌های "GOOSE lockout، Resetو Request" نمی‌باشد. به این ترتیب الگوریتم پیشنهاد شده راه‌حلی توانا به منظور عملکرد مطمئن سیستم حفاظتی در برابر هر سطح نفوذ DG، بدون مواجه با مسئله تأخیر در فرآیندهای سطوح کنترل بالاتر می‌باشد.

### ۳-۲- الگوریتم تک سطح کنترل و حفاظت پیشنهادی

همانطور که در فلوچارت شکل (۳) نشان داده شده است، الگوریتم حفاظتی پیشنهادی توابع سطح کنترل اول و دوم را در یک تک سطح کنترل بدون استفاده از لایه‌های مخابراتی بالاتر و با به کارگیری حداقل تعداد عامل اجرا می‌کند. این فرآیند مطابق با مراحل زیر شروع و گام به گام به ترتیب پیش می‌رود:

- عامل‌ها با توجه به ارتباطی که بر روی بستر مخابراتی با یکدیگر برقرار می‌کنند، پیوسته با هم در ارتباط می‌باشند و تغییرات جریان خود را به‌یکدیگر گزارش خواهند داد.
- IEDها مطابق با تنظیمات تعیین شده برای آن‌ها در شرایط عادی شبکه، نسبت به جریان عبوری از خود حساسیت نشان می‌دهند. بر این اساس در صورت عبور جریانی بیشتر از آستانه تحریک IEDها، جریان خطا توسط توابع حفاظتی آن‌ها تشخیص داده می‌شود. پس از آن، عامل‌ها حفاظت‌های اصلی و پشتیبان را با توجه به مکان خطا و جهت IEDها در رویت یا عدم رویت جریان خطا مشخص خواهند کرد.
- در ادامه، با توجه به منحنی مشخصه IEDها بر اساس سطح جریان خطا رویت شده، وضعیت هماهنگی IEDهای اصلی و پشتیبان توسط عامل‌ها بررسی می‌شود. در صورت عدم هماهنگی، الگوریتم کمکی پیشنهادی فراخوانی خواهد شد.

- چنانچه هماهنگی برقرار باشد، IED اصلی پیام "GOOSE lockout" را برای IED پشتیبان ارسال و با توجه به زمان عملکرد خود بر اساس منحنی مشخصه، عمل می‌نماید.
- در صورتی که IED اصلی موفق به رفع خطا نباشد، پیام "GOOSE Reset" را برای IED پشتیبان منتشر می‌کند. به این ترتیب عامل پشتیبان با دریافت این پیام از حالت قفل خارج خواهد شد.
- IED پشتیبان که نسبت به عامل اصلی در یک وضعیت هماهنگ قرار دارد مطابق با منحنی مشخصه و زمان عملکرد خود عمل جداسازی ناحیه خطا دیده را انجام می‌دهد.

لازم به ذکر است که چنانچه هرگونه سوءعملی در سیگنال‌های ارسال یا دریافت IEDها، در یک زمان مشابه رخ دهد، طرح حفاظت در پاکسازی خطا شکست می‌خورد. به عبارت دیگر در صورت ناتوانی IED اصلی در انجام وظایف مهم خود، امکان خارج شدن IED پشتیبان از حالت قفل وجود ندارد که این خود یک نگرانی بزرگ به شمار می‌آید. در چنین شرایطی IEDهای پشتیبان در انجام وظایف مورد انتظار ناتوان می‌باشند. به منظور غلبه بر این مشکل، عملگر ناظر در IEDهای پشتیبان پس از گذشت یک زمان از پیش تعیین شده ($T_{SO}$) فعال می‌شود. با فعال شدن این عملگر، دستور لغو تمامی سیگنال‌های دریافت شده از جمله "GOOSE lockout" صادر شده که به دنبال آن وظایف مورد انتظار انجام می‌شوند. بر این اساس مسئله باقی مانده، زمان عملکرد عملگر ناظر $T_{SO}$ می‌باشد. برای پیدا کردن زمان مناسب، باید دو شرط لازم زیر برآورده شود:

اول، باید زمان انتخاب شده بزرگتر از فاصله زمانی هماهنگی (CTI)[۲۳] معمول میان IED اصلی و پشتیبان در نظر گرفته شود و دوم، برای اطمینان در مورد حدود حرارتی سیستم مطابق با منحنی I2t، باید به اندازه کافی کوچک باشد.

در لحظه جداسازی ناحیه خطا دیده، پس از باز شدن کلید مربوطه IED پیام "GOOSE Adaptive Reconfiguration" برای دیگر IEDها منتشر می‌شود و تنظیمات آن‌ها مطابق با گروه تنظیمات از پیش تعریف شده به روز رسانی خواهد شد. به این ترتیب شبکه در وضعیت عادی قرار می‌گیرد. لازم به ذکر است که تنظیمات قطع حفاظت جریان زیاد این IEDها نیز از طریق یک تحلیل حفاظتی بر اساس منحنی مشخصه رله، که دارای دو بخش معکوس و آنی می‌باشند، محاسبه و در تنظیمات فعال آن‌ها جایگذاری می‌شود.

هنگامی که تابع حفاظتی جهتی یا غیرجهتی (LN PTOC/PDOC) از IED اصلی، اضافه جریان را تشخیص می‌دهد، عملگر Str.general آن فعال خواهد شد، شمارنده داخلی IED شروع و پیام "GOOSE lockout" را به عملگر BlkOpn از IED پشتیبان می‌فرستد تا آن را فعال و فرمان باز شدن کلید مربوطه دستگاه را مسدود کند. سپس با به اتمام رسیدن شمارنده IED اصلی پس از تأخیر در نظر گرفته شده، عملگر Op.general فعال و قطع انجام خواهد شد. لازم به ذکر است که این تأخیر توسط عامل بر اساس منحنی مشخصه و میزان جریان خطا، تنظیم شده است. چنانچه رفع خطا توسط IED اصلی موفقیت آمیز نباشد، عامل این دستگاه پیام "GOOSE Reset" را به IED پشتیبان جهت رهایی از وضعیت قفل ارسال می‌نماید. در ادامه با توجه به هماهنگ بودن IEDها، عامل پشتیبان بر اساس زمان عملکرد خود با توجه به منحنی مشخصه، اقدام به پاکسازی خطا می‌کند.

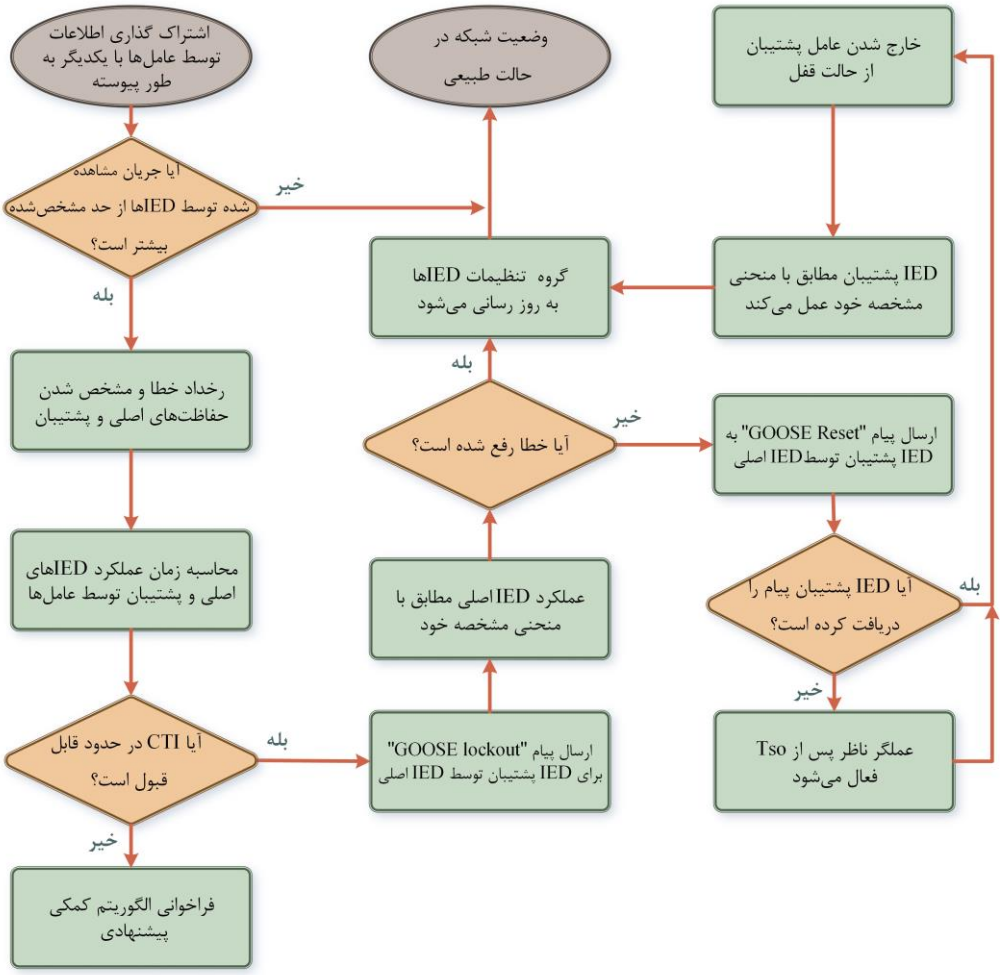
به منظور بیان جزئیات بیشتر، زمان عملکرد IED مطابق رابطه (۱) [۲۸]، محاسبه می‌شود:

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

که $I_F$ جریان خطا، $I_p$ جریان قطع و $TMS$ ضریب تنظیم زمانی را نشان می‌دهند. $A$ و $B$ نیز بسته به نوع منحنی مشخصه تعیین خواهند شد. بر اساس این پارامترها، هماهنگی حفاظت‌های اصلی و پشتیبان مطابق با 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 $m$ به نسب جریان خطا به جریان قطع اشاره می‌کند و $\Delta T$ زمان در نظر گرفته شده برای IEDها را بیان می‌کند که باید یک CTI مناسب (۴۰۰ تا ۳۰۰ میلی‌ثانیه) را دارا باشند.

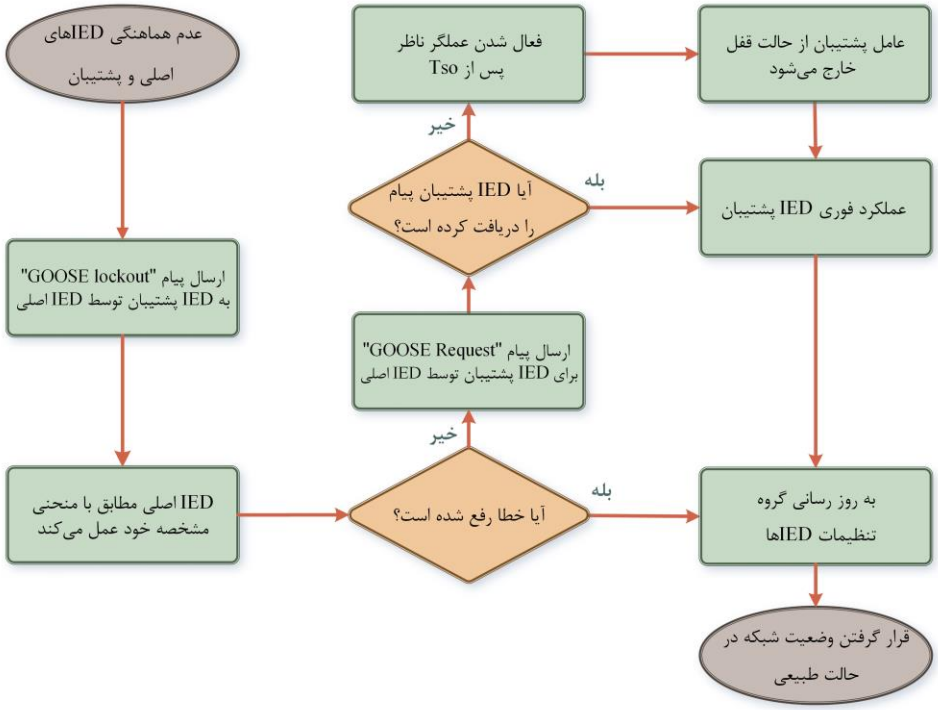



**شکل (۳): فلوچارت الگوریتم حفاظتی پیشنهادی**

### ۳-۳- الگوریتم کمکی مستقل از نفوذ پیشنهادی

مطابق با معادلات (۱,۲)، عامل‌ها با انتقال اطلاعات به یکدیگر، مقدار $\Delta T$ را بررسی می‌نمایند. در صورتی که این مقدار در حدود یک CTI استاندارد باشد حفاظت‌های اصلی و پشتیبان هماهنگ هستند و IEDها مطابق با زمان محاسبه شده توسط عامل‌ها بر اساس رابطه (۱) عمل خواهند کرد. در غیر این صورت، هماهنگی میان IEDهای اصلی و پشتیبان برقرار نمی‌باشد و می‌تواند به معنی تغییر نفوذ منابع تجدیدپذیر در نظر گرفته شود. به این ترتیب الگوریتم کمکی پیشنهادی شکل (۴) به منظور عملکرد سیستم حفاظت مستقل از نفوذ DG، به شرح زیر به ترتیب اجرا می‌شود:

- IED اصلی پیام "GOOSE lockout" را برای IED پشتیبان منتشر می‌کند.
- عامل اصلی با توجه به سطح جریان خطا عبوری از آن، بر اساس زمان عملکرد محاسبه شده از منحنی مشخصه خود، عمل می‌نماید.
- در صورت عدم عملکرد موثر IED اصلی و وجود خطا، عامل اصلی پیام "GOOSE Request" را به IED پشتیبان به منظور پاکسازی سریع خطا ارسال می‌کند.
- چنانچه IED پشتیبان هر کدام از سیگنال‌های"GOOSE lockout" یا "GOOSE Request" را دریافت نکرده باشد، عامل پشتیبان عملگر ناظر را پس از Tso به منظور رفع خطا مستقل از IED اصلی فعال خواهد نمود.
- پس از پاکسازی خطا و تغییر حالت کلید، عملگر Pos.stVal از IED فعال می‌شود و تنظیمات IEDها به روز رسانی خواهد شد. به این ترتیب شبکه در وضعیت طبیعی قرار می‌گیرد.



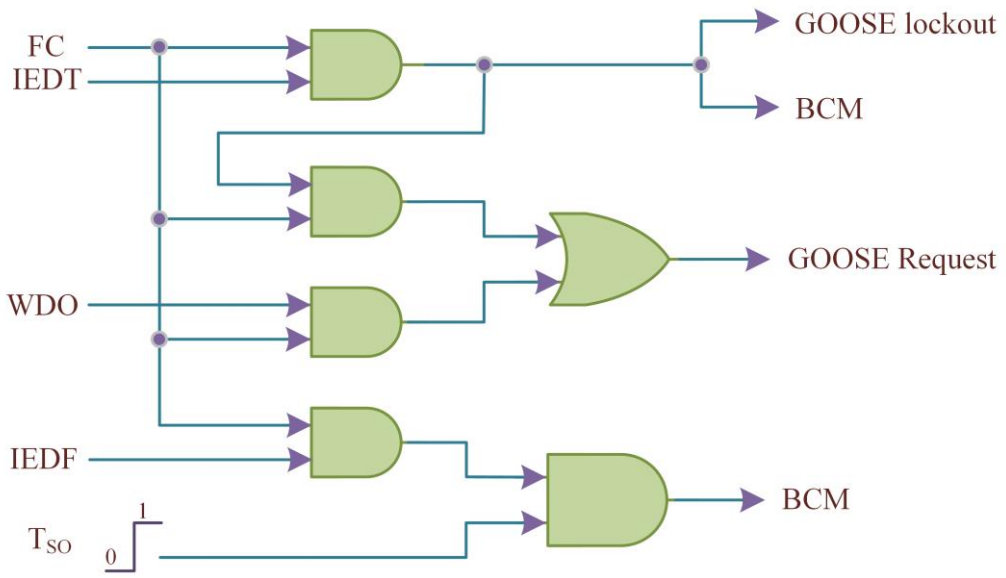

**شکل (۴): فلوچارت الگوریتم کمکی مستقل از نفوذ DG**

لازم به ذکر است که با تغییر نفوذ واحدهای DG، منطق هر یک از پیام‌های GOOSE ارسالی و دریافتی میان عامل‌ها در هر مرحله از اجرای الگوریتم و حتی سرعت انتقال دستورات تغییر نمی‌یابد. از اینرو الگوریتم ارائه شده قابلیت بهره‌برداری در هر شبکه‌ای را دارا می‌باشد و افزایش قابلیت اطمینان سیستم را به دنبال دارد.

### ۳-۴- دیاگرام مدار منطقی الگوریتم کمکی

به‌منظور بیان جزئیات بیشتر، چگونگی پیاده‌سازی الگوریتم کمکی بر روی ساختار منطقی IEDها در شکل (۵) نشان داده شده است. برای توصیف این شکل ابتدا لازم است که منطق‌های مورد استفاده و حالات آن‌ها را به شرح زیر تعریف نمود:

- منطق FC: زمانی که سیستم در حالت طبیعی کار می‌کند، این منطق برابر با صفر است، در حالی که با مواجه شدن سیستم با یک شرایط خطا برابر با یک منطقی خواهد شد.
- منطق IEDT: هنگامی که IED عملی انجام نمی‌دهد حالت این منطق برابر با صفر و در صورت عملکرد موفق IED برابر با یک منطقی است.
- منطق WDO: به منظور درک بهتر این منطق ابتدا لازم است که کارکرد عملگر Watch Dog بیان شود. بر این اساس، لازم به ذکر است که در صورت وجود هر گونه خطا در مدار داخلی IED، عملگر Watch Dog فعال شده و تمامی توابع حفاظت را لغو و از سرویس خارج می‌کند. با انجام این کار، شناسایی عیوب داخلی، خطاها و خرابی‌هایی که باعث عملکرد نامناسب یا سوءعمل IED می‌شوند، امکان پذیر است. بر این اساس زمانی که این عملگر غیرفعال است، حالت منطقی WDO برابر با صفر و در صورت فعال بودن عملگر، برابر با یک منطقی می‌باشد.
- منطق IEDF: چنانچه منطق IEDT برابر با صفر و همچنین t بزرگتر از Tso باشد، این منطق برابر با یک در غیر این صورت برابر با صفر می‌باشد.
- منطق BCM: زمانی که پیام فرمان کلید ارسال نشده است حالت این منطق برابر با صفر و هنگامی که پیام با موفقیت ارسال شده است برابر با یک می‌باشد.




**شکل (۵): دیاگرام مدار منطقی الگوریتم مستقل از نفوذ**

همانطور که در شکل (۵) نشان داده شده است، در صورت رخداد خطا FC به یک تغییر می‌کند. سپس IED اصلی ظرف یک تاخیر محاسبه شده مطابق با (۱) عمل می‌کند (IEDT=1). به‌طور همزمان پیام "GOOSE lockout" فعال و ارسال خواهد شد. سپس BCM به‌منظور تریپ کلید یک خواهد شد. اکنون اگر پیام فرمان کلید با موفقیت فعال نشده باشد یا کلید عمل نکند، ممکن است یکی از رویدادهای زیر رخ دهد:

۱. اگر این مشکل به خطای داخلی IED مربوط باشد، WDO به منظور ارسال پیام "GOOSE Request" فعال خواهد شد.

۲. اگر BCM=1 باشد اما پیام به کلید ارسال نشده باشد یا کلید در عمل ناتوان باشد، FC همچنان یک باقی خواهد ماند و باعث می‌شود که IED پیام "GOOSE Request" را فعال نماید.

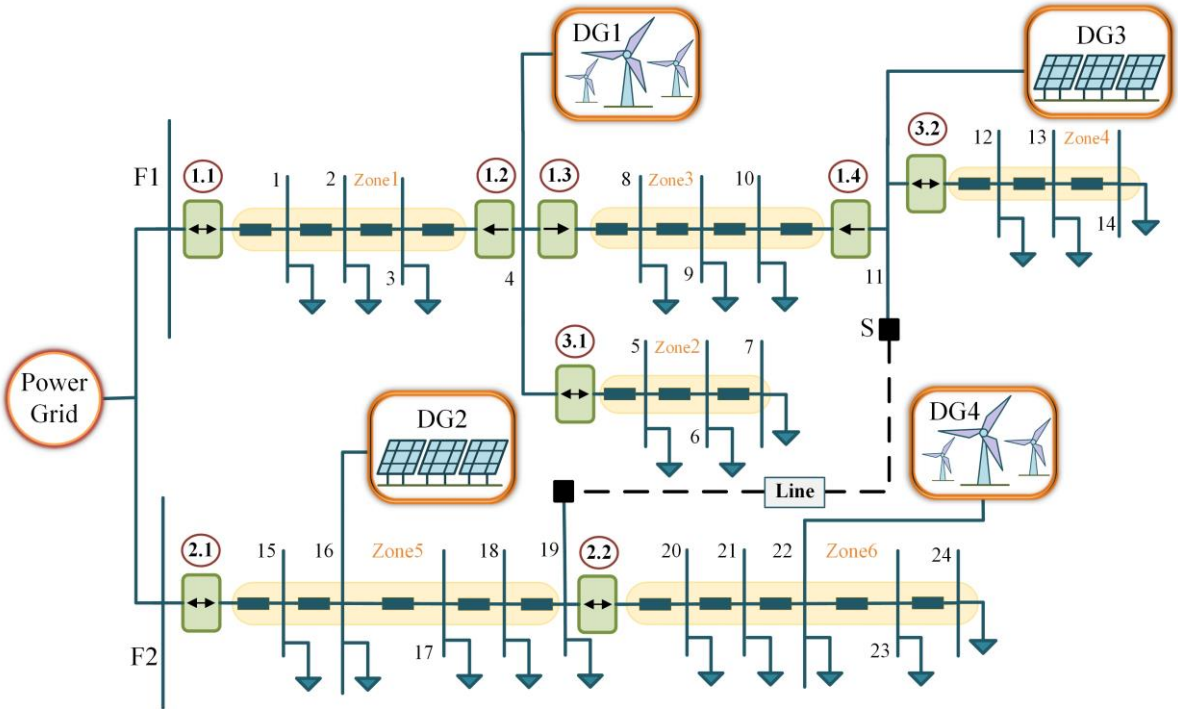
۳. اگر IED در عمل شکست بخورد (IEDF=1)، با توجه به FC=1، عملگر ناظر به منظور فرمان به کلید پس از Tso ثانیه فعال خواهد شد.

## ٤- نتایج شبیه‌سازی

به‌منظور بررسی کارایی روش پیشنهادی، شبکه رسم شده در شکل (۶) توسط نرم‌افزار ETAP مورد ارزیابی قرار می‌گیرد. همانطور که در این شکل نشان داده شده است، دو فیدر F1 و F2 متصل به یک پست ۶۳/۲۰ کیلو ولت برای تامین بارهای مربوطه هستند. همچنین همه بارهای متصل شده به فیدرها از طریق دو ترانسفورماتور ۲۰/۰/۴ کیلو ولت تغذیه خواهند شد. در این مطالعه، DGهای تجدیدپذیر، واحدهای بادی و خورشیدی در نظر گرفته شده است که بر روی فیدر F1 یا F2 نصب می‌باشند. DG1 و DG4 تجدیدپذیر بادی، MVA ۱۰ را برای سیستم تامین می‌کند و به ترتیب به باس‌های ۴ و ۲۲ متصل شده‌اند، در حالی که DG2 و DG3 به دو واحد خورشیدی MVA ۵ اشاره می‌کنند که به باس‌های ۱۱ و ۱۶ متصل می‌باشند. لازم به ذکر است که زمان مورد نیاز برای انتقال یک سیگنال، عملکرد کلید قدرت و نیز اجرای توابع و پردازش داده در IEDها به ترتیب ۴، ۵۰ میلی‌ثانیه و ۵۰ میکروثانیه (که صرف نظر شده) لحاظ شده است [۲۸].

با توجه به شکل (۶)، از میان شش ناحیه شبکه مورد مطالعه، ناحیه‌های ۴ و ۶ به دلیل برخی ضروریات عملکردی، بحرانی‌ترین بارها را دارا هستند. از اینرو طراح شبکه، دو فیدر F1 و F2 را به واسطه کلید S به گونه‌ای متصل کرده است که بارهای موجود در هر دو ناحیه قابلیت تغذیه از طریق هر یک از ناحیه‌های ۳ یا ۵ را داشته باشند. البته به منظور اجرای این طرح در یک فیدر شعاعی، یک اینترلاک میان IEDها برای بررسی حالت کلیدها وجود دارد. بر این اساس اگر هر دو فیدر F1 و F2 در مدار باشند، در این صورت بسته بودن کلید S و تغییر آرایش شبکه به حلقوی امکان پذیر نمی‌باشد. به عبارت دیگر چنانچه کلید S بسته باشد، یکی از کلیدهای مربوط به IED1.1 یا IED2.1 باز خواهند شد. برای محافظت از این شبکه، از شش IED بر روی فیدر F1 و دو IED بر روی فیدر F2 استفاده

شده است. IED1.2، IED1.3 و IED1.4 به عنوان IEDهای جهتی که جریان خطا را فقط در جهت تعیین شده تشخیص می‌دهند، در نظر گرفته شده‌اند. دیگر IEDهای موجود نیز غیرجهتی انتخاب شده‌اند. لازم به ذکر است که IED3.1 و IED3.2 به عنوان دستگاه‌های حفاظتی فیدر بار در نظر گرفته می‌شوند، به این معنی که با تعریف و لحاظ یک تأخیر زمانی بسیار کوتاه برای این IEDها، پس از رخداد خطا در هر نقطه مکانی از پایین دست آن‌ها، در کمترین زمان ممکن عمل می‌کنند. بنابراین تأخیر مورد نظر ۲۰ میلی‌ثانیه لحاظ شده است. در ادامه، حالت کلیدها می‌تواند منجر به سه سناریو از لحاظ حفاظتی شود که در زیربخش‌های بعدی، طرح ارائه شده با توجه به عدم قطعیت DGهای تجدیدپذیر بر اساس سناریوهای مختلف بررسی خواهد شد.



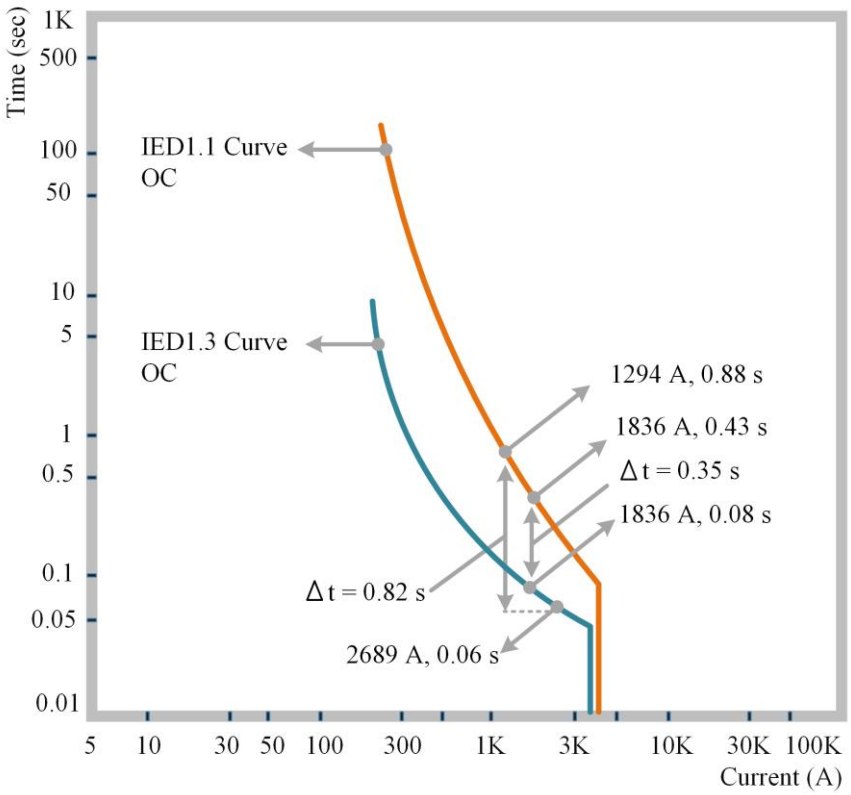

**شکل (۶): دیاگرام تک خطی شبکه مورد مطالعه در حضور منابع تولید پراکنده تجدیدپذیر**

### ٤-١- سناریو اول (S باز است و فیدرهای F1 و F2 در مدار هستند)

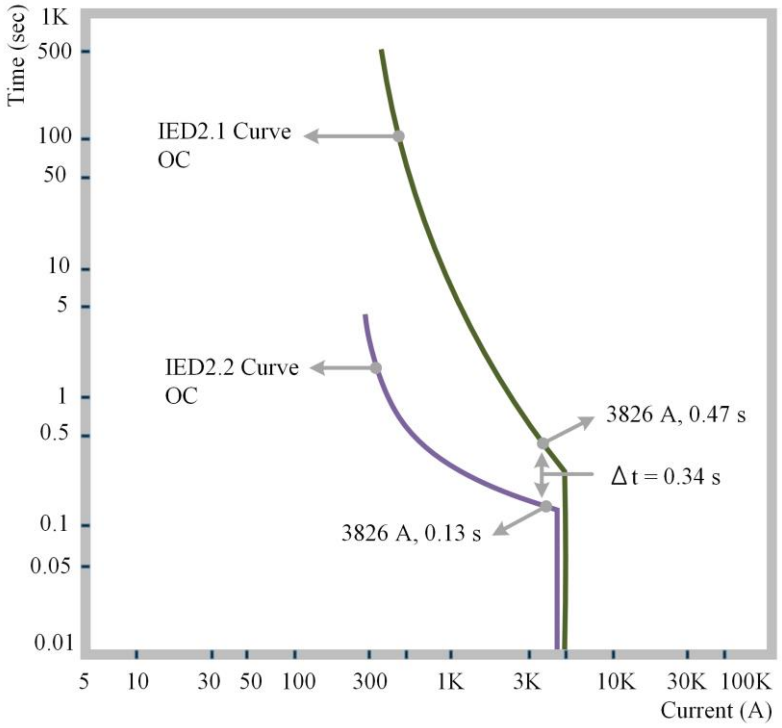
مادامی که S باز است، دو فیدر F1 و F2 و حفاظت‌های مربوط به آن‌ها به طور مستقل عمل می‌کنند. از اینرو بر روی فیدرF1، دستگاه‌های حفاظتی IED1.1 پشتیبان IED1.3 و IED1.4 پشتیبان IED1.2 هماهنگ با یکدیگر هستند. همچنین به طور مشابه IED2.1 پشتیبان IED2.2 برروی فیدر F2 است.

به منظور بررسی تاثیر عدم قطعیت DGها بر طرح حفاظتی، ابتدا فرض می‌شود که هیچ DG در شبکه وجود ندارد. IED1.1 دارای مشخصه "به‌شدت معکوس" و IED1.3 دارای مشخصه "خیلی معکوس" هستند. مینیمم جریان خطا بر فیدر F1، ۱۳۱۵ آمپر است درحالی‌که IED1.3 حداکثر جریان خطا ۱۸۳۶ را شناسایی می‌کند. با توجه به این‌که IED1.1 پشتیبان IED1.3 است، باید به طور صحیح در محدوده [۱۸۳۶-۱۳۱۵] آمپر عمل کند. هماهنگی انجام شده میان این IEDها در شکل (۷) نشان داده شده است.

در این حالت نیز با روشی مشابه، IED2.1 و IED2.2 از فیدر F2 به ترتیب با مشخصه‌های "به‌شدت معکوس" و "معکوس" حفاظت خواهند کرد. انتظار می‌رود که در این فیدر IED2.1، IED2.2 را با توجه به محدوده جریان خطا [۳۸۲۶-۱۶۹۵] پشتیبانی نماید. هماهنگی میان این دستگاه‌ها بر روی این فیدر در شکل (۸) نشان داده شده است.

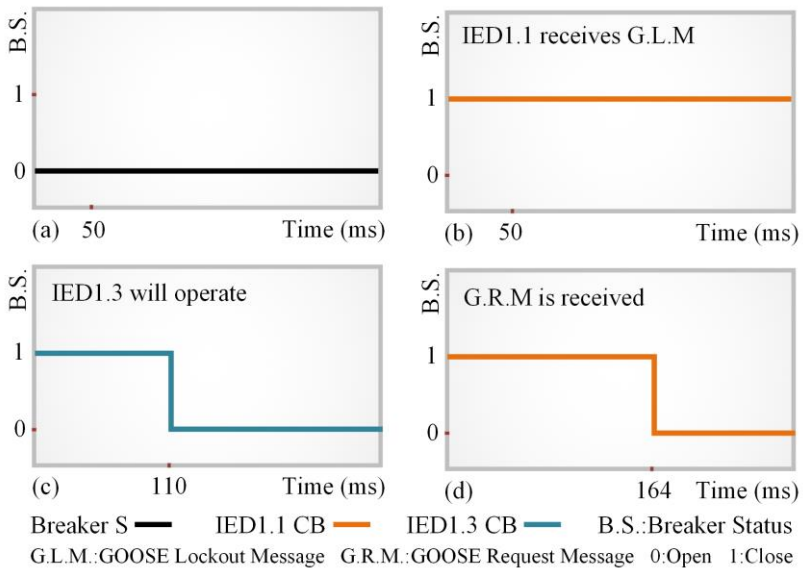



**شکل (۷): هماهنگی میان IED1.1 و IED1.3 روی فیدر F1**




**شکل (۸): هماهنگی میان IED2.1 و IED2.2 روی فیدر F2**

زمانی‌که DGها شروع به تولید توان نمایند، احتمال تغییر اندازه‌های جریان خطا و حتی جهت آن در F1 و F2 می‌باشد. با این حال سیستم حفاظتی باید به طور صحیح برای سطح نفوذ مختلف DGها عمل کند. به عنوان نمونه فرض کنید فقط DG1 با تولید حداکثر توان خود به فیدر F1 متصل باشد. با رویداد خطا بر باس ۸، هنگامی‌که توابع حفاظتی از IED1.1 و IED1.3 اضافه جریان را رویت کنند، تایمر داخلی آن‌ها آغاز به کار می‌کنند. جریان عبوری از IED1.1 و IED1.3 به ترتیب ۱۲۹۴ و ۲۶۸۹ آمپر است که عامل‌ها باید وضعیت هماهنگی خود را با این جریان‌ها بررسی و مشخص کنند. بر این اساس متأسفانه CTI حاصل مناسب نمی‌باشد. از اینرو IED1.3 پیام "GOOSE lockout" را برای IED1.1 ارسال می‌نماید. سپس IED1.3 با اتمام تایمر خود (۶۰ میلی‌ثانیه)، عمل می‌کند. اگر خطا با موفقیت پاکسازی شده باشد، وظیفه حیاتی سیستم حفاظت به درستی انجام شده است. در غیر این صورت پیام "GOOSE Request" را برای IED1.1 منتشر می‌نماید تا خطا را بلافاصله مانند یک رله آنی رفع کند. زمان صرف شده برای این مرحله بر اساس زمان تریپ کلیدها در شکل (۹) رسم شده است.

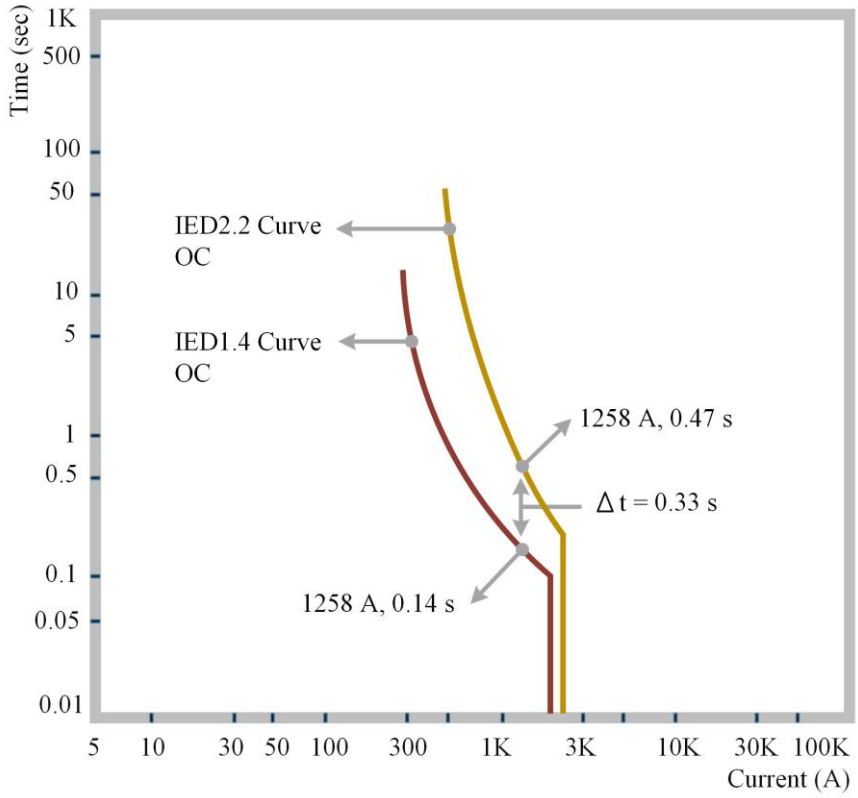



**شکل (۹): زمان تریپ کلیدها بر اساس رویه پیام GOOSE در سناریو اول**

لازم به ذکر است که چنانچه IED1.1، به هر دلیلی هیچکدام از سیگنال‌های"GOOSE lockout" یا "GOOSE Request" را دریافت نکرده باشد، عملگر ناظر از این دستگاه پس از سپری شدن زمان $T_{SO}$ توسط عامل پشتیبان فعال خواهد شد تا با لغو تمامی دستورات از پیش دریافت شده، عملیات پاکسازی خطا را مستقل از عامل اصلی (IED1.3) انجام دهد.

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

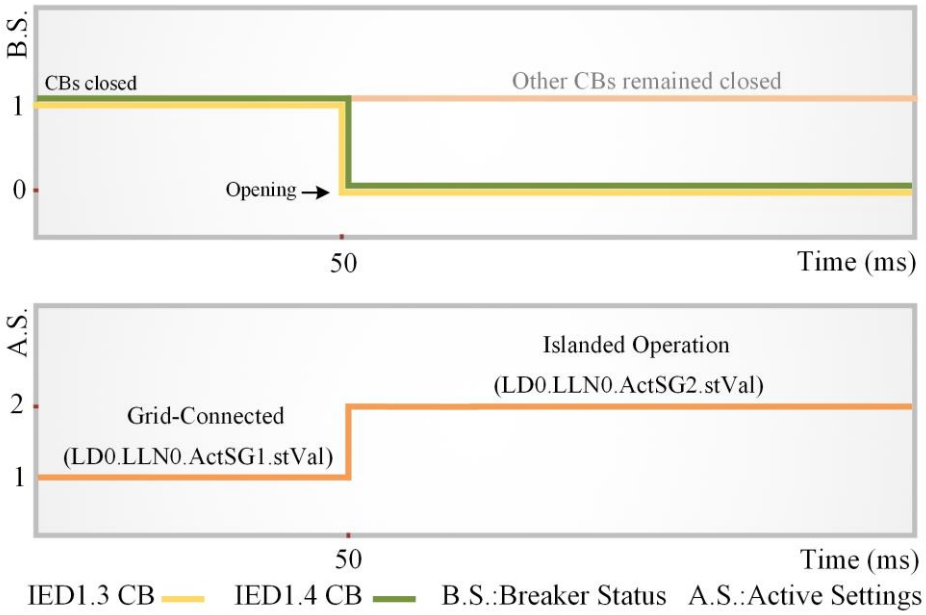
در این سناریو IED2.1 از سرویس خارج است و حفاظت به وسیله سایر IEDها انجام می‌شود. به این ترتیب با فرض رخداد خطا بر باس ۸ و حضور دو DG1 و DG4 با ماکزیمم توان، پس از تشخیص اضافه جریان توسط توابع حفاظتی IEDها، عملگر Str.general آن‌ها فعال و شمارنده داخلی آن‌ها شروع می‌شود. سپس حفاظت‌های اصلی و پشتیبان توسط عامل‌ها مشخص خواهند شد. لازم به ذکر است که با توجه به جریان‌های خطا، عملکرد IED1.1 و IED1.3 مشابه با سناریو اول است. همچنین در این وضعیت IED1.4 و IED2.2، به ترتیب با مشخصه‌های "بسیار معکوس" و "به‌شدت معکوس" نسبت به جریان خطا رویت شده (۱۲۵۸ آمپر) با توجه به شکل (۱۰) در یک وضعیت هماهنگ هستند. بر این اساس IED1.4 پیام "GOOSE lockout" را برای عملگر CTRL.XCBR.BlkOpn از IED2.2 به منظور جلوگیری از عملکرد آن به عنوان پشتیبان منتشر می‌نماید. سپس IED1.4 بر اساس منحنی مشخصه و زمان عملکرد خود (۱۴۰ میلی‌ثانیه)، با فعال‌سازی عملگر LD0.PDOC.Op.general عمل می‌کند. در ادامه، در صورتی که خطا با موفقیت پاکسازی نشده باشد، IED1.4 با ارسال پیام "GOOSE Reset" به IED2.2 باعث خارج شدن آن از حالت قفل می‌شود. به این ترتیب IED2.2 بر اساس منحنی مشخصه مربوطه، پس از سپری شدن زمان ۴۷۰ میلی‌ثانیه، خطا را رفع می‌کند.




**شکل (۱۰): هماهنگی میان IED1.4 و IED2.2**

**در سناریو دوم روی فیدر F1**

پس از عملکرد حفاظت‌های اصلی و جدا شدن ناحیه خطا دیده، شبکه به دو قسمت تقسیم خواهد شد. به این ترتیب بخش بالایی آن متصل به شبکه اصلی باقی مانده و بخش پایین، در مد جزیره‌ای به عملکرد خود ادامه می‌دهد. بر اساس گروه تنظیمات از پیش تعریف شده برای IEDها، می‌توان تنظیمات آن‌ها را برای ساختار جدید شبکه به روز رسانی نمود. به عنوان مثال، در این مورد خطا ActSG1 بیانگر تنظیمات در حالت شبکه متصل و ActSG2 بیانگر تنظیمات پس از رفع این مورد خطا برای IEDها می‌باشند.

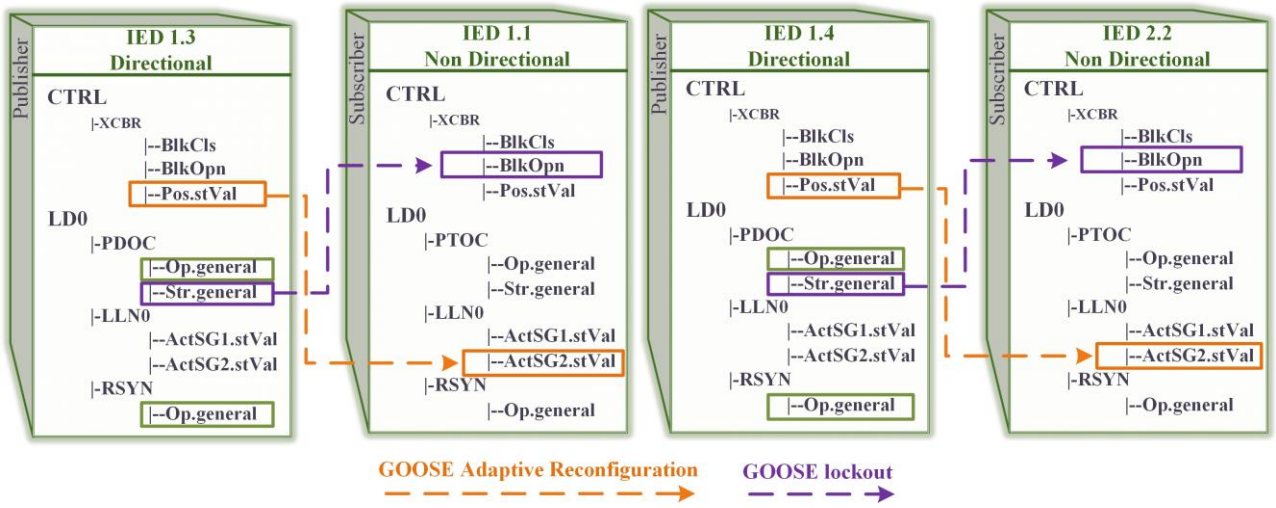



**شکل (۱۱): وضعیت کلیدها و تنظیمات فعال IEDها**

در ابتدا تمام IEDها دارای تنظیمات گروه یک (ActSG1) هستند. به دنبال رخداد خطا بر باس ۸، مطابق با شکل (۱۱) هنگامی‌که کلیدهای IED1.3 و IED1.4 باز شوند، عملگر CTRL.XCBR.Pos.stVal از این IEDها فعال شده و پیام " GOOSE Adaptive Reconfiguration" را برای سایر IEDها ارسال خواهند کرد تا تنظیمات فعال آن‌ها از LD0.LLN0.ActSG1.stVal به LD0.LLN0.ActSG2.stVal تغییر کنند.

با توجه به الگوریتم حفاظتی بیان شده و عملگرهای فعال شده از IEDها در این نقطه خطا، در شکل (۱۲) الگوی فرستنده/گیرنده و ارتباطات نقطه به نقطه میان IEDها ترسیم شده است.

ناحیه خطا دیده پس از رفع خطا، یکبار دیگر توانایی اتصال به شبکه اصلی را دارد. این عمل از طریق گره منطقی (RSYN)[۲۴] از IEDها امکان پذیر است. این گره منطقی، اختلاف ولتاژ، زاویه فاز و فرکانس ناحیه جدا شده را با شبکه اصلی بررسی می‌نماید. بنابراین بستن کلید درصورتی مجاز است که این پارامترها در حدود تعیین شده قرار داشته باشند. به این ترتیب با فعال شدن عملگر LD0.RSYN.Op.general از IEDها اتصال مجدد انجام خواهد شد.




**شکل(۱۲): پیام‌های GOOSE منتشر شده میان IEDها در سناریو دوم، خطا بر باس۸**

ساختار سیستم حفاظت به گونه‌ای طراحی شده است که مکان‌یابی دقیق برخی نقاط خطا امکان‌پذیر است. این قابلیت با توجه به جهت IEDها در رویت یا عدم رویت جریان خطا انجام می‌شود. به عنوان مثال اگر IED1.1 و IED1.4 اضافه جریان خطا را رویت کنند، در حالی که هیچ اضافه جریانی توسط IED1.2 و IED1.3 مشاهده نشود، مکان دقیق خطا بر باس ۴ شبکه تعیین می‌شود. همچنین در صورتی که IED1.3 جریان خطا را رویت کند در حالی‌که هر دو IED1.4 و IED3.2 هیچ اضافه جریانی را مشاهده نکنند، نقطه خطا دقیقاً بر روی باس ۱۱ شبکه مکان‌یابی خواهد شد.

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

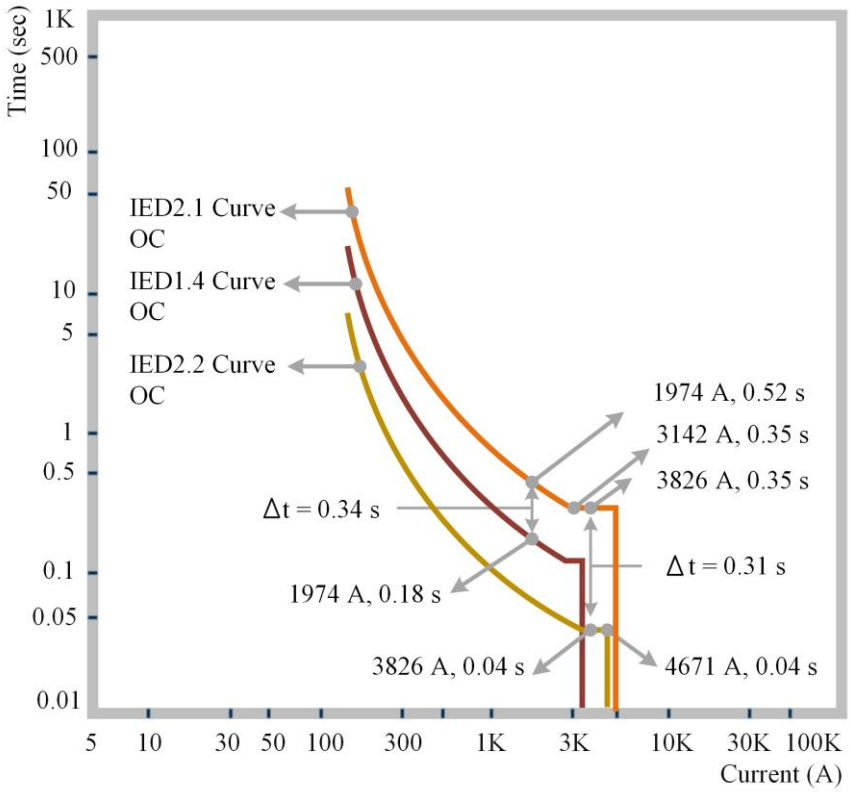
در این وضعیت، حفاظت از شبکه به تمام IEDها به جز IED1.1 واگذار می‌شود. بر این اساس، IED2.1 باید به طور صحیح هر دو IED2.2 و IED1.4 را به منظور حفظ یک هماهنگی لازم روی هر دو فیدر پشتیبانی کند. نسبت به سناریو اول، IED2.1 و IED1.3 دارای ناحیه‌های حفاظتی مختلفی هستند و باید گروه تنظیمات مناسب با توجه به این ساختار برای IEDها لحاظ شود. این گروه تنظیمات، هم می‌توانند از پیش تعریف شده باشند و هم از گروه تنظیمات سناریو اول اتخاذ شوند. به این معنی که عامل‌ها با در اختیار داشتن گروه تنظیمات سناریو اول، می‌توانند آن‌ها را بر اساس شرایط موجود مورد اصلاح قرار دهند و بهره‌برداری کنند. البته در صورت نامناسب بودن تنظیمات و عدم هماهنگی، روش پیشنهادی همانطور که در سناریوی اول بیان شد باید مورد استفاده قرار گیرد. به این ترتیب در این سناریو ابتدا سعی می‌شود که هماهنگی را با اصلاح زمان عملکرد از طریق تنظیمات برقرار نماییم و درصورت عدم موفقیت، الگوریتم پیشنهادی را اجرا می‌کنیم.

ابتدا فرض عدم وجود واحدهای DG در شبکه در نظر گرفته می‌شود. با توجه به این که ماکزیمم جریان خطا IED2.2 برابر با ۳۸۲۶ آمپر می‌باشد، تنظیم قبلی IED2.1 که در محدوده [۳۸۲۶-۱۶۹۵] تعیین شده بود، برای پشتیبانی IED2.2 مناسب نیست. از طرف دیگر با توجه به این که IED2.1 باید با IED1.4 هماهنگ باشد، تنظیم جدید IED2.1 نیز باید نیازهای هر دو ناحیه ۶ و ۳ را مرتفع نماید.

در چنین شرایطی با اصلاح TMS و Ipickup از رابطه (۱) نمی‌توان مشکل عدم هماهنگی را به تنهایی برطرف نمود. به این منظور که در کنار این پارامترها نوع منحنی مشخصه نیز باید تغییر یابد. بر این اساس برای IED2.2 منحنی مشخصه به "خیلی معکوس" تغییر می‌یابد، در حالی که تنظیمات جدید شامل TMS و Ipickup به ترتیب ۰/۰۵ ثانیه و ۱۶۲/۵ آمپر هستند. همچنین IED1.4 یک منحنی مشخصه "بسیار معکوس" با ۰/۱۸ ثانیه و ۱۵۹ آمپر به ترتیب برای TMS و Ipickup، را دارا می‌باشد. به دلیل این که انتظار می‌رود IED2.1، از هر دو IED2.2 و IED1.4 پشتیبانی کند، در ۰/۰۵ ثانیه، ۱۶۱/۵ آمپر و همچنین منحنی مشخصه "طولانی معکوس" تنظیم خواهد شد. هماهنگی میان این دستگاه‌ها برای مقادیر به روز شده در حداقل و حداکثر جریان خطا در شکل (۱۳) نشان داده شده است.

با توجه به اینکه اصلاح تنظیمات توسط عامل، در شرایط نفوذ صفر انجام شده است، باید نسبت به حداکثر نفوذ نیز مورد ارزیابی قرار گیرد تا در مورد اینکه نیاز به استفاده از گروه تنظیمات از پیش تعریف شده می‌باشد یا خیر تصمیم‌گیری شود. به همین منظور ابتدا فرض می‌شود که DG2 و DG3 به شبکه متصل هستند و به طور ناگهانی یک خطا در ناحیه تحت حافظت IED2.2 اتفاق افتاده است. در این شرایط، جریان عبوری از IED2.2، ۴۶۷۱ آمپر می‌باشد در حالیکه IED2.1، ۳۱۴۲ آمپر را رویت می‌نماید. به هر حال با توجه به شکل (۱۳) این مقدار تغییر میان IED اصلی و پشتیبان توانایی ایجاد ناهماهنگی را ندارد.

برای بررسی دقیق‌تر سیستم حفاظت، IED3.1 و IED3.2 به ترتیب مسئول ناحیه‌های دوم و چهارم هستند. این IEDها، به عنوان دستگاه‌های حفاظتی فیدر بار در نظر گرفته شده‌اند و در لحظه خطا عملکرد مشابهی را دارند. بر این اساس به محض تشخیص اضافه جریان در پایین دست خود، پیام "GOOSE lockout" را برای سایر IEDها ارسال می‌کنند و پس از طی یک تأخیر بسیار کوتاه ثابت (۲۰ میلی‌ثانیه)، جداسازی خطا را انجام خواهند داد. در این موقعیت، تغییر تنظیمات ضروری نیست و شبکه نیز بدون نیاز به هیچ بازپیکربندی به عملکرد خود ادامه می‌دهد.




**شکل (۱۳) حفظ هماهنگی میان IED2.1، IED2.2 و IED1.4 در سناریو سوم**

طرح‌های خود ترمیمی در شبکه‌های توزیع به عنوان مکان‌یابی خطا، جداسازی و بازگردانی سرویس بیان می‌شوند. بر این اساس همانطور که در سناریوهای مختلف نشان داده شد طرح پیشنهادی این مقاله نیز با ارائه یک عملکرد خود ترمیمی هوشمند، وظایف حیاتی سیستم حفاظت را به درستی در معرض نمایش قرار می‌دهد. به منظور بیان جزئیات بیشتر، ساختار سیستم حفاظت پیشنهادی به نوعی طراحی شده است که در مقایسه با مرجع [۲۸]، کاملاً مستقل از واحد کنترل مرکزی می‌باشد. همچنین در این ساختار شناسایی مکان دقیق برخی نقاط خطا امکان‌پذیر است. قابلیت مذکور بر اساس جهت IEDها در رویت یا عدم رویت خطا اجرا می‌شود. مثلاً در صورتی که IED1.1 و IED1.4 اضافه جریان خطا را مشاهده کنند، در حالی‌که هر دو IED1.2 و IED1.3 هیچ اضافه جریانی را تشخیص ندهند، مکان دقیق خطا باس ۴ شبکه شناسایی می‌شود. همچنین چنانچه IED1.3 جریان خطا را تشخیص دهد در حالی که هر دو IED1.4 و IED3.2 هیچ اضافه جریانی را رویت نکنند، نقطه خطا دقیقاً بر باس ۱۱ شبکه مکان‌یابی خواهد شد. به این ترتیب مطابق با منحنی مشخصه IEDها در سناریوهای مطرح شده، فرآیندهای حفاظتی از طریق توابع حفاظتی و گره‌های منطقی مربوطه در یک ساختار غیرمتمرکز مبتنی بر عامل به خوبی اجرا خواهد شد.

## ۵- نتیجه‌گیری

حضور DGهای تجدیدپذیر در شبکه‌های توزیع و سطح نفوذ متغیر آن‌ها، باعث می‌شود که عامل‌ها نسبت به آن‌ها با تصحیح یا حداقل بررسی گروه تنظیمات کنونی واکنش نشان دهند. در نتیجه این ارتباطات بیشمار در یک ساختار MAS، احتمال تأخیر یا خرابی در برقراری ارتباطات را به دنبال دارند که وظایف حیاتی سیستم حفاظتی در رفع خطا و حفظ هماهنگی را تحت تاثیر قرار خواهند داد. بر این اساس این مقاله یک روش هماهنگی حفاظتی هوشمند را در یک ساختار غیرمتمرکز برای حل چنین مشکلی که سیستم حفاظت مبتنی بر MAS با آن روبه‌رو است پیشنهاد می‌دهد. به این ترتیب، ابتدا با بازبینی ساختار کنترل و ارتباطات MAS متداول، دقیقاً بیان می‌شود که چطور MAS ممکن است توانایی حفاظت از سیستم را به طور موثر نداشته باشد. سپس با توجه به ویژگی‌های یک راه حل مناسب، الگوریتمی برای حل مسأله با استفاده از IEDها و سرویس‌های استاندارد IEC-61850 به منظور انجام توابع سطح کنترل اول و دوم یک سیستم حفاظت مبتنی بر MAS، در یک تک سطح کنترل جهت کاهش حجم ارتباطات ارائه می‌شود. همچنین یک الگوریتم مستقل از نفوذ DG با استفاده از قابلیت‌های پیام GOOSE بیان شده است تا سیستم را در برابر هر رویداد غیرقابل پیشبینی، با کمترین تأخیر پشتیبانی نماید. با توجه به اهمیت پاکسازی خطا و احتمال تأخیر ارتباطات در شبکه‌های توزیع با حضور منابع تجدیدپذیر، چنین الگوریتم کمکی سریع و کارآمدی، توانایی پوشش موفقیت‌آمیز هر سطح نفوذی را دارا می‌باشد و افزایش قابلیت اطمینان سیستم را به دنبال دارد.

## مراجع


[1] B. Fani, H. Bisheh, and I. Sadeghkhani, “Protection coordination scheme for distribution networks with high penetration of photovoltaic generators”, *IET Generation, Transmission & Distribution*, vol. 12, no. 8, pp. 1802-1814, March. 2018, doi: 10.1049/iet-gtd.2017.1229.

[2] S. F. Zarei, H. Mokhtari and F. Blaabjerg, "Fault Detection and Protection Strategy for Islanded Inverter-Based Microgrids," in IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 9, no. 1, pp. 472-484, Feb. 2021, doi: 10.1109/JESTPE.2019.2962245.

[3] M. Tariq, K. Khatri, M. I. U. Haque, M. A. Raza, S, Ahmed and M. Muzammil, “Investigation of the Effects of Distributed Generation on Protection Coordination in a Power System”, Engineering, Technology and Applied Science Research, vol. 11, no. 5, pp. 7628-7634, Oct. 2021, doi: 10.48084/etasr.4338.

[4] H. Bisheh, B. Fani and G. Shahgholian, “A novel adaptive protection coordination scheme for radial distribution networks in the presence of distributed generation”, *International Transactions on Electrical Energy Systems*, vol. 31, no. 3, Jan. 2021, doi: 10.1002/2050-7038.12779.

[5] S. B. Naderi, M. Negnevitsky, A. Jalilian, M. Hagh and K. Muttaqi, “Optimum Resistive Type Fault Current Limiter: An Efficient Solution to Achieve Maximum Fault Ride-through Capability of Fixed Speed Wind Turbines during Symmetrical and Asymmetrical Grid Faults”, *IEEE Transactions on Industry Applications*, vol. 53, no. 1, pp. 538-548, Jan-Feb, 2017, doi: 10.1109/TIA.2016.2611665.

[6] Q. Zeng, Z. Zhang, M. Xu, J. Zhu, T. Chi and T. Wei, “A coordinated relay protection strategy of distribution network based on fault current limiting”, *E*nergy *Reports*, vol. 8, no. 13, pp. 380-387, Nov. 2022, doi: 10.1016/j.egyr.2022.08.036.

[7] S. F. Zarei and S. Khankalantary, “Protection of active distribution networks with conventional and inverter-based distributed generators”, *International Journal of Electrical Power & Energy Systems*, vol. 129, July. 2021, doi: 10.1016/j.ijepes.2020.106746.

[8] 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, doi: 10.1049/iet-rpg.2019.0996.

[9] H. A. Abdel-Ghany, A. M. Azmy, N.I. Elkalashy and E. M. Rashad, “Optimizing DG penetration in distribution networks concerning protection schemes and technical impact”, *Electric Power Systems Research*, vol. 128, pp. 113-122, Nov. 2015, doi: 10.1016/j.epsr.2015.07.005.

[10] M. A. Gaber, R. A. El-Sehiemy, T. F. Megahed, Y. Ebihara and S. M. Abdelkader, “Optimal settings of multiple inverter-based distributed generation for restoring coordination of DOCRs in mesh distribution networks”, *Electric Power System Research*, vol. 213, Dec. 2022, doi: 10.1016/j.epsr.2022.108757.

[11] S. Conti, “Analysis of distribution network protection issues in presence of dispersed generation”, *Electric Power Systems Research*, vol. 79, no. 1, pp. 49-56, Jan. 2009, doi: 10.1016/j.epsr.2008.05.002.

[12] 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, doi: 10.1109/ECTICon.2012.6254264.

[13] L. F. D. F. Gutierres, L. Mariotto, G. Cardoso and F. Loose, “Recloser-fuse coordination protection for inverter-based distributed generation systems”, *IEEE, 50th International Universities Power Engineering Confrence (UPEC)*, pp. 1-6, Sept. 2015, Doi: 10.1109/UPEC.2015.7339778.

[14] M. Singh, T. Vishnuvardhan and S. G. Srivani, “Adaptive protection coordination scheme for power networks under penetration of distributed energy resources”, *IET Generation, Transmission & Distribution*, vol. 10, pp. 3919-3929, Nov. 2016, doi: 10.1049/iet-gtd.2016.0614.

[15] P. Dorosti, M. Moazzami, B. Fani and P. Siano, “An adaptive protection coordination scheme for microgrids with optimum PV resources”, *Journal of Cleaner Production*, vol. 340, pp. 130723, March 2022, doi: 10.1016/j.clepro.2022.130723.

[16] A. Abbasi, H. KazemiKargar and T. SoleymaniAghdam, “Adaptive Protection Coordination with Setting Groups Allocation”, *International Journal of Renewable Energy Research*, vol. 9, no. 2, pp. 1-9, April 2019, doi: :10.20580/ijrer.v9i2.9266.g7647.

[17] A. Ataee-Kachoee, H. Hashemi-Dezaki and A. Ketabi, “Optimized adaptive protection coordination of microgrids by dual-setting directional overcurrent relays considering different topologies based on limited independent relays' setting groups”, *Electric Power Systems Research*, vol. 214, no. 6, Jan 2023, doi: 10.1016/j.epsr.2022.108879.

[18] M. Yousaf, A. Jalilian, K. M. Muttaqi and D. Sutanto “An Adaptive Overcurrent Protection Scheme for Dual-Setting Directional Recloser and Fuse Coordination in Unbalanced Distribution Networks With Distributed Generation”, *IEEE Transactions on Industry Applications*, vol. 58, no. 2, pp. 1831-1842, March 2022, doi: 10.1109/TIA.2022.3146095.

[19] A. H. El-Hamrawy, A. A. M. Ebrahiem and A. I. Meghdad, “Improved Adaptive Protection Scheme Based Combined Centralized/Decentralized Communications for Power Systems Equipped With Distributed Generation”, *IEEE ACCESS*, vol. 10, pp. 97061-97074, Jan. 2022, doi: 10.1109/ACCESS.2022.3205312

[20] S. F. Zarei, and M. Parniani. “A comprehensive digital protection scheme for low-voltage microgrids with inverter-based and conventional distributed generations”, IEEE Transactions on Power Delivery 32.1 (2016): 441-452.

[21] M. Hojjati, M. Tavoosi, M. R. Yousefi, G. Shahgholian and A. R. Seifi, “MAS based intelligent protection coordination scheme for distribution network with distributed generation”, *Technovations in Electrical Engineering & Green Energy System*, vol. 1, no. 2, pp. 45-62, July. 2022, doi: 10.30486/teeges.2022.1960240.1018.

[22] E. Abbaspour, B. Fani, E. Heydarian-Forushani, & A. Al-Sumaiti, (2022). "A multi-agent based protection in distribution networks including distributed generations", Energy Reports, 8, 163-174.

[23] D. Alibeigi, E. Abbaspour, B. Fani and H. Samet, "An Intelligent Multi-Agent Based Approach For Protecting Distribution Networks", *Technovations in Electrical Engineering & Green Energy System*, vol. 1, no. 1, pp. 36-62, June. 2022, doi: 10.30486/teeges.2022.691104.

[24] A. Zidan and E. El-Saadany, "A cooperative multiagent framework for self-healing mechanisms in distribution system", *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1525-1539, Sept. 2012, doi: 10.1109/TSG.2012.2198247.

[25] P. Peidaee, A. Kalam and J. Shi, "Integration of a Heuristic Multi-Agent Protection System into a Distribution Network Interconnected with Distributed Generation", *Energies*, vol. 13, no. 20, pp. 1-25, Oct. 2020, doi: 10.3390/en13205250.

[26] 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", *IEEE Transactions on Industry Applications*, vol. 46, no. 5, pp. 2118-2124, Oct. 2010, doi: 10.1109/TIA.2010.2059492.

[27] E. Abbaspour, B. Fani and E. Heydarian-Foroushani, "A bi-level multi agent based protection scheme for distribution networks with distributed generation", *International Journal of Electrical Power & Energy Systems*, vol. 112, pp. 209-220, Nov. 2019, doi: 10.1016/j.ijepes.2019.05.001.

[28] 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, doi: 10.1109/TPWRD.2016.2585579.

[29] 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, doi: 10.1109/TIE.2011.2167891.

[30] A. Manickam, S. Kamalasadan, D. Edwards and S. Simmons, "A novel self-evolving intelligent multiagent framework for power system control and protection", *IEEE Systems Journal*, vol. 8, no. 4, pp.1086-1095, Dec. 2014, doi: 10.1109/JSYST.2013.2269731.

[31] Z. Zhu, B. Xu, Ch. Brunner, T. Yip and Y. Chen, "IEC 61850 Configuration Solution to Distributed Intelligence in Distribution Grid Automation", *Energies*, vol. 10, no. 4, pp. 1-17, April. 2017, doi: 10.3390/en10040528.

[32] T. Strasser, F. Andren, J. Kathan, C. Cecati, C. Buccella, P. Siano, P. Leitao, G. Zhabelova, V. Vyatkin, P. Vrba and V. Marik, "A Review of Architectures and Concepts for Intelligence in Future Electric Energy Systems", *IEEE Transactions on Industrial Electronics*, vol. 62, no. 4, pp. 2424-2438, April 2015, doi: 10.1109/TIE.2014.2361486.

[33] H. Lei, C. Singh and A. Sprintson , "Reliability Modeling and Analysis of IEC 61850 Based Substation Protection Systems", *IEEE Transactions on Smart Grid*, vol. 5, no. 5, pp. 2194-2202, Sept. 2014, doi: 10.1109/TSG.2014.2314616.

[34] M. G. Maleki, H. Javadi, M. Khederzadeh, M. Bayrami and S. Farajzadeh, "Data Exchange Standardization in a Microgrid Protection Scheme According to the IEC 61850", *IEEE Smart Grid Conference (SGC)*, pp. 130-137, Dec. 2015, doi: 10.1109/SGC.2015.7857422.

[35] Communication networks and systems for power utility automation – Part7–4: Basic communication structure – Compatible logical node classes and data object classes, IEC61850, *International Electrotechnical Commission*, 2010.

[36] P. Jamborsalamati, A. Sadu, F. Ponci and A. Monti, "Design implementation and real-time testing of an IEC 61850 based FLISR algorithm for smart distribution grids", *IEEE, Applied Measurements for Power Systems (AMPS)*, pp. 114-119, Nov. 2015, doi: 10.1109/AMPS.2015.7312748.

[37] C. Kriger, S. Behardien and J-C Retonda-Modiya, "A detailed analysis of the GOOSE message structure in an IEC 61850 standard-based substation automation system", *International Journal of Computers Communications & Control*, vol. 8, no. 5, pp. 708-721, Oct. 2013, doi: 10.15837/IJCCC.2013.5.329.

[38] P. Ledesma, P. Jafari, S. Repo, A. Alvarez, F. Ramos, D. D. Giustina and A. Dede, "Event-Based Simulation of a Decentralized Protection System Based on Secured GOOSE Message", *Energies*, vol. 13. No. 12, pp. 1-17, June. 2020, doi: 10.3390/en13123250.

## زیرنویس‌ها

[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] Load Agent

[10] International Electrotechnical Commission

[11] Physical Device

[12] Logical Node

[13] Data Object

[14] Protection Time Over Current

[15] Transformer Active Curve Characteristic

[16] Start Value

[17] Time Dial Multiplier

[18] Logical Device

[19] Data Attribute

[20] Circuit Breaker

[21] Status Value

[22] Generic Object Oriented Substation Event

[23] Coordination Time Interval

[24] Synchronism Check