DOI: 10.20998/EREE.2025.1(10).334222

УДК 621.316.925

ДАНИЛЬЧЕНКО ДМИТРО ОЛЕКСІЙОВИЧ – кандидат технічних наук, доцент, старший дослідник, професор кафедри передачі електричної енергії, Національний технічний університет «Харківський політехнічний інститут»; м. Харків, Україна; ORCID: https://orcid.org/0000-0001-7912-1849; e-mail: dmytro.danylchenko@khpi.edu.ua

ЦЮПА ВЛАДИСЛАВ МИКОЛАЙОВИЧ ✉ – аспірант кафедри передачі електричної енергії, Національний технічний університет «Харківський політехнічний інститут»; м. Харків, Україна; ORCID: https://orcid.org/0000-0002-4269-1941; e-mail: vladyslav.tsiupa@ieee.khpi.edu.ua.

СПОСІБ РЕАЛІЗАЦІЇ ЦИФРОВІЗАЦІЇ РЕЛЕЙНОГО ЗАХИСТУ ТА АВТОМАТИКИ ДЛЯ ЕЛЕКТРОЕНЕРГЕТИЧНИХ ОБ'ЄКТІВ РОЗПОДІЛЕННЯ З НАПРУГОЮ 6-10 КВ

У статті представлено нову концепцію проектування централізованої багатоканальної системи управління середньовольтовими розподільними пристроями, основна інновація якої полягає в інтеграції алгоритмів первинної та резервної релейної захисту в обчислювальну інфраструктуру підстанції, а саме в резервний або дублюючий серверний блок, відомий як Front-End Controller. Ця архітектура спрямована на підвищення економічної ефективності та практичної експлуатації рішень з релейного захисту та автоматизації для енергетичних компаній та операторів електромереж. Запропонований підхід особливо застосовний до найпоширеніших типів розподільних мереж середньої напруги, а також до систем електропостачання на промислових підприємствах. Завдяки переміщенню логіки захисту з розподілених апаратних реле до центрального обчислювального вузла, система забезпечує більш гнучке впровадження сучасних адаптивних алгоритмів релейного захисту та автоматизації, що полегшує їх інтеграцію в сучасну енергетичну інфраструктуру. Крім того, це рішення сприяє впровадженню технологій, що відповідають стандарту IEC 61850, забезпечуючи взаємодію та стандартизацію між системами автоматизації. У статті наведено детальну оцінку надійності та експлуатаційних характеристик запропонованої централізованої системи релейного захисту та автоматизації, яка призначена для виконання всіх основних функцій захисту середньовольтних розподільних пристроїв, включаючи захист ліній та шин. Крім того, в роботі описано архітектуру системи управління, охарактеризовано її основні компоненти та оцінено продуктивність центрального контролера. Показано, що обчислювальні вимоги такого контролера для типової розподільної підстанції середньої напруги залишаються в межах діапазону продуктивності сучасних контролерів, сумісних з SCADA, що постачаються провідними виробниками автоматики в електроенергетичному секторі. Результати підкреслюють доцільність переходу до централізованих архітектур захисту без шкоди для функціональної цілісності або швидкості реагування системи.

Ключові слова: релейний захист та автоматизація; автоматизовані системи керування технічним процесом; захист підстанцій; підвищення надійності систем електропостачання; перехідні процеси; алгоритми адаптації; інтелектуальні мережі.

Вступ. В сучасних реаліях розвитку енергетичної галузі, фахівці електроенергетики активно обговорюють проблеми та перспективи цифровізації пристроїв і систем релейного захисту та автоматики, можливості їх об’єднання. Це стосується як функцій релейного захисту та автоматики, так і функцій різних систем автоматики в електроенергетиці в єдиній системі або в комбінації мікропроцесорних пристроїв [1] (інтелектуальних електронних пристроїв), а також створення та практичного використання технологій, які були створені або розроблені в рамках міжнародного стандарту «цифрових підстанцій та мереж» [2, 3].

Слід зазначити, що розподільчі пункти та підстанції середньої напруги є одними з найбільш поширених і важливих енергетичних об’єктів, але фактично вони позбавлені більшості інновацій, пов’язаних з технологіями інтелектуальних мереж. Це пов’язано з надзвичайно високою вартістю більшості рішень в рамках концепції «розумних мереж», а також з неоптимальними або надлишковими вимогами міжнародного стандарту IEC 61850 при побудові цифрових підстанцій в розподільчих мережах середньої напруги.

Навіть сучасний традиційний підхід до розгортання в розподільчих мережах середньої напруги систем релейного захисту та автоматики, різноманітних автоматизованих систем в електроенергетиці не є прийнятним через високу вартість обладнання, монтажних та пусконалагоджувальних робіт, причому такі витрати як мінімум співставні з вартістю основного обладнання середньої напруги, а часто перевищують її.

Одним із шляхів мінімізації витрат на створення повноцінної системи релейного захисту та автоматики, автоматизованих систем в електроенергетиці є відмова від їх побудови як набору окремих термінальних пристроїв обчислювальної техніки та засобів зв’язку і об’єднання всіх необхідних функцій в єдину систему, яка повинна бути виконана на мікропроцесорній елементній базі [4]. Обчислювальна потужність та об’єм пам’яті сучасних моделей мікропроцесорів дозволяє реалізовувати досить складні алгоритми релейного захисту, автоматики та вимірювань, а необхідна надійність досягається дублюванням функцій в програмному та апаратному забезпеченні. Такий підхід дозволить впровадити багато ефективних рішень в рамках технології інтелектуальних мереж та стандарту IEC 61850, а також мінімізувати фінансові та часові витрати. Це стосується все ще обмеженої можливості застосування найсучасніших адаптивних алгоритмів захисту та автоматики в розподільчих пунктах та підстанціях середньої напруги, включаючи елементи штучного інтелекту [5], а також системи безперервного моніторингу та діагностики [6].

Мета статті. Розвиток і модернізація релейного захисту та автоматики, систем автоматики в Україні і за кордоном призвели до появи таких термінів, як

Конфлікт інтересів: Автори заявили про відсутність конфлікту

«цифрова підстанція», «адаптивний алгоритм безпеки», «розумні мережі» тощо.

Літературний огляд. Аналіз літературних джерел показав, що сьогодні багато уваги приділяється інноваціям, у тому числі цифровим системам станцій і підстанцій релейного захисту та автоматики [7–9].

Поштовхом до цього став, зокрема стандарт IEC 61850, який визначає вимоги до архітектури побудови систем релейного захисту та автоматики, автоматизованих систем управління, систем обліку та вимірювань в електричних підстанціях та мережах, а також стандартну специфікацію для обміну інформацією, координації та сумісності між застосовуваними мікропроцесорними пристроями різних виробників [10–12].

Незважаючи на привабливість і потенційний ефект багатьох рішень в рамках стандарту IEC 61850, на сьогоднішній день він не знайшов свого належного застосування в розподільчих мережах середньої напруги як в Україні, так і в закордонних компаніях.

Так, на найбільшому і провідному ринку автоматизації в електроенергетиці – в Китаї – до 2020 року було побудовано більше п'яти тисяч цифрових підстанцій, але всі вони представляють класи підстанцій високої і дуже високої напруги [13, 14].

Вирішення проблеми побудови економічних та ефективних систем релейного захисту та автоматики, систем автоматизації в електроенергетиці, а також цифровізації розподільчих мереж середньої напруги лежить в площині пропонованої нами системи централізованого управління розподільчими пристроями середньої напруги з адаптивним алгоритмом релейного захисту та автоматики [15,16].

Дослідження методів створення систем централізованого релейного захисту та автоматики. Важливою частиною робіт у напрямку створення «цифрових підстанцій» є централізована система релейного захисту та автоматики. Одними з основних питань, які необхідно розглянути для створення централізованої системи релейного захисту та автоматики, є:

- Забезпечення надійності роботи централізованого пристрою при зупинках і відмовах обладнання та каналів зв'язку, зокрема за рахунок дублювання.
- Дослідження складу та структури централізованої системи.

Для досягнення цих цілей пропонується перенести логіку релейного захисту та автоматики на центральний сервер, а логіку MU (merging unit) залишити на вихідних лініях:

- Оцифрування аналогових сигналів (блоки ФНЧ, АЦП).
- Керування перемикачами (логічні виходи).
- Інтерфейс (з'єднання з сервером).

Це відповідає блок-схемі, зображеній на рис. 1. У цій централізованій системі вся логіка захисту і автоматики зосереджена в одному пристрої – сервері; важливу роль відіграє лінія зв'язку сервера з розподільником, з його блоками. Важлива роль ліній зв'язку проявляється в тому, що цифрова лінія зв'язку повинна забезпечувати необхідну швидкість, надійність лінії зв'язку впливає на загальну надійність системи з центральним сервером; надійність лінії зв'язку впливає на загальну надійність системи з центральним сервером.

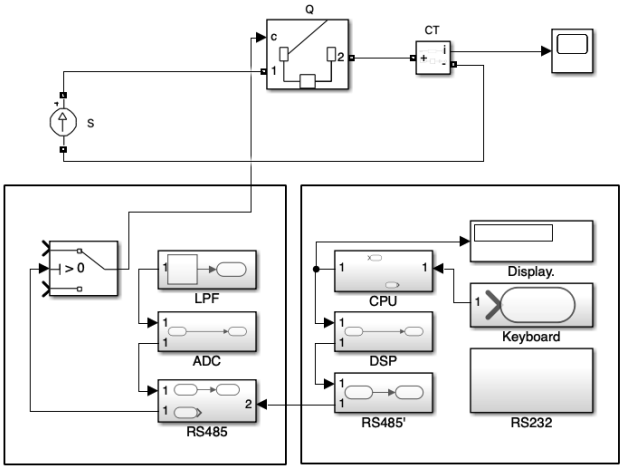

Рисунок 1 – Структурна схема централізованої системи релейного захисту та автоматики:
LPF – фільтр нижніх частот,
ADC – аналого-цифровий перетворювач (АЦП),
RS485 – інтерфейс RS-485,
DSP – цифровий сигнальний процесор,
CPU – центральний процесор

Front-End-Controller (Front End Processor, FEC, FEP) (два робочих і один резервний) – це два контролери, які використовуються в якості центрального сервера.

FEC є основою систем дистанційного керування, систем автоматизації та диспетчерського управління в енергетиці. Додатковий (другий) FEC може працювати в резервному режимі, або може бути налаштований як основний FEC разом з першим, або в програмному режимі «гарячого» резервування, а може бути налаштований як резервний FEC. При цьому підвищується надійність і доступність процесів моніторингу та управління. Це дозволяє змінювати технологічний процес на FEC без переривання керування процесом.

Обидва FEC з'єднані периферійною шиною. Але в останньому випадку тільки один FEC є активним (master) і має повний контроль над картами шини вводу/виводу, а другий FEC – гарячого резерву (slave) – постійно обмінюється інформацією про стан з активним FEC через послідовне або TCP/IP-з'єднання. Арбітр вибирає режим провідний/ведений, який може включити резерв, коли ведучий не функціонує належним чином.

У першому випадку може використовуватися принцип мажоритарної системи, тобто коли факт настання події, що вимагає реакції з боку системи захисту і управління, виявляється шляхом «голосування», і обидві FEC приймають рішення про подальші дії при формуванні або неформуванні двох однакових команд.

Необхідно враховувати відносну надійність комплекту мікропроцесорних терміналів релейного захисту та автоматики і FEC при паралельній конфігурації, коли від однієї шини відходить декілька ліній і кожна лінія захищається одним терміналом. Найпростіша підстанція показана на рис 2. Об'єкти захисту з терміналами захисту (Q) захищають лінію електропередач (P).

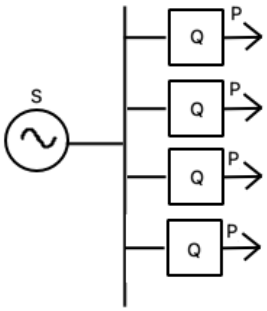

Рисунок 2 – Структурна схема централізованої системи релейного захисту та автоматики:
S – енергосистема,
Q – термінал лінійного захисту,
P – лінія електропередачі

Щоб мати можливість порівняти дві конфігурації, зробимо припущення: ймовірність виходу з ладу терміналів мікропроцесора P і терміналів FEC однакова. Нам також потрібно ввести ймовірність пошкодження X (наприклад, короткого замикання) на лінії живлення. Для паралельної схеми це буде ймовірність пошкодження P ліній, з Q захистами.

При порівнянні терміналів і сервера застосовується наступний метод: ми вибираємо ймовірності, лінійні по X (в цьому випадку ми вважаємо, що $X << 1$), тоді при порівнянні двох систем ми можемо ігнорувати X (відрізати).

Ймовірність відмови захисту від пошкоджень в лінії становить [17]:

$$P \cdot X \tag{1}$$

відповідно, ймовірність того, що відмова лінії захисту не призведе до відмови всієї лінії дорівнює:

$$\left(1 - P_{(\cdot)X}\right). \tag{2}$$

Оскільки всі P ліній незалежні, то ймовірність того, що відмова жодної з n ліній захисту не призведе до відмови всього захисту, дорівнює:

$$\left(1 - P_{(\cdot)X}\right)^n. \tag{3}$$

Таким чином, ми отримуємо ймовірність відмови Y для всього захисту:

$$Y = 1 - \left(1 - P_{(\cdot)X}\right)^n. \tag{4}$$

Лінійна частина:

$$Y = n_{(\cdot)P(\cdot)X} \tag{5}$$

відповідно:

$$Y \sim n \cdot P. \tag{6}$$

Для цієї схеми n буде рівним 4.

Крім виходу з ладу клеми, можливе помилкове спрацьовування клеми (і FEC), коли за відсутності пошкоджень на лінії, клема подає команду на вимикач. Назвемо ймовірність такої події Z за умови, що всі чотири клеми підключені однаково. Тоді для чотирьох терміналів сумарна ймовірність хибної тривоги дорівнює [17]:

$$(1 - (1 - Z)^4) = 4Z - 6Z^2 + 4Z^3 - Z^4. \tag{7}$$

Для двох FEC (у випадку однієї робочої та однієї резервної) пристрій контролю працездатності FEC реагує тільки на наявність певних сигналів від FEC (наприклад, сигналів опитування Ofsted), якщо вони не надходять протягом деякого часу – основна FEC зупиняється, починає роботу резервна FEC. Це буде відбуватися тільки в певних випадках виходу з ладу основної FEC:

- Втрата живлення FEC.
- Вихід з ладу логічної схеми FEC (наприклад: вихід з ладу центрального процесора).

При цьому не будуть виявлені складні типи несправностей, такі як:

- Неправильна логіка роботи FEC (наприклад, опитування Ofsted триває, але логіка захисту не працює).
- Неправильна логіка роботи захисту.

Слід зазначити, що резервування за допомогою трьох і більше FEC в гарячому резерві (коли всі три FEC працюють паралельно і працює більшість системи) дозволяє виявляти і складні види відмов (коли один з FEC не буде працювати як інший FEC), але ці варіанти є більш дорогими і можуть бути економічно доцільними для розподільчих центрів і підстанцій середньої напруги.

Питання надійності в розподільчих центрах та підстанціях середньої напруги можна вирішувати поетапно, збільшуючи складність системи:

- Один FEC.
- Два паралельних (з резервуванням або дублюванням) FEC.

Важливим фактором у системі захисту є використання вищих (вище першої гармоніки 50 Гц) гармонік. В основному, вищі гармоніки використовуються для визначення несправного фідера в мережі з ізольованою нейтраллю: абсолютне значення струму вищих гармонік у пошкодженому фідері буде більшим, ніж у неушкоджених фідерах.

Важливим фактором захисту системи є використання найвищої (вище першої гармоніки 50 Гц) гармоніки захисту. В основному, вищі гармоніки використовуються для визначення несправного фідера в мережі з ізольованою нейтраллю: абсолютне

значення струму вищих гармонік у пошкодженому фідері буде більшим, ніж у непошкоджених фідерах.

Оскільки існують й інші методи визначення пошкодження фідера (наприклад, у пошкодженому фідері амплітуда струмів нульової послідовності буде найбільшою), використання гармонік (і співвідношення фаз) також може здійснюватися поетапно:

- Визначення амплітуди синусоїдальних сигналів за значеннями струмів (без фази синусоїдальних сигналів, без гармонік).
- Визначення амплітуди та фази синусоїдальних сигналів за допомогою перетворення Фур'є (реєстрація фази синусоїдальних сигналів з урахуванням гармонік).

В результаті заплановано три етапи:

- Виділення FEC, метод поточного значення.
- Одинарний FEC, метод перетворення Фур'є.
- Два паралельно працюючих FEC, метод перетворення Фур'є.

Поетапна розробка системи дозволяє поступово набувати досвіду в проектуванні, виготовленні систем і це підвищує ймовірність успішного завершення проекту.

Крім того, три різні за складністю системи допоможуть нам сегментувати ринок: пропонувати різні (за складністю і вартістю) пристрої різним замовникам, відповідно до їх вимог до складу захисту, відповідно до їх вимог до систем надійності. Це охоплює широкий спектр ринку пристроїв захисту та автоматики.

Оціночні вимоги:

1. Єдиний FEC, метод поточного значення. Максимально дешевий варіант з мінімальними вимогами до надійності та структури захисту:

а. Кількість точок дискретизації на період першої гармоніки 50 Гц – 12.

б. Розрядність АЦП – 10.

в. До складу MU (пристрій зв'язку з об'єктом, що знаходиться на кожному фідері) – логічні входи, виходи, 3 аналогових входи, АЦП, інтерфейс RS485 (2400 кбіт/с до 100 м, дві екрановані виті пари).

г. До 30 MU. MU для сигналів струму, MU для сигналів напруги (до 2 штук).

д. FEC: DSP (визначення амплітуд синусоїдальних сигналів, метод поточного значення), процесор логічного захисту і автоматики, 2 інтерфейси RS485 (підключення до БП, зв'язок з рівнем управління), інтерфейс RS232 (або USB) – зв'язок з комп'ютером для конфігурації FEC, лицьова панель.

2) Одинарний FEC, метод перетворення Фур'є. Варіант з мінімальними вимогами до надійності і високими вимогами до складу захистів:

а. Кількість точок дискретизації в періоді першої гармоніки 50 Гц – 40.

б. Розрядність АЦП – 12.

в. До складу MU (виносний модуль, розташований на кожному фідері) – логічні входи, виходи, 3 аналогових входи, тактовий вхід (задає фазу напруги), АЦП, DSP (перетворення Фур'є, що визначає амплітуду і фазу), інтерфейс RS485 (2400 кбіт/с до 100 м, дві екрановані виті пари).

г. До 30 MU. MU для сигналів струму, MU для сигналів напруги (до 2 штук).

д. FEC: процесор логічного захисту і автоматики, 2 інтерфейси RS485 (підключення до БП, зв'язок з рівнем управління), інтерфейс RS232 (або USB) – зв'язок з комп'ютером для конфігурації FEC, передня панель.

3) Два паралельно працюючих FEC, метод перетворення Фур'є. Варіант з підвищеними вимогами до надійності і підвищеними вимогами до складу захистів: кожен FEC пов'язаний з MU окремими лініями:

а. Кількість точок вибірки в періоді першої гармоніки 50 Гц – 40.

б. Розрядність АЦП – 12.

в. До складу MU (виносний модуль, розташований на кожному фідері) - логічні входи, виходи, 3 аналогових входи, вхід синхронізованих сигналів (заданий сигнал часу), АЦП, ЦОС (перетворення Фур'є, визначення амплітуди і Ф-PS), 2 інтерфейси RS485 (2400 кбіт/с до 100 м, дві екрановані виті пари), вбудована система мажоритарного керування.

г. Визначення амплітуд синусоїдальних сигналів – в MU, метод перетворення Фур'є.

д. До 30 MU. MU для сигналів струму, MU для сигналів напруги (до 2 штук).

е. FEC: процесор логічного захисту та автоматики, 2 інтерфейси RS485 (зв'язок з БП, зв'язок з рівнем управління), інтерфейс RS232 (або USB) – зв'язок з комп'ютером для конфігурації FEC, лицьова панель.

Існує проблема низької швидкості передачі даних стандартного модуля через інтерфейс RS485. В результаті, при низькій швидкості, багато (до 30) модулів на спільній шині не зможуть встигати передавати інформацію.

В такому випадку необхідна топологія «зірка» для побудови мережі передачі даних: кожен MU підключається до сервера власною виділеною лінією. Зрозуміло, що таке рішення дорожче: більша довжина кабелю, більша кількість (32) інтерфейсів RS485 для FEC.

У цьому випадку, однак, ми отримуємо:

- Значний виграш у надійності ліній зв'язку: одна несправність лінії вплине лише на один модуль.
- Кожна лінія зв'язку інтерфейсу RS485 буде працювати з меншою швидкістю, що підвищує надійність зв'язку, знижує вартість MU, значно розширює номенклатуру промислових MU (за рахунок зниження вимог до них).

Розрахунок необхідної продуктивності (вимоги до швидкодії) центрального процесора пристрою захисту.

1) Одиночний FEC, метод поточного значення.

У цьому варіанті MU виробляє тільки оцифровку вхідного сигналу (кількість точок дискретизації на період першої гармоніки 50 Гц – 12; розрядність АЦП – 10). Таким чином, на єдиний FEC надходить «сирий», опціонально оброблений цифровий потік, що зменшує

максимальне значення MU (кількість яких може досягати 30, і величина яких суттєво впливає на вартість всього комплексу).

У випадку максимуму, при 30 MU ми отримуємо цифровий потік (без урахування накладних витрат), який є максимальним, порівняно з іншими варіантами:

$$12 \cdot 10 \cdot 30 \cdot 30 = 180000 \text{ біт/с} \quad (8)$$

При цьому максимальне навантаження йде на центральний процесор з визначенням амплітуди синусоїдального сигналу методом поточного значення, який розраховує середньоквадратичне значення за період першої гармоніки (серед 12 точок з 10-бітної розрядності). За час роботи захисту і контролю (час повного циклу перетворення, близько 10 мілісекунд) необхідно (для сигналів одиночних MU, в даному випадку відзначимо, що немає необхідності обчислювати квадратний корінь і ділити на кількість точок):

- 12 операцій множення.
- 11 операцій додавання.

За 30 MU отримуємо 360 множень, 330 операцій додавання. За одну секунду, відповідно, потрібно 36000 множень, 33000 операцій додавання. Якщо припустити, що для цілочисельного множення буде потрібно близько 10 операцій додавання, то мінімальна продуктивність процесора (тільки на визначенні амплітуди синусоїдального сигналу) порядку 400 тис. операцій додавання в секунду. У мережах середньої напруги використовуються прості максимальні і мінімальні захисти, проста логіка автоматики, які практично не створюють серйозного навантаження на центральний процесор. При цьому всі сервіси (обчислювальні), не пов'язані безпосередньо з роботою захистів і управління, лягають на спеціалізовані контролери і розвантажують, таким чином, центральний процесор:

- 2 інтерфейси RS485 (зв'язок з MU, зв'язок з рівнем управління).
- Інтерфейс RS232 (або USB) – для зв'язку з комп'ютером для налаштування FEC.
- Передня панель (алфавітно-цифровий дисплей, світлодіод).

2) Інше розташування опцій.

- Варіант з мінімальними вимогами до надійності і високими вимогами до складу захисту.
- Варіант з підвищеними вимогами до надійності та підвищеними вимогами до складу захистів: кожен FEC пов'язаний з MU окремими лініями.

Основне навантаження по визначенню амплітуди і фази синусоїдального сигналу припадає на FEC (на FEC передається інформація у вигляді амплітуди і фази сигналу).

Тому на FEC передаються тільки навантаження обробки логіки захисту і автоматики, які не створюють великого навантаження на центральний процесор (прості струмові захисти, проста логіка автоматики). [18–20].

Висновки. Сьогодні фінансові та часові витрати промислових підприємств і електромережевих компаній на проектування, впровадження та обслуговування в розподільчих підстанціях середньої напруги традиційних систем релейного захисту та автоматики, систем автоматизації в електроенергетиці є неприйнятними. Більше того, незважаючи на велику кількість енергоблоків в енергосистемі, вони фактично позбавлені більшості інновацій у сфері автоматизації та «цифровізації», які в першу чергу визначені технологіями в частині міжнародного стандарту IEC 61850 «Цифрові підстанції та мережі».

Розроблюваний проект централізованої системи управління розподільчим пристроєм середньої напруги, основною частиною якої є централізована система релейного захисту та автоматики, дозволить вирішити більшість вищезазначених проблем шляхом ліквідації комплексу окремих мікропроцесорних терміналів релейного захисту та автоматики, який був розгорнутий на підстанціях збору та передачі інформації, включаючи комутаційне обладнання, та об'єднання всіх необхідних функцій в централізовану та багатоканальну систему, при цьому на єдиному обчислювальному вузлі застосовано два дубльованих або резервних центральних сервера – FEC/FEP.

Такий підхід вимагає вирішення проблеми забезпечення необхідної надійності системи релейного захисту та автоматики на електростанції середньої напруги та забезпечення необхідного складу і структури централізованої системи, в тому числі з урахуванням нормативних вимог у сфері релейного захисту та автоматики. Авторами виконано оцінку зміни ймовірності відмов та хибних спрацьовувань систем релейного захисту та автоматики за запропонованим підходом у порівнянні з традиційним, коли така система будується як сукупність окремих терміналів для кожного приєднання (комірки) розподільчого пристрою підстанції середньої напруги. В даному варіанті розглядаються два варіанти реалізації більшості систем, коли розглядається розгортання централізованої системи. Оцінка та аналіз показали, що найбільш надійним з точки зору ймовірності відмови всього захисту є варіант двох FEC з мажоритарною системою «1 з 2» (схема «АБО»). Найбільш надійним з точки зору ймовірності хибного спрацьовування системи є варіант двох FEC з мажоритарною системою «2 з 2» (схема «І»). Якщо не враховувати вплив ліній зв'язку, а також аналогових (вимірювальних) кіл на кожному приєднанні, то традиційний варіант побудови систем релейного захисту та автоматики з точки зору ймовірності відмови та хибного спрацьовування знаходиться між двома варіантами, незалежно від випадку, що розглядається. Варіант централізованої системи релейного захисту і автоматики при експлуатації одного об'єктового FEC, хоча і є економічним і цілком прийнятним з точки зору надійності, не дозволяє змінювати FEC без переривання технологічного процесу і є дуже вимогливим до продуктивності центрального процесора. Такий варіант можна розглядати як проміжний для накопичення досвіду

проектування і виготовлення централізованої системи, а також для використання на некритичних електроустановках споживачів.

Варіант централізованої системи з резервуванням одного FEC іншим FEC близький за надійністю до варіанту системи з одним централізованим FEC, оскільки у випадку хибних тривог, як і в більшості випадків відмов, ввімкнення резервного FEC не може відбутися. Таким чином, цей варіант корисний для порівняння з одним FEC лише з точки зору можливості заміни робочого FEC без переривання керування технологічним процесом. Продуктивність центрального сервера системи при будь-якому сценарії її побудови для розподільчої підстанції середньої напруги (до 30 приєднань) не перевищує продуктивності сучасних контролерів FEC/FEP, і може бути легко досягнута з використанням контролерів SCADA, які представлені на ринку автоматизації в енергетиці.

Список літератури

1. Possibility of building a data-driven modern power systems / S. Shevchenko et al. *Scientific Papers of Donetsk National Technical University. Series: Electrical and Power Engineering*. 2022. No. 2(27). P. 5–9. DOI: https://doi.org/10.31474/2074-2630-2022-2-5-9.
2. ДСТУ IEC 61850-5:2019. Комунікаційні мережі та системи для автоматизації електроенергетичних підприємств. Частина 5. Технічні вимоги до функцій і моделей приладів (IEC 61850-5:2013, IDT). На заміну ДСТУ IEC 61850-5:2014 ; чинний від 2020-10-01. Вид. офіц.
3. Danylchenko D., Potryvai A., Tsiupa V. Implementation of digital remote line protection in Java language. *2023 IEEE 5th International Conference on Modern Electrical and Energy System (MEES)*, Kremenchuk, Ukraine, 27–30 September 2023. DOI: https://doi.org/10.1109/mees61502.2023.10402459.
4. Loukkalahti M., Majer K., Valtari J. Experiences on the Kalasatama Digital Substation. *Protection, Automation&Control World Confeerence 2024 (PACW 2024)*, Athens, 17–20 June 2024.
5. Power quality impact and its assessment: A review and a survey of Lithuanian industrial companies / V. Liubčuk et al. *Inventions*. 2025. Vol. 10, no. 2. 30. DOI: https://doi.org/10.3390/inventions10020030.
6. Relay protection mirror operation technology based on digital twin / Z. Yao et al. *Protection and control of modern power systems*. 2023. Vol. 8, no. 1. 51. DOI: https://doi.org/10.1186/s41601-023-00328-4.
7. Radimov S. M., Plis V. P. Relay protection devices functionality comparative analysis. *Herald of Advanced Information Technology*. 2023. Vol. 6, no. 3. P. 227–239. DOI: https://doi.org/10.15276/hait.06.2023.15.
8. Данильченко Д. О., Потривай А. Е. Система динамічного прогнозування технічного стану обладнання Об'єднаної електроенергетичної системи. *Вісник Національного технічного університету «ХПІ». Серія: Енергетика: надійність та енергоефективність*. 2023. № 1 (6). С. 16–21. DOI: https://doi.org/10.20998/2224-0349.2023.01.10.
9. Digitalization of protection relay management / M. F. B. Hamdan et al. *2022 IEEE International Conference on Power and Energy (PECon)*, Langkawi, Kedah, Malaysia, 5–6 December 2022. P. 95–98. DOI: https://doi.org/10.1109/pecon54459.2022.9988859.
10. Черкашина В. В., Цюпа В. М. Аналіз алгоритмів роботи диференційного релейного захисту та їх моделювання у середовищі MATLAB. *Вісник Національного технічного університету «ХПІ». Серія: Енергетика: надійність та енергоефективність*. 2023. № 1 (6). С. 113–118. DOI: https://doi.org/10.20998/2224-0349.2023.01.13.
11. Modelling and analysing security threats targeting protective relay operations in digital substations / M. F. Elrawy et al. *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, Venice, Italy, 31 July – 2 August 2023. P. 523–529. DOI: https://doi.org/10.1109/csr57506.2023.10224964.
12. Danylchenko D., Tsiupa V., Mylko V. Digital implementation of relay protection algorithms. Transformer differential protection. *2023 IEEE 4th KhPI Week on Advanced Technology (KhPIWeek)*, Kharkiv, Ukraine, 2–6 October 2023. DOI: https://doi.org/10.1109/khpiweek61412.2023.10312912.
13. Розробка моделей складних схем релейного захисту в програмному комплексі MATLAB / М. В. Петровський та ін. *Вісник Національного технічного університету «ХПІ». Серія: Енергетика: надійність та енергоефективність*. 2023. № 1 (6). С. 58–64. DOI: https://doi.org/10.20998/2224-0349.2023.01.05.
14. Danylchenko D., Potryvai A., Mazur M. System for Prediction of the Technical Condition of Electric Power Equipment. *2023 IEEE 4th KhPI Week on Advanced Technology (KhPIWeek)*, Kharkiv, Ukraine, 2–6 October 2023. DOI: https://doi.org/10.1109/khpiweek61412.2023.10312919.
15. Cyberattacks on power systems / A. Presekal et al. *Smart Cyber-Physical Power Systems*. 2025. Vol. 1 : Fundamental Concepts, Challenges, and Solutions. P. 365–403.
16. Розробка моделей струмових реле та реле напрямку потужності в програмному комплексі MATLAB / М. В. Петровський та ін. *Вісник Національного технічного університету «ХПІ». Серія: Енергетика: надійність та енергоефективність*. 2023. № 1 (6). С. 51–57. DOI: https://doi.org/10.20998/2224-0349.2023.01.04.
17. Operation monitoring platform of relay protection equipment at distribution network side under the background of new power system / Q. Li et al. *Energy Informatics*. 2024. Vol. 7, no. 1. 145. DOI: https://doi.org/10.1186/s42162-024-00440-1.
18. Моделювання напрямленого дистанційного захисту лінії електропередач в програмному комплексі PSCAD\EMTDC / В. В. Волохін та ін. *Вісник Національного технічного університету «ХПІ». Серія: Енергетика: надійність та енергоефективність*. 2016. № 3 (1175). С. 36–42.
19. Abilzhanova F., Bulatbaev F., Kuanyshtaeva A. Development of a method for reliability assessment of distribution power networks up to 110 kV. *Eastern-European Journal of Enterprise Technologies*. 2025. Vol. 1, no. 8 (133). P. 15–23. DOI: https://doi.org/10.15587/1729-4061.2025.322920.
20. Analysis of false data injection attacks against automated control for parallel generators in IEC 61850-based smart grid systems / M. M. Roomi et al. *IEEE Systems Journal*. 2023. Vol. 17, no. 3. P. 4603–4614. DOI: https://doi.org/10.1109/jsyst.2023.3236951.

References

1. S. Shevchenko, V. Tsiupa, D. Danylchenko, and A. Potryvai, "Possibility of building a data-driven modern power systems", *Scientific Papers of Donetsk National Technical University. Series: Electrical and Power Engineering*, no. 2(27), pp. 5–9, Nov. 2022, doi: https://doi.org/10.31474/2074-2630-2022-2-5-9
2. *Communication Networks and Systems for Power Utility Automation. Part 5: Communication Requirements for Functions and Device Models (IEC 61850- 5:2013IDT)*, DSTU IEC 61850-5:2019Tekhnichnyi komitet standartyzatsii «Keruvannia enerhetychnymy systemamy ta poviazani z nym protsesy informatsiinoi vzaiemodii» (TK 162) [Technical Committee for Standardisation "Energy Systems Management and Related Information Interaction Processes" (TC 162)]. (in Ukrainian)
3. D. Danylchenko, A. Potryvai, and V. Tsiupa, "Implementation of digital remote line protection in Java language", in *2023 IEEE 5th International Conference on Modern Electrical and Energy System (MEES)*, Kremenchuk, Ukraine, Sep. 27–30, 2023. IEEE, 2023, doi: https://doi.org/10.1109/mees61502.2023.10402459
4. M. Loukkalahti, K. Majer, and J. Valtari, "Experiences on the Kalasatama Digital Substation", in *Protection, Automation&Control World Confeerence 2024 (PACW 2024)*, Athens, Greece, Jun. 17–20, 2024.
5. V. Liubčuk, V. Radziukynas, G. Kairaitis, and D. Naujokaitis, "Power quality impact and its assessment: A review and A survey of lithuanian industrial companies", *Inventions*, vol. 10, no. 2, Apr. 2025, Art. no. 30, doi: https://doi.org/10.3390/inventions10020030
6. Z. Yao, D. Li, Z. Li, P. Zhou, and L. Li, "Relay protection mirror operation technology based on digital twin", *Protection and Control of Modern Power Systems*, vol. 8, no. 1, Oct. 2023, Art. no. 51, doi: https://doi.org/10.1186/s41601-023-00328-4

7. S. M. Radimov and V. P. Plis, “Relay protection devices functionality comparative analysis”, *Herald of Advanced Information Technology*, vol. 6, no. 3, pp. 227–239, Oct. 2023, doi: https://doi.org/10.15276/hait.06.2023.15
8. D. Danylchenko and A. Potryvai, “System for dynamic prediction of the technical condition of the equipment of a combined electric power system”, *Bulletin of the National Technical University "KhPI". Series: Energy: Reliability and Energy Efficiency*, no. 1 (6), pp. 16–21, Jul. 2023, doi: https://doi.org/10.20998/2224-0349.2023.01.10 (in Ukrainian)
9. M. F. B. Hamdan, W. U. Bt Wan Nowalid, M. T. B. Iskandar, A. F. B. M. Kamal, M. F. B. A. Rahman, and F. B. Shafe'i, “Digitalization of protection relay management”, in *2022 IEEE International Conference on Power and Energy (PECon)*, Langkawi, Kedah, Malaysia, Dec. 5–6, 2022. IEEE, 2022, pp. 95–98, doi: https://doi.org/10.1109/pecon54459.2022.9988859
10. V. Cherkashyna and V. Tsyupa, “Analysis of differential relay protection algorithms and their modelling in MATLAB”, *Bulletin of the National Technical University "KhPI". Series: Energy: Reliability and Energy Efficiency*, no. 1 (6), pp. 113–118, Jul. 2023, doi: https://doi.org/10.20998/2224-0349.2023.01.13 (in Ukrainian)
11. M. F. Elrawy, L. Hadjidemetriou, C. Laoudias, and M. K. Michael, “Modelling and analysing security threats targeting protective relay operations in digital substations”, in *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, Venice, Italy, Jul. 31–Aug. 2, 2023. IEEE, 2023, pp. 523–529, doi: https://doi.org/10.1109/csr57506.2023.10224964
12. D. Danylchenko, V. Tsiupa, and V. Mylko, “Digital implementation of relay protection algorithms. Transformer differential protection”, in *2023 IEEE 4th KhPI Week on Advanced Technology (KhPIWeek)*, Kharkiv, Ukraine, Oct. 2–6, 2023. IEEE, 2023, doi: https://doi.org/10.1109/khpiweek61412.2023.10312912
13. M. V. Petrovskyi, I. O. Kramskyi, I. M. Diahovchenko, S. M. Lebedka, and I. I. Borzenkov, “Development of complex relay protection models in the MATLAB software”, *Bulletin of the National Technical University "KhPI". Series: Energy: Reliability and Energy Efficiency*, no. 1 (6), pp. 58–64, Jul. 2023, doi: https://doi.org/10.20998/2224-0349.2023.01.05 (in Ukrainian)
14. D. Danylchenko, A. Potryvai, and M. Mazur, “System for prediction of the technical condition of electric power equipment”, in *2023 IEEE 4th KhPI Week on Advanced Technology (KhPIWeek)*, Kharkiv, Ukraine, Oct. 2–6, 2023. IEEE, 2023, doi: https://doi.org/10.1109/khpiweek61412.2023.10312919
15. A. Presekal, V. S. Rajkumar, A. Ştefanov, K. Pan, and P. Palensky, “Cyberattacks on power systems”, in *Smart Cyber-Physical Power Systems, vol. 1, Fundamental Concepts, Challenges, and Solutions*. Wiley-IEEE Press, 2025, pp. 365–403.
16. M. V. Petrovskyi, I. O. Kramskyi, I. M. Diahovchenko, S. M. Lebedka, and I. I. Borzenkov, “Development of models of current relays and power direction relays in the MATLAB software”, *Bulletin of the National Technical University "KhPI". Series: Energy: Reliability and Energy Efficiency*, no. 1 (6), pp. 51–57, Jul. 2023, doi: https://doi.org/10.20998/2224-0349.2023.01.04 (in Ukrainian)
17. Q. Li, Y. Zhang, Z. Zhang, and Z. Li, “Operation monitoring platform of relay protection equipment at distribution network side under the background of new power system”, *Energy Informatics*, vol. 7, no. 1, Dec. 2024, Art. no. 145, doi: https://doi.org/10.1186/s42162-024-00440-1
18. V. V. Volokhin, M. V. Petrovskyi, S. Yu. Shevchenko, O. O. Ivanov, and O. I. Ihnatova, “Modeliuvannia napriamlenoho dystantsiinoho zakhystu linii elektroperedach v prohramnomu kompleksi PSCAD\EMTDC [Modelling of directional remote protection of power lines in the PSCAD\EMTDC software package]”, *Bulletin of the National Technical University "KhPI". Series: Energy: Reliability and Energy Efficiency*, no. 3 (1175), pp. 36–42, 2016. (in Ukrainian)
19. F. Abilzhanova, F. Bulatbaev, and A. Kuanyshtaeva, “Development of a method for reliability assessment of distribution power networks up to 110 kV”, *Eastern-European Journal of Enterprise Technologies*, vol. 1, no. 8 (133), pp. 15–23, Feb. 2025, doi: https://doi.org/10.15587/1729-4061.2025.322920
20. M. M. Roomi, S. M. S. Hussain, D. Mashima, C. Chang, and T. S. Ustun, “Analysis of false data injection attacks against automated control for parallel generators in IEC 61850-based smart grid systems”, *IEEE Systems Journal*, vol. 17, no. 3, pp. 4603–4614, Feb. 2023, doi: https://doi.org/10.1109/jsyst.2023.3236951

Надійшла (received) 23.06.2025

UDC 621.316.925

DMYTRO DANYLCHENKO – Candidate of Technical Sciences (PhD), Docent, Senior Researcher, Professor of the Department of Electric Power Transmission, National Technical University “Kharkiv Polytechnic Institute”; Kharkiv, Ukraine. Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0001-7912-1849; e-mail: dmytro.danylchenko@khpi.edu.ua

VLADYSLAV TSYUPA ✉ – Postgraduate Student of the Department of Electric Power Transmission, National Technical University “Kharkiv Polytechnic Institute”; Kharkiv, Ukraine. Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0002-4269-1941; e-mail: vladyslav.tsiupa@ieee.khpi.edu.ua.

METHOD OF IMPLEMENTING DIGITISATION OF RELAY PROTECTION AND AUTOMATION FOR POWER DISTRIBUTION FACILITIES WITH A VOLTAGE OF 6-10 KV

The paper presents a new concept for designing a centralized multi-channel control system for medium-voltage switchgear, the main innovation of which is the integration of primary and backup relay protection algorithms into the substation's computing infrastructure, namely, into a backup or redundant server unit known as the Front-End Controller. This architecture is aimed at improving the cost-effectiveness and practical operation of relay protection and automation solutions for energy companies and grid operators. The proposed approach is particularly applicable to the most common types of medium-voltage distribution networks, as well as to power supply systems at industrial enterprises. By moving the protection logic from distributed hardware relays to a central computing node, the system provides a more flexible implementation of modern adaptive relay protection and automation algorithms, which facilitates their integration into modern energy infrastructure. In addition, this solution promotes the implementation of IEC 61850-compliant technologies, ensuring interoperability and standardization between automation systems. The paper presents a detailed evaluation of the reliability and performance characteristics of the proposed centralized relay protection and automation system, which is designed to perform all the main protection functions of medium-voltage switchgear, including line and busbar protection. In addition, the paper describes the architecture of the control system, characterizes its main components, and evaluates the performance of the central controller. It is shown that the computational requirements of such a controller for a typical medium-voltage distribution substation remain within the performance range of modern SCADA-compatible controllers supplied by leading manufacturers of automation in the electric power sector. The results emphasize the feasibility of moving to centralized protection architectures without compromising the functional integrity or responsiveness of the system.

Keywords: relay protection and automation, automated process control systems, substation protection, improving the reliability of the power system, transients, adaptation algorithms, smart grids.