Актуальные проблемы стандартизации в области микропроцессорных устройств релейной защиты

В. И. Гуревич, канд. техн. наук

Введение

Сегодня микропроцессорные устройства релейной защиты (МУРЗ) выпускаются десятками крупнейших мировых компаний, таких как ABB, Siemens, General Electric, Alstom (Areva), SEL, Nari Relays, Beckwith Electric, Schneider Electric, Cooper Power, Orion Italia, VAMP, Woodward и другие, а также многочисленными компаниями в России и Украине (АББ Реле-Чебоксары, НПП «Экра», НПП «Бреслер», ЗАО «ЧЭАЗ», Радиус-Автоматика, Хартрон-Инкор, Киевприбор, РЕЛСiС, РЗА СИСТЕМЗ, Энергомашвин, НТЦ «Механотроника» и др. Все эти устройства отличаются между собой не только алгоритмами действия, что было бы вполне естественно, но и внешними размерами (рис. 1), внутренней конструкцией, программным обеспечением и т. д., т. е. являются абсолютно не взаимозаменяемыми.

Рис. 1. МУРЗ ведущих мировых производителей в корпусах различных типов

А ведь взаимозаменяемость является одним из важнейших параметров изделия, в очень сильной степени влияющим на такой показатель ремонтопригодности, как ***среднее время восстановления*** изделия. С учетом того, что современные МУРЗ выполнены по технологии, не допускающей их ремонта (восстановления) на месте установки силами оперативного персонала, а предусматривают лишь замену целых блоков (модулей), то взаимозаменяемость модулей МУРЗ (а точнее отсутствие такой взаимозаменяемости) отрицательно влияет на ремонтопригодность МУРЗ — один из показателей надежности.

Таким образом, отсутствие унификации блоков (модулей) современных МУРЗ даже одного производителя является фактором, снижающим надежность релейной защиты. И не только надежность. Отсутствие такой унификации является фактором, сдерживающим конкуренцию и повышение качества МУРЗ (поскольку не существует отдельного рынка универсальных модулей, позволяющего выбрать лучшие из них), а также фактором, обусловливающим значительные денежные затраты потребителя, вынужденного приобретать для замены только модули определенного типа и только у одного производителя, пользующегося своим монопольным положением для взвинчивания цен на модули, необходимые для ремонта конкретных типов МУРЗ. А если по истечении 10—12 лет с начала производства производитель вообще прекратит выпуск модулей устаревших типов, то потребителю придется вообще выбросить все МУРЗ и купить новые.

Проблемы терминологии в релейной защите

Рассматривая проблемы стандартизации в области МУРЗ, нельзя не затронуть тему стандартизации терминологии в релейной защите (РЗ) вообще. Как оказалось, не существует даже стандартных определений терминов «релейная защита» и «реле защиты», что позволяет разработчикам и производителям МУРЗ навешивать на них функции, не имеющие никакого отношения к релейной защите. Такая тенденция, получившая широкое распространение в последнее время, вовсе не так безобидна, как это может показаться на первый взгляд. Навешивание большого числа дополнительных функций на МУРЗ,

таких, например, как мониторинг электрооборудования, приводит к усложнению программного интерфейса и алгоритма работы МУРЗ, подключению к нему дополнительных цепей от всевозможных датчиков, увеличению количества ошибок персонала (так называемый «человеческий фактор»), которые даже без дополнительных функций составляют немалую долю в общем количестве неправильных действий РЗ.

В действительности между системами мониторинга электрооборудования и релейной защитой имеется одна очень существенная разница: системы мониторинга не должны отключать электрооборудование, как релейная защита, а должны лишь выдавать обслуживающему персоналу информацию о возникновении потенциальной проблемы. В большинстве случаев лишь человек может оценить целесообразность отключения электрооборудования с учетом важности контролируемого параметра, степени развития нежелательной тенденции и скорости ее развития, выбрать наиболее удобный момент для выведения из эксплуатации этого электрооборудования. Попытка авторов [1,2] придать релейной защите несвойственные ей функции мониторинга электрооборудования и лишь на основании собственных прогнозов осуществлять так называемое «упреждающее» отключение ни к чему хорошему не приведет, так как неоправданное отключение важного электрооборудования в совершенно неподходящее с точки зрения технологического процесса время, когда такое мгновенное отключение вовсе не является обязательным, может привести лишь к значительному экономическому ущербу.

Стандартизация в области терминологии таких понятий, как «реле защиты» и «релейная защита» позволит избежать такого неконтролируемого развития ситуации.

Подробно проблемы терминологии в РЗ описаны в [3] и там же предложены следующие определения терминам:

Реле защиты *— устройство, предназначенное для выявления аварийного режима работы защищаемого объекта и выдачи команды на исполнительный элемент, обеспечивающий прекращение этого режима.*

Система релейной защиты *— совокупность взаимосвязанных устройств, обеспечивающих выявление аварийного режима работы электрооборудования и его прекращение.*

Реле сигнализации *— устройство, предназначенное для выявления ненормального режима работы контролируемого объекта и выдачи тревожного сигнала.*

В связи с использованием в предлагаемых формулировках понятий «ненормальный режим работы» и «аварийный режим работы», необходимо также определиться и с этими понятиями. Для первого из них имеется стандартное определение (ГОСТ 18311 – 80), вполне пригодное для использования в РЗ с небольшим дополнением:

Ненормальным *называется* ***продолжающийся режим работы*** *электротехнического изделия (электротехнического устройства, электрооборудования), при котором значение хотя бы одного из параметров режима выходит за пределы наибольшего или наименьшего допустимого рабочего значения.*

А вот для второго («аварийный режим работы») общего стандартного определения нет, а есть лишь частные определения, «подогнанные» под определенные области техники, в связи с чем, нами было предложено собственное определение:

Аварийным *называется такой ненормальный режим работы оборудования (устройства, системы), при котором дальнейшее его продолжение является недопустимым.*

По нашему мнению, внедрение в практику предлагаемой единой системы определений позволит навести порядок в стандартах, нормативных документах, в учебной литературе, а главное — избежать спекуляций и опасных перекосов в процессе развития реле защиты и релейной защиты при использовании новых технологий.

Стандартизация конструкции и программного обеспечения МУРЗ

Как уже отмечалось выше, отсутствие стандартизации и унификации в области МУРЗ и их функциональных модулей обусловливает снижение надежности релейной защиты и рост затрат на нее. Как показано в [4] никаких принципиально неразрешимых проблем в унификации аппаратной части МУРЗ и программного обеспечения для них сегодня нет. Однако, сегодня, блоки, из которых состоят МУРЗ, далеко не всегда представляют собой отдельные функциональные модули, а часто имеют вид «сборной солянки», когда на одной печатной плате размещены разные функциональные части.

Для реализации идеи универсализации МУРЗ такая конструкция не подходит, поэтому каждая печатная плата будущих МУРЗ должна представлять собой однофункциональный модуль, унифицированный по габаритам, используемым разъемам и протоколам связи с другими модулями. Например: модуль центрального процессора, модуль источника питания, модуль аналоговых входов, модуль логических входов, модуль выходных реле.

При таком конструктивном выполнении МУРЗ на рынке появились бы новые «игроки», одни из которых специализировались бы на выпуске модулей аналоговых входов с трансформаторами тока и напряжения, другие — на выпуске материнской платы, третьи — на модулях логических входов. Например, десятки специализированных компаний, разрабатывающих и производящих сегодня импульсные источники питания, могли бы предложить множество моделей более совершенных и надежных модулей источников питания для МУРЗ. Компании, специализирующиеся на выпуске миниатюрных капсулированных эпоксидным компаундом трансформаторов, могли бы предложить для МУРЗ модули аналоговых входов. Фирмы, разрабатывающие и производящие промышленные контроллеры, могли бы расширить рынок предложения модулей центрального процессора, а некоторые компании, занимающиеся разработкой программного обеспечения, могли бы предложить новые универсальные высококачественные программные интерфейсы, специальные программные модули для отдельных видов зашит.

Потребитель мог бы компоновать свой МУРЗ из модулей различных производителей, точно так, как это происходит сегодня с персональными компьютерами, с учетом стоимости и качества этих модулей. При этом, конечным изделием, на которое распространялись бы гарантии производителей, стали бы функциональные модули МУРЗ, а не терминал в целом, как сейчас, а для проверки исправности отдельных функциональных модулей у потребителя могли бы служить специальные тестовые устройства, которые были бы намного проще и дешевле существующих сегодня тестовых систем для проверки полностью комплектного МУРЗ, производимых компаниями Omicron, Doble, Megger и др.

Как показано в [4], при переходе на модульный принцип в большинстве случаев становятся излишними и корпуса МУРЗ. Отдельные универсальные модули можно было бы монтировать с помощью направляющих с втычными разъемами в специально защищенных от внешних электромагнитных воздействий шкафах различного объема: от небольших подвесных, рассчитанных на два – три МУРЗ, до полногабаритных напольных, предназначенных для размещения модулей пяти – шести МУРЗ и более. Можно было бы установить в таком шкафу много разных сервисных модулей, повышающих надежность работы МУРЗ.

Переход на модульный принцип производства и продажи МУРЗ, т. е. на такой, который сегодня существует в области персональных компьютеров, позволил бы, кроме всего прочего, резко ускорить технический прогресс в области МУРЗ.

Свободный рынок функциональных модулей и их низкая стоимость позволили бы отказаться от сервисного обслуживания и ремонта МУРЗ, ограничившись лишь простой заменой вышедшего из строя модуля, приобретя его на свободном рынке или получив по гарантии от производителя. Значительно упростилась бы работа служб релейной защиты, поскольку теперь им не нужно было бы изучать толстенные фолианты каждого из установленных типов МУРЗ и разбираться с особенностями каждого из них. Кроме существенного облегчения работы с МУРЗ и сокращением времени освоения новых защит, существенно снизился бы процент ошибок, вызванных так называемым «человеческим фактором».

Программное обеспечение МУРЗ должно быть реализовано, по нашему мнению, также на принципах, хорошо зарекомендовавших себя в персональных компьютерах, т. е., должна быть базовая программная оболочка, аналогичная Windows (но существенно более простая, конечно) и набор прикладных программ и библиотек, предназначенных для конкретных типов защит. При наличии универсальной программной платформы и унифицированной блочной конструкции МУРЗ неизбежно появился бы и рынок прикладных программ для различных типов защит. Более того, можно было бы добиться, чтобы интерфейсы этих прикладных программ были бы также стандартизированы и чтобы потребителю не приходилось каждый раз при покупке нового МУРЗ или новой программы переучиваться и изучать с нуля новый программный интерфейс, как это происходит сегодня.

Совершенно очевидно, что для реализации этой концепции должна быть проделана большая работа по стандартизации таких универсальных функциональных модулей (общий стандарт на терминал, состоящий из универсальных функциональных модулей и отдельные стандарты на каждый функциональный модуль), а также внутренних протоколов связи между функциональными модулями. Говоря о необходимости стандартизации технических требований на отдельные модули МУРЗ, хотелось бы особо выделить необходимость особых требований к модулю логических входов, таких как минимально допустимые нижние уровни напряжения и тока активации логических входов. Отсутствие сегодня таких требований приводит к очень серьезным проблемам в эксплуатации МУРЗ [5, 6] и заставляет обслуживающий персонал для решения проблемы применять всякие доморощенные методы, например, такие как шунтирование входов внешними резисторами.

Оптимизация количества функций МУРЗ

В последнее время в специальной технической литературе все чаще можно встретить утверждения о целесообразности увеличения количества функций в одном модуле микропроцессорного устройства релейной защиты, вплоть до концентрации всех функций всех защит, имеющихся на подстанции, в едином микропроцессорном модуле.

На страницах многих специализированных журналов и на многочисленных конференциях уже давно обсуждаются вопросы создания так называемой «умной подстанции», в которой все ее основные элементы: трансформаторы тока и напряжения, выключатели, разъединители и короткозамыкатели должны быть снабжены цифровым блоком преобразования информации, IP-адресом и должны быть объединены посредством центрального компьютера (сервера) через обычную компьютерную сеть Ethernet.

В такой подстанции информация о токе и напряжении должна передаваться через сеть в цифровом виде на сервер (который иногда называют централизованной релейной защитой — ЦРЗА), обеспечивающий реализацию всех функций релейной защиты и автоматики (РЗА) и выдающий через сеть команды на соответствующие IP-адреса, принадлежащие выключателям или разъединителям.

Сегодня раздаются голоса о том, что даже проводная компьютерная сеть уже не нужна, и нужно поскорее переходить на беспроводную связь (WiFi) в релейной защите. Идя навстречу этим тенденциям, ведущие зарубежные производители МУРЗ уже сегодня снабжают свои новые изделия встроенными модемами WiFi.

Такая концентрация имеет только один плюс: снижение стоимости РЗ. Основным ее недостатком является снижение надежности РЗ, которое происходит сразу по нескольким причинам:

- конструктивное и программное усложнение собственно реле защиты, что автоматически (по теории надежности) ведет к снижению надежности защиты подстанции;
- неизбежное усложнение программного интерфейса ведет к увеличению доли «человеческого фактора» в общем количестве неправильных действий РЗ, которая уже сегодня очень существенна;
- усложнение периодических проверок исправности РЗ и увеличение времени, затрачиваемого на такие проверки. Во многих случаях при проверке одной функции РЗ приходится блокировать другие «мешающие» функции на время проверки, а затем возвращать их. Иногда вместо блокирования применяют изменение параметров мешающих функций на время проверки. С увеличением количества функций в одном устройстве резко увеличивается и вероятность ошибок персонала в результате таких проверок;
- увеличение вероятности отказа сразу всей подстанции целиком, так сказать, при отказе в реле центральной защиты даже какого-то единичного электронного компонента (транзистора, конденсатора) в таких узлах, как: источник питания, модуль выходных реле, элемент памяти, микропроцессор и др.;
- резкое усложнение анализа действий релейной защиты при разборе аварийных ситуаций;
- рост вероятности неправильных действий РЗ в результате непредсказуемости ее реакции при наложении событий во время сложных аварий и во время сложных переходных процессов;
- резкий рост уязвимости РЗ к кибератакам [7] и к преднамеренным деструктивным электромагнитным воздействиям [8,9].

Что касается предлагаемого некоторыми авторами [10] использования двух одинаковых комплектов ЦРЗА для резервирования действий РЗ, то это предложение не выдерживает критики по той простой причине, что отказами РЗ являются как излишние срабатывания, так и несрабатывания. Если использовать основной и резервный блоки ЦРЗА, то как соединить между собой их выходные контакты: последовательно или параллельно? При любом соединении будет иметь место увеличение надежности по одному из видов отказа и такое же снижение надежности по другому виду. Поэтому речь должна идти не о простом резервировании, а о мажорировании, по принципу два из трех, например. То есть использовать не два, а три одинаковых комплекта ЦРЗА.

Даже если предположить снижение стоимости оборудования РЗ при концентрации всех функций в одном модуле, то все равно придется признать наличии двух встречно направленных тенденций:

- снижение затрат на РЗ при увеличении числа функций в одном реле;
- увеличение затрат за счет снижения надежности РЗ и увеличения ущерба от ее неправильных действий (по разным причинам, перечисленным выше) при увеличении числа функций в одном реле.

То есть, имеет место типичная оптимизационная задача: определение оптимального числа функций реле защиты по критерию минимума затрат. Задача

эта непростая ввиду отсутствия достоверных статистических данных о влиянии числа функций на надежность РЗ, но, все же, решаемая, хотя бы на основе использования специальных математических моделей и известных приемов теории надежности. Для упрощения решения задачи и повышения достоверности результатов на первом этапе целесообразно строить такие модели и решать оптимизационную задачу отдельно для каждого вида защит, например, отдельно для защит генератора, трансформатора, линии и т. д.

На основании вышеизложенного можно сделать вывод о том, что такой серьезный вопрос как увеличение числа функций в одном модуле микропроцессорной защиты требует значительно более осторожного подхода, проведения глубоких исследований и непростых расчетов, а не вбрасывания с кондачка общих идей, способных еще более запутать и без того сложную ситуацию с выбором тенденций развития РЗ и привести к катастрофическим последствиям в будущем.

Свободно-программируемая логика

Реле защиты предыдущих поколений (электромеханические, электронные) разрабатывались и выпускались со строго детерминированной логикой. На стадии разработки функционирование таких реле подвергалось тщательному исследованию во всех возможных режимах работы и поэтому неожиданные «сюрпризы» при эксплуатации таких реле встречались крайне редко.

Микропроцессорные устройства релейной защиты существенно расширили возможности релейной защиты, придав ей несвойственную ранее гибкость, в частности, за счет свободно-программируемой логики. Использование свободно-программируемой логики позволило буквально всем желающим программировать функции релейной защиты по своему усмотрению, соответствующему имеющемуся уровню знаний в области релейной защиты и в области правил логического программирования. Однако, далеко не всегда достаточная для таких манипуляций с релейной защитой квалификация персонала приводит к резкому снижению надежности такой РЗ. Статистические данные, приводимые различными авторами [11, 12], подтверждают существенный вклад так называемого «человеческого фактора» в общее количество случаев неправильных действий релейной защиты, доходящий до 50 – 70 %.

Комбинация таких особенностей МУРЗ, как свободно-программируемая логика, избыточность функций, сложность программного интерфейса приводит к образованию весьма опасного вектора, резко снижающего надежность релейной защиты [13]. Решение проблемы заключается, по нашему мнению, в существенном ограничении использования свободно-программируемой логики в МУРЗ, что должно быть закреплено юридически, т. е. должно найти отражение в соответствующем стандарте.

Стандартизация технических требований

В настоящее время существуют несколько основных нормативных документов, определяющих технические требования к МУРЗ:

1. **РД 34.35.310–97.** Общие технические требования к микропроцессорным устройствам защиты и автоматики энергосистем, 1997.
2. **РД 153–34.1–35.137–00.** Технические требования к подсистеме технологических защит, выполненных на базе микропроцессорной техники, 2000.
3. **СТО 56947007–33.040.20.022–2009.** Устройства РЗА присоединений 110 – 220 кВ. Типовые технические требования, 2009.
4. **СТО 56947007–29.120.70.042–2010.** Требования к шкафам управления и РЗА с микропроцессорными устройствами, 2010.
5. **СТО 56947007–29.240.044–210.** Методические указания по обеспечению электромагнитной совместимости на объектах электросетевого хозяйства, 2010.

Однако, несмотря на наличие большого количества нормативных документов, пользуясь ими, практически невозможно составить достаточно полные, четкие и понятные технические требования на МУРЗ. Единственным документом, в котором эти требования были четко сформулированы, систематизированы и упорядочены были «Общие технические требования... РД 34.35.310 – 97». Изначально, срок действия этого документа был установлен два года, тем не менее, он многократно продлевался в течение 15 лет. На сегодняшний день этот документ сильно устарел: большинство стандартов, на которые он ссылается, уже или не существуют, или заменены другими, а многие технические параметры претерпели изменения, дополнены новыми значениями и условиями.

Не лучше обстоит дело и со стандартами. Большинство стандартов РФ, изданных в 90-годах прошлого столетия и декларируемых как «аутентичные копии» того или иного стандарта Международной электротехнической комиссии (МЭК), на деле уже давно не являются таковыми, поскольку оригинальные стандарты МЭК с тех пор претерпели существенные изменения.

В результате сложившейся ситуации, производители МУРЗ записывают в документации на свои

изделия технические параметры в виде, мало понятном потребителю; не могут правильно, четко и полно сформулировать условия испытания своих изделий, передавая их в сертификационные центры и испытательные лаборатории. Потребитель, в свою очередь, не может правильно сформулировать технические требования в тендерной документации; не может сравнить между собой изделия различных производителей, технические параметры которых записаны в различной форме и содержат ссылки на разные стандарты; не может оценить насколько записанные им требования со ссылками на одни стандарты соотвествуют изделиям, в документации которых имеются ссылки на другие стандарты. Особенно актуальной эта проблема становится в связи с закупкой МУРЗ зарубежных производителей, ориентирующихся на стандарты МЭК, а не на стандарты РФ.

Запись технических параметров в спецификации многих производителей МУРЗ, а также в тендерной документации заказчика часто производится в виде ссылок только лишь на номера стандартов, без указания технических параметров, без критериев качества функционирования и даже без указания степени жесткости. Такая ссылка лишь на номер стандарта не говорит ровным счетом ничего о конкретных технических параметрах, которые даже в одном стандарте могут отличаться в 2—3 раза.

К сожалению, даже некоторые стандарты вместо важных технических параметров содержат лишь ссылки на другие стандарты, в которых эти параметры указаны. Все это создает большие трудности в использовании стандартов и приводит к неоправданному разнобою в спецификациях на МУРЗ. В результате страдают все: и производители, и потребители МУРЗ.

Анализ десятков технических спецификаций на МУРЗ как российских, так и всех ведущих мировых производителей, а также множества стандартов, РФ, МЭК и Американского общества инженеров электриков (IEEE), позволил составить некую универсальную базовую Спецификацию, использование которой и производителями и потребителями МУРЗ способствовало бы решению многих проблем, перечисленных выше. Эта спецификация представлена автором в [14] и могла бы послужить хорошей основой при решении проблем стандартизации в области МУРЗ.

Стандартизация испытаний МУРЗ

В разных энергосистемах были установлены различные сроки периодических проверок релейной защиты (1 раз в 2—3 года), но они, обычно, соблюдались неукоснительно.

С появлением на рынке микропроцессорных устройств релейной защиты ситуация кардинально изменилась. Производители этих устройств заявили, что микропроцессорные реле якобы не нуждаются в периодических проверках потому, что имеют мощную встроенную систему самодиагностики. Эта особенность МУРЗ фигурировала в рекламных проспектах чуть ли не как главное их преимущество перед электромеханическими и аналоговыми электронными реле. Мощная рекламная компания, развернутая производителями МУРЗ, сыграла свою роль. Многие специалисты релейной защиты безоговорочно поверили в этот рекламный трюк, не имея возможности на практике проверить достоверность этого утверждения, хотя было совершенно очевидно, что невозможно создать систему самодиагностики на базе внутреннего микропроцессора МУРЗ, которая проверяла бы физическую исправность многих тысяч электронных компонентов.

Да и функционально невозможно проверить исправность, например, модуля входов или модуля выходов без включения этих блоков и проверки реакции реле на подачу на них сигналов. На практике оказывается, что большинство МУРЗ попросту не замечают замену целой печатной платы одного вида на плату другого вида, не совместимой с текущими уставками реле. Об этом и о других рекламных трюках, связанных с «самодиагностикой» МУРЗ уже упоминалось ранее в многочисленных публикациях автора на эту тему [15 и др].

В отличие от производителей МУРЗ, производители тестовых систем релейной защиты (ТСКЗ), наоборот, всегда утверждали, что все реле защиты должны обязательно проходить периодические проверки, включая также и МУРЗ, поскольку так называемой «самодиагностикой» в них охвачены не более 15% программного обеспечения и «железа». Несмотря на утверждения производителей МУРЗ о нецелесообразности периодических проверок защит, фирмы-производители ТСРЗ продолжали интенсивно разрабатывать и выбрасывать на рынок все новые и новые тестовые системы.

Исправность устройств релейной защиты обычно принято проверять на тех конкретных уставках, которые будут использоваться в дальнейшем при реальной работе реле в данной конкретной точке сети. При изменении уставок в процессе эксплуатации требовалась повторная проверка работоспособности реле с этими новыми уставками. Во времена электромеханических реле защиты это было вполне оправданной мерой, так как переход с одной уставки на другую осуществлялся путем механического перемещения внутренних элементов реле или переключения отпаек встроенных трансформаторов и т.п.

При изменении настроек таких реле вполне могло оказаться, что внутренние цепи реле,

подключенные к новой отпайке трансформатора неисправны (обрыв провода, нарушение контакта, поврежденная изоляция и т. п.) или, что в новом положении механических элементов реле нарушается его балансировка, появляется «затирание» и т. п. неприятности. Поэтому, нормальная работоспособность электромеханического реле с одним набором уставок еще не гарантировала его работоспособности с другими уставками.

В МУРЗ переход с одного набора уставок на другой не сопровождается физическими изменениями в его внутренней структуре. Независимо от конкретных уставок и режимов работы в МУРЗ работают одни и те же входные и выходные цепи, одни и те же логические элементы, тот же самый процессор, тот же самый источник питания и т. д. Даже включение или отключение отдельных функций МУРЗ не связано с изменениями физического состояния его цепей. Проверка же правильности выбора логики защиты и правильности расчета уставок для конкретных условий конкретной сети — это совсем другая задача, которая не имеет отношения к проверке исправности реле и решается не персоналом, эксплуатирующим реле и отвечающем за его исправность, а инженерной службой, отвечающей за расчеты уставок и выбор внутренней логики работы реле. Да и невозможно в процессе тестирования исправности реле смоделировать все реальные ситуации и все возможные комбинации факторов, действующих в реальной сети. Выявление таких ситуаций не является целью проверки исправности реле защиты. Более того, можно показать, что отказ от проверки реле с использованием расчетных уставок является положительной мерой, снижающей риск неправильных действий защиты вследствие так называемого «человеческого фактора».

Как уже отмечалось выше, в многофункциональных микропроцессорных защитах уставки для конкретных условий работы выбираются таким образом, что проверить определенные функции реле можно только при загрублении или полном отключении другой, конкурирующей функции. Невозврат такой загрубленной или отключенной функции в исходное положение после окончания тестирования реле часто является причиной неправильных действий защиты в аварийных режимах.

Аналогичный подход к проблеме испытаний реле защиты принят и в [16]. В этом документе, имеющем статус стандарта, все испытания реле разделены на два вида: *калибровочные испытания* (предназначенные для проверки уставок и конфигурации реле) и *функциональные*. Если для функциональных испытаний установлена периодичность 1 раз в 4 года *для всех типов реле* (включая электромеханические и микропроцессорные), то для калибровочных испытаний установлена периодичность 1 раз в 4 года *только для электромеханических реле*. Периодическая калибровка (т. е. проверка уставок) микропроцессорных реле защиты вообще не предусмотрена.

Таким образом, для проверки исправности МУРЗ достаточно проверить их правильное функционирование лишь в некоторых, *заранее заданных,* наиболее критичных точках характеристики; в некоторых, *заранее заданных,* наиболее сложных (комбинированных) режимах работы, включая динамические режимы работы с *заранее заданными* переходными процессами, характерными для типовых электрических сетей (но не обязательно для данной конкретной сети). Такие испытания должны охватывать все физические входы и выходы реле. Такое тестирование микропроцессорной защиты в наиболее сложных режимах работы позволит, по нашему мнению, значительно лучше проверить исправность МУРЗ, нежели ограниченная проверка в очень ограниченных пределах конкретных уставок, при которых МУРЗ будет в дальнейшем функционировать.

Современные тестовые системы релейной защиты обладают поистине супергибкостью и широчайшими функциональными возможностями. Эти ТСРЗ позволяют симулировать практически любые встречающиеся на практике условия работы реле защиты, включая создание под собственные требования искусственных COMTRADE-файлов; искусственное искажение формы кривой тока; симуляция гармоник; смещение синусоиды тока относительно оси (симуляция апериодической составляющей); симуляция ответной реакции выключателя; автоматическое построение самых сложных полигональных характеристик дистанционных защит; синхронизация дифференциальных защит через спутники и т. п.

Такие супервозможности современных ТСРЗ обусловливают наличие и оборотной стороны медали: необходимости вводить сотни параметров в десятки таблиц для выполнения каждого отдельного испытания реле. При этом встроенные библиотеки тестовых процедур на практике мало помогают, так как не освобождают от необходимости заполнения десятков таблиц. Малейшее несоответствие между собой настроек МУРЗ и ТСРЗ приводит к неправильным результатам. Причем, далеко не всегда можно понять, что полученные результаты неверны. И даже в тех случаях, когда ошибка очевидна (например, полученная характеристика реле не соответствует теоретической), очень сложно определить, где именно допущена ошибка: в настройках МУРЗ или в настройках ТСРЗ.

На собственном опыте автор может подтвердить, что поиск ошибки такого рода чрезвычайно сложен и требует много усилий и времени.

Не менее сложна работа с моделью электрической сети (Power System Model), применяемой в ТСРЗ некоторых типов, для проверки дистанционных защит. Для настройки параметров ТСРЗ в этом режиме необходимо знание множества параметров реальной электрической сети, которые необходимо занести со специальными коэффициентами во множество таблиц. Технику и даже инженеру службы релейной защиты многие из этих параметров реальной сети и применяемых коэффициентов часто неизвестны, что требует участия в процедуре проверки реле инженеров из других служб энергосистемы.

По нашему мнению, для тестирования современных сложных многофункциональных МУРЗ должна быть разработана общая (стандартная) для всех типов ТСРЗ программная платформа, требования к которой должны быть узаконены международным стандартом. Примером такой общей программной платформы является общеизвестная Sybase SQL Anywhere, которая широко используется для создания базы данных в различных устройствах сбора и обработки данных, симуляторах, испытательных установках различных изготовителей.

Другим примером является универсальный формат COMTRADE, который используется во всех типах микропроцессорных регистраторов аварийных режимов и, собственно, во всех типах ТСРЗ для симуляции переходных режимов.

Прикладные программы для работы с ТСРЗ различных типов могут иметь совершенно разные интерфейсы, но все они должны быть выполнены на общей стандартной программной платформе. Производители МУРЗ должны снабжать свои защиты двумя компакт-дисками. На одном из них под соответствующими номерами должны быть записаны полные наборы уставок для специфических режимов работы защит, или для характерных точек характеристики, или для типовых примеров электрических сетей. На втором, под номерами, соответствующими наборам уставок защиты, должны быть записаны полные наборы уставок для ТСРЗ и схемы внешних подключений МУРЗ к выходам и входам ТСРЗ. Эффективное использование современных ТСРЗ для тестирования современных многофункциональных МУРЗ обеспечивается, по нашему мнению, только в том случае, если вся процедура тестирования сведется к загрузке в МУРЗ набора уставок номер XX1, загрузке в ТСРЗ набора уставок номер YY1 и подключению МУРЗ к ТСРЗ [17].

После окончания проверки реле и подтверждения его исправности все тестовые уставки должны быть *автоматически* заменены заранее приготовленным набором (файлом) реальных расчетных уставок.

Кибербезопасность и устойчивость к преднамеренным деструктивным электромагнитным воздействиям

Это наиболее сложные области, требующие стандартизации. Сами по себе эти проблемы хорошо известны и описаны во многих общедоступных источниках, например, в [7 — 9]. Однако, технические подробности решения этих проблем, по понятным причинам, широко не обсуждаются. Тем не менее, проблемы не становятся от этого менее актуальными, скорее наоборот. Направленность развития современных технологий с их уклоном в сторону все более широкого применения микропроцессорной техники даже в тех областях, где до недавнего времени царила аналоговая электроника, все расширяющееся использование сетевого подключения силового оборудования для дистанционного управления им и даже переход на беспроводные технологии — все эти и многие другие тенденции развития современной техники не могут не вызывать серьезной озабоченности. Эта озабоченность лишь усиливается при чтении в средствах массовой информации сообщений о создании то в одной, то в другой стране специальных подразделений по разработке кибернетических средств ведения войны и о том, что основными целями в этой войне будут базовые системы инфраструктуры страны (водо- и электроснабжение, связь). Не отстают от них и разработчики электромагнитных средств поражения микроэлектроники [8, 9].

В этой связи МУРЗ представляют собой одну из основных целей для кибератак и деструктивных электромагнитных воздействий. Поскольку, с одной стороны, в структуре сегодняшнего энергетического оборудования именно МУРЗ являются наиболее чувствительными к электромагнитным воздействиям элементами энергосистем, к которым подключены многочисленные антенны (кабели), абсорбирующие электромагнитное излучение с огромной территории. А с другой стороны, именно МУРЗ являются каналами связи с силовыми коммутационными аппаратами, дистанционное воздействие на которые при кибератаке может привести к тяжелейшим авариям в энергосистеме, вплоть до ее полного развала.

Задачей новых стандартов в этих областях нам представляется создание неких ограничительных рамок, сдерживающих бесконтрольное развитие технологий в направлениях, представляющих собой

угрозу национальной безопасности. Должно стать правилом, что все новые технологии в области РЗ должны развиваться параллельно с разработкой средств и методов защиты РЗ и приниматься к практическому применению только совместно с этими методами и средствами защиты.

Стандартизация в области расчетов надежности и показателей надежности МУРЗ

В соответствии с ГОСТ 27.002—89 [18] надежность трактуется как свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, ремонта, хранения и транспортирования. Как видно из определения, надежность является комплексным показателем, который в зависимости от назначения объекта и условий его применения может включать безотказность, долговечность, ремонтопригодность и сохраняемость или определенное сочетание этих свойств.

Одним из важнейших показателей надежности является ***наработка на отказ*** — показатель, определяемый как отношение суммарной наработки *восстанавливаемого* объекта к математическому ожиданию числа его отказов в течение этой наработки. Иными словами, это один из параметров надежности *восстанавливаемого* устройства или технической системы, характеризующий среднюю продолжительность работы устройства (в часах) между отказами (ремонтами). Международный аналог этому параметру: *MTBF* — Mean (operating) time between failures.

В технической документации производителей этот показатель составляет, обычно период, эквивалентный 50—90 лет. Означает ли это, что интервал времени между двумя отказами МУРЗ должен быть 50—90 лет? Определение, данное этому термину, утверждает именно это, хотя здравый смысл подсказывает, что в реальной, а не виртуальной жизни, такого быть не может.

В западной технической литературе используются несколько дополнительных показателей надежности, одним из которых является «Mean Time Between Unit Replacement» (MTBUR) — ***средняя наработка до отказа*** (замены) сменного элемента. Аналогичный показатель рекомендуется использовать и в отраслевом российском РД 34.35.310—97 [19], хотя он и не предусмотрен в ГОСТ 27.002—89.

Совершенно очевидно, что при модульной конструкции МУРЗ и неремонтопригодности многослойных печатных плат с электронными микрокомпонентами поверхностного монтажа — основы современных МУРЗ, под «сменными элементами» могут пониматься лишь целые модули (печатные платы), а ремонт (восстановление) МУРЗ может быть реализован в большинстве случаев лишь путем замены модуля (печатной платы). В этом случае никакой практической разницы между показателями MTBF и MTBUR не будет и потребители по-прежнему будут недоуменно разглядывать занятные цифры со многими нулями, соответствующие 50—90 годам, и гадать, как это соотносится с 15—18 годами реального срока службы МУРЗ.

Еще одна проблема с использованием MTBF может появиться в ближайшем будущем. Как отмечалось выше, появление на рынке универсальных функциональных модулей, которые будут продаваться и приобретаться как отдельные независимые изделия из которых будет компоноваться МУРЗ переводит эти отдельные печатные платы-модули из разряда сменных комплектующих в разряд самостоятельных неремонтируемых изделий, причем, изделий, весьма разнородных, имеющих различные показатели надежности. Очевидно, что в этом случае, во-первых, показатели надежности должны рассчитываться для каждого такого модуля отдельно, а во-вторых, показатель MTBF к ним не может быть применим вообще, как к невосстанавливаемым изделиям.

Еще одно сомнение в использовании MTBF для МУРЗ заключается в том, что даже при единичном его отказе ущерб может быть очень значительным и поэтому тот факт, что между первым и вторым отказами будет большой интервал времени (большое значение MTBF), мало чем поможет делу.

В связи с тем, что показатель MTBF себя полностью дискредитировал огромными значениями, абсолютно не соответствующими действительности и не дающими никакой реальной информации о надежности МУРЗ, а также его очевидными недостатками, использование MTBF для оценки надежности МУРЗ должно быть прекращено.

В качестве нового показателя надежности для МУРЗ рекомендуется [20, 21] использование ***гамма-процентной наработки до отказа,*** т. е. наработки, в течение которой отказ объекта не возникает с определенной вероятностью, выраженной в процентах.

Например, 95%-ная наработка до отказа в течение не менее 5 лет означает, что за 5 лет работы должно отказывать не более 5% устройств, находящихся в эксплуатации. Причем, значение это должно указываться не для МУРЗ в целом, а для составляющих его функциональных модулей. Имея такой удобный и понятный показатель, потребитель мог бы отследить

количество вышедших из строя модулей за определенный промежуток времени и предъявить производителю претензии, если в течение этого промежутка отказало значительно большее их количество, чем это было гарантировано производителем. Имея такой показатель, потребителю будет значительно легче ориентироваться и на будущем рыке универсальных модулей, выбирая для себя наиболее приемлемый вариант, по соотношению цена/качество.

В дополнение к этому от производителей необходимо потребовать указания в технической и тендерной документации ***среднего срока службы отдельных модулей*** и рекомендации относительно периодичности превентивной замены этих модулей в целях поддержания высокого уровня надежности релейной защиты. Например, для источника питания это может быть 8 — 10 лет; для модуля логических входов — 12 лет; для модуля центрального процессора — 15 лет; для модуля аналоговых входов — 17 лет, и т. д. Эти данные должны быть известны добросовестному производителю, отслеживающему статистику отказов и повреждений своих изделий. Вопрос о том, за чей счет должна производиться такая превентивная замена модулей должен решаться по договоренности между производителем и потребителем. Например, производитель может гарантировать разовую (возможно, частичную, например, только для источников питания) превентивную замену модулей, а все последующие замены должны производиться за счет потребителя.

Использование предлагаемого критерия оценки надежности МУРЗ и дополнительных сведений о надежности, рассмотренных выше, позволит изменить характер взаимоотношений между потребителями и производителями МУРЗ и существенно увеличить надежность релейной защиты.

Выводы

1. Полное отсутствие стандартизации в области производства МУРЗ приводит к снижению надежности релейной защиты и к большим экономическим потерям.

2. Все расширяющееся применение МУРЗ и, в перспективе, полная замена ими всех остальных типов реле защиты требует принятия неотложных мер по стандартизации МУРЗ, как средства повышения надежности релейной защиты и снижения затрат на нее.

3. Стандарты в области МУРЗ должны охватывать все перечисленные выше области:

- терминологию;
- конструкцию и программное обеспечение;
- оптимизацию количества функций в одном модуле МУРЗ;
- использование свободно-программируемой и недетерминированной логики в МУРЗ;
- унификацию набора технических требований к МУРЗ;
- тестирование и испытание МУРЗ;
- обеспечение кибербезопасности и устойчивости к преднамеренным деструктивным электромагнитным воздействиям;
- показатели надежности МУРЗ.

Литература

1. **Нудельман Г. С., Булычев А. В.** Совершенствование за счет упреждающих функций//Новости электротехники. 2009. № 4 (58).

2. **Булычев А. В.** Защита упреждающего действия для электродвигателей//Новости электротехники. 2011. № 5.

3. **Гуревич В. И.** Реле защиты и релейная защита: проблемы терминологии//Вести в электроэнергетике. 2012. № 4. С. 23 — 33.

4. **Гуревич В. И.** Новая концепция построения микропроцессорных устройств релейной защиты//Компоненты и технологии. 2010. № 6. С. 12 — 15.

5. **Гуревич В. И.** О надежности логических входов микропроцессорных устройств релейной защиты// Электроника-Инфо. 2009. № 2. С. 28 — 30.

6. **Гуревич В. И.** Оперативные цепи постоянного тока. Проблемы контроля изоляции//Новости электротехники. 2012. № 1. С. 30 — 33.

7. **Гуревич В. И.** Кибероружие против энергетики// PRO Электричество. 2011. № 1. С. 26 — 29.

8. **Гуревич В. И.** Проблема электромагнитных воздействий на микропроцессорные устройства релейной защиты//Компоненты и технологии. 2010. № 2. С. 60 — 64; № 3. С. 91 — 96. № 4. С. 46 — 51.

9. **Гуревич В. И.** Проблема устойчивости микропроцессорных систем релейной защиты и автоматики к преднамеренным деструктивным электромагнитным воздействиям//Компоненты и технологии. 2011. № 4 (часть 1); 2011. № 5 (часть 2).

10. **Гуревич В. И.** Про многофункциональную релейную защиту//PRO Электричество. 2012. № 3. С. 14 — 17.

11. **Коновалова Е. В.** Основные результаты эксплуатации устройств РЗА энергосистем Российской Федерации/ Сборник докладов XV научно-технической конференции «Релейная защита и автоматика энергосистем», Москва, 2002.

12. **Kjolle G. H., Heggset J., Hjartsjo B. T., Engen H.** Protection System Faults 1999 — 2003 and the Influence on the Reliability of Supply//2005 IEEE St. Petersburg Power Tech, St. Petersburg, Russia, June 27 — 30, 2005.

13. **Гуревич В. И.** Технический прогресс в релейной защите. Опасные тенденции развития РЗА//Новости электротехники. 2011. № 5. С. 38 — 40.

14. **Гуревич В. И.** Проблемы стандартизации в области микропроцессорных устройств релейной защиты// Компоненты и технологии. 2012. № 1. С. 6 — 9.

15. **Гуревич В. И.** Микропроцессорные реле защиты. Устройство, проблемы, перспективы. М.: Инфра-Инженерия, 2011.

16. PJM Relay Testing and Maintenance Practices. PJM Interconnection. Relay Subcommittee. Rev. 2/26/04, 2004.

17. **Гуревич В. И.** Испытания микропроцессорных реле защиты//PRO Электричество. 2008. № 1 (25). С. 41 — 43.

18. **ГОСТ 27.002–89.** Надежность в технике. Основные понятия. Термины и определения, 1989.

19. **РД 34.35.310–97.** Общие технические требования к микропроцессорным устройствам защиты и автоматики. М.: ОРГРЭС, 1997.

20. **Гуревич В. И.** Проблемы оценки надежности релейной защиты//Электричество. 2011. № 2. С. 28 — 31.

21. **Гуревич В. И.** Для оценки надежности микропроцессорных устройств релейной защиты нужен новый критерий//Электротехнический рынок. 2011. № 6. С. 70 — 74.