

Релейная защита энергосистем – НЕ ИСПЫТАТЕЛЬНЫЙ ПОЛИГОН ДЛЯ МОДНЫХ ИДЕЙ!

В. И. Гуревич, канд. техн. наук

В последние годы мы стали свидетелями бурного расцвета множества новомодных идей и тенденций в области релейной защиты, автоматики и систем управления в электроэнергетике. Началось все примерно два десятилетия тому назад в связи с появлением на рынке микропроцессорных устройств релейной защиты (МУРЗ). По мере развития этой техники и по мере повышения производительности микропроцессоров, аппетиты апологетов микропроцессорной техники начали возрастать. От простейших микропроцессорных аналогов реле защиты предыдущих поколений, рис. 1, современные МУРЗ отличаются резко возросшей сложностью, огромным количеством функций, заложенных в одном терминале.

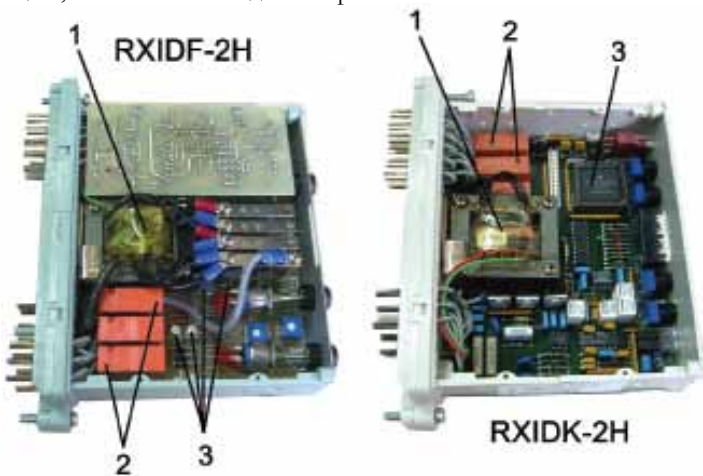


Рис. 1. Два токовых реле с зависимой выдержкой времени, с одинаковыми техническими параметрами, характеристиками и размерами, выполненных в одинаковых стандартных корпусах COMBIFLEX® и произведенных одной и той же компанией (ABB), слева – статическое полупроводниковое типа RXIDF-2H, справа – микропроцессорное RXIDK-2H

1 – входной трансформатор тока; 2 – выходные электромагнитные реле; 3 – транзисторы в статическом реле и специализированный микропроцессор – в микропроцессорном.

Это усложнение, и аппаратное и программное, не прошло даром. Как показано в [1, 5 - 9] переход на МУРЗ уже сегодня сопровождается заметным снижением надежности релейной защиты. Однако, несмотря на это, апологеты микропроцессорной релейной защиты считают, что не следует останавливаться на достигнутом, а нужно и дальше продолжать усложнять МУРЗ, увеличивая количество функций, выполняемых одним терминалом; используя в МУРЗ свободно-программируемую логику; недетерминированную логику на основе теории нейронных сетей; алгоритмы упреждающего действия; навешивая на МУРЗ функции информационно-измерительных систем и систем мониторинга силового электрооборудования; использования беспроводных каналов связи (Wi-Fi) между реле и т.д. Современные новомодные идеи и разработки в области МУРЗ уже не ограничиваются функциями только релейной защиты.

Да что там релейная защита, если все энергосистемы в недалеком будущем предполагается выполнять по технологии Smart Grid, подразумевающей оснащение всех силовых элементов энергосистем микропроцессорами, обеспечивающими обмен сигналами синхронизации и командами управления между ними посредством Wi-Fi.

Какие прекрасные перспективы и маящие горизонты! Какие огромные средства из государственных бюджетов, выделяемые на новые программы в области электроэнергетики! Как много научных и производственных коллективов могут прокормиться на этих бюджетах, периодически выдвигая все более невероятные, но необычайно красивые идеи, выбрасывая на рынок все более «навороченные», но менее надежные изделия. Ведь это огромный бизнес, и никто не хочет быть отлученным от этого сладкого «пирога». Участники этого бизнеса отнюдь не озбочены отдаленными последствиями их деятельности, а стремятся лишь побыстрее «протолкнуть» свои новомодные идеи на рынок. Бизнес – есть бизнес и его основополагающие законы действуют одинаково во всех странах и во всех областях, включая такую чувствительную область, как релейная защита, системы управления и контроля в электроэнергетике. Не верите? Тогда познакомьтесь с девизом к отчету о симпозиуме “Distribution systems of the future: Novel ICT solutions as the backbone for smart distribution” опубликованному в журнале PAC World:

Ключевые слова в этом тезисе: «неотложное» и «обязательное». Ну конечно, зачем что-то там проверять, зачем сомневаться?! Сварганили – и вперед! Главное, побыстрее! И без отговорок! Не правда, ли, что-то очень знакомое из прошедшей эпохи напоминает этот тезис?



Рис. 2. Девиз к одной из публикаций в популярном среди специалистов во всем мире журнале “Protection, Automation and Control Magazine” – PAC World, September, 2011 (выделенный рамкой), который можно перевести как: «неотложное внедрение новых разработок сегодня должно стать обязательным».

В предыдущих многочисленных публикациях мы уже неоднократно обращали внимание на опасность некоторых тенденций в развитии релейной защиты, усиленно пропагандируемых разработчиками и производителями МУРЗ. Речь идет о следующих тенденциях:

1. Снижение надежности релейной защиты, по мере расширения применения МУРЗ [1, 5 - 9].
2. Непрерывное усложнение МУРЗ и увеличение концентрации защитных функций в одном терминале [6, 10].
3. Навешивание на МУРЗ несвойственных релейной защите функций, например таких, как мониторинг электрооборудования [11, 12].
4. Использование в МУРЗ недетерминированной логики, а также, так называемых «упреждающих действий», обуславливающих опасность потери контроля над действиями релейной защиты [11, 12].

5. Расширение использования в МУРЗ свободно-программируемой логики [13], сопровождающееся значительным увеличением процента ошибок персонала и неправильных действий защит.

6. Усложнение проверок исправности и вообще эксплуатации релейной защиты по мере накопления в одной энергосистеме множества типов МУРЗ разных производителей, закупаемых по тендерам и отличающихся между собой как конструкцией, так и программным обеспечением. Отсутствие стандартов, оговаривающих единые универсальные требования к конструкции и к программному обеспечению МУРЗ, увеличивающее интеллектуальную нагрузку на персонал и приводящее к значительным экономическим потерям [14]. Эта ситуация усугубляется с каждым годом.

7. Существенное ослабление электромагнитной защищенности релейной защиты и в целом энергосистемы по мере расширения использования МУРЗ [15-17].

8. Повышение уязвимости энергосистем хакерским атакам по мере расширения применения микропроцессорной техники и при использовании более дешевых сетей Ethernet и Wi-Fi вместо относительно защищенных оптоэлектронных кабелей в системах релейной защиты [18].

По нашему мнению, пора положить конец процессу бесконтрольного развития непроверенных и опасных тенденций в релейной защите и системах автоматизации, включая Smart Grid. Для этого необходимо создание специального Координационного Совета по релейной защите и интеллектуальным сетям, который должен заниматься анализом существующих тенденций, выработкой национальной стратегии и координацией стандартизации в этих областях. В состав этого Совета должны войти независимые эксперты и специалисты в области релейной защиты, микроэлектроники, защиты информации, электромагнитной совместимости, не имеющие экономических связей с разработкой и производством МУРЗ или элементов Smart Grid. Следует иметь виду, что чисто меркантильные финансовые интересы отдельных специалистов и даже целых научных и производственных коллективов, заинтересованных в финансировании любых новых цифровых технологий в области электроэнергетики и, в частности, в области релейной защиты, независимо от отдаленных последствий использования этих технологий, не ограниченных какими бы то ни было рамками, может привести в недалеком будущем к национальным катастрофам. Новые технологии в области релейной защиты, автоматики, систем связи и передачи данных не должны внедряться в эксплуатацию до тех пор, пока не будут всесторонне рассмотрены возможные отрицательные последствия их широкого распространения с учетом уже накопленного опыта, пока не будут разработаны эффективные меры защиты от преднамеренных дистанционных деструктивных воздействий (ПДДВ), будь то хакерские атаки или преднамеренные электромагнитные воздействия. Разработке мер защиты от ПДДВ чувствительной электронной аппаратуры, применяемой в электроэнергетике, должно уделяться не меньшее внимание и должны выделяться не меньшие средства, чем разработке новых технологий, таких как Smart Grid. Разработка никакой новой технологии, основанной на использовании цифровой микроэлектроники, не может считаться завершенной и готовой к применению в электроэнергетике без разработки мер ее защиты от ПДДВ. В новые стандарты по микропроцессорной релейной защите, необходимость создания которых обоснована в [20, 21], обязательно должны войти требования по защите от ПДДВ, поскольку имеющиеся сегодня стандарты в области электромагнитной совместимости (ЭМС) отражают

требования по устойчивости аппаратуры лишь к естественным, а не к преднамеренным разрушающим электромагнитным воздействиям. Необходимо тщательно изучить пути повышения надежности функционирования МУРЗ за счет резервирования ее современными гибридными реле [22, 23].

По нашему мнению, только в таком направлении должен дальше развиваться технический прогресс в важнейшей области электроэнергетики – основе национальной инфраструктуры любой страны.

Литература

1. Гуревич В. И. Микропроцессорные реле защиты: новые перспективы или новые проблемы? - Новости электротехники, 2005, № 6 (36), с. 57 - 60.
2. Гуревич В. И. Микропроцессорные реле защиты: альтернативный взгляд – Электро-инфо, 2006, N 4 (30), с. 40 – 46.
3. Гуревич В. И. Цена прогресса - Компоненты и технологии, 2009, № 8, с. 112-118
4. Гуревич В. И. Интеллектуальные сети: новые перспективы или новые проблемы? -Электротехнический рынок, 2010, № 6 (часть 1); 2011, № 1 (часть 2).
5. Гуревич В. И. Надежность микропроцессорных устройств релейной защиты: мифы и реальность. - Проблемы энергетики, 2008, № 5 - 6, с. 47 - 62.
6. Гуревич В. И. Еще раз о надежности микропроцессорных устройств релейной защиты. - Электротехнический рынок, 2009, № 3 (29), с. 40 - 45.
7. Гуревич В. И. О некоторых оценках эффективности и надежности микропроцессорных устройств релейной защиты. - Вести в электроэнергетике, 2009, № 5, с. 29 - 32.
8. Гуревич В. И. Актуальные проблемы релейной защиты: альтернативный взгляд. - Вести в электроэнергетике, 2010, № 3, с. 30 - 43.
9. Гуревич В. И. Критерии оценки релейной защиты: следует ли усложнять ситуацию? - Вести в электроэнергетике, 2009, № 6, с. 45 - 48.
10. Гуревич В. И. Энергобезопасна ли релейная защита? - Энергобезопасность и Энергосбережение, 2010, № 2, с. 6 - 8.
11. Гуревич В. И. "Интеллектуализация" релейной защиты: благие намерения или дорога в ад? - Электрические сети и системы, 2010, № 5, с. 63- 67.
12. Гуревич В. И. Сенсационные открытия в области релейной защиты. – Энергетика и промышленность России, 2009, № 23-24, с. 60.
13. Гуревич В. И. Логика в свободном полете. - PRO Электричество, 2011, № 2, с. 28 - 31.
14. Гуревич В. И. Испытания микропроцессорных реле защиты. - PRO Электричество, 2008, № 1 (25), с. 41 - 43.
15. Гуревич В. И. Электромагнитный терроризм - новая реальность 21 века. – Мир техники и технологий, 2005, N. 12, с. 14 – 15.
16. 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.
17. 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).
18. Гуревич В. И. Кибероружие против энергетики. - PRO Электричество, 2011, №1, с. 26 - 29.
19. Проблемы микропроцессорных устройств релейной защиты - http://digital-relay-problems.tripod.com
20. Гуревич В. И. Назрела необходимость стандартизации в области конструирования микропроцессорных защит. - Вести в электроэнергетике, 2011, № 4, с. 34 - 42.
21. Гуревич В. И. Новая концепция построения микропроцессорных устройств релейной защиты. - Компоненты и технологии, 2010, № 6, с. 12-15.
22. Гуревич В. И. Перспективы применения гибридной технологии в релейной защите и автоматике. - Компоненты и технологии, 2011, № 10, с. 70 - 73.
23. Гуревич В. И. Гибридные герконо-полупроводниковые устройства - новое поколение реле защиты - Проблемы энергетики, N. 9-10, 2007, с. 27 - 36.