

УДК 621.316.925

Энергобезопасна ли релейная защита?



В. И. Гуревич,

кандидат технических наук,
почетный профессор,
эксперт комитета ТС-94
Международной электротехнической комиссии,
Israel Electric Corp., Израиль

Повышение технического уровня устройств релейной защиты не обязательно ведет к эквивалентному повышению эффективности в части реагирования на возникающие повреждения. Назначением же релейной защиты видится непосредственно релейная защита (то есть выявление аварийного режима и выдача команды на электрические аппараты, производящие изменения режима работы защищаемого объекта с целью ликвидации аварийного режима). Автором рассмотрены возможные последствия придания релейной защите дополнительных функций.

Ключевые слова: «интеллектуальная» электрическая сеть, релейная защита, цифровые реле, упрещающие функции.

Компьютерами с сетевым подключением сегодня оснащены практически все виды современных промышленных производств, системы управления водоснабжением и электроснабжением, системы телекоммуникации и связи. В технической литературе появились термины «разумная электрическая сеть» (Smart Grid), «релейная защита с искусственным интеллектом» (Artificial Intelligence), «умный дом» (Smart House). Микропроцессоры сегодня используются повсеместно [1].

Но реальность такова, что основными причинами крупных аварий в энергосистемах, происшедших на разных континентах (США – 1965, 1977, 2003; Франция – 1978; Канада – 1982, 2003; Италия – 2003; Лондон – 2003; Швеция – 1983, 2003), оказались неправильные, а вернее, непредсказуемые действия релейной защиты в сложных аварийных режимах, отключивших не те участки сети, которые нужно было отключить в данных ситуациях. Речь идет об энергосистемах США и Западной Европы, в значительной степени оборудованных компьютерами и микропроцессорными защитами. Для сравнения отметим, что в энергосистеме России с достаточно изношенным оборудованием таких случаев не было. Каково объяснение?

«Само по себе повышение технического уровня устройств релейной защиты (УРЗ) не обязательно ведет к эквивалентному повышению эффективности

в части реагирования на возникающие повреждения. Так, например, устаревшие к настоящему времени электромеханические и, отчасти, электронные статические УРЗ при правильном выборе защитных функций и уставок, безусловно, обеспечат более эффективную защиту сети, чем микропроцессорные УРЗ без достаточно обоснованного выбора указанных параметров.» [2]. Действительно, поведение в аварийных ситуациях электромеханических и электронных статических УРЗ было жестко детерминировано принципом их действия и заложенными в них уставками. Современные же тенденции [2–7] в развитии микропроцессорных устройств релейной защиты (МУРЗ) связаны с увеличением степени их «самостоятельности» (то есть, фактически, непредсказуемости) в выборе решений. Речь идет об использовании в релейной защите возможности самообучения, характерной для адаптивных нейронных сетей, использовании технологий искусственного интеллекта с нечеткой логикой и т.д.

Еще одной тенденцией, четко просматривающейся в развитии современных МУРЗ, является их чрезмерное усложнение за счет придания им посторонних функций, совершенно не характерных для релейной защиты. Вот, например, как выглядит перечень функций, выполняемых так называемым «разумным контроллером» (Intelligent Protection and Automation Controller Ipac, Dynatrol Systems Inc.).

Измеряемые величины:

- действующие значения токов и напряжений;
- действующее значение тока в нейтрали;
- коэффициент мощности;
- полная мощность;
- активная мощность;
- реактивная мощность;
- измерение гармоник в токе и напряжении на основе разложения в ряд Фурье;
- вычисление коэффициента гармоник (THD – Total Harmonic Distortion);
- измерение частоты.

Защитные функции:

- синхронизация с сетью;
- пониженное напряжение;
- направление мощности;
- асимметрия фазных напряжений;
- токовая отсечка;
- зависимая токовая защита;
- повышенное напряжение;
- баланс напряжений;
- токовая направленная защита;
- автоматическое повторное включение с функциями контроля режима;
- понижение и повышение частоты;
- управление отключающей катушкой выключателя;
- дифференциальная защита трансформатора.

Добавьте к этому мониторинг внешних цепей тока и напряжения, регистрацию событий, функции цифрового осциллографа аварийных режимов и другие, ставшие уже обычными, функции МУРЗ.

Придание релейной защите дополнительных, не свойственных собственно защите, функций приводит не только к физическому усложнению устройства и, как следствие, к снижению его надежности, но и к усложнению программного обеспечения и пользовательского интерфейса. Это, в свою очередь, приводит к резкому возрастанию ошибок при работе с программным обеспечением (так называемый «человеческий фактор»). При наличии такого большого количества функций, использующих одни и те же внутренние ресурсы МУРЗ при возможности конкуренции между встроенными логическими функциями во время сложного аварийного режима, сопровождающегося переходом одного вида повреждения в другое, уже далеко не всегда становится возможным предугадать поведение защиты. А повреждение одного из общих для всех функций внутренних элементов МУРЗ (источника питания, ватчдога, памяти, микропроцессора или вспомогательных узлов, обслуживающих его, и т.п.) приведет к мгновенной потере сразу всех защитных функций.

Помимо опасности потери контроля над действиями релейной защиты, современные тенденции ее развития повышают и опасность хакерских атак на энергосистемы, поскольку через компьютеризированные системы релейной защиты имеется возможность изменять состояние и воздействовать на режимы работы энергосистемы. Несмотря на серьезную озабоченность специалистов этой проблемой [8], тенденция

все большей и большей подверженности энергосистем хакерским атакам лишь увеличивается.

Еще одной серьезной угрозой устойчивости энергосистем, основывающейся на современных тенденциях ее развития, является развитие технологий искусственного преднамеренного деструктивного воздействия на электронную и компьютерную аппаратуру [9–15]. Развитию этих технологий во всем мире способствуют, с одной стороны, все большее распространение микропроцессорных технологий и элементов памяти, обладающих высокой чувствительностью к внешним электромагнитным излучениям, и тенденция постоянного увеличения плотности элементов микроэлектроники за счет снижения толщины рабочих и изоляционных слоев в кристаллах, с другой стороны. Эти две противоположные тенденции образуют весьма опасный вектор развития современной технологии. В сети Интернет можно найти множество описаний таких устройств [15].

В отличие от изолированных компьютерных систем измерения и мониторинга релейная защита непосредственно связана с возможностью воздействия на режимы работы энергосистемы. В этом заключается главное и основополагающее отличие релейной защиты от всех других компьютеризированных устройств и систем, используемых в электроэнергетике, которое обуславливает и необходимость иного подхода к релейной защите. А иной подход – это максимальное повышение надежности РЗ за счет отказа от использования в ней функций, не свойственных релейной защите, ограничение количества функций в одном МП-терминале, отказ от использования алгоритмов с недетерминированной логикой, допускающих непредсказуемые действия релейной защиты, максимальное упрощение программного интерфейса, проведение специальных исследований и разработок, обеспечивающих функционирование релейной защиты в условиях преднамеренных деструктивных электромагнитных воздействий, например, за счет введения резервного комплекта РЗ при чрезвычайных ситуациях. На роль такого резервного комплекта РЗ, устойчивого к воздействию преднамеренных электромагнитных воздействий, не требующего оперативного питания и всегда готового к работе, подходят лишь электромеханические реле. Поэтому электромеханические реле еще рано списывать со счетов. Наоборот, их необходимо совершенствовать за счет использования новых технологий и материалов и обновлять их номенклатуру.

Поскольку алгоритмы собственно релейной защиты не так уж сложны (если все они могли быть с большой надежностью реализованы на электромеханике, составляющей сегодня свыше 90% всех реле защиты в России), то это означает, что современные защиты могут быть максимально простыми. Никаких новых функций в релейной защите с началом использования МУРЗ не появилось, а были лишь улучшены некоторые характеристики РЗ, в частности у дистанционных защит появилась полигональная характеристика вместо круговой характеристики старых электромеханических реле. Поэтому никаких объ-

активных причин для существенного усложнения функций релейной защиты, наблюдаемого сегодня, в действительности не существует.

С другой стороны, в последнее время появляются все более сложные и совершенные системы мониторинга режимов работы электрооборудования на основе постоянного контроля электрических характеристик (тангенса угла диэлектрических потерь, частичных разрядов в изоляции, тока утечки разрядников, количества и качественного состава газов, растворенных в трансформаторном масле, и т.п.) и прогнозирования развития процессов во времени. Все более сложными становятся системы АСУТП, системы измерения в реальном времени векторных значений токов, напряжений и мощностей, системы регистрации и осциллографирования аварийных режимов и т.д. В отличие от релейной защиты все эти системы не могут непосредственно воздействовать на режим работы энергосистем и поэтому никаких ограничений в тенденциях их развития не существует.

Выводы

Назначением релейной защиты видится непосредственно релейная защита (то есть выявление

аварийного режима и выдача команды на электрические аппараты, производящие изменения режима работы защищаемого объекта с целью ликвидации аварийного режима) и не более того. Все остальные проблемы должны решаться другими, независимыми от релейной защиты системами. Поэтому дальнейшее развитие микропроцессорной релейной защиты и других микропроцессорных и компьютерных систем в электроэнергетике должно происходить независимыми параллельными курсами, не связанными между собой.

Для того чтобы пресечь навязывание производителями энергетикам все более «навороченные» и менее надежные МУРЗ, необходимо сформулировать основные требования к принципам конструирования МУРЗ (не к техническим параметрам, а именно к принципам конструирования) в соответствующем стандарте. В эти же принципы могли бы войти и высказанные ранее предложения по конструктивному исполнению МУРЗ в виде набора отдельных универсальных по функциям, размерам и контактному присоединениям заменяемых модулей (печатных плат) по аналогии с персональными компьютерами.

Литература

1. Гуревич В. И. Цена прогресса // Компоненты и технологии. – 2009. – № 8.
2. Шнеерсон Э. М. Цифровая релейная защита. – М.: Энергоатомиздат, 2007.
3. Bittencourt A., Carvalho de M. R., Rolim J. G. Adaptive Strategies in Power Systems Protection using Artificial Intelligence Techniques. – The 15th International Conference on Intelligent System Applications to Power Systems, Curitiba, Brazil November 8 – 12, 2009.
4. Laughton M. A. Artificial Intelligence Techniques in Power Systems, In book “Artificial intelligence techniques in power systems”, The Institution of Engineering and Technology, 1997. – P. 1–18.
5. Khosla R., Dillion T. Neuro-Expert System Applications in Power Systems. – In book “Artificial intelligence techniques in power systems”, The Institution of Engineering and Technology, 1997. – P. 238 – 258.
6. Лямец Ю. Я., Кержаев Д. В., Нудельман Г. С., Романов Ю. В. Многомерная релейная защита. Тезисы докладов Второй Международной научно-технической конференции «Современные направления развития систем релейной защиты и автоматики энергосистем». Москва 7–10 сентября 2009 г.
7. Камель Т. С., Хассан М. А., Эль-Моршеди А. (Cairo University, Египет). Применение систем искусственного интеллекта в дистанционной защите линии электропередачи. Тезисы докладов Второй Международной научно-технической конференции «Современные направления развития систем релейной защиты и автоматики энергосистем». Москва 7–10 сентября 2009 г.
8. ЦРУ: Хакинг электрических сетей возможен. CNews.ru: Лента новостей. 24.01.2008. [Электронный ресурс]. Код доступа: <http://www.cnews.ru/news/line/index.shtml?2008/01/24/285018>.
9. Гуревич В. И. Электромагнитный терроризм – новая реальность XXI века // Мир техники и технологий. – 2005. – № 12. – С. 14 – 15.
10. Daamen D. Avant-garde Terrorism: Intentional Electro Magnetic Interference. 2002. 23 p.
11. Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. [Электронный ресурс]. Код доступа: http://www.empcommission.org/docs/empc_exec_rpt.pdf
12. Ганнота А. Объект поражения – электроника // Независимое военное обозрение. – 2001. – № 13.
13. Лоборев В., Парфенов Ю., Фортов В. Коллапс бесшумного взрыва // ЛГ. – 2002. – № 5 (5865). – 6–12 февраля.
14. Покровский В. Электромагнитный фактор // Независимая газета. – 2003. – 08 окт.
15. Вдкстрцм М. Is Intentional EMI a Threat Against the Civilian Society? SAAB Communication, 2006.