УДК 621.318.5.001.8

НАДЕЖНОСТЬ МИКРОПРОЦЕССОРНЫХ УСТРОЙСТВ РЕЛЕЙНОЙ ЗАЩИТЫ: МИФЫ И РЕАЛЬНОСТЬ

В.И. ГУРЕВИЧ

Центральная лаборатория электрической компании Израиля

В статье рассмотрены четыре основных тезиса о якобы чрезвычайно высокой надежности микропроцессорных защит (МЗ), выдвигаемых, обычно, сторонниками всеобъемлющей компьютеризации электроэнергетики и скорейшего перехода на МЗ. На основе подробного анализа с привлечением большого количества литературных источников показано, что в основе утверждений о высокой надежности МЗ лежат распространенные мифы и на самом деле надежность МЗ ниже надежности электромеханических и электронных реле защиты на дискретных элементах.

Введение.

Неправильные действия релейной защиты являются одной из основных причин возникновения тяжелых аварий, периодически происходящих в энергосистемах во всем мире. По данным North American Electric Reliability Council [1] в 74% случаев причиной тяжелых аварий в энергосистемах были неправильные действия релейной защиты в процессе развития аварии. Поэтому от надежности релейной защиты во многом зависит надежность всей энергосистемы.

Интенсивные научно-исследовательские и конструкторские работы в области электромеханических реле защиты (ЭМЗ) были фактически полностью заморожены около 30 – 35 лет тому назад, и все усилия разработчиков были переключены на создание электронных, а затем и микропроцессорных устройств релейной защиты (МУРЗ). ЭМЗ полностью обеспечивали и обеспечивают до сих пор надежную защиту объектов электроэнергетики, поэтому причиной полного забвения ЭМЗ и перехода на МУРЗ является не неспособность ЭМЗ выполнять свои функции, а нечто совершенно иное. Вследствие проводимой ведущими компаниями-производителями реле защиты технической политики, прогресс последних десятилетий в области новых материалов и технологий никак не затронул ЭМЗ. Находящиеся десятки лет в эксплуатации ЭМЗ на сегодняшний день сильно износились и устарели, и поэтому вызывают справедливое недовольство обслуживающего персонала. С другой стороны, демонтаж ЭМЗ и переход на микропроцессорные реле защиты на действующих объектах электроэнергетики связан с необходимостью инвестирования значительных денежных средств, причем не только на приобретение МУРЗ, компьютеров и специального дорогостоящего тестового оборудования, на замену вышедших из строя и не подлежащих ремонту весьма дорогостоящих блоков МУРЗ. Значительные капиталовложения потребуются также и на реконструкцию системы заземления подстанции, на обучение обслуживающего персонала и т.д. Все это существенно тормозит процесс перехода на МУРЗ. По данным [2], к 2002 году в энергосистемах России находилось в эксплуатации 98,5% ЭМЗ и только 1,5% различных электронных устройств релейной защиты, а по данным [3], количество МУРЗ составляет около 0,12% от общего количества устройств

релейной защиты. На Западе темпы замены релейной защиты на действующих объектах также не очень высоки. По данным [4], при существующих темпах потребуется около 70 лет для замены всех реле защиты на микропроцессорные. Такие низкие темпы обновления парка релейной защиты на действующих объектах электроэнергетики во всем мире обуславливает интенсивную рекламную деятельность компаний-производителей МУРЗ и их торговых агентов.

Одним из основных доводов, приводимых обычно в доказательство преимуществ МУРЗ, является их, якобы, значительно более высокая надежность по сравнению с электромеханическими и электронными защитами. Этот тезис представляется настолько очевидным, что, обычно, не вызывает возражений и часто повторяется менеджерами и даже техническим персоналом электроэнергетических компаний. Однако при более глубоком анализе ситуации оказывается, что основу этого тезиса составляет целый набор распространенных мифов о микропроцессорных защитах [5].

Миф 1. ***Надежность МУРЗ выше надежности ЭМЗ потому, что МУРЗ не содержит подвижных частей [6].***

Отказы ЭМЗ связывают в литературе, обычно, со старением и повреждением изоляции (истирание, высыхание), ржавлением винтов и клеммных зажимов, износом в механической части реле. Однако с учетом того, что количество циклов срабатывания (то есть движения подвижных частей) за весь срок службы ЭМЗ в реальных условиях эксплуатации в энергосистемах не превышает нескольких сотен, говорить о механическом износе подвижных частей реле можно только в случае явного брака завода-изготовителя или использования неподходящих для этих целей материалов. Что касается коррозии металлических элементов или высыхания изоляции, то это следствие использования при изготовлении реле некачественных материалов. Такие дефекты являются характерными для ЭМЗ Российского производства и практически не встречаются в реле ведущих Западных компаний, находящихся в эксплуатации по 30-40 лет даже в условиях тропического климата [7]. Таким образом, говорить о недостаточном механическом ресурсе ЭМЗ, как вида реле, абсолютно необоснованно. С другой стороны, если подвижные элементы ЭМЗ находятся в движении *только в моменты срабатывания реле*, то тысячи электронных компонентов МУРЗ *постоянно находятся в работе*: постоянно работают генераторы сигналов, многочисленные транзисторные ключи, усилители, стабилизаторы напряжения, микропроцессор постоянно обменивается сигналами с элементами памяти, аналого-цифровой преобразователь постоянно ведет обработку входных сигналов и т.д. Многие элементы постоянно находятся под воздействием высокого рабочего напряжения (220 - 250 В) и импульсов перенапряжений, периодически возникающих во входных цепях и цепях питания, постоянно рассеивают мощность (то есть греются) и т.д. В особо тяжелом режиме работают в МУРЗ импульсные высокочастотные источники питания, которые очень часто являются причиной отказов МУРЗ.

Миф 2. ***Надежность полупроводниковых реле на дискретных компонентах выше надежности электромеханических реле [8]. Надежность полупроводниковых устройств защиты на основе интегральных микросхем с высокой степенью интеграции выше, чем надежность устройств на дискретных электронных компонентах [8]. Надежность микропроцессорных реле выше надежности электронных не микропроцессорных устройств.***

Утверждение о безусловно большей надежности электронных реле перед электромеханическими – распространенное заблуждение [9]. Повышенной надежностью полупроводниковые реле обладают только при очень большом (сотни тысяч, миллионы) количестве коммутационных циклов или при большой частоте коммутации. Во многих других случаях надежность полупроводниковых реле существенно ниже надежности электромеханических [10].

Дискретные электронные элементы имеют гораздо более высокую устойчивость к перенапряжениям и другим неблагоприятным воздействиям, чем интегральные микросхемы [11]. По данным [12], 75% всех повреждений микропроцессорных устройств происходит по причине воздействия перенапряжений. Такие перенапряжения с амплитудой от десятков вольт до нескольких киловольт, возникающие вследствие коммутационных процессов в цепях [13] или при воздействии электростатических разрядов, являются «смертельными» для внутренних микроэлементов микросхем и процессоров. По данным [12], обычные транзисторы (дискретные элементы) могут выдерживать напряжение электростатического разряда почти в 70 раз более высокое, чем, например, микрочип памяти (EPROM) микропроцессорной системы. Самое страшное, что случайные сбои в работе микропроцессора, вызванные электромагнитными шумами, могут быть временными [14], такими как самопроизвольные изменения содержания оперативной памяти (RAM) и регистров, а внутренние повреждения могут носить скрытый характер [15]. Оба этих вида повреждений не выявляются никакими тестами и могут проявляться в самые неожиданные моменты.

В докладе [16] отмечается, что, в связи с низкой устойчивостью МУРЗ к переходным процессам и перенапряжениям, МУРЗ предъявляют особо жесткие требования к защите от электромагнитных воздействий. Попытки использования микропроцессорных реле без усиленной электромагнитной защиты часто приводят к их отказам [16, 17]. Электронные устройства на дискретных элементах содержат гораздо меньше компонентов, чем аналогичные по параметрам устройства на интегральных микросхемах (рис. 1), что уже само по себе отнюдь не способствует более высокой надежности интегральных микросхем.

Да и статистика по повреждениям элементов МУРЗ, собранная представителями различных компаний-производителей МУРЗ (рис. 2) [18], очень убедительно опровергает очередной миф о более высокой надежности интегральных микросхем.

По данным статистики, представленным в работе [8], хорошо видно, что реле защиты на электронных элементах имеют втрое большую повреждаемость, чем электромеханические, а микропроцессорные – в 50 раз большую повреждаемость.

Надежность микропроцессоров таких производителей, как Intel, AMD может быть очень высокой, но ведь микропроцессор – это всего лишь небольшая, хотя и очень важная часть МУРЗ, содержащего много десятков микросхем. В [19] утверждается, что блок микропроцессора (то есть печатная плата с микропроцессором, памятью, аналого-цифровым преобразователем, библиотекой программ и всеми вспомогательными элементами) – наиболее подверженная отказам часть МУРЗ. Кроме того, в отличие от обычных микросхем, отказом микропроцессора является не только его физическое повреждение, но также и сбои в его программном обеспечении – повреждения, не известные ранее для электромеханических и электронных реле. Как отмечено в [19], программные багги далеко не всегда обнаруживаются при тестировании МУРЗ.

Дополнительным источником проблем является необходимость периодического обновления (upgrade) версий программ, используемых МУРЗ, при котором часто возникает несоответствие между «железом» и программой (hardware and software incompatibilities) [19]. Такого рода проблемы могут проявиться в самые неожиданные моменты и могут привести к очень тяжелым последствиям для сети. Как известно, одной из причин крупнейшей аварии в энергосистемах США и Канады в августе 2003 года была именно «компьютерная проблема», обусловленная «зависанием» компьютерной системы управления в энергосистеме "First Energy" [20].

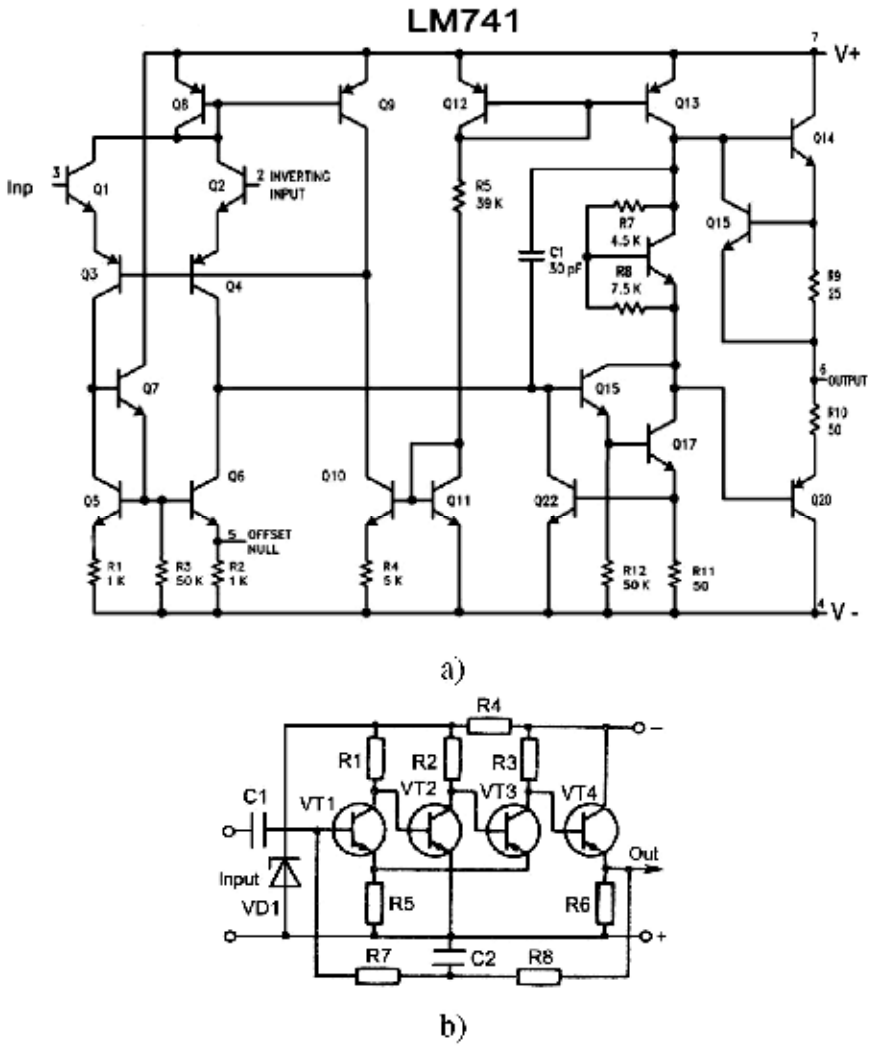

Рис. 1. Принципиальные схемы двух усилителей сигналов с близкими параметрами: вверху – интегральной микросхемы типа LM741 широкого применения, содержащего 20 транзисторов; внизу – усилителя на дискретных элементах, содержащего 4 транзистора

Рис. 2. Статистические данные по повреждениям МУРЗ ведущих Японских компаний [18]

<u>Миф 3.</u> ***Надежность МУРЗ значительно выше надежности всех остальных типов реле защиты благодаря наличию встроенной самодиагностики. Самодиагностикой в МУРЗ охвачено 70 – 80 % всех элементов МУРЗ [21, 30].***

Этот тезис является очень распространенным и встречается практически во всех публикациях, посвященных преимуществам МУРЗ. Рассмотрим особенности этой самодиагностики подробнее.

- ***Аналого-цифровой преобразователь (АЦП)*** **– это устройство, преобразующее входной аналоговый сигнал с трансформаторов тока и напряжения в двоичный код, передаваемый через специальные фильтры на обработку в микропроцессор. Все АЦП работают путём выборки входных значений через фиксированные интервалы времени и, таким образом, преобразуют синусоидальный сигнал в набор фиксированных амплитуд. Как можно видеть из приведенного на рис. 3 примера, это довольно сложное устройство, осуществляющее довольно сложный алгоритм и содержащее множество внутренних узлов.**

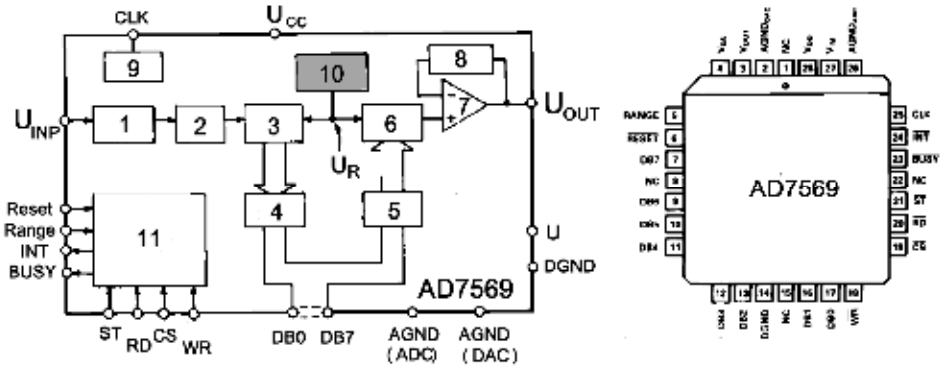

Рис. 3. Структура аналого-цифрового преобразователя типа AD7569: 1 – блок установки диапазона; 2 - блок слежения/хранения; 3 – аналого-цифровой преобразователь (АЦП); 4 – регистр АЦП; 5 – регистр цифро-аналогового преобразователя (ЦАП); 6 – ЦАП; 7 – усилитель; 8 – блок установки диапазона; 9 – блок синхронизации; 10 – источник опорного напряжения

Некоторые современные АЦП настолько сложны, что включают в себя даже небольшой микропроцессор, управляющий их работой. АЦП – это фактически главный узел измерительного устройства. Как и любому сложному измерительному устройству, АЦП свойственны различные погрешности и ошибки преобразования входной величины. Это ошибки квантования; аддитивная и мультипликативная погрешности; дифференциальная и интегральная нелинейности передаточной характеристики; апертурная погрешность; ошибка, вызванная наложением частот (aliasing). Как же можно контролировать в процессе непрерывно изменяющейся входной величины исправность такого сложного устройства? Поскольку единственным элементом с неизменным уровнем сигнала в процессе работы АЦП является источник опорного напряжения *10*, то именно на его мониторинге и основана так называемая «самодиагностика» АЦП [21]. О пользе и эффективности такой самодиагностики читатель может судить сам.

● *Память*. В МУРЗ имеется два различных вида памяти: ПЗУ (постоянное запоминающее устройство или ROM), предназначенное для хранения управляющей программы и уставок, и ОЗУ (оперативное запоминающее устройство или RAM), предназначенное для временного хранения результатов измерения входных величин и промежуточных вычислений. Управляющий алгоритм представляет собой набор определенных числовых кодов. Из этих кодов составляется некая контрольная сумма, которая запоминается в отдельной ячейке памяти. В процессе работы МУРЗ эта предварительно записанная контрольная сумма периодически сравнивается с фактической. Несовпадение этих сумм должно указывать на неисправность ПЗУ [21]. Понятно, что процесс вычисления фактической контрольной суммы и сравнения ее с предварительно записанной суммой - это процесс дискретный, производимый с определенными интервалами. А что будет, если повреждение возникнет в промежуток времени между интервалами сравнения контрольных сумм? Произойдет ложное срабатывание реле защиты и отключение линии электропередач? Вопрос отнюдь не гипотетический. Такие реальные случаи невыявленных системой самодиагностики сбоев описаны в литературе [19].

Ситуация с самотестированием ОЗУ обстоит намного сложнее, так как содержимое ОЗУ постоянно изменяется случайным образом, причем с большой частотой, в процессе работы МУРЗ. Трудно даже себе представить, как вообще можно тестировать в процессе функционирования постоянно перезаписываемые с большой частотой ячейки памяти, то есть диагностировать так называемые «динамические сбои». Производители МУРЗ решили особо не утруждать себя решением этой проблемы и тестировать ОЗУ в автоматическом режиме путем периодического записывания в специально зарезервированные для этого ячейки памяти некоего постоянного числа и периодического считывания этого числа с последующим сравнением этих двух чисел. Совпадение этих чисел должно, по замыслу производителей, якобы подтверждать исправность всего ОЗУ [21], хотя совершенно не понятно, как можно судить об исправности всего ОЗУ по факту сохранности информации в нескольких ячейках памяти. Кроме того, хорошо известно, что отсутствие статических ошибок памяти абсолютно не гарантирует возникновение динамических ошибок [22, 23], то есть ошибок, возникающих непосредственно в процессе записи и считывания информации.

Вопрос о надежности элементов памяти МУРЗ в действительности намного сложнее. Оказывается, элементы памяти подвержены случайным

непредсказуемым сбоям, не связанным с физическим повреждением ячеек памяти. Такие случайные обратимые сбои, обусловленные самопроизвольным изменением содержания ячеек памяти, называются «мягкими ошибками» (“soft-failures” или “soft errors”, не путать с программными ошибками - “software programming errors”). Ошибки такого рода были не известны ранее для электронных устройств, выполненных на дискретных полупроводниковых элементах или на обычных микросхемах. Прогресс последних лет в области нанотехнологий привел к существенному снижению размеров полупроводниковых элементов (речь идет о единицах и даже долях микрона), уменьшению толщины слоев полупроводниковых и изоляционных материалов, уменьшению рабочих напряжений, увеличению рабочей скорости, уменьшению электрической емкости отдельных ячеек памяти, увеличению плотности размещения элементарных логических ячеек в одном устройстве. Все это вместе взятое привело к резкому повышению чувствительности элементов памяти к ионизирующим излучениям [24, 25]. Эта чувствительность стала настолько высокой, что обычный (то есть совершенно нормальный) радиационный фон на уровне моря стал опасным для ячеек памяти. Особенно опасными являются потоки высокоэнергетических элементарных частиц, приходящих из космоса. Даже одна такая частица при попадании в ячейку памяти рождает вторичные потоки электронов и ионов, вызывающие самопроизвольное переключение элементарного транзистора или разряд емкости в элементах с зарядовой памятью. Проблема усугубляется тем, что в современных микропроцессорных структурах наблюдается устойчивая тенденция расширения использования элементов памяти [25]. Многие современные интегральные микросхемы высокого уровня интеграции, входящие в состав микропроцессорного устройства, содержат встроенные элементы памяти достаточно большого объема, исправность которых вообще никак не контролируется. Как показано в [26, 27], проблема резкого увеличения чувствительности к ионизирующим излучениям актуальна не только для элементов памяти, но также и для высокоскоростных логических элементов, компараторов и т.д., то есть, практически, для всей современной микроэлектроники.

● *Центральный процессор (ЦП)*. В отличие от описанных выше сложностей с контролем исправности памяти, самоконтроль ЦП выглядит достаточно простым, рис. 4.

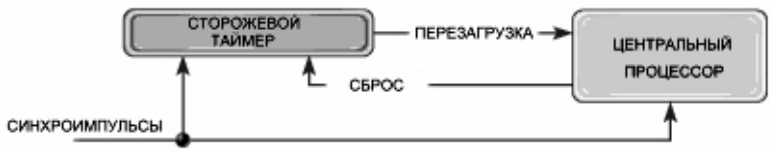

Рис. 4. Принцип автоматического контроля исправности микропроцессора с помощью сторожевого таймера

Он просто посылает контрольные импульсы с заданным периодом следования в так называемый «watchdog timer» – сторожевой таймер (“watchdog” - дословно «сторожевой пес»), который сбрасывается в исходное состояние с приходом каждого нового контрольного импульса, после чего начинает новый отсчет времени. Если к определенному моменту времени с ЦП не поступил очередной контрольный импульс, таймер запускает процесс перезагрузки ЦП. При серьезной неисправности микропроцессора и его «зависании» при перезагрузке, которое обнаруживается таймером как повторное отсутствие контрольного сигнала, происходит блокирование

ЦП и выдача сигнала о неисправности центрального процессора. Работа по отслеживанию контрольных импульсов сторожевым таймером синхронизирована с помощью внешних синхроимпульсов (так называемое «стробирование»). Иногда сторожевые таймеры встраиваются непосредственно в микропроцессор, иногда (что предпочтительнее) представляют собой внешние специализированные интегральные микросхемы. Примером таких устройств могут служить микросхемы из серии ADM690 – ADM695, производимые компанией Analog Devices. Такой маленький чип содержит не только сторожевой таймер, но также и монитор напряжения питания ЦП. Пауза между контрольными импульсами сторожевого таймера этой серии может быть 0,1 или 1,6 сек.

Совершенно очевидно, что проверить таким образом исправность сотен тысяч транзисторных наноструктур, из которых собственно и состоит любой микропроцессор, абсолютно невозможно. Речь может идти о мониторинге лишь общей работоспособности ЦП, то есть о том, жив он или мертв. При очень сложной внутренней структуре ЦП (рис. 5), содержащей большое количество узлов (регистры для временного хранения команд, данных и адресов; арифметико-логическое устройство; стек, система управлении и синхронизации и т.д.) и микроэлементов, контрольные сигналы с ЦП могут продолжать поступать на сторожевой таймер даже если часть внутренней структуры ЦП окажется поврежденной. Очевидно, что повреждения участков структуры ЦП (или участков его внутренней управляющей программы) могут проявиться только во время работы (то есть активизации) этих участков. Если эти участки ЦП активизируются лишь при сигналах, соответствующих аварийным режимам в электрической сети, то это означает, что сторожевой таймер – это слабое утешение.

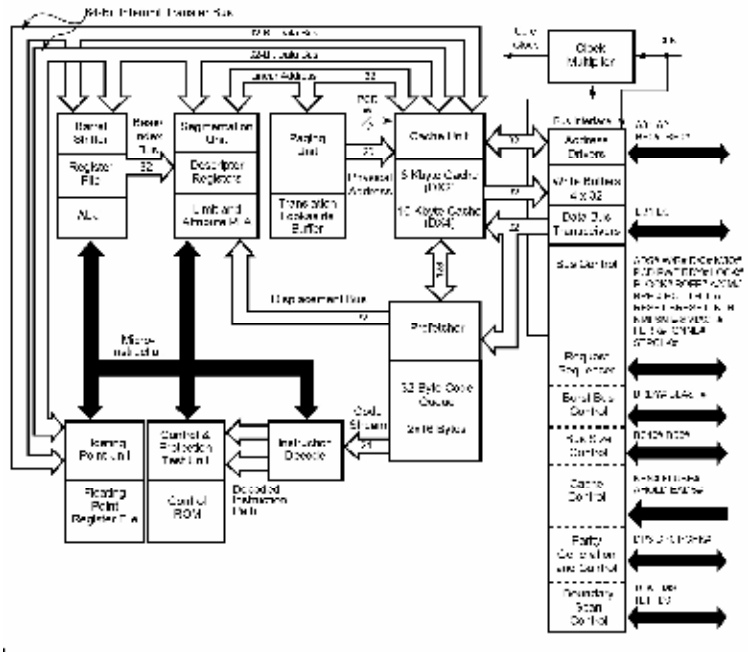

Рис. 5. Блок-схема микропроцессора Intel 486 SX

Сам по себе сторожевой таймер – это устройство, выполненное по такой же самой технологии, как и все остальные устройства микроэлектроники (рис. 6), и точно так как и все остальные устройства, содержащие микроэлектронные компоненты, подвержен отказам и сбоям в работе. Вследствие описанного выше

алгоритма работы сторожевого таймера, его отказ в процессе нормального функционирования МУРЗ может привести либо к блокированию ЦП и выходу из строя всего МУРЗ, либо к тому, что он не заметит «зависания» ЦП, в результате чего релейная защита не сработает должным образом при возникновении аварийного режима. Таким образом, работоспособность всего МУРЗ оказывается в очень сильной зависимости от исправности одного маленького чипа, называемого «watchdog».

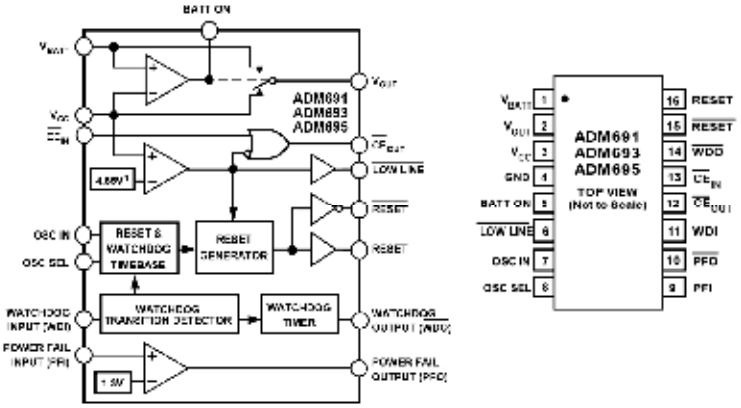

Рис. 6. Блок-схема сторожевого таймера (“watchdog”) серии ADM691 – ADM695, производимого компанией Analog Devices

Еще одним важным обстоятельством является то, что ЦП вовсе не является каким-то отдельно стоящим элементом, правильное функционирование которого в составе МУРЗ не зависит от исправности десятков других сложных интегральных микросхем, с которыми связан ЦП, но самодиагностика которых не предусмотрена. Достаточно взглянуть на печатную плату блока центрального процессора (рис. 7), чтобы понять, что исправность самого ЦП еще не говорит об исправности всего этого блока. Повреждение любого из многочисленных микроэлектронных (и не только!) компонентов этой многослойной платы с неизбежностью приведет к нарушению правильного функционирования МУРЗ, и никакой watchdog здесь не поможет, что и подтверждается данными, приведенными в [19].

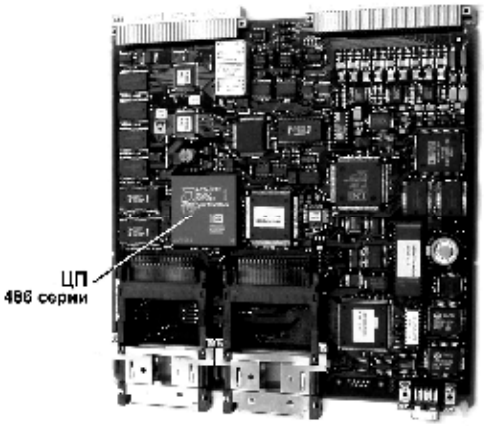

Рис. 7. Печатная плата блока центрального процессора МУРЗ серии RE*_316 (производитель – компания ABB)

● ***Источник питания*. МУРЗ всех типов снабжаются так называемыми импульсными источниками питания, в которых входное напряжение (переменное или постоянное) поступает на выпрямитель и фильтр, после чего прерывается с большой частотой (десятки килогерц) с помощью мощного транзисторного коммутирующего элемента, то есть превращается в переменное высокочастотное. Это высокочастотное напряжение трансформируется с помощью высокочастотного трансформатора в напряжение низкого уровня (чаще всего, 12В), выпрямляется,**

фильтруется и стабилизируется. Далее из этого постоянного напряжения формируются более низкие напряжения (5 В, например), необходимые для работы МУРЗ. Микропроцессоры, обычно, весьма чувствительны к уровню питающего напряжения и могут производить непредсказуемые операции при определенном снижении напряжения питания, в связи с чем в МУРЗ осуществляется постоянный мониторинг уровня напряжения питания ЦП. Как отмечалось выше, микросхемы семейства ADM 691-695 могут быть использованы для непрерывного контроля напряжения питания МУРЗ. Как и в случае со сторожевым таймером, эта микросхема производит генерацию сигнала, блокирующего работу ЦП при недопустимом снижении напряжения питания. Блокирующий сигнал остается до тех пор, пока напряжение питания не восстановится. Можно ли считать такой контроль уровня напряжения источника питания его самодиагностикой, повышающей надежность его функционирования? Вряд ли, поскольку речь идет о чисто технологической внутренней блокировке, предотвращающей сбои в ЦП. К надежности источника питания такой контроль не имеет никакого отношения. А между тем, именно источники питания МУРЗ являются самым ненадежным узлом МУРЗ. Во-первых, элементы источника питания работают в очень напряженном режиме: они постоянно подвержены воздействию высоких значений напряжения и тока, рассеивают довольно высокие мощности на своих элементах. Во-вторых, они содержат большое количество алюминиевых электролитических конденсаторов, весьма плохо переносящих воздействие токов высокой частоты, на которой работают источники питания, и часто являющихся причиной полного отказа источника питания, (а следовательно, и всего МУРЗ). Ну и чем тут может помочь мониторинг выходного напряжения источника? Разве он может заранее просигнализировать об ухудшении состояния конденсаторов и предотвратить, таким образом, внезапный отказ МУРЗ?

● ***Выходные электромагнитные реле.*** **Как показано в исследованиях, выполненных автором [28, 29], контакты миниатюрных электромеханических реле (обычно используемых во всех типах МУРЗ в качестве выходных элементов, непосредственно управляющих отключающими катушками высоковольтных выключателей или катушками промежуточных реле) работают со значительной перегрузкой. Поэтому надежность этих реле существенно снижена по сравнению с величиной, нормируемой заводом-изготовителем. С другой стороны, в рекламных проспектах МУРЗ различных производителей обязательно отмечается, что исправность таких важных элементов, как выходные реле, непрерывно контролируется средствами самодиагностики МУРЗ. На первый взгляд весьма трудно представить, как можно проверить исправность электромеханического реле в работающем МУРЗ, если контакты этого реле включены непосредственно в цепь отключающей катушки выключателя. Ну, нельзя проверить исправность контактов реле, ну и ладно. Будем проверять то, что можно проверить, решили производители МУРЗ и стали контролировать целостность обмотки управления реле путем пропускания через нее постоянного слабого тока. Но при чем здесь обмотка, если самым напряженным и ненадежным элементом электромеханического реле является вовсе не обмотка, а контакты? Но это уже не столь важно для рекламной компании. Нужно было лишь громко заявить потребителю МУРЗ о самодиагностике выходных реле, а то, что такая самодиагностика совершенно неэффективна и ничего не дает, то об этом, как правило, почти никто не знает.**

● ***Узлы цифровых и аналоговых входов.*** **Узел цифровых входов – это набор мощных гасящих резисторов, оптронов, электронных фильтров, мультиплексоров и**

т.д., смонтированных, обычно, на плате вместе с выходными реле (рис. 8). Узел аналоговых входов – это трансформаторы тока и напряжения, смонтированные, как правило, на отдельной плате (рис. 9). По признанию авторов [30], эти узлы только частично охвачены самодиагностикой, причем без всяких пояснений того, как именно это сделано, а в [31] отмечается, что они вовсе не охвачены самодиагностикой. Платы аналоговых и цифровых входов МУРЗ имеют, как правило, несколько различных конфигураций (рис. 8). Тип платы, установленной в данном конкретном МУРЗ, должен быть обязательно введен в его память. Для того, чтобы прояснить ситуацию и расставить точки над *i*, мы заменили плату входов у МУРЗ типа REL316, тип которой записан в его памяти, на плату другого типа (рис. 8), без изменения записи в памяти МУРЗ, и включили его.

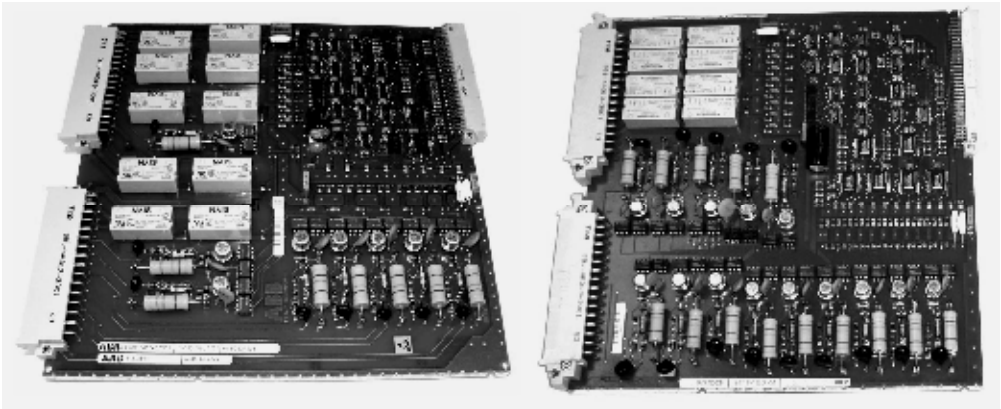

Рис. 8. Блоки цифровых входов различной конфигурации МУРЗ типа REL316

Оказалось, что МУРЗ загружается в нормальный режим работы, совершенно не замечая подмены целой платы. Естественно, что правильно функционировать он уже не будет. О какой же самодиагностике исправности внутренних компонентов этих узлов вообще может идти речь в такой ситуации? Как говорится, комментарии излишни.

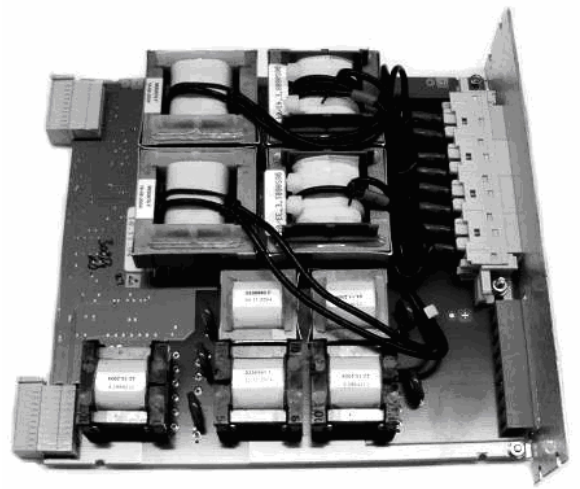

Рис. 9. Блок аналоговых входов МУРЗ, содержащий входные трансформаторы тока и напряжения

В заключение этого раздела следует отметить, что вопреки распространенному мнению, внутренняя самодиагностика на самом деле не является средством, предназначенным для снижения интенсивности отказов МУРЗ, то есть повышения его надежности. Целью такой самодиагностики является блокирование работы МУРЗ и выдача об этом сигнала тревоги до возникновения аварийного режима в сети, а не во время его.

Миф 4. ***МУРЗ являются существенно более надежными по сравнению с устройствами релейной защиты предыдущего поколения, так как содержат значительно меньшее число элементов и эти элементы значительно меньше подвержены физическому старению. МУРЗ также содержит меньшее количество внутренних соединений [32].***

Тезис о том, что МУРЗ содержит меньшее количество элементов, не выдерживает никакой критики и, по нашему мнению, вообще не требует даже обсуждения, поскольку в действительности количество элементов, из которых состоит МУРЗ на несколько порядков больше, чем количество элементов, из которых состояли реле защиты предыдущих поколений. Что касается якобы более интенсивного физического старения элементов реле защиты предыдущего поколения, то этот тезис также не выдерживает критики. Автор этого тезиса сравнивает современные материалы, применяющиеся в МУРЗ, с материалами (пропиточными и покровными лаками, пластмассами, изоляционными материалами и электрическими контактами), разработанными в СССР 50 лет тому назад и проработавшими в реле защиты десятки лет. Как мы уже отмечали выше, старые электромеханические реле западного производства, в которых применялись высококачественные материалы и покрытия, до сих пор успешно работают и прекрасно выглядят.

Кроме того, за последние десятилетия прогресс в области материалов достигнут не меньший, чем прогресс в области микроэлектроники. С другой стороны, не все обстоит так радужно со старением электронных компонентов, широко используемых в МУРЗ. Так даже высококачественные электролитические конденсаторы японского производства начинают изменять свои параметры через 7-10 лет работы в высокочастотных импульсных источниках питания, применяемых в МУРЗ.

В результате всего лишь изменения параметров одного из таких конденсаторов (рис. 10) полностью перестают функционировать, например, источники питания типа SPGU240A1, применяемые в МУРЗ типов SPAC, SPAD, SPAU, SPAJ.

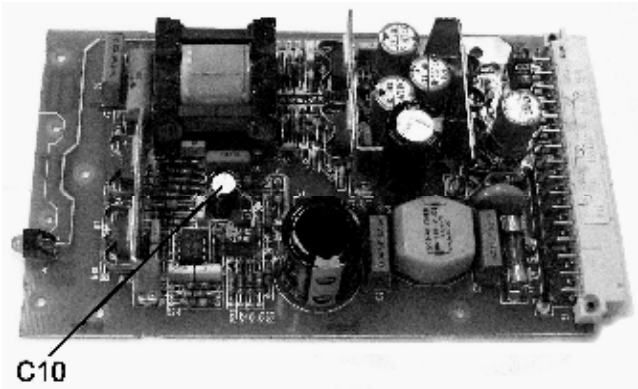

Рис. 10. Импульсный источник питания типа SPGU240A1, применяемый в МУРЗ различных типов. С10 – конденсатор, изменение параметров которого во времени приводит полной потере работоспособности источника питания

В других случаях имеет место разрушение не только электронных компонентов, но даже растворение участков медных дорожек под действием вытекшего из конденсаторов электролита (рис. 11).

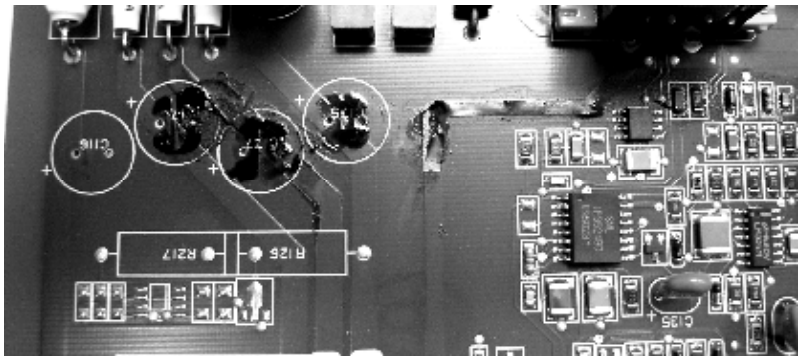

Рис. 11. Разрушение медных дорожек печатной платы, проходящих под конденсаторами, из-за просочившегося электролита

Еще одной проблемой является стремление производителей к миниатюризации МУРЗ любой ценой, что приводит к использованию в МУРЗ электронных элементов, работающих с перегрузкой и рассеивающих повышенное количество тепла, что отнюдь не способствует повышению их надежности и уменьшению старения. Особенно актуальна эта проблема для цепей цифровых входов, на которые подается напряжение до 250 В [33].

Многослойные печатные платы МУРЗ предполагают огромное количество контактных переходов (перемычек) между слоями. Из личной практики автора известны случаи неправильных действий МУРЗ вследствие возрастания переходного сопротивления этих переходов.

Конструкция многих типов МУРЗ предполагает наличие материнской печатной платы с многоконтактными разъемами и функциональных печатных плат с ответными разъемами, сочленяемыми с материнской платой. Вместо материнской платы иногда используются гибкие многожильные шины с многочисленными контактными разъемами, соединяющими между собой отдельные печатные платы. Далеко не всегда все эти контактные соединения обеспечивают надежную передачу низкоуровневых слаботочных сигналов между платами. Во всяком случае, вопреки распространенному мифу, МУРЗ содержит намного больше всевозможных контактных соединений, чем реле предыдущих поколений.

<u>Еще один класс проблем, о котором предпочитают не вспоминать.</u> В свете повышенной чувствительности современной микроэлектроники к электромагнитным излучениям, особенно актуальной для МУРЗ становится проблема электромагнитной совместимости (ЭМС). Многие специалисты обращают внимание на частое несоответствие реальных параметров систем заземления на подстанциях требованиям, предъявляемым МУРЗ [34, 35], и, как следствие этого, на отказы в работе МУРЗ. Но мало что известно специалистам в области релейной защиты о проблеме электромагнитного терроризма, то есть о преднамеренных воздействиях на устройства релейной защиты мощных электромагнитных излучений [36], а также о проблеме хакерских атак (Cyber Security) [37]. Эти проблемы были неизвестны ранее в релейной защите и стали актуальными лишь в связи с применение МУРЗ, поскольку их чувствительность

к электромагнитным помехам в 10000 раз выше, чем у электромеханических реле [34], и они имеют встроенное программное обеспечение, также подверженное внешним воздействиям. А если, в дополнение ко всему вышесказанному, принять во внимание, что один МУРЗ выполняет функции 3 – 5 ЭМЗ, то положение с надежностью МУРЗ усугубляется еще больше, так как отказ одного из общих элементов МУРЗ эквивалентен по своим последствиям одновременному отказу сразу нескольких видов защиты. В связи с этим в докладе [38] даже предлагается при переходе на МУРЗ предусматривать дополнительную независимую, простую, недорогую, *не микропроцессорную* резервную защиту на случай чрезвычайных ситуаций.

Выводы

1. Надежность МУРЗ ниже надежности электромеханических реле и электронных реле на дискретных элементах.

2. Встроенная самодиагностика МУРЗ малоэффективна и вообще не является средством повышения надежности МУРЗ.

3. Нанотехнологии, применяемые при производстве комплектующих элементов, на основе которых построены МУРЗ, приводят к возникновению неизвестных ранее для релейной защиты проблем, игнорирование их может привести к катастрофическим последствиям. Менеджеры, принимающие решения в области релейной защиты, и персонал энергокомпаний должны быть осведомлены об этих особенностях МУРЗ.

4. Функция записи аварийных режимов и функция передачи информации по современным каналам связи не являются прямыми функциями релейной защиты и для их осуществления существуют отдельные микропроцессорные системы, которые выполняют эти функции намного лучше, чем МУРЗ. В отличие от релейной защиты, отказ в работе этих устройств не приводит к тяжелым авариям в энергосистемах. Поэтому к устройствам собственно релейной защиты должны предъявляться иные требования по надежности и, соответственно, использоваться иные подходы при конструировании, направленные на повышение надежности и снижение уязвимости.

5. Ответственные лица, принимающие решения о реконструкции релейной защиты и путях ее дальнейшего развития, должны четко понимать свойства и особенности МУРЗ, учитывать не только широко рекламируемые преимущества МУРЗ, но также и их, обычно замалчиваемые, серьезные недостатки, одним из которых является пониженная надежность.

Summary

In the article four basic theses about ostensibly extremely high reliability of microprocessor-based relay protection (MP) which usually supporters by apologists of MP, are considered. Detailed analysis based on a lot of references it is shown that the basis of these theses are widespread myths, and actually MP reliability is lower than reliability of electromechanical and electronic protective relays on discrete components.

Литература

1. Hunt R. K. Hidden Failure in Protective Relays: Supervision and Control. Thesis to Master of Science in Electrical Engineering, Virginia Polytechnic Institute, 1998.

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

3. Белотелов А. К. Научно-техническая политика РАО «ЕС России» в развитии систем релейной защиты и автоматики: Сборник докладов XV научно-технической конференции «Релейная защита и автоматика энергосистем». – Москва, 2002.

4. Johnson G., Thomson M., Reliability Consideration of Multifunction Protection. – Basler Electric Corp.

5. Гуревич В. И. Как нам обустроить релейную защиту: мнения российских специалистов и взгляд со стороны // Вести в электроэнергетике, 2007 – № 2.

6. Projjalkumar R. Is the Era of Electromechanical Relays Over? - Frost & Sullivan Market Insight, 5 Mar 2004.

7. Гуревич В. И. Микропроцессорные реле защиты: альтернативный взгляд // Электро-инфо. – 2006. – № 4.

8. Heising C. R., Patterson R. C. Reliability Expectations for Protective Relays. Developments in Power Protection. Fourth International Conference in Power Protection, 11 – 13 Apr., 1989, Edinburgh, UK.

9. Mahaffey T. R. Electromechanical Relays Versus Solid-State: Each Has Its Place. Electronic Design, September 16, 2002.

10. Electromechanical vs. Solid State Relay Characteristics Comparison. Application Note 13c3235. Tyco Electronics.

11. Gurevich V. Electronic Devices on Discrete Components for Industrial and Power Engineering. Boca Raton – New York – London, CRC Press, 2008, 420 p.

12. Clark O. M., Gavender R. E. Lighting Protection for Microprocessor-based Electronic Systems. IEEE Transactions on Industry Applications, vol. 26, No. 5, 1990.

13. Uchimura K., Michida J., Nozu S., Aida T. Multifunction of Digital Circuits by Noise Induced in Breaking Electric Contacts. Electronics and Communications in Japan, vol. 72, issue 6, 2007.

14. Henderson I. A., McGhee J., Szaniawski W., Domaradzki P. Incorporating High Reliability into the Design of Microprocessor-based Instrumentation. IEE Proceedings, vol. 138, No. 2, 1991.

15. Phadke A. G. Hidden failures in electric power systems. International Journal of Critical Infrastructures, vol. 1, No. 1, 2004.

16. Ковалев Б. И., Наумкин И. Е. Основные проблемы и задачи электромагнитной совместимости вторичных цепей высоковольтных подстанций: Сборник докладов XV научно-технической конференции «Релейная защита и автоматика энергосистем», Москва, 2002.

17. Information Notice No. 94-20: Common-Cause Failures Due to Inadequate Design Control and Dedication. US Nuclear Regulatory Commission, Washington, 1994

18. Matsuda T., Kovayashi J., Itah H., Tanigushi T., Seo K., Hatata M., Andow F. Experience with Maintenance and Improvement in Reliability of Microprocessor-based Digital Protection Equipment for Power Transmission Systems. Report 34-104, SIGRE, Session 30 Aug. – 5 Sept., 1992, Paris.

19. He S., Shen L., Lui J. Analyzing Protective Relay Misoperation Data and Enhancing Its Correct Operation Rate. IEEE/PES Transmission and Distribution Conference & Exhibition: Asia and Pacific, Dalian, China, 2005.

20. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes

21. Шмурьев В. Я. Цифровые реле защиты. Библиотечка электротехника, вып. 1 (4), Москва, НТФ «Энергопрогресс», 1999.

22. Hamdioui S., Al-Ars Z., Goor A. J. Testing Static and Dynamic Faults in Random Access Memories. Proceedings of the 20th IEEE VLSI Test Symposium, 2002, IEEE Computer Society

23. Hamdioui S, Gaudadjiev G. N. Future Challenges in Memory Testing. proceddings of PRORISC'03, pp. 78-83, Veldhoven, November 2003.

24. Soft Errors in Electronic Memory – A White Paper, Terrazon Semiconductor, January 2004.

25. Soft Errors in Advanced Semiconductor Devices – Part I: The Three Radiation Sources. IEEE Transactions on Device and Material Reliability, vol. 1, No. 1, 2001.

26. Dodd P. E., Shaneyfelt M. R., Felix J. A., Schwank J. R. Production and Propagation of Single-Event Transient in High-Speed Digital Logic ICs. IEEE Transactions on Nuclear Science, vol. 51, No. 6, 2004.

27. Johnson A. H., Miyahira T. F., Irom F., Edmonds L. D. Single-Event Transients in High-Speed Comparators. IEEE Transactions on Nuclear Science, vol. 49, issue 6, part 1, 2002.

28. Gurevich V. Nonconformance in Electromechanical Output Relays of Microprocessor-Based Protection Devices Under Actual Operation Conditions, Electrical Engineering & Electromechanics, No.1, 2006.

29. Gurevich V. Peculiarities of the Relays Intended for Operating Trip Coil of the High-Voltage Circuit Breakers, Serbian Journal of Electrical Engineering, vol. 4, No. 2, 2007.

30. Kumm J. J., Schweitzer E. O., Hou D., Assessing the Effectiveness of Self-Test and Other Monitoring Means in Protective Relays, 21st Annual Western Protective Relay Conference, Spokane, WA. Oct. 18-20, 1994

31. Advanced Digital Relay Systems - Is testing still needed? Omicron Electronics, vol. 5, issue 1, 2000.

32. Шнеерсон Э. М. Цифровая релейная защита. – М.: Энергоатомиздат, 2007.

33. Gurevich V. Microprocessor Protection Relays – the Present and the Future, Serbian Journal of Electrical Engineering, vol. 5, No. 2, 2008.

34. Борисов Р. Невнимание к проблеме ЭМС может обернуться катастрофой // Новости электротехники. – 2001. – № 6(12).

35. Матвеев М. Электромагнитная обстановка на объектах определяет ЭМС цифровой аппаратуры // Новости электротехники. – 2002. – № 1(13).

36. Gurevich V. Electromagnetic Terrorism: New Hazards. Electrical Engineering & Electromechanics, No. 4, 2005.

37. IEEE Std 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities.

38. Пуляев В. И. Итоги работы устройств релейной защиты и автоматики ОАО «ФСК ЕЭС»: Сборник докладов XV научно-технической конференции «Релейная защита и автоматика энергосистем». – Москва, 2002.

Поступила 21.03.2008