

6 (36) 2005



НОВОСТИ Электротехники

ИНФОРМАЦИОННО-СПРАВОЧНОЕ ИЗДАНИЕ

Поиск

Очередной номер	Архив	Вопрос-ответ	Гостевая книга	Подписка	О журнале
Нормы. Стандарты	Проекты. Методики	Форум	Выставки	приложение Вопрос • Ответ	

[< Предыдущая](#)] [[Следующая](#) >

1. *Микропроцессорные устройства релейной защиты в последнее время существенно потеснили электромеханические и даже электронные, особенно в энергосистемах западных стран. Специалисты спорят, хорошо это или плохо, но такова всеобщая тенденция. Россия пока находится только в начале этого пути, однако процесс более широкого применения микропроцессорных реле набирает силу и в нашей стране. Опыт применения микропроцессорных устройств релейной защиты во многих энергосистемах позволил не только оценить их преимущества, но и выявить серьезные недостатки. Владимир Гуревич считает, что микропроцессорные реле зачастую приносят лишь дополнительные проблемы эксплуатирующему персоналу.*



Микропроцессорные реле защиты Новые перспективы или новые проблемы?

*Владимир Гуревич,
к. т. н., Israel Electric Corporation
г. Хайфа, Израиль*

Микропроцессорные устройства релейной защиты являются весьма сложными устройствами со специфическим принципом действия, не имеющим ничего общего с обычными (традиционными) реле защиты. В связи с этим возникает вопрос о том, насколько вообще микропроцессорное реле является собственно реле.

Микропроцессорное реле – это самый настоящий компьютер на основе процессора фирмы Intel или AMD (рис. 1), содержащий дополнительно плату с входными трансформаторами тока и напряжения (рис. 2), согласованными по параметрам с внешними трансформаторами тока и напряжения, а также плату с набором миниатюрных выходных электромагнитных реле.

Записанная в специальный чип (так называемый «software-key», фактически это постоянное запоминающее устройство – ПЗУ) программа позволяет обрабатывать входные сигналы таким образом, чтобы смоделировать действие того или иного вида защитного реле. Заменяв один такой чип на главной плате на другой, можно получить реле любого типа. То есть микропроцессорное реле является всего лишь виртуальным, а не настоящим реле.

Можно возразить, что многие из имеющихся на рынке устройств защиты на самом деле являются узкоспециализированными устройствами, предназначенными для выполнения строго определенного и весьма ограниченного набора функций, присущих только реле конкретного вида. Да и называются такие устройства как конкретный вид реле, например «реле частоты». Программирование такого реле сводится в основном к записи в его память требуемых порогов срабатывания, временных интервалов, выбора того или иного типа рабочей характеристики из некоторых возможных. Но и в этом случае ограничения на выполняемые функции накладываются вовсе не микропроцессором, которому совершенно всё равно, какие сигналы обрабатывать, а ПЗУ, в котором записана программа работы этого микропроцессора, и количеством входных и выходных каналов.

Если использовать в устройствах, выполняющих функции реле защиты, не ПЗУ с программой, записанной производителем, а СППЗУ – стираемое программируемое запоминающее устройство или ЭСППЗУ – электрически стираемое программируемое запоминающее устройство, и портативный программатор, позволяющий записать в память любой алгоритм действия микропроцессора, то вместо реле частоты получим некое универсальное устройство защиты.

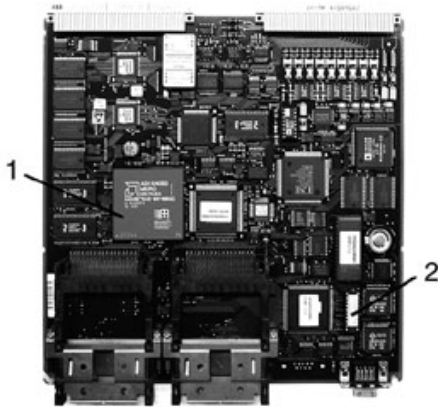
При этом оно практически ничем не будет отличаться от широко применяемых сегодня

универсальных микропроцессоров с цифровыми и аналоговыми входами, например таких, как Modicon, Siemens 7S-200, и многих других. Каждое такое устройство может иметь десятки входных модулей для преобразования входных сигналов в двоичный или шестнадцатиричный цифровой код, сотни виртуальных таймеров разных видов, компараторов, счетчиков с различной конфигурацией, разных типов триггеров, одновибраторов, огромное количество регистров памяти, используемых для записи промежуточных результатов, мощные выходные модули и т.д.

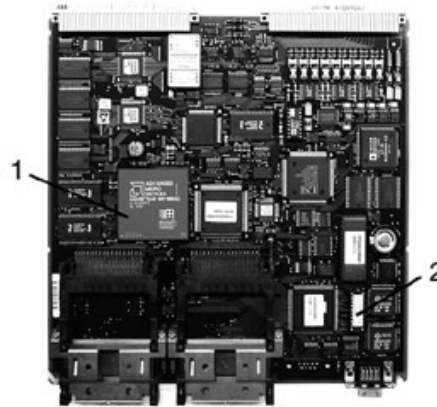
Из этого набора виртуальных элементов с помощью компьютерной программы, работающей под Windows, рисуют на экране (почти как в известных графических программах) сложнейшие системы автоматики, которые затем загружают в контроллер. Включив опцию «симуляция», можно увидеть на экране компьютера, как будет работать вся эта система автоматики в режиме реального времени или в специально смоделированных аварийных режимах.

Совершенно очевидно, что внутренняя архитектура и принципы работы микропроцессорных устройств имеют очень мало общего с устройствами, определенными как электрические реле. Поэтому, по мнению автора, внутреннее устройство и принцип действия микропроцессорных устройств, в том числе и реле защиты, должны рассматриваться и изучаться не специалистами по релейной защите, а специалистами в области компьютерной техники.

Однако, поскольку такие виртуальные микропроцессорные устройства широко применяются в качестве реле защиты, целесообразно рассмотреть некоторые важные аспекты, связанные с применением таких реле. Сначала рассмотрим те преимущества микропроцессорных реле, которые отмечаются в рекламных проспектах производителей.



*Рис. 1
Главная плата универсального микропроцессорного реле с установленными на ней стандартным «компьютерным» микропроцессором (1) и постоянным запоминающим устройством (2) с программой, определяющей тип реле*



*Рис. 2
Плата микропроцессорного реле с входными трансформаторами тока и напряжения*

«Преимущества» микропроцессорных реле

Позволяют записывать и потом воспроизводить для анализа аварийной ситуации режимы, непосредственно предшествовавшие аварии и в течение аварии.

А раньше такой возможности у энергетиков не было? Разве не существует огромное количество всевозможных регистраторов аварийных режимов и регистраторов срабатываний реле? ABB, Areva, Siemens, Ametek, NextPhase, Dewetron – далеко не полный перечень ведущих мировых производителей таких регистраторов и анализаторов аварийных режимов.

Позволяют с помощью подключенного компьютера изменять уставки срабатывания и переходить с одной характеристики на другую чисто программными средствами.

Это действительно удобнее, чем настраивать реле с помощью потенциометров и отвертки, но сколько раз в течение 10–20 лет приходится в реальных условиях изменять режимы настройки реле? Два-три, не больше.

Позволяют передавать всю информацию об их состоянии на удаленные диспетчерские пункты через специальные каналы связи.

А разве до микропроцессорных реле не применялись дистанционные многоканальные системы передачи данных (например, SCADA), осуществляющие передачу информации о срабатывании каждого электромеханического реле на главный диспетчерский пульт?

Позволяют менять конфигурацию комплекта релейной защиты: включать или отключать отдельные функции (то есть как бы подключать или отключать отдельные реле) чисто программными средствами, с помощью подключенного внешнего компьютера.

Это действительно намного удобнее, чем устанавливать дополнительные реле и переделывать монтаж в панелях релейной защиты. Но опять возникает тот же самый вопрос: как часто приходится прибегать к таким операциям? Один (или два в самом неблагоприятном случае) раза за весь срок службы реле (25 – 30 лет).

Одно небольшое по размерам микропроцессорное реле может заменить целую группу обычных электромеханических реле. Особенно это относится к сложным защитам типа дистанционных. Благодаря этому можно сэкономить дорогостоящие площади, занимаемые шкафами с релейной защитой.

Действительно, сложные микропроцессорные реле занимают площади для монтажа в 5–10 раз меньшие, чем аналогичный по функциональным возможностям комплект обычных реле. Но вот каверзный вопрос: какую часть площади всей электростанции или подстанции удастся сэкономить при переходе от обычных электромеханических реле к микропроцессорным? Одну сотысячную или одну миллионную?

Позволяют реализовать значительно более высокую чувствительность к аварийным режимам, чем электромеханические реле.

И это чистейшая правда, но вопрос в том, всегда ли нужна такая чувствительность и точность в релейной защите энергетических объектов? Яркий пример тому – микропроцессорные реле частоты, обеспечивающие срабатывание при отклонении частоты на 0,005 Гц, в отличие от простых аналоговых электронных реле с точностью срабатывания 0,01–0,05 Гц (для разных моделей). Интересно, есть ли где-нибудь в мире электростанция или подстанция, на которых используется реле частоты, производящее какие-либо операции в энергосистеме при отклонении частоты на 0,005 Гц от номинального значения? Во многих случаях бывает избыточной чувствительность даже обычных электромеханических или аналоговых электронных реле и их приходится искусственно загрублять.

Более высокая надежность статических микропроцессорных реле по сравнению с электромагнитными реле, содержащими механически перемещающиеся элементы.

Действительно, кажется неоспоримым тот факт, что статическое устройство, не содержащее подвижных элементов, намного надежнее в работе, чем сложный механизм со множеством взаимодействующих элементов. Но это только на первый взгляд. При более тщательном рассмотрении оказывается, что всё не так просто.

Во-первых, количество срабатываний (то есть перемещений подвижных элементов) электромеханических реле защиты совершенно мизерно по сравнению с их ресурсом. В личной практике автора были случаи, когда на проверку поступали реле с заводским дефектом, которые находились в эксплуатации свыше 10 лет. Тот факт, что эти дефекты не были выявлены в течение свыше 10 лет, говорит лишь о том, что в течение всего этого времени реле ни разу не сработало (а еще о том, что недопустимо проводить проверки реле так редко). О каком механическом износе подвижных частей может идти речь в таких случаях?

Во-вторых, количество элементов, из которых построено микропроцессорное реле, в сотни-тысячи раз больше, чем количество элементов, из которых состоит электромеханическое реле. А из теории надежности известна обратная пропорциональная зависимость между количеством элементов и надежностью сложных систем. Что касается надежности самих элементов, то и тут не всё так просто. В электромеханическом реле под воздействием внешних факторов, способных вызвать повреждение, находятся лишь катушки электромагнитов и изоляция внутренних монтажных проводов. Сами по себе это очень надежные и устойчивые элементы, но если бы возникла необходимость в дальнейшем повышении надежности, то катушки можно было бы пропитать эпоксидным компаундом под вакуумом и использовать монтажные проводники во фторопластовой изоляции.

В микропроцессорных реле практически все электронные элементы находятся под воздействием приложенного напряжения питания, а часть из них – и под воздействием входного тока или напряжения. Часть элементов постоянно находится в режиме генерации сигналов. Некоторые компоненты (например, электролитические конденсаторы) усиленно стареют при постоянном воздействии рабочего напряжения. Что касается микросхем – основных активных элементов микропроцессорных реле, то именно они являются причиной большинства отказов реле (см. рис. 4 в [1]).

Не удивительно поэтому, что исследования, выполненные исследовательским отделом Israel Electric Corporation [2], привели к выводу о том, что надежность микропроцессорных реле ниже, чем электромеханических и полупроводниковых статических реле. Компоненты микропроцессорных реле выходят из строя чаще, чем элементы реле других видов. При этом отмечается, что имеющийся в сложных микропроцессорных реле внутренний мониторинг исправности не спасает дело, так как, во-первых, это мониторинг только основных режимов крупных функциональных блоков, а не исправности элементов, а во-вторых, информация о выходе из строя какого-то блока реле поступает к персоналу уже после того, как состоялся отказ реле. То есть наличие такой внутренней самодиагностики не увеличивает надежность реле.

Это были так называемые «преимущества» микропроцессорных реле защиты. Рассмотрим далее их недостатки.

Недостатки микропроцессорных реле

Влияние на работу реле электромагнитных возмущений со стороны питающей сети:

- 1 Внезапная потеря оперативного питания во время работы реле, вызванная перегрузкой или коротким замыканием в сети, срабатыванием автоматических выключателей в цепи оперативного питания, попаданиями молнии в линии электропередачи, обрывами проводов и др. Такие повреждения могут привести к прерыванию текущей работы

оперативной памяти и кэша, зависанию микропроцессора, а иногда и к полной потере данных в том случае, если не приняты специальные меры по организации бесперебойного питания реле.

1. Электромагнитные шумы или помехи в цепях питания и во входных цепях реле. Такие помехи могут быть вызваны различными факторами и явлениями, например, коммутационными или атмосферными перенапряжениями, излучениями передатчиков или мощного промышленного оборудования, несинусоидальностью напряжения. Из практики эксплуатации микропроцессорных реле известны случаи, когда источником такого излучения, нарушившего нормальную работу микропроцессорного реле, был обычный телефон сотовой связи.
1. Несимметричные режимы в сети и режимы, связанные с провалами напряжения и с длительным (в течение нескольких секунд и более) понижением уровня напряжения. Такие режимы возникают при включении мощной однофазной нагрузки, при пусках мощных электродвигателей компрессоров, лифтов и др., а также при дефиците мощности в энергосистеме в часы пик. Сложные микропроцессорные реле обычно снабжаются сложными и дорогими источниками питания, способными обеспечить необходимый уровень напряжения на элементах схемы даже при глубоких провалах напряжения питания. Однако в более простых реле такие режимы приводят к нарушению их правильной работы. Причем такие нарушения иногда приводят к очень тяжелым авариям в сети, так как работа микропроцессора при пониженном уровне напряжения питания становится совершенно непредсказуемой.
1. Перенапряжения в сетях, вызванные сбросом нагрузки, или импульсные коммутационные перенапряжения, которые могут проникнуть в реле через питающую сеть и привести к повреждению внутренних элементов реле и его полному отказу. Конечно, существуют международные стандарты, в которых изложены требования по защите реле от всех этих воздействий, и разработчики реле принимают специальные меры. Однако практика показывает, что далеко не всегда это спасает от повреждений даже реле ведущих фирм мира.

В литературе описано много случаев сбоев и даже повреждения микропроцессоров от перенапряжений. Известны, например, случаи массовых отказов микропроцессорных реле времени, установленных на атомных электростанциях США. В информационном бюллетене, посвященном этой проблеме [3], описаны случаи повреждения микропроцессорных реле времени от перенапряжений, возникших при отключении катушек промежуточных электромагнитных реле.

Микропроцессорные системы релейной защиты, особенно сложные, например такие, как дистанционные, не всегда адекватно ведут себя при сложных авариях.

Довольно часто наблюдаются случаи сбоев и неправильной работы сложных микропроцессорных защит в реальных условиях эксплуатации. Причем, если проверять такое реле на обычном лабораторном стенде при стандартных сигналах на его входах, то оно будет работать четко и надежно. Проблема заключается в том, что на таком стенде невозможно заранее симулировать все возможные комбинации и искажения сигналов, которые могут произойти в реальной ситуации. Невозможно заранее предусмотреть такие случаи и при разработке реле.

Эта ситуация чем-то напоминает проблемы с персональным компьютером, когда совершенно исправная мощная машина, снабженная неповрежденной мощной программной оболочкой Windows, неожиданно зависает при определенном наборе команд или при одновременном запуске нескольких программ. В большинстве случаев такие проблемы невозможно заранее предусмотреть и предупредить.

Существует довольно странная, на первый взгляд, ситуация, при которой быстродействующие микропроцессорные защиты реагируют на аварийный режим гораздо медленнее, чем электромеханические.

В некоторых энергосистемах для повышения надежности на параллельную работу включены и микропроцессорные, и электромеханические реле. При анализе аварийных ситуаций неоднократно оказывалось, что электромеханическое реле срабатывало и отключало выключатель до того, как успевало отреагировать микропроцессорное реле.

В общем случае, если для срабатывания электромеханического или электронного реле мгновенного действия достаточно 5–15 мс, то для микропроцессорного реле уже необходимо 30–40 мс (по данным производителей). В реальных же условиях оказывалось 80–100 мс. Это связано с тем, что, в отличие от электромеханического или аналогового электронного реле, микропроцессорное реле работает со входными величинами дискретно. Оно «захватывает» текущие значения входных величин, помещает их в буфер, затем захватывает еще один комплект входных величин через определенный промежуток времени и сравнивает его с помещенным в буфер. Если второй комплект окажется идентичным первому, входные величины отправляются в микропроцессор для обработки. В аварийных переходных режимах микропроцессору приходится обрабатывать большие массивы информации в режиме реального времени, сопровождающегося быстрыми и значительными изменениями входных сигналов, и для этого ему необходимо определенное время (иногда сотни миллисекунд). Более того, если уже после запуска микропроцессора ситуация изменилась (например, замыкание на землю одной фазы перешло в двухфазное, а затем и трехфазное), то запущенный процесс вычисления

прерывается и все измерения начинаются сначала.

Информационная избыточность.

Многие реле имеют среди параметров для уставок множество таких, которые не являются однозначно необходимыми и только загромождают и без того сложную процедуру настройки реле. Особенно это касается реле со сложными функциями, например, дистанционных с их сотней уставок.

Речь идет о таких уставках, как степень яркости экрана, цвет свечения экрана, цвет информационных сообщений, выводимых на экран, время сохранения данных на экране после их вывода на экран, многочисленные варианты назначения функций каждого из полудюжины светодиодов, расположенных на передней панели реле, и т.д. Для выбора уставок реле в программе, приданной к реле, имеются чуть ли не десятки вариантов каждого параметра, которые могут быть выбраны из библиотеки параметров. Часто эти варианты также избыточны.

Например, в микропроцессорном реле MiCOM P437 только контроль целостности предохранителя в цепи трансформатора напряжения может быть выбран по четырем разным алгоритмам.

Такая явная избыточность приводит к тому, что общее количество вариантов уставок переваливает за тысячу для реле со сложными функциями. Это в свою очередь приводит к резкому возрастанию вероятности ошибки и увеличения веса так называемого «человеческого фактора». Проблемы, связанные с человеческим фактором, возрастают многократно, если одной и той же группе людей приходится обслуживать реле разных производителей, имеющих различные программы, интерфейсы, принципы выбора уставок.

Возможность преднамеренных дистанционных воздействий на микропроцессорную релейную защиту с целью нарушения ее нормальной работы.

Сегодня интенсивные исследования в области электромагнитного оружия ведутся в России, США, Англии, Германии, Китае. В последние годы многие разработки прошлых лет, например такие, как компактные сверхмощные импульсные источники направленного электромагнитного излучения мощностью до 1 ГВт, были рассекречены и теперь свободно предлагаются к продаже как на Западе, так и в России [4].

Вопросы «электромагнитного терроризма», способного вызвать техногенные аварии национального масштаба (подобные той, которая произошла в Нью-Йорке в августе 2003 года), были сформулированы в статье Мануэля Вика [5]. В этой статье, в частности, отмечается, что электронные компоненты, такие как микропроцессоры, работающие на высоких частотах при низких уровнях напряжений, особенно подвержены воздействию внешних преднамеренных электромагнитных излучений. Однако лишь совсем недавно в ряде организаций начаты серьезные практические исследования воздействий таких излучений на электронную аппаратуру электроэнергетических систем. Эти исследования возглавляются и координируются в США KEMA и Sandia National Laboratory.

Но даже без специальных исследований совершенно очевидно, что микропроцессорные реле гораздо менее устойчивы к таким воздействиям, чем электромеханические и даже аналоговые электронные. Кроме того, оказывается, что «электромагнитный терроризм» – не единственный вид современного дистанционного терроризма, которому подвержены микропроцессорные реле. Существует еще и такой вид электронных интервенций, как «кибер-атаки». В наше время хакерские атаки через компьютерные сети, телефонные линии, Интернет всё чаще становятся оружием террористов.

Выводы

- 1 Микропроцессорные реле не привнесли в релейную защиту какие-то новые функции. Они всего лишь объединили функции отдельных реле, добавив функции, выполнявшиеся ранее регистрирующими приборами.
- 1 Микропроцессорные реле не обеспечили более высокий уровень надежности электроснабжения и не облегчили работу обслуживающего персонала.
- 1 Как отмечается в исследовании, выполненном в Israel Electric Corporation, «микропроцессорные реле возникли как результат прогресса в области электроники и в развитии статических электронных реле». Так зачем же потребовалось усложнять себе жизнь и вводить в эксплуатацию сложные микропроцессорные реле, с одной стороны, не имеющие никаких существенных преимуществ перед традиционными, а с другой, обладающие целым веером собственных проблем?

Оказывается, на это есть одна очень существенная причина. Но она лежит не в сфере электроэнергетики, которую мы рассматривали до сих пор, а в сфере производства реле. Производить микропроцессорные реле несравненно более выгодно, чем электромеханические и даже аналоговые электронные. Это объясняется возможностью полной автоматизации всех технологических процессов производства и контроля параметров микропроцессорных реле. Крупнейшие международные концерны, такие как ABB, General Electric, Siemens, Alstom, уже давно стали «законодателями моды» в области электроэнергетики и определяют сегодня магистральные пути развития не только релейной защиты, но и всей электроэнергетики.

- 1 Несмотря на отмеченные недостатки и проблемы, тенденции развития релейной защиты таковы, что широкое и всё возрастающее применение микропроцессорных реле защиты неизбежно. В связи с этим энергетические компании должны четко представлять те

трудности и проблемы, с которыми им придется столкнуться, и заблаговременно принять все необходимые меры.

В частности, нейтрализация возможности преднамеренного дистанционного воздействия на такие реле террористами и криминальными элементами обеспечивается заменой всех электрических проводов, подключенных к микропроцессорному реле (за исключением питания, разумеется), на оптоволоконные кабели и использованием оптоэлектронных трансформаторов тока и напряжения вместо традиционных электромагнитных.

Цепи питания микропроцессорных реле должны иметь полную гальваническую изоляцию от электрической сети, например, за счет использования системы мотор-генератор. Если по экономическим причинам это невозможно, должны быть использованы мощные высокочастотные фильтры и ограничители напряжений во всех ступенях цепей питания, цепей тока и напряжения. Реле должны быть установлены в полностью металлических шкафах, изготовленных по специальной высокочастотной технологии (с использованием электропроводных резиновых прокладок и смазок и т.п.). Необходимо принять специальные меры по снижению сопротивления цепей заземления, разделению цепей заземления высокочувствительной электронной аппаратуры и силовой высоковольтной.

Это та цена, которую необходимо заплатить за прогресс в области релейной защиты.

Литература

1. Matsuda T., Kovayashi J., Itoh 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 August – 5 September 1992, Paris.
2. Aspects of Digital Protective Relaying. Report RE-626. Research and Development Division of Israel Electric Corp., 1991.
3. Information Notice No. 94–20: Commoncause Failures Due to Inadequate Design Control and Dedication. – Nuclear Regulatory Commission, March 17, 1994.
4. Gurevich V. Electromagnetic Terrorism: New Hazards. – Electrical Engineering & Electromechanics, 2005, No. 12.
5. Wik M. W. Electromagnetic Terrorism – What are the Risks? What can be Done? – International Product Compliance Magazine, 1997.