Цена вопроса

"Перестройка" и возникшее вслед за ней ослабление централизованного управления телекоммуникациями и энергетикой, в сочетании с лавинообразным развитием техники связи, появлением новой аппаратуры и новых принципов построения сетей и каналов связи, развитие цифровой техники релейной защиты, появление у нее новой функциональной наполненности, приводит к необходимости пересмотра традиционных методов построения систем релейной защиты и противоаварийной автоматики, а так же их привязки к каналам связи.

В настоящий момент наиболее привлекательно выглядят волоконно-оптические технологии. Причем совершенно равноправно рассматривается построение таких сетей как специализированных (то есть принадлежащих энергокомпаниям); специализированных, но с возможностью наполнения их общедоступным трафиком; аренда волокон в сетях общего пользования (то есть принадлежащих третьим лицам); и, наконец, аренда трафика в общественных сетях. И речь идет не только о межстанционных и межсистемных каналах связи. Все более реально выглядит шинная или сетевая структура построения внутри станционных связей касающихся не только безбумажных технологий, но и систем АСКУЭ / ФОРЭМ, технологии (SCADA), и даже защиты.

Взгляд со стороны

Традиционно системы защиты строились с использованием узкополосных каналов связи. Как правило, это были ВЧ каналы, но даже в тех случаях, когда существовала возможность получить широкополосные каналы (например, при использовании кабелей), с целью унификации аппаратуры все равно использовались узкие полосы частот. Это определяло функциональные возможности систем защиты и автоматики, причем ограничения наступали как со стороны емкости каналов, так и со стороны реализуемых скоростей передачи. Кроме того, низкая надежность существующей аппаратуры вынуждала энергетиков строить специализированные сети / каналы для всех видов передаваемого трафика: отдельно для связи и телемеханики, отдельно для защиты, а так же гибридные - для защиты и автоматики.

В современном мире, в котором технологии общественной связи шагнули далеко вперед, энергетикам очень хочется использовать дешевые массовые "коробочные" решения для собственных нужд. Это понятно и объяснимо, как с точки зрения снижения аппаратных затрат, так и с точки зрения кадровой политики - не надо готовить собственных высококлассных специалистов связи. Но так ли все просто?

Общественные сети

Укрупнено общественные сети связи можно поделить на три уровня: транспортный, сетевой и доступ. Лидерами здесь в настоящий момент являются:

Транспорт – SDH / PDH

Произошло это не только благодаря высоким скоростям передачи 155 Мбит/с - 10 Гбит/с и низким вероятностям ошибки, но и из-за возможности получить весьма высокие показатели готовности, что связано с заложенным в стандарт принципом резервирования топологии. Кроме того, наиболее критичным приложениям по определению может быть выделен фиксированный сетевой ресурс. А это очень важно.

Например, какая основная проблема при построении ДФЗ на сети общего пользования: передача каждого последующего тайм-слота или контейнера по новому сетевому пути с другим временем передачи. Решить эту проблему можно либо использованием адаптивной ДФЗ с независимой синхронизацией, либо, что более естественно, выделением ДФЗ фиксированного сетевого ресурса, в частности - сетевого пути.

> **Старый конь борозды не портит**
>
> Не следует сбрасывать со счетов и традиционных сетевых технологий - PDH (PCM), которые по самой своей структуре предназначены для оказания гарантированных сервисов. Главным недостатком этих технологий с точки зрения современных телекоммуникационных воззрений является низкая эффективность использования сетевых ресурсов. Главным достоинством перед современными устройствами является низкая цена.

Сетевой - ATM

Для этого есть три основные причины:

- возможность интеграции различных трафиков в универсальной архитектуре мультиплексирования и коммутации
- возможность предоставления каждому трафику фиксированного сетевого ресурса: виртуального (по запросу) или выделенного (постоянного пути)
- эффективной и скоростной коммутации

ATM, так же как и SDH, позволяет специфицировать не только время передачи, но и его вариации. Практически это означает, что сигналу защиты присваивается высший приоритет, и он либо совсем не ожидает освобождения занятого сетевого ресурса, либо ожидает его заданное малое время . Кроме того, в ATM мало и само время доступа (для > 2 Мбит/с).

Однако, в сетях общего пользования, построенных без учета специальных требований энергетики, имеющееся разделение на тайм-слоты (домены) не позволяет реализовать фиксированные времена передачи и задержки сигналов защиты без принятия специальных мер.

Доступ - IP

Главные особенности IP сетей - это то, что они создавались для передачи не чувствительного к задержкам трафика - почта, Интернет, данные; и то, что они имеют исключительную надежность. Правильно спроектированную IP сеть практически невозможно разрушить.

Развитие мультимедиа технологий породило новые IP стандарты. Последние из них IPv6, RVSP (resource reservation protocol) и RTP/RTCP (real time protocol / associated control protocol) направлены на то, что бы обеспечить определенным видам трафика выделенные сетевые ресурсы.

Однако, хотя эти искусственные надстройки над "родным" протоколом и позволяют получить надежные, безопасные, с малыми вариациями времени передачи каналы связи, тем не менее, неразрешимой проблемой для них остается абсолютное время передачи.

Метания

Естественно, такое деление на три уровня условно. ATM, например, часто используется как средство доступа (великолепные мультиплексоры), а IP - для построения сетей. Существуют и другие технологии. Все более популярен Frame Relay, который, однако, существенно уступает ATM в части гарантированных сервисов.

Производители аппаратуры других сетевых технологий, понимая присущие им недостатки, начинают выпускать странные гибриды: Frame Relay через ATM, IP через Frame Relay, IP через ATM и т.д., главная задача которых добиться изначально присущих SDH и ATM свойств - гарантированных сервисов для определенных видов трафика.

Среда	Время передачи (Б)-(Б)	Джиттер	Симметрия Та (дифф.задержка)	Время операции Добавить / Изъять	Время восстановления	Ошибки кросскомутации	BER	Полоса частот или емкость
кабель / провода	5-10 мкс/км (распространение)	<< 1 мс	< 1 мс, один путь	для Точка-точка отсутствует	не применимо	мало (человек)	не применимо	несколько кГц; << 64 кБит/с
ВЧ канал	3,3 мкс/км (распространение) + ~1,5 мс на терминал	<< 1 мс	< 1 мс	для Точка-точка отсутствует	не применимо	мало (человек)	< 10-3	4 - 8 - 16 кГц; < 80 кБит/с
РР	3,3 мкс/км (распространение) + ~1 - 2 мс на терминал	<< 1 мс	< 1 мс, один путь	для Точка-точка отсутствует	не применимо	мало (человек)	< 10-3	> 64 кБит/с
ВОЛС	~ 5 мкс/км (распространение в волокне)	<< 1 мс	< 1 мс, один путь	не применимо	не применимо	мало (человек)	< 10-6	> 64 кБит/с
GEO	250-280 мс (вверх-вниз)	нет данных	нет данных	не применимо	нет данных	нет данных	< 10-3	> 64 кБит/с
MEO	~ 100 мс (вверх-вниз)	нет данных	нет данных	не применимо	нет данных	нет данных	< 10-3	> 64 кБит/с
LEO	10-30 мс (вверх-вниз)	>> 1 мс	>> 1 мс	не применимо	нет данных	нет данных	< 10-3	> 64 кБит/с
PCM кабельная	~ 5 мкс/км (распространение) + 0,6 мс макс. для 64 -> 2048 кБит/с мультиплексор	< 1 мс	< 0,1 мс	не применимо	не применимо	Есть - ошибки синхронизации	< 10-6	> 64 кБит/с
PDH сеть	~ 5 мкс/км (распространение) + 0,6 мс макс. для 64 -> 2048 кБит/с мультиплексор + 15 мкс на 2 -> 8 MUX + 1 мкс на повторитель	< 1 мс	< 1 мс	~ 0.6 мс	~ 15 мин.	Есть - ошибки синхронизации	< 10-6	> 64 кБит/с
SDH сеть	~ 5 мкс/км (распространение) + 35 мкс 2048 -> STM-1 + 40 мкс STM-1 агрегатные + 110 мкс STM-1 -> 2048	< 3 мс типично	< 1 мс для двунаправленной защиты	< 120 мкс на ADM или повторитель	~ 1 мс для одиночной ошибки, зависит от проектировщика сети	Есть - ошибки синхронизации	< 10-6	> 64 кБит/с
ATM сеть	~ 5 мкс/км (распространение) + 1 мс первичный MUX + 6 мс пакетизация 64 кБит/с + 0,5 мс каждое коммутация главного MUX. ITU-T I.356 нормирует макс. Время доставки ячейки (CTD) 400 мс для межгосударственных сетей	< 3 мс задержка прихода ячейки (CDV) QoS класс 1 (ITU-T I.356)	нет данных	%	тоже, что и SDH, если SDH используется как транспорт	Есть - ошибка MUX < 1/день (ITU-T I.356)	< 10-6	> 64 кБит/с
IP сеть	не прогнозируется, не гарантируется	не гарантируется	Критично - не гарантируется	не применимо	не применимо	Есть - ошибки маршрутизации	< 10-5	> 64 кБит/с по требованию
Ethernet 10 MB сеть	5-15 мс разделяемый хаб / 1-2 мс переключаемый хаб + 6-12 мс время передачи	несколько мс, не гарантируется	нет данных	не применимо	не применимо	Есть - ошибки адресации	< 10-5	> 64 кБит/с
Ethernet 100 MB сеть	1-3 мс разделяемый хаб / < 1 мс переключаемый хаб + 6-12 мс время передачи	несколько мс, не гарантируется	нет данных	не применимо	не применимо	Есть - ошибки адресации	< 10-5	> 64 кБит/с

Новости с полей

На решение все той же проблемы - обеспечения гарантированного сервиса - направлены усилия создателей двух новейших технологий: dynamic time-slot multiplexing (DTM) и dynamic packet transport (DPT).

Обе они основаны на концепции передачи IP через SDH, и отличаются только принципом реализации и возможностью масштабирования. В обоих случаях SDH ресурс, выделяемый для передачи IP потока, может динамически изменяться за время жизни потока. Только DPT все-таки больше ориентирован на передачу традиционного IP трафика, а DTM предназначен для передачи любых видов информации.

Энергетика

Все сказанное выше в основном относится к большим распределенным сетям национального масштаба: общегосударственной или уровня ОДУ или МЭС. В России, благодаря ее размерам, сказанное может быть применимо и к сетям крупных энергосистем.

Но в любом случае, они составят лишь малую часть специализированных сетей связи энергетиков, в основном состоящих из станционных и межстанционных телефонных сетей и компьютерных сетей, если речь идет о цифровых сетях.

Каналы автоматики на самом деле образуют системную и межсистемную специализированные аналогово-цифровые сигнальные сети. Релейные каналы сетью назвать никак нельзя.

Общие вопросы совместимости сетевых технологий с требованиями релейной защиты и автоматики к каналам связи рассмотрены в обзоре "Транспорт для Защиты"

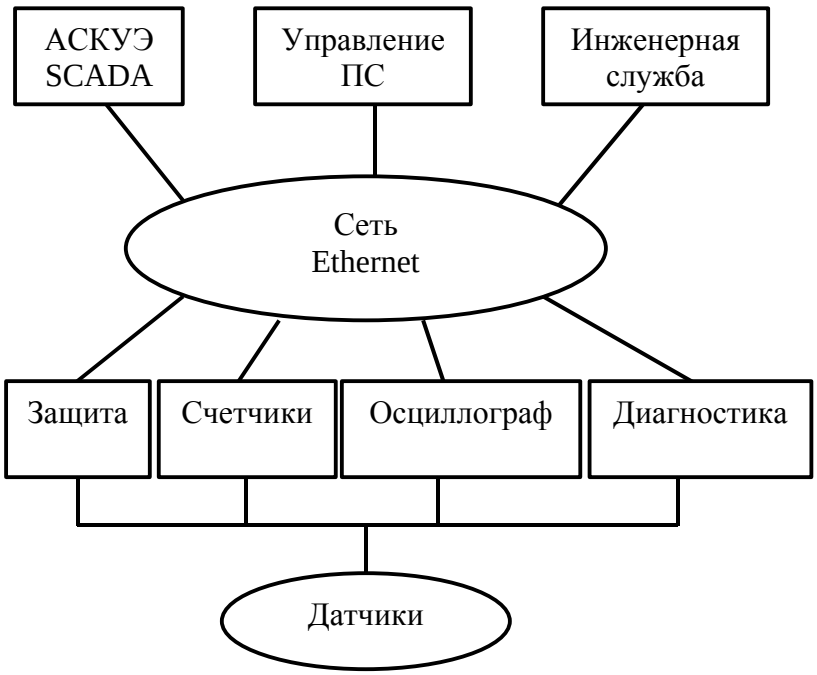
Станционные сети

в настоящее время в массе своей используются как компьютерные реализации без бумажной технологии, в основе которых лежит разного вида Ethernet. Появление микропроцессорных систем управления технологией и защиты должно изменить эту ситуацию.

UCA

Один из предлагаемых подходов к осуществлению станционной интеграции называется UCA (Utility Communications Architecture, RP3599-01, EPRI). Суть его состоит в следующем: UCA определяет специали-

зированный протокол, по которому должны взаимодействовать все станционные устройства, соединенные Ethernet: датчики, выключатели, счетчики, система АСКУЭ, устройства защиты, система управления подстанцией, офисные приложения и др., то есть любые IED (Intelligent electronic devices) цифровые устройства и сервисы, имеющиеся на ПС.



Привлекательность данного подхода состоит в его простоте: существующую на ПС Ethernet-сеть надо дооснастить UCA, установить всевозможные (в том числе РЗ и ПА) устройства, имеющие Ethernet-интерфейс, и готово! Но здесь-то и кроется основной подвох.

Для опроса силовых элементов / датчиков расположенных на ПС обычно используется IEEE 802.4 Token bus оптическая технология (защищенная от мощных помех звезда), которая, так же как и Ethernet IEEE 802.3 не имеет фиксированной временной сетки.

Поэтому, для того, чтобы получить фиксированное время опроса, например, выключателя или трансформатора, трафик специально "забивается" избыточной информацией, чтобы удлинить короткие сообщения, или, наоборот, длинные сообщения разбиваются на множество отрезков требуемой длины (опять проблема обеспечения гарантированного сервиса). Это приводит к тому что, при обеспечении шага временной сетки, например, 1 мс, такая интегрированная сеть становится способной обслуживать только ограниченное число устройств:

- при 10 Мбит/с Ethernet (концентратор с разделяемыми портами) - менее 20 устройств за 4 мс

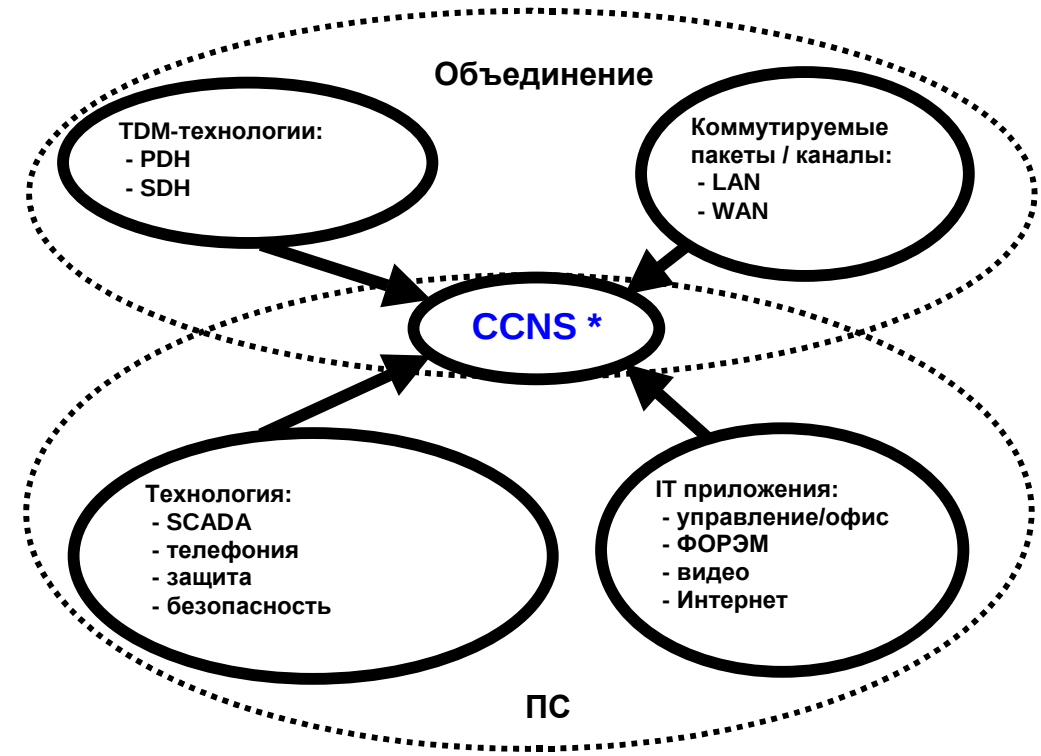
- при 10 Мбит/с (концентратор с переключаемыми портами) и 100 Мбит/с (концентратор с разделяемыми / переключаемыми портами) Ethernet - не более 100 устройств за 4 мс

Именно поэтому IEC рассматривает это решение только как временное для небольших ПС. Хотя допускается использование подобной сети для контроля и наблюдения за системами релейной защиты, и для обмена служебной информацией между устройствами РЗ и ПА. Но не для передачи сигналов защит (кроме сигналов состояния).

CCNS

Другой принцип реализуется в технологии CCNS (Converged corporate network solutions) - термин, пришедший из общественных сетей. Причем, все, что применимо или используется в связи с этим в общественных сетях, применимо и к специализированным сетям энергетиков (правый нижний овал на рисунке). Простое включение существующих корпоративных сетей в сети нового качества, их последующая модернизация параллельно развитию общественных технологий - огромное преимущество данного решения.

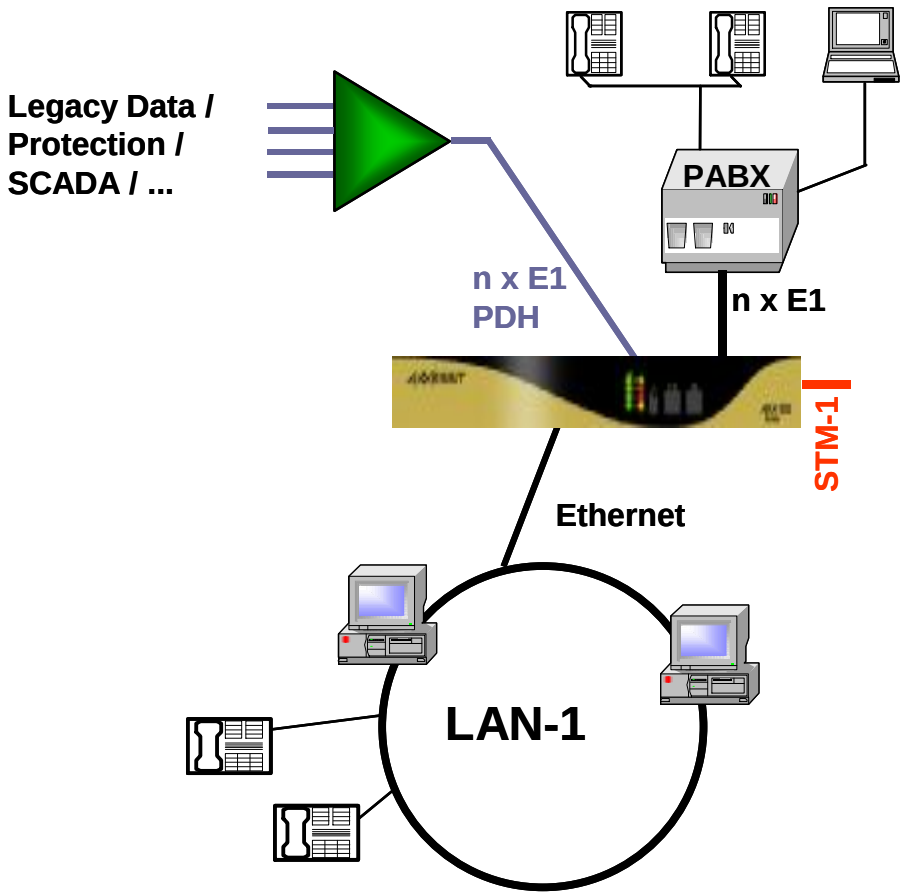
Изюминка метода состоит в том, что для подключения к корпоративной сети чувствительных ко времени (требующих гарантированного сервиса) трафиков - SCADA, защита и др. - используется обеспечивающий их по определению принцип PDH.



*** Смешанная станционная сеть**

Это обеспечивает безболезненное совмещение существующих технологий / каналов / сетей защиты с новой архитектурой. Это позволяет использовать уже имеющиеся на ПС датчики и устройства РЗ и ПА, обладающие интерфейсами N*64 Кбит/с, для объединения в специализированную сеть защиты. Когда уже не надо будет для каждого вида защит устанавливать собственный набор датчиков и систем, а можно будет использовать сигналы одних и тех же датчиков для обработки всеми типами защит. Да и самих устройств защит можно будет сделать гораздо меньше, если интегрировать их функции.

Новая концепция реализуется установкой на ПС специального объединяющего в один агрегатный поток Ethernet IP и PDH трафики устройства (Gateway), отличие которого от традиционного устройства Gateway состоит в том, что в нем изначально заложена функция обеспечения гарантированного времени передачи для трафиков защиты и технологии.



Межстанционные сети

Организация межстанционного или внутрисистемного взаимодействия требует объединения множества станционных сетей. Для сопряжения интерфейсов, протоколов и технологий локальных и транспортных сетей обычно устанавливается специализированное устройство Gateway. Тогда общее время передачи сигналов в системе будет определяться: задержками в станционной сети, обработкой трафика в Gateway, и временем распространения в транспортной сети.

UCA

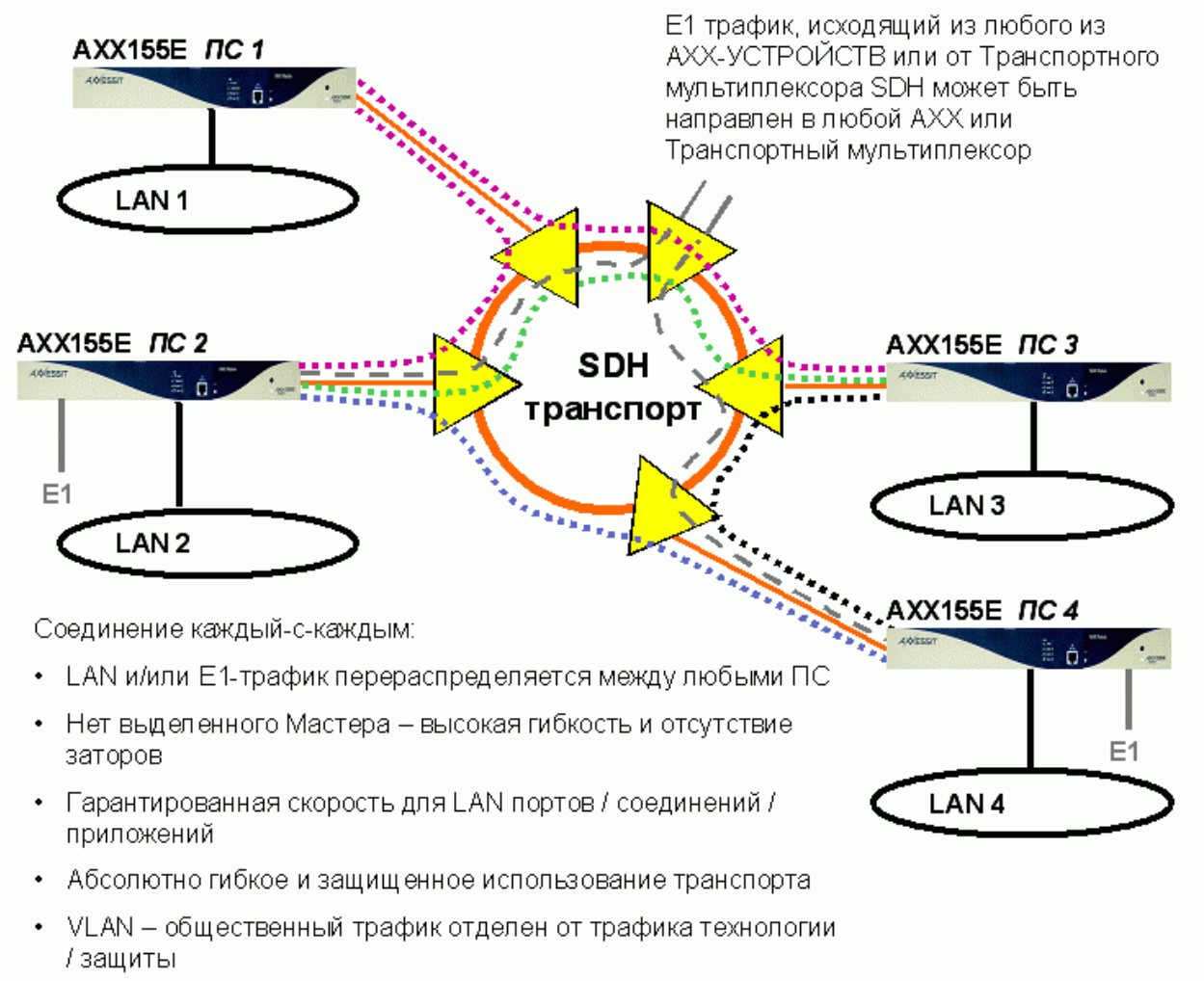
Устройства Gateway общего пользования (Ethernet - SDH / ATM) бывают ориентированными на соединение, и нет. Для неориентированных на соединение устройств каждый пакет данных имеет свой собственный путь в сети, и соответственно имеет место разновременность поступления информации. Что передачи сигналов защит недопустимо.

В ориентированных на соединение устройствах перед началом передачи данных приемник и передатчик устанавливают соединение, то есть резервируют некоторый сетевой путь, по которому и будут в дальнейшем передаваться данные. Это исключает временной джиттер приема данных в текущем сеансе связи, но увеличивает время передачи (+ время установления соединения). К тому же в следующий сеанс связи может быть установлен другой путь соединения, и будет иметь место непостоянство времени передачи от сеанса к сеансу.

CCNS

В технологии CCNS специализированный Gateway является основным звеном системы, реализующим за счет объединения технологий PDH-SDH фиксированные с постоянными временными параметрами каналы передачи сигналов защиты и технологии.

Причем для каналов защиты и технологии устанавливаются "постоянные" внутри сетевые соединения каждый-с-каждым или один-со-всеми, а для всего остального трафика (ТЛФ, компьютеры) действуют правила соединения общественных сетей (IP).



Защита. Новая философия

Строго говоря, информационные технологии, работающие в режиме реального времени, используются энергетиками и сегодня. По большей части это старые аналоговые принципы реализации. На новом сетевом (цифровом) уровне в настоящее время работают только технологи (SCADA-системы). И время от времени встречаются цифровые защиты, включенные в бог весть какие каналы.

Поскольку одним из наиболее важных аспектов построения ведомственных сетей является денежный, то разумно было бы использовать существующий опыт построения SCADA-систем, дополнив его специфическими функциями защиты, автоматики и некоторыми другими.

Предпосылками для этого являются следующие факторы:

- отработанные SCADA технологии реального времени
- наличие квалифицированного персонала
- наличие и быстрое развитие цифровых защит

- возможность использования всеми системами (защита + технология + коммерция + …) одних и тех же датчиков, указателей и измерителей
- наличие пригодных для реализации новой концепции сетевых технологий
- наличие работающих фрагментов будущей сети (SCADA + Ethernet)

Системы защиты

Наиболее употребительными в настоящий момент являются следующие системы защиты:

- ДФЗ
- Телезащита
- и иногда сравнения состояний

использующие очень ограниченные частотные ресурсы - соединения точка-точка через аналоговые и иногда 64 кБит/с цифровые каналы.

Системы нового поколения должны включать в себя:

- аналоговые защиты
- сигнальные защиты (сравнения состояний)
- системные защиты (ПА)
- сети, объединяющие все, в том числе силовое, оборудование на ПС
- межстанционные и т.д. SDH (ATM) сети
- интегрированные устройства, объединяющие в себе функции защиты, контроля и управления, с разделяемыми программными модулями
- полную информацию о перетоках (напряжение, токи, активная / реактивная мощности и т.п.)

Построение таких систем станет возможным при грамотном, учитывающем требования технологии и защиты, построении системы связи, гарантирующей время передачи информации между любыми точками внутри станционной и глобальной сетей не более 5 мс. Сами сетевые технологии это позволяют.

Первые шаги – технологическая станционная сеть

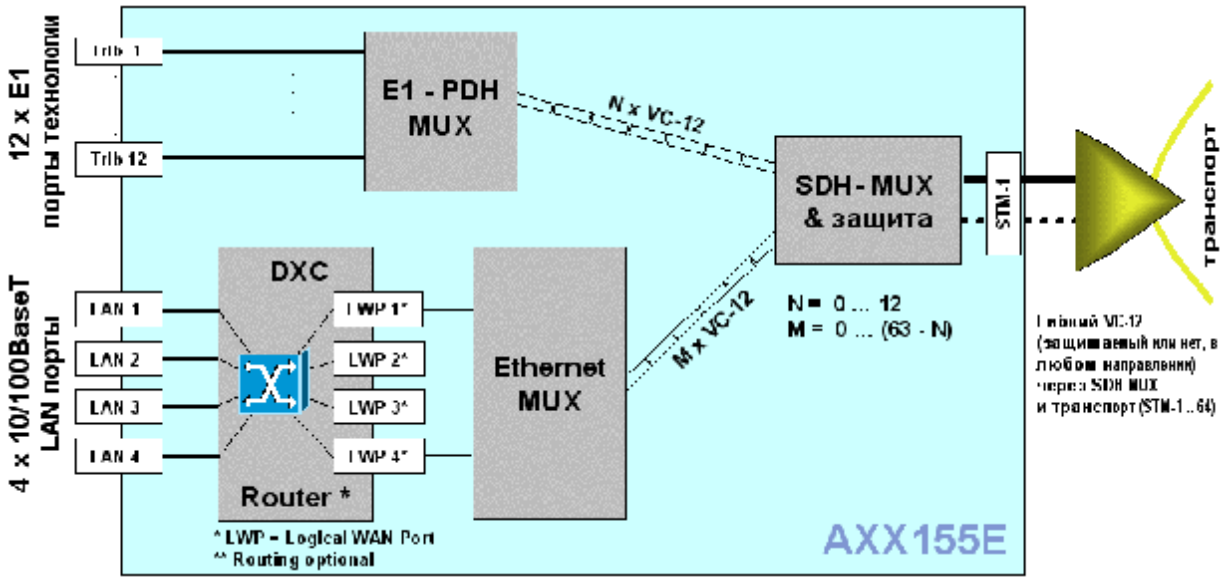
Такой подход предполагает, что все первичные элементы (силовое оборудование, счетчики и т.д.) обладают сетевыми интерфейсами; и информация об их состоянии, показаниях и т.п. циркулирует в станционной PDH сети. Причем доступ к этой информации имеют все устройства защиты, управления и коммерции.

Устройства защиты, защищающие конкретное присоединение (ВЛ), при принятии решения учитывают информацию о состоянии всех элементов ПС, в том числе об управляющих воздействиях от других устройств защиты на ПС или в системе. Из этого логично следует, что устройства защиты должны стать не на присоединение ориентированными, а комплексными - защищающими всю подстанцию или систему. Дифференциация должна быть только по типам защит. Это позволит сократить аппаратный парк защит в разы, существенно уменьшая капитальные и эксплуатационные расходы, без снижения требований к готовности, надежности и безопасности.

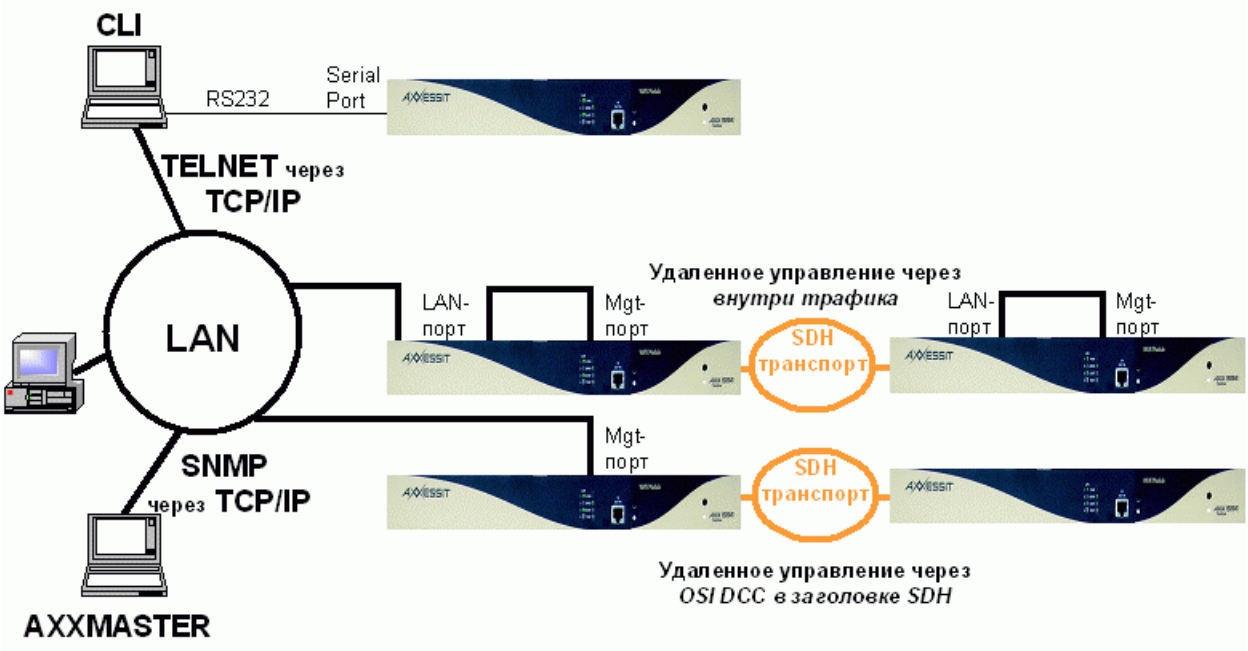
Кстати, принцип работы защиты, когда один терминал следит за работой другого / других, давно используется в системах защиты со сравнением состояний - командные системы / телезащита.

Следующие шаги

Для завершения автоматизации работы ПС необходимо объединить технологическую (PDH) и общего пользования (Ethernet / IP) сети в рамках CCNS подхода, предполагающего полную изоляцию трафиков и обеспечивающего наилучшие условия транспортировки технологической информации.



Создание взаимоувязанной транспортной SDH сети, объединяющей в единый комплекс все подстанции данного региона, позволит реализовать новый уровень Противоаварийной Автоматики, когда при вычислении управляющих воздействий будет учитываться вся - теперь доступная - первичная информация о состояния каждого элемента системы. (Кстати, здесь может пригодиться опыт самовосстановления, противостояния заторам и пере трассировки, накопленный в цифровых сетях - тех же SDH или IP, так аналогия между цифровой и высоковольтной сетями очевидна: есть присоединения, есть сетевая структура и необходимо доставить информацию / энергию из пункта А в пункт Б)



Но еще раз хочется повторить, что построение таких систем возможно только при соблюдении определенных правил, что "общественных" проектировщиков или совсем нельзя подпускать к этому процессу (у них другие цели), или надо их очень жестко контролировать, чтобы они не забывали, для кого они строят сеть. И нельзя напрямую использовать решения или компоненты, применяемые в общественных сетях. Технологическая сеть - это не "коробочное" решение.

Конец – сказке венец

Волоконно-оптические линии являются наиболее перспективной коммуникационной средой для построения глобальных сетей энергетиков, и технологических сетей защиты в частности.

Наиболее подходящими сетевыми технологиями для сетей защиты являются: ВЧ связь, PDH и SDH (ATM может использоваться при благополучном разрешении оговоренных ранее условий / ограничений). Наибольшее внимание при проектировании таких сетей должно уделяться:

- определению заданных и фиксированных (предсказуемых) временных параметров передачи: времени передачи, джиттеру и асимметрии
- определению заданных и фиксированных (предсказуемых) временных параметров восстановления сети
- решению проблемы потери синхронизации или ошибочной трассировки
- достижению параметра не готовности сети не более 0,001%