ПЕРЕХОД К Smart Grid И ЦИФРОВЫМ ПОДСТАНЦИЯМ. ГИБРИДНЫЙ ВАРИАНТ ПОСТРОЕНИЯ СЕТИ СВЯЗИ И ПЕРЕДАЧИ ДАННЫХ

научно-производственный центр "Приоритет"

А.М. ЛИФШИЦ (ООО “НПЦ Приоритет”)

Рассмотрен вариант построения сети связи и передачи данных для перехода на современные технологии в электроэнергетике.

«Среди немыслимых побед цивилизации мы одиноки, как карась в канализации.

И. Губерман

Программа инновационного развития ОАО “ФСК ЕЭС” предусматривает “Разработку технических требований к созданию каналов связи между цифровой подстанцией и другими объектами и каналами передачи команд РЗ и ПА по каналам связи от ЦП”. Последние 20 лет технологические сети связи развивались главным образом, путем замены аналогового оборудования на цифровое, использующее технологию PDH и SDH.

В 1992-1993 г. “НПЦ Приоритет” разработал и реализовал проект синхронной цифровой сети, ставшей первой в энергетике и одной из первых в России. Имея большой опыт в области технологических систем связи, остановимся на предусмотренной ФСК разработке технических требований, указанных выше. На самом деле задача проектирования новых технологических сетей передачи данных (ТСПД), основанных на пакетных технологиях, гораздо сложней, чем это представляется специалистам, занимающимся созданием сетей операторов связи по методикам, разработанным за рубежом [1]. Это касается не только передачи информации цифровых подстанций, но и отдельных типов технологического оборудования, в первую очередь, существующего оборудования релейной защиты и противоаварийной автоматики. Переход от цифровых сетей (SDH и PDH) к пакетным сетям будет достаточно длительным, и основной технологической проблемой станет процесс конвергенции сетей в этот период [2]. “Красивые” решения, представленные в ряде проектов создания ТСПД, при малейшем отклонении от ряда требований к пакетным сетям могут привести к катастрофическим последствиям для энергетики.

Достаточно подробный анализ проблем перехода технологического информационного обмена на пакетные сети описан в ряде зарубежных публикаций [3]. Рассмотренный в данной статье вариант создания гибридных сетей, обеспечивающих сочетание различных технологий передачи информации, дает возможность сохранить высочайшую надежность при внедрении новейших образцов энергетического оборудования на существующих энергообъектах и обеспечить информационный обмен при сооружении “цифровых подстанций”.

ПЕРЕХОД НА СЕТИ С ПАКЕТНОЙ ТЕХНОЛОГИЕЙ ДЛЯ ПЕРЕДАЧИ СИГНАЛОВ РЕЛЕЙНОЙ ЗАЩИТЫ

Сигналы релейной защиты – это наиболее критичные данные, передаваемые через технологические телекоммуникационные сети, и поэтому при возникновении аварийной ситуации должно гарантироваться минимальное время прохождения информации, вернее, команды РЗ должны передаваться с гарантированным временем доставки. Эти требования сохраняются при переходе от сетей SDH/SONET к сетям с пакетной технологией. Соответственно, проблема реализации этих требований является основной [4].

ВИДЫ ТРАФИКА В ПЕРЕХОДНОЙ ПЕРИОД

В настоящее время основные сети связи для всех приложений используют технологию SDH/SONET, однако прежняя инфраструктура и оборудование подстанции постепенно сокращаются, уступая место современным, поддерживающим протокол IEC 61850, что приводит к необходимости поэтапного перехода на технологию передачи сигналов взаимодействия через сети Ethernet и IP. Движение к Smart Grid является ключевым фактором для этого процесса, поскольку пакетная транспортная сеть, имеющая большую пропускную способность и более низкую стоимость, должна обрабатывать большое количество трафика, генерируемого современными технологическими приложениями, используемыми в интеллектуальных сетях электроснабжения. Системы SCADA на основе IP, измерительные системы WASA (wide area situation awareness), синхронизированные векторные измерения и новейшие разработки в области автоматизации подстанций, такие как стандарт IEC 61850, являются примером новых приложений, требующих в системах передачи и распределения электроэнергии применения пакетной передачи и использования возможностей технологии Ethernet.

ПРОБЛЕМЫ ПЕРЕХОДА

Энергетические компании, большинство из которых имеет собственные сети, с осторожностью воспринимают переход к IP. Будучи традиционно консервативными организациями, энергетики не спешат переходить к IP, если не видят четких параметров обеспечения высокой надежности и предсказуемости, как в сетях SDH/SONET. Однако возникают экономические проблемы, вызванные увеличением капитальных затрат, связанных с применением новых технологий, при необходимости сохранения сетей SDH/SONET на переходной период. С технической точки зрения реализация интеллектуальных коммуникаций на основе пакетных сетей должна гарантировать безотказную работу механизмов, обеспечивающих низкую задержку при передаче сигналов, высокую готовность и надежность при передаче важных приложений в среде с коммутацией пакетов. Для сигналов Релейной Защиты потребность в быстрой и достоверной передаче информации диктует необходимость низкой симметричной задержки и минимального джиттера. Оба этих параметра представляют большую проблему для сетей с коммутацией пакетов. Тем не менее, техника Ethernet имеет различные механизмы, чтобы преодолеть эти проблемы и обеспечить необходимую производительность, что будет описано ниже. В то же время переход на пакетные сети – процесс длительный и имеет ряд неоднозначных факторов. Таким образом сохранение технологии TDM позволит обеспечить на время перехода требуемую надежность и безопасность передачи данных критически важных приложений.

Сегодня типовой реализацией передачи TDM трафика, включая сигналы Р3, через пакетные сети является “псевдопроводная” эмуляция (PWE). В будущем ожидается появление новых методов, включая прямое отображение полезной нагрузки на соединение Ethernet, без этапов обработки TDM и псевдопроводной инкапсуляции. Для реализации современных релейных защит используют каналы волоконно-оптической связи с интерфейсом С37.94.

ПЕРЕДАЧА СИГНАЛОВ РЕЛЕЙНОЙ ЗАЩИТЫ (рис. 1)

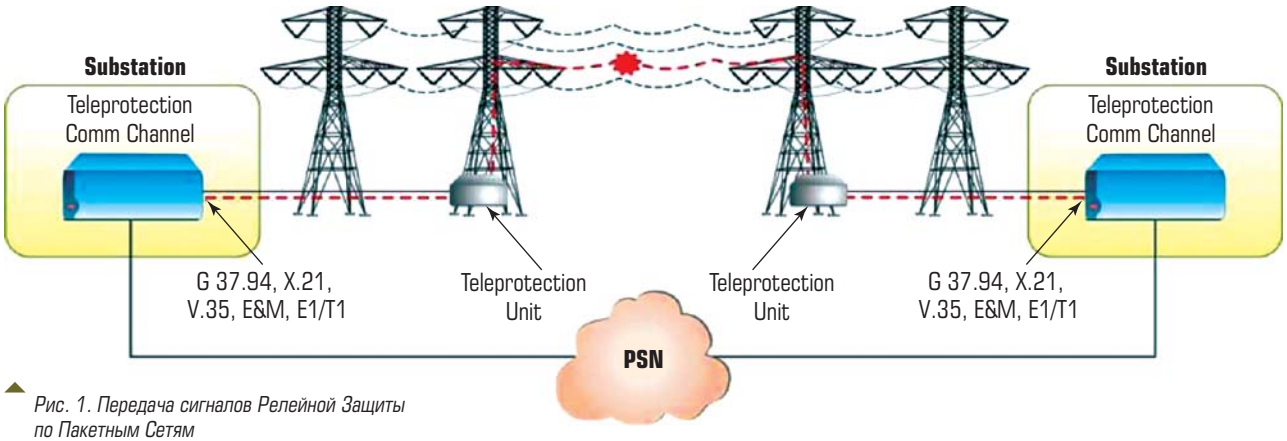

Рис. 1. Передача сигналов Релейной Защиты по Пакетным Сетям

ТРЕБОВАНИЯ К ТЕЛЕКОММУНИКАЦИОННЫМ СЕТЯМ ДЛЯ ПЕРЕДАЧИ СИГНАЛОВ РЕЛЕЙНОЙ ЗАЩИТЫ

Время передачи: Полное время работы системы Релейной Защиты включает время для того, чтобы инициировать команду на передающем конце, время распространения по телекоммуникационному каналу и время на принятие решения на приемном конце, включая дополнительную задержку на защиту от помех.

Надежность: возможность передать и получить достоверные команды в условиях интерференции и/или помех, минимизируя вероятность пропадания команды (Pmc). Надежность определяется при заданной частоте передачи ошибочных битов (BER).

Безопасность: возможность предотвратить ошибки, возникающие вследствие воздействия шумов, минимизируя вероятность ложных команд. Параметры безопасности задаются для определенной частоты передачи ошибочных битов (BER).

Дополнительные элементы, которые воздействуют на характеристики передачи сигналов РЗ, включают требования к пропускной способности, используемой системой РЗ, ее отказоустойчивости и способности восстановления. Из вышеупомянутых критериев время передачи, требования к пропускной способности и надежность прямо относятся к аппаратуре связи и среде передачи.

РАССМОТРЕНИЕ ЗНАЧЕНИЙ ВРЕМЕНИ ЗАДЕРЖКИ

Требования к времени задержки в корпоративных сетях имеют тенденцию изменяться в зависимости от многих параметров, включая тип оборудования релейной защиты. Большинство силового оборудования линий электропередачи может выдержать до пяти циклов включения и выключения питания прежде, чем возникнет необратимое ухудшение или влияние на другие сегменты в сети. В линиях 50 Гц это определяет полное время устранения повреждения 100 мс. В качестве меры безопасности, однако, время действия систем защиты ограничивается 70 – 80 % этого периода, включая время на распознавание аварии, время передачи команды и время переключения линейного выключателя. Некоторые компоненты системы, такие как большие электромеханические переключатели, требуют длительного времени срабатывания, что занимает большую часть полного времени выполнения команды на конкретное действие, оставляя окно только 10 мс для передачи сигналов защиты. Учитывая серьезность проблемы, в новых сетях эти требования изложены в Стандарте Международной электротехнической комиссии 61850: пределы времени передачи сигналов для самых критичных сообщений составляют **5-10 Мс** для силовых линий на 50 Гц.

АСИММЕТРИЯ ЗАДЕРЖКИ

В дополнение к минимальной задержке сигналов взаимодействия дифференциальной защиты используемый канал связи должен быть симметричным, то есть иметь симметричную задержку передачи и приема. Как упомянуто выше, это требует особого внимания в пакетных сетях к значению джиттера. Для сигналов взаимодействия РЗ оптимально иметь нулевую асимметричную задержку, в основном оборудование РЗ может выдерживать расхождения до **250 мкс.** Основные инструменты, доступные для понижения изменения задержки ниже этого порога:

Jitter “buffer” на каждом конце линии может использоваться для изменения задержки, ставя в очередь отправленные и полученные пакеты. Длина очередей должна компенсироваться увеличением скорости передачи, поскольку при увеличении буфера увеличивается задержка.

Инструменты управления трафиком гарантируют, что сигналы Релейной Защиты получают самый высокий приоритет передачи и минимизируют число точек маршрутизации, в которых возникает джиттер.

Стандарт технологии синхронизации для сети коммутации пакетов, такой как 1588-2008 Precision Time Protocol (PTP) и Синхронный Ethernet (Sync-E), помогает поддерживать устойчивость сети.

ИСТОЧНИКИ ЗАДЕРЖКИ В РЕЛЕЙНОЙ ЗАЩИТЕ

- Важно понять воздействие сетевых ограничений, поскольку каждый элемент и процесс обработки в системе защиты добавляется в суммарную задержку:
- *Задержка оборудования Релейной Защиты:* Эта неотъемлемая задержка включает идентификацию сбоев в силовом оборудовании, инициирование команды и время на принятие решения.

- *Мультиплексор доступа (TDM interface):* задержка в оборудовании Мультиплексора – результат функций, таких как время на reframe после потери сигнала, выделения и формирования временных интервалов, буферизации при формировании DS0 и E1, синхронизации и рассинхронизации, время переключения в кольце SDH (PDH), время обнаружения неисправностей. Задержка мультиплексора минимизируется через оптимальные механизмы ICs и функции кросс-соединения DS0.
- *"Псевдопроводная" задержка инкапсуляции и пакетирования:* процесс преобразования TDM в пакеты включают фиксированную задержку 1-5 мс, в зависимости от размера пакета и числа TDM фреймов, которые содержит каждый пакет. Более короткие пакеты увеличивают потребность в пропускной способности, но уменьшают задержку.
- *Сетевые элементы сети коммутации пакетов:* Если оборудование релейной защиты соединяется по пакетной сети (рис. 1), каждый элемент вдоль пути трафика добавляет фиксированную и переменную задержку, как следствие, соответственно, обработки информации и организации очередей. Переменная задержка представляет большую угрозу производительности Релейной Защиты вследствие высокого уровня неопределенности, которую она представляет, что требует использовать средства управления трафиком.

ДОПОЛНИТЕЛЬНЫЕ ПРОБЛЕМЫ, КАСАЮЩИЕСЯ ПЕРЕДАЧИ СИГНАЛОВ РЕЛЕЙНОЙ ЗАЩИТЫ

Надежность. Системы Релейной Защиты, учитывая их роль для решения ответственных задач, должны быть обеспеченны отказоустойчивыми средствами в случае неправильного функционирования любого из компонентов системы. Много приложений применяют избыточные методы повышения надежности, так, дистанционная и дифференциальная защита используют разные каналы. С телекоммуникационной точки зрения надежность может быть достигнута на многих уровнях:

Аппаратная Избыточность: надежность Мультиплексора должна быть основана на защите от отказов одиночных модулей с использованием аппаратной избыточности и возможностью замены блоков в горячем режиме.

Линейная Избыточность: 1+1 топология защиты с автоматическим переключением между трактами при возникновении дефектов оборудования или кабеля. Трафик, основанный на Ethernet, использует схему Link Aggregation Group (LAG), IEEE 802.3-2005 LACP (link aggregation control protocol), в котором параллельные ссылки привязываются к единственному виртуальному каналу.

Защита Маршрута: стандарты Промышленного Ethernet обеспечивают различные инструменты, чтобы гарантировать Высокую доступность. Они включают защитное переключение Линий Ethernet (G 8031) – также механизмы защиты, названные "EVC (Ethernet Virtual Connection)" и Ethernet Ring Protection Switching (G 8032 ERP), разработаны, чтобы обеспечить "Пять Девяток" (99.999%), надежность сервисов и быстрое восстановление.

УПРАВЛЕНИЕ ТРАФИКОМ И КАЧЕСТВОМ ОБСЛУЖИВАНИЯ

Развитие технологии Ethernet позволяет использовать сложные механизмы, предоставляющие сигналам Релейной Защиты детерминированный уровень качества обслуживания и приоритета, которого они требуют. Это является особенно критичным при прохождении информационных пакетов различных коммутаторов и других сетевых элементов, при этом возникает потребность изменить значения параметров, таких как задержка при организации очередей. Управляя ресурсом пропускной способности и приоритетами передачи посредством механизмов CoS (Class of Service), многоуровневое иерархическое управление трафиком позволяет получить предсказуемую задержку и джиттер. Усовершенствованный набор инструментальных средств включает следующее:

Классификация входящего трафика в потоках, согласно типу и требованиям QoS. Ethernet поддерживает большое разнообразие критериев сортировки, такие как VLAN-ID, P-bit marking, MAC/IP-адресация и т.д., что позволяет тщательно разделять трафик.

Иерархическое планирование трафика определяет порядок отправки различных потоков с помощью двухступенчатого механизма планирования, в результате каждый поток получает необходимый приоритет. Таким образом, приоритетный трафик обслуживается в первую очередь, в то же время очередь для трафика с низким приоритетом тоже продвигается. Развитые

способы управления очередями также служат для предотвращения переполнений и обеспечения минимальной задержки и джиттера даже в ситуациях, когда большое количество неравномерного трафика передается по тому же каналу. Формирование трафика позволяет сглаживать выбросы и избежать переполнения буфера в последующих элементах сети. Редактирование пакетов передает указания по правильной их обработке последующим элементам сети и обеспечивает целостность данных.

МОНИТОРИНГ ПРОИЗВОДИТЕЛЬНОСТИ И ТЕСТИРОВАНИЕ

Технология Ethernet операторского класса предлагает множество инструментов для тестирования, мониторинга и устранения сбоев в работе линий связи. Полный набор служебных пакетов Ethernet (OAM), методов измерения задержки, джиттера и потери пакетов, диагностические петли и другие средства можно применять удаленно, автоматически выполняя следующие процедуры:

- проверка соединения;
- интенсивное тестирование;
- мониторинг производительности;
- определение сбоя;
- передача сообщения о сбое и его локализация.

Удаленное тестирование, активный мониторинг и полная картина сетевых событий позволяют администраторам сетей предвидеть ухудшение качества сервиса, обеспечить постоянную производительность сети и сократить капиталовложения.

СИНХРОНИЗАЦИЯ СИГНАЛИЗАЦИИ В ПАКЕТНЫХ СЕТЯХ

Пакетные сети не разрабатывались со встроенными механизмами синхронизации, и поэтому требуют дополнительных решений передачи тактовой частоты с точностью, необходимой для стабильной работы сети с предсказуемой производительностью. В электроэнергосетях это особо необходимо для поддержки традиционного оборудования и приложений, чувствительных к задержке и джиттеру, таких как релейная защита, SCADA. До недавнего времени было принято использовать GPS в каждом узле/пункте обслуживания, однако это приводит к значительному росту затрат. Для синхронизации в пакетной среде на сегодня применяются несколько способов:

Метод ITU-T Synchronous Ethernet (Sync-E) использует физический уровень сети Ethernet для точной передачи тактовой частоты. Для этого нужно, чтобы каждый физический канал не прерывался на протяжении всего маршрута.

Другой метод – адаптивное восстановление тактовой частоты (Adaptive Clock Recovery, ACR) – опирается на время прибытия пакетов в псевдопроводном потоке TDM, независимом от физического уровня. Протоколы IETF NTP и IEEE 1588-2008 Precision Time Protocol (PTP) обмениваются информацией о временных метках в иерархии устройств “ведущий-ведомый”, чтобы передать тактовую частоту и данные TOD (Time of Day) таким образом, как это необходимо для нормальной работы датчиков распределенных измерений и предупреждения каскадных отключений. Использование протокола PTP на всем протяжении сетевого маршрута является хорошей альтернативой GPS для синхронизации времени. Хотя с помощью PTP можно передавать и тактовую частоту и метки времени, многие сетевые операторы предпочитают использовать физический уровень сети для передачи частоты (т.е. TDM или Synchronous Ethernet), а сервис PTP – только для синхронизации времени. Более того, поскольку на многих подстанциях устройства по-прежнему используют временные коды IRIG-B, необходимо надежное преобразование между PTP и IRIG-B для подключения традиционного оборудования к новым системам Smart Grid.

Стандарт IEC 61850 подробно рассматривает потребности электроэнергосетей в передаче сигнализации и синхронизации в пакетных сетях. Он ссылается на стандартный профиль IEEE C37.238 для применения IEEE Std. 1588 Precision Time Protocol в приложениях для подстанций и профиль 1588 PTP Telco для связи между подстанциями по глобальной сети. Современные коммуникационные устройства Релейной Защиты, которые поддерживают передачу точного времени, способствуют снижению издержек, поскольку они избавляют от необходимости приобретать дорогостоящие аппаратные средства или установки GPS.

ВЫБОР ПРАВИЛЬНОЙ ПАКЕТНОЙ СЕТИ

При переходе электроэнергетических сетей к коммуникациям нового поколения выбор пакетных технологий включает Ethernet

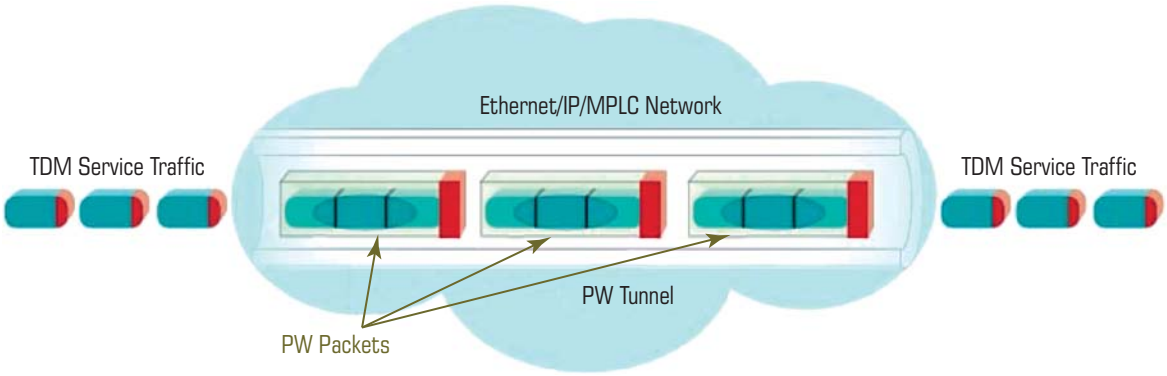

Рис. 2. Прохождение TDM сигналов через пакетную сеть

операторского класса, IP, стандартный MPLS (Multi- Protocol Label Switching), MPLS-TE и новейший вариант MPLS-TP. Кроме того, можно рассматривать новое поколение коммутации каналов (Circuit Switching, CS) на основе оптических транспортных сетей OTN (Optical Transport Networks). Подобно SDH/SONET, OTN можно использовать в качестве физического уровня для надежной передачи трафика Ethernet или IP по оптоволокну на скоростях от 50 Мбит/с до более 100 Гбит/с. Каждая из перечисленных пакетных технологий способна надежно доставлять информацию, но обладает разными характеристиками. Решение о типе технологии зависит от таких факторов как число узлов, которые будут соединены, их размера, возможности выбранного решения обеспечить соответствующую производительность, используя различную среду передачи, доступную на каждом узле, и, конечно, от стоимости. Несмотря на то, что сервис VPLS (Virtual Private LAN Service), основанный на передаче Ethernet по MPLS, может обеспечить необходимую устойчивость для критических приложений с помощью защитного механизма FRR (Fast Re-Route) с низкой задержкой, у него есть несколько серьезных недостатков с точки зрения защиты, определяемые встроенные средства OAM для мониторинга сети и высокая цена на порт. Сочетание доступа Layer 2 Ethernet с магистралью MPLS позволяет снизить цену на порт, иметь больший функционал OAM и инструменты PM для соединений Layer 2 Ethernet и использовать развитые защитные механизмы посредством Ethernet Ring Protection Switching и Ethernet Linear Protection Switching. Кроме того, такой подход позволяет сохранить установленную базу оборудования доступа и может являться оптимальным вариантом для большого числа распределенных энергообъектов, подключенных по медной, оптоволоконной и беспроводной инфраструктуре.

РЕЛЕЙНАЯ ЗАЩИТА ЧЕРЕЗ ПАКЕТНЫЕ СЕТИ. ТЕСТИРОВАНИЕ SDH-МУЛЬТИПЛЕКСОРА ДОСТУПА [3]

Для тестирования была выбрана одна из мультисервисных платформ доступа (мультиплексор, прошедший аттестацию ФСК) как элемент сети при передаче сигналов Релейной Защиты при использовании пакетной технологии. Тестирование состояло из преобразования данных TDM, полученных от модулей релейной защиты, в пакеты. Затем инкапсулированный трафик был передан по сети Cisco MPLS с использованием статической маршрутизации, чтобы убедиться в постоянстве тракта, обеспечивая требования к производительности для минимальной задержки сигналов релейной защиты (рис. 2).

Для тестирования использовалось оборудование дифференциальной Защиты производства AREVA, ABB и Siemens, используя следующие интерфейсы сопряжения: **G 703; X. 21; RS-232; C37.94**. Тестируемый Мультиплексор успешно выполнил эти требования, обеспечив допустимую задержку и необходимое качество обслуживания для приоритетных сигналов с помощью инструментов формирования и организации трафика. Кроме того, была обеспечена синхронизация времени через сеть передачи. Одна из тестовых схем включала дублирование на уровне E1 посредством создания двух псевдопроводных соединений для резервирования E1 в сети MPLS по различным трактам. В сценариях, где сеть SDH/SONET сохраняется в качестве резерва, дублирование E1 может использовать одно соединение как псевдопроводное по пакетной сети, а другое по резервной сети TDM.

Задержка передачи сигнала через сеть MPLS (мс)	Устройства релейной защиты						
	ABB NSD570 (100Fx)	ABB NSD70 (E&M)	Siemens 7XV5653 (X.21)	Siemens 7XV5653 (RS232)	Siemens 7SD52 (X.21)	Areva P541 (G703)	Areva P541 (C37.94)
Величина задержки	6,3	6,1	5,5	7	6,1	5,7	6

РЕЛЕЙНАЯ ЗАЩИТА ПО ПАКЕТНЫМ СЕТЯМ

Механизмы решения проблемы передачи сигналов РЗ через пакетные сети, благодаря их сложности и многообразию, вызывают обоснованное беспокойство у “традиционных” связистов и релейщиков. Разработка новых стандартов и рекомендаций для пакетных сетей, включая средства защиты от всевозможных угроз, – процесс постоянный. Последние разработки технологии SDN (Software-Defined Networking) и технологии виртуализации сетевых функций NFV (Network Function Virtualization) позволят создавать интеллектуальные сети с высоким уровнем гибкости, унифицировать производимое оборудование, снизить затраты на внедрение новых сервисов. Естественно, все технологии должны проходить проверку, поэтому до наступления эры великой интеграции необходимо сформулировать конкретные Технические Требования к создаваемым сетям уже сегодня.

Все понимают, что один неверный шаг или несоблюдение всех мыслимых и немыслимых мер сетевой безопасности может привести к катастрофе. В любом случае “бежать впереди паровоза”, как предлагают некоторые энтузиасты прогресса, – занятие довольно опасное, особенно в области электроэнергетики.

Телекоммуникационные Стандарты разрабатывались на весь период эксплуатации оборудования и, в основном, не менялись. Высочайшая надежность, отсутствие возможности несанкционированного доступа – это рай для ответственных консерваторов. Использование этих свойств технологии SDH для передачи только критичных данных позволит значительно снизить затраты при создании сетей.

Наилучший вариант для систем доступа, предназначенных для энергетического рынка, – это гибридное SDH и PSN в одном оборудовании. Это позволяет обеспечить работу всех приложений с выполнением всех технических требований: надежности, скорости и т.д. Посредством комбинации возможности промышленного Ethernet и сетей TDM для приложений могут быть выбраны лучшие маршруты, обеспечивая передачу сигналов существующих сервисов и интерфейсов.

Это решение позволяет:

- *со стороны технологи TDM:*
  - легкое интегрирование Интеллектуальных электронных устройств (IEDs) и NG сервисов и оборудования в существующую инфраструктуру TDM;
  - непрерывность сервиса для существующих приложений и оборудования, даже после того как базовая сеть заменяется на IP/MPLS;
  - найти решения для эмуляции схем, которые не ставят под угрозу качество обслуживания или величину задержки;
  - многочисленные средства резервирования для обеспечения заданной надежности;
- *со стороны технологии PSN:*
  - гарантия определенного QoS для служб NGN и передачи современных приложений по пакетным сетям, использующим мультиприоритетное управление трафиком, OAM, диагностику и контроль производительности;
  - перспективные решения, разработанные для связи в интеллектуальных системах Smart Grid и архитектуры IEC-61850, включая надежные Ethernet сервисы с малым временем задержки при передаче данных между узлами, требующими обмена сообщениями в реальном времени, такими как GOOSE/GSSE;
  - защита критически важной инфраструктуры и основанных на IP систем SCADA от кибератак с помощью протоколов аутентификации и обеспечения кибербезопасности, таких как SSH, SSL, SNMPv3 и RADIUS и т.д.

При использовании в качестве транспортной сети технологии OTN или ее отдельных элемен-

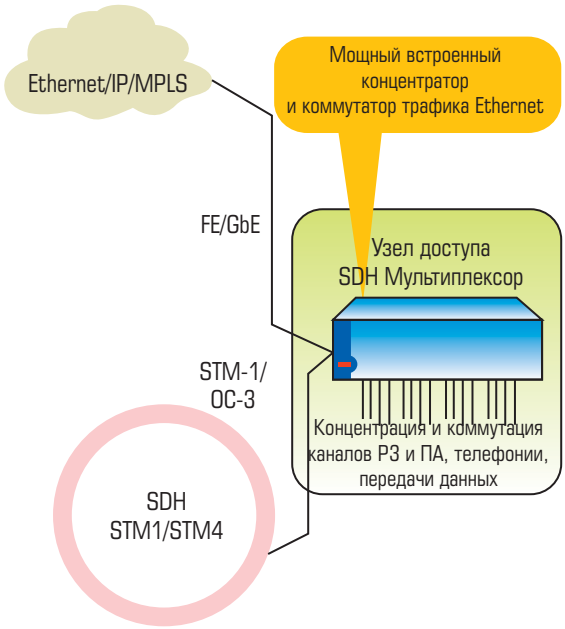

Рис. 3. Гибридный узел доступа

тов (рис. 3), возможен еще ряд вариантов создания защищенных гибридных сетей с минимальными капитальными вложениями и гарантией надежности, которую обеспечивает применение оборудования SDH или PDH (рис. 4).

ЗАКЛЮЧЕНИЕ

Переход к Smart Grid и сетям следующего поколения идет уже полным ходом, однако чрезвычайно важные приложения, такие как Релейная Защита, требуют особого внимания. Только решения, которые обеспечивают жесткие требования технологического оборудования: минимальное время передачи, надежности и безопасности, – можно рассматривать в качестве вариантов для реализации.

Гибридный вариант, включающий технологию TDM и Пакетные решения, позволяет энергетическим компаниям безболезненно и свободно выбрать путь перехода к новым технологиям, удовлетворяющим их потребности.

Среди различных вариантов телекоммуникационной инфраструктуры, предлагаемых для электроэнергетических сетей, целесообразно применение гибридного решения:

1. *Трафик, не имеющий критического значения, передавать по новой пакетной среде.*
2. *Трафик релейной защиты и другой критически важный трафик передавать по традиционной SDH сети.*
3. *Использовать одно устройство доступа для разделения и перевода трафика в сеть PSN и TDM.*
4. *В технических требованиях по проектированию ТСПД должна предусматриваться реконфигурация сети SDH.*
5. *Требования к оборудованию SDH должны содержать возможность поддержки гибридных решений.*

Такой поход позволяет осуществить поэтапный переход к Пакетным Сетям, исполь-

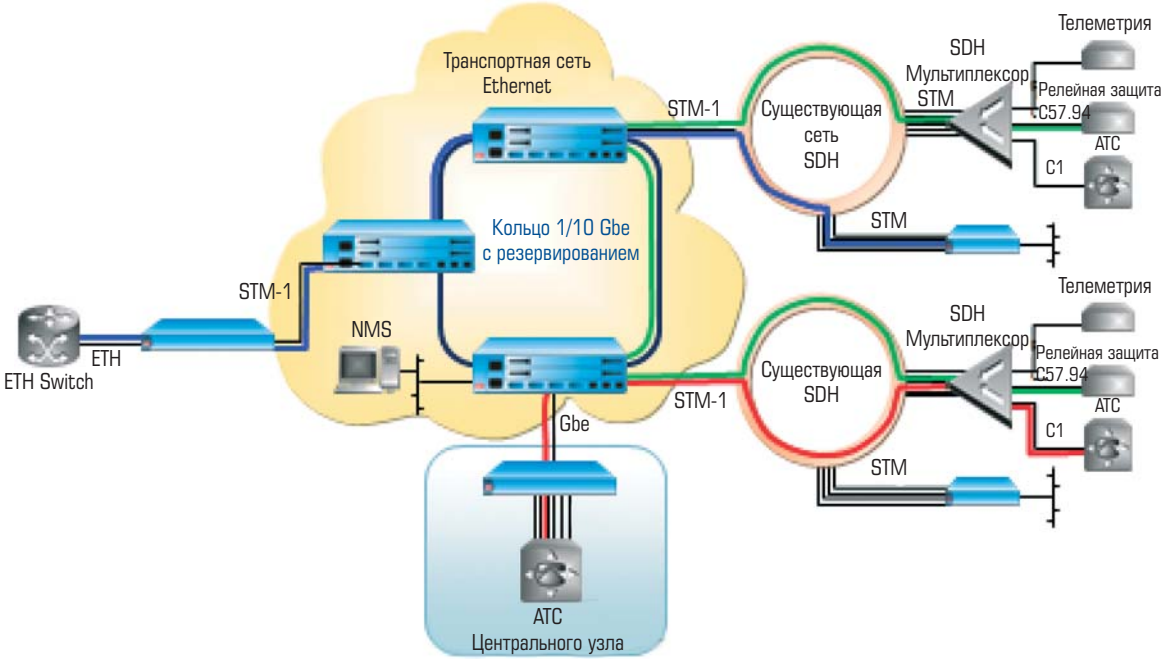

Рис. 4. Проект по объединению узлов подстанций через транспортную сеть

зуя установленное на объектах оборудование SDH и перераспределяя освободившиеся ресурсы на удаленные объекты. При этом топология сети SDH может быть значительно оптимизирована и упрощена.

Список литературы

1. *Кобец Б.Б., Волкова И.О.* Smart Grid в электроэнергетике / Энергетическая политика, № 6, 2009.
2. *Волобуев В.В.* Что такое Smart Grid? Каковы перспективы развития технологий Смарт Грид в России? – http://www.rsci.ru/sti/3755/208683.php.
3. *RAD* Data Communications Inc. 900 Corporate Drive Mahwah, NJ 07430 USA Tel: (201) 529-1100, Toll free: 1-800-444-7234 Fax: (201) 529-5777 E-mail: market@radusa.com <mailto:market@radusa.com>
4. *Гуревич В.И.* Интеллектуальные сети: новые перспективы или новые проблемы?

Лифшиц Александр Михайлович *– генеральный директор ООО “НПЦ Приоритет” .*