Обзор V Международной научно-технической конференции «Современные направления развития систем релейной защиты и противоаварийной автоматики энергосистем» применительно к тематике Исследовательского комитета D2 РНК СИГРЭ.

С 1 по 4 июня 2015 года в г. Сочи прошла организованная ОАО «СО ЕЭС» совместно с исследовательским комитетом B5 РНК СИГРЭ и ОАО «ВНИИР» V Международная научно-техническая конференция «Современные направления развития систем релейной защиты и противоаварийной автоматики энергосистем». Конференция проводилась при поддержке Министерства энергетики РФ и Исследовательского комитета B5 CIGRE. На ней были рассмотрены тенденции развития систем РЗА, вопросы противоаварийного и режимного управления, моделирования работы энергосистем, внедрения систем мониторинга и управления на базе синхронных векторных измерений (WAMPAC), применения стандарта МЭК 61850 и обеспечения информационной безопасности систем РЗА.

В последние годы наблюдается тенденция «сращивания» телекоммуникационных и информационных технологий с системами РЗА. Как следствие, на конференции обсуждались вопросы, интересные для исследовательского комитета D2 РНК СИГРЭ.

К большому сожалению, автор данного обзора физически не смог присутствовать на всех интересующих его докладах, т.к. часть из них проводилась в одно и то же время в разных залах.

На пленарном заседании в докладе заместителя директора по управлению режимами ЕЭС ОАО «СО ЕЭС» А.В. Жукова среди многих вопросов отмечено все более широкое внедрение в России систем мониторинга переходных режимов на базе технологии синхронизированных векторных измерений. Докладчик считает перспективным направлением развития систем синхронизированных векторных измерений их использование в системах релейной защиты, противоаварийной автоматики и управления режимами. Очевидно, что для построения данных перспективных систем потребуется реализация цифровых каналов связи.

Выступивший на пленарном заседании председатель Исследовательского комитета B5 CIGRE I. Patriota de Siqueira отметил, что с развитием удаленного управления и мониторинга в энергосистемах все большую актуальность приобретает обеспечение информационной безопасности.

В рамках пленарного заседания директор Ситуационно-аналитического центра ОАО «»Россети» Д.Б. Гвоздев отметил, что перспективным направлением развития является проведение оперативных переключений без присутствия на объекте оперативного и ремонтного персонала и постоянный контроль правильности выставленных уставок и конфигурации, качества работы устройств РЗА, что так же остро ставит вопрос об обеспечении информационной безопасности.

На последующем семинаре Исследовательского комитета B5 докладчиками отмечалась все большая роль телекоммуникаций и информационных технологий в системах РЗА будущего.

Интересным был доклад J. Cardenas (General Electric, Испания), подготовленный совместно с работающими в области информационной безопасности сыновьями. По их мнению, в

электроэнергетике необходимо не только защищаться от кибератак, но и находить, атаковать и уничтожать источники кибератак. Данный способ защиты у автора данного обзора вызывает много вопросов, т.к., например, источником кибератаки может быть взятый под контроль злоумышленником компьютер ничего не подозревающего пользователя и он будет уничтожен действием системы. По мнению докладчика, технологии для обеспечения информационной безопасности в электроэнергетике должны быть более высокого уровня и отличными от технологий, используемых в индустрии, и быть недоступными для коммерческого использования. В этом есть определенный смысл, т.к. злоумышленнику гораздо сложнее обойти систему, которая ему не известна. Кроме того, в ответственных процессах последнее слово должно быть за человеком. Докладчик считает, что сегодня безопасность устройств, обеспеченная физическими средствами гораздо более надежна, чем программными.

Как всегда для специалистов в области телекоммуникаций интересными были доклады D. Dolezilek (SEL, США). В секции «Современные системы РЗА. Идеология построения и концептуальные вопросы развития» им был представлен доклад «Simplifying Teleprotection Communications With New Packet Transport Technology». Докладчик отметил недостатки традиционно используемого протокола RSTP для резервирования каналов РЗА в сетях Ethernet из-за большого времени переключения при отказе путей. Предложено использование для организации Ethernet каналов для систем РЗА технологию Software-Defined Networking (SDN). Отмечено, что SDN позволяет распределять пакеты в зависимости от приложения и обеспечивать их соответствующую обработку. Использование таблиц статических маршрутов в SDN позволяет обеспечить минимальное время переключения (микросекунды) при отказе пути в сети. Но вопрос усложнения проектирования и реализации SDN по сравнению с традиционными сетями Ethernet к сожалению в докладе не рассматривался.

В секции «Вопросы эксплуатации РЗА» D. Dolezilek представил два доклада «Lessons Learned Through Commissioning and Analyzing Data from Ethernet Network Installations» и «Modern Ethernet Failure Recovery Methods for Teleprotections and High Speed Automation». В первом докладе отмечена важность измерения времени доставки сообщений и правильной конфигурации сетевого оборудования именно для систем РЗА. Для полномасштабного тестирования сетей Ethernet для РЗА необходимо специализированное оборудование и сервисы. Отмечается, что IT дизайнеры, не знающие особенностей систем РЗА, могут допускать ошибки и практический опыт показал это. Пример ошибки – определение пропускной способности Ethernet канала исходя из того, сколько требуется передать бит или байт в секунду без учета требуемого времени доставки сообщения. К сожалению, докладчик не осветил вопросы тестирования при штормовых нагрузках в сети. Во втором докладе D. Dolezilek рассмотрел протоколы PRP и HSR для резервирования каналов для систем РЗА. Отметил, что кольцо – не очень удачная топология для резервирования, т.к. в ней возможен только один отказ и для РЗА нужны другие топологии. По его мнению, лучший вариант – использование технологии SDN для резервирования в РЗА, но пока это находится только на стадии лабораторных испытаний.

Автор данного обзора в секции «Современные системы РЗА. Идеология построения и концептуальные вопросы развития» сделал два доклада «Перспективы использования ВЧ каналов в системах РЗА» и «Высоконадежные каналы по цифровым сетям связи существующих и перспективных систем РЗА». В первом докладе автор рассмотрел

особенности ВЧ каналов, показал, что использование цифровых ВЧ каналов в системах РЗА крайне затруднительно. Но в то же время использование ВЧ каналов, использующих в среде передачи традиционные сигналы, эффективно как в существующих, так и в перспективных системах РЗА. При этом совместное использование ВЧ каналов и цифровых каналов по оптическим волокнам может существенно повысить надежность системы РЗА. Во втором докладе автор показал, что цифровые высоконадежные каналы для существующих и перспективных систем РЗА можно строить как с использованием традиционной технологии SDH/PDH, так технологий пакетной коммутации. Переход от широко распространенной сегодня в российской электроэнергетике к технологиям пакетной коммутации вместо SDH/PDH требует решения целого ряда вопросов.

В секции в секции «Современные системы РЗА. Идеология построения и концептуальные вопросы развития» А.Г. Чирков (ООО «Прософт-Системы») представил доклад «Возможные способы резервирования каналов связи РЗ и ПА». Докладчик отметил существующий дефицит частот для резервирования ВЧ каналов, и предложил использовать аппаратуру, реализующую в одном диапазоне частот как передачу сигналов дифференциально-фазных защит (ДФЗ), так и устройств передачи аварийных сигналов и команд (УПАСК). Говоря о резервировании цифровых каналов для УПАСК, автор ограничился только кольцевыми топологиями, что во многих случаях является не самым удачным решением.

В секции «Вопросы эксплуатации РЗА» большой интерес вызвал доклад J. Cardenas (General Electric, Испания) «The Azerbaijani Experiences in Digital Substation Deployment». Для реконструкции ПС 110 кВ в Баку с момента начала монтажа оборудования до завершения наладки заказчиком было выделено время 10 дней (использовалось традиционное первичное оборудование). Используя традиционный подход к построению ПС такие сроки ввода объекта в эксплуатацию обеспечить невозможно. Поэтому General Electric реализовал цифровую ПС. В ней самым существенным отличием от концепции МЭК 61850 явился отказ шины процесса в виде сети Ethernet, что позволяет существенно повысить надежность и повысить информационную безопасность. Вместо этого между устройствами использовались множественные радиальные связи, по которым передавались SV и GOOSE. Докладчик отметил, что цифровые ПС далеко не всегда лучше старых традиционных. Новые технологии надо использовать там, где они действительно эффективны. В данном случае удалось уменьшить объем и стоимость кабелей, технической документации и сократить время ввода в эксплуатацию. В процессе обсуждения доклада возник вопрос о жизненном цикле оборудования цифровых ПС, т.к. оно для первичного оборудования оно должно составлять не менее 40 лет, а для вторичного – не менее 20 лет. Результат обсуждения – основной проблемой здесь является снятие с производства комплектующих.

В секции «Опыт реализации и проблемы внедрения стандарта IEC 61850» российский представитель Alstom Grid выступил с докладом своих бразильских коллег «Анализ надежности шины процесса». Докладчик отметил, что далеко не всегда надежность цифровой ПС даже при наличии резервирования может превзойти надежность традиционной ПС с резервированием. Использование кольцевой топологии сети Ethernet и протокола HSR не позволяет обеспечить надежность традиционной ПС с резервированием. При частичном резервировании с использованием протокола PRP уровень надежности вариантов с шиной процесса ниже, чем у традиционной системы РЗА с резервированием элементов. При этом

отмечено, что среднее время наработки на отказ элементов может отличаться у различных производителей, и зависит от условий эксплуатации, что приведет к несколько другим результатам по оценке надежности.

В секции «Опыт реализации и проблемы внедрения стандарта IEC 61850» X. Dong (Tsinghua University, Китай) представил доклад «Smart Power Substation Development in China», подготовленный совместно с коллегами из энергосистем Китая. В Китае начиная с 2009 года накоплен большой опыт внедрения пилотных проектов цифровых ПС на базе МЭК 61850 на классах напряжения от 6 до 750 кВ. С точки зрения телекоммуникаций отмечено невысокое качество коммутаторов при наружной установке и то, что информационные перегрузки в сети Ethernet могут привести к блэкаутам в энергосистемах.

Широкое обсуждение в секции «Опыт реализации и проблемы внедрения стандарта IEC 61850» вызвал доклад В.Н. Козлова (ООО НПП «Бреслер») «Этапы эволюции РЗА от электромеханики к МЭК 61850. Что делать?», По мнению докладчика, каналы связи – наиболее уязвимые элементы в РЗА из-за высокой повреждаемости, проникновения помех, перегрузок в аварийных ситуациях, сбоях, несанкционированном доступе и др. Проблема обострилась в рамках концепции цифровой ПС в формате МЭК 61850, где сеть Ethernet играет наиважнейшую роль. Докладчик считает, что подход «МЭК 61850 любой ценой» неоправдан. Доклад вызвал у отечественных и зарубежных специалистов как критику, так и согласие с рядом положений.

Интересными были все доклады в секции «Вопросы обеспечения кибербезопасности систем управления в электроэнергетике».

В докладе ИСЭМ СО РАН «Человеческий фактор при обеспечении кибербезопасности объектов электроэнергетики» отмечено, что стандартные подходы к обеспечению информационной безопасности (логическое разделение потоков, межсетевые экраны, контроль доступа, шифрование и т.д.) хорошо работают при правильном проектировании, правильной настройке и отсутствии ошибок в программном обеспечении сетевых устройств. После чего докладчик задал вопрос, а не утопия ли все это? Интересным является предложение совмещения цифровых, аналоговых и электромеханических устройств, что может явиться простым и эффективным средством обеспечения информационной безопасности. Одним из предложений является отказ от монотехнологичности в информационных сетях, т.е. отказ от IP и Ethernet, и использование для выполнения ответственных функций узкоспециализированных протоколов.

В докладе М.В. Никандрова (ООО «Интеллектуальные сети») «Концепция построения комплекса кибербезопасности информационной инфраструктуры современных объектов электросетевого хозяйства», подготовленного совместно с ОАО «НТЦ ФСК ЕЭС», подчеркнуто отсутствие изолированности информационных сетей в российской электроэнергетике. Докладчик отметил, что мы сами строим благоприятную среду для развития кибератак тотальным переходом на Ethernet и унифицированный протокол МЭК 61850, не сегментируя при этом сети и не контролируя трафик, при наличии развитого рынка уязвимостей и повышенного внимания со стороны спецслужб различных государств. Практика Международного форума DHDays V (2015) показала, что за два дня студентами без знаний в электроэнергетике в физической модели цифровой ПС на базе МЭК 61850 был

осуществлен вывод из строя информационной сети 6 раз, 1 раз перепрограммирован сервер времени и 2 раза реализованы воздействия на терминал, приведшие к несанкционированному отключению. Предложена комплексная структура обеспечения информационной безопасности, включающая в себя корпоративный центр, встраиваемый в государственные структуры, и программно-технические средства защиты и обнаружения кибератак на уровне объектов.

H.-J. Herrmann (Siemens AG, Германия) в докладе «Security Management for Substation Automation and Protection» считает, что полностью цифровые ПС станут реальностью через несколько лет, но уже сейчас необходимо думать о защите от несанкционированного доступа. Приведены данные ICS-CERT констатирующие, что в 2014 году 33% процента инцидентов с кибербезопасностью в жизненно важной инфраструктуре США были связаны с энергетикой. Предложен ряд как организационных, так и программно-технических мер обеспечения информационной безопасности.

K. Hagman (ABB Power Systems, Швеция), выступивший с докладом «Cyber Security measures in Protection and Control IED's», выразил согласие со всеми предыдущими докладчиками по тематике обеспечения кибербезопасности и рассмотрел организационные и программно-технические меры обеспечения информационной безопасности. Докладчик выразил мнение, что для обеспечения информационной безопасности в электроэнергетике требуется ограничить использование некоторых протоколов и IT технологий.

Вопросы в области интересов исследовательского комитета D2 РНК СИГРЭ, поднятые на данной конференции, являются крайне важными и неоднозначными, не имеют простых решений и требуют обсуждения широким кругом технических специалистов, а не менеджеров по продажам, на основе однобоких, показывающих только позитивные моменты презентаций которых часто принимаются решения о технической политике.

Сборник докладов и презентации размещены на сайте http://cigre.ru/activity/conference/relayprotect5/participants/materials/