

Методы экспресс-анализа в задаче оценки режимной надежности с учетом краткосрочного прогнозирования поведения системы

**А.Б. ОСАК, А.И. ШАЛАГИНОВ, А.В. ДОМЫШЕВ
Д.А. ПАНАСЕЦКИЙ, Е.Я. БУЗИНА**
Институт систем энергетики им. Л.А. Мелентьева СО РАН
Россия
osakalexey@mail.ru

КЛЮЧЕВЫЕ СЛОВА

Цифровая подстанция, РЗА, ПА, безопасность, надежность, живучесть.

1 ВВЕДЕНИЕ

В последнее время все больше внимания уделяется вопросам создания цифровых подстанций. Ключевым свойством цифровой подстанции является минимизация аналоговых и дискретных трактов в системах мониторинга и управления, что обеспечивается за счет максимально полной цифровизации систем оперативного и автоматического управления. Сегодня существует большое количество публикаций, посвященных общепринятому (на текущий момент) подходу к созданию цифровых подстанций, когда на основе стандарта МЭК-61850 создаются шины процессов и шины объектов [1].

Авторы, полностью поддерживая тенденции к цифровизации систем оперативного и автоматического управления, с осторожностью относятся к предлагаемой многими структуре, видя в этом угрозу надежности электроэнергетических систем и даже угрозу энергетической безопасности России. В работе предлагается рассмотреть возможные угрозы нарушения работы электроэнергетических объектов и сопоставить подходы, минимизирующие эти угрозы, сравнивая при этом традиционные (с традиционной РЗА, ПА и АСУ ТП) и цифровые подстанции.

2 ОСНОВНАЯ ЧАСТЬ

Рассматривая с позиции надежности и безопасности элементы цифровых подстанций, следует отметить, что здесь любая подсистема содержит типовые интеллектуальные микропроцессорные программируемые компоненты. С одной стороны, это обеспечивает гибкость и функциональность при относительно низкой цене. С другой стороны, специалист-электроэнергетик не в состоянии глубоко вникнуть в аспекты реального функционирования таких компонентов, более того, даже специалист-кибернетик не в состоянии досконально изучить функциональные схемы всех микропроцессоров и программного обеспечения. Конечно, и в традиционных подстанциях специалист-электроэнергетик не владеет, например, всеми аспектами производства меди для проводников или вопросами функционирования полупроводниковых компонентов традиционных РЗА. Безусловно, некачественная медь может привести к отказу элементов традиционной подстанции, но потенциальная угроза от злонамеренного искажения микропрограмм интеллектуальных компонентов на несколько порядков выше, чем угроза невыявленного брака при производстве медного кабеля. При этом заметим, что вопросы отстройки РЗ от обрыва измерительных цепей разрабатываются не одно десятилетие.

Авторы предлагают пересмотреть ставшие уже типовыми структурные схемы цифровых подстанций (на основе стандарта МЭК-61850). Одним из предложений является полный отказ от каких-либо физических или информационных шин (шин процессов, шин объектов), так как атака на шину является наиболее простым способом нарушить функционирование цифровой подстанции. Вместо создания шин предлагается создавать множественные соединения типа точка-точка. При этом необходимо учитывать малую стоимость интегральных схем. Например, себестоимость цифрового измерительного трансформатора тока с 2 цифровыми портами будет незначительно меньше стоимости цифрового измерительного трансформатора тока с 30 цифровыми портами, а стоимость оптического кабеля с 2 жилами практически равна стоимости оптического кабеля с 30 жилами и т.д. Применяя топологию точка-точка, можно применять более простые коммуникационные протоколы, в том числе с односторонней передачей информации, что исключит возможность кибернетической атаки и нарушения работы цифровых измерительных приборов (трансформаторов тока, напряжения и т.п.).

Также в работе предлагается рассмотреть возможность отказа от монотехнологичности в компонентах цифровых подстанций. В традиционной РЗА надежность ее функционирования обеспечивалась за счет резервирования, в том числе с использованием различных принципов выявления повреждений. При этом отказ устройств, использующих один принцип, не приводил к общему отказу системы. В цифровых подстанциях на основе стандарта МЭК-61850 монотехнологиями являются такие технологии, как Ethernet, TCP/IP, информационные протоколы стандарта МЭК-61850 и т.п. Например, некий вредоносный код, приводящий к переполнению в типовом микрокоде реализующем стек протоколов TCP/IP, позволит одной атакой парализовать все цифровые подстанции страны, так как одновременно откажут все виды виртуальных защит и автоматик на всех объектах, оснащенных оборудованием одного производителя. В качестве примера можно привести вирус Stuxnet [2, 3], перехватывающий и модифицирующий информационный поток.

Авторами предлагается подход к созданию структуры цифровых подстанций, когда заказчик рассматривает поставщика и подрядчика, как потенциальных «шпионов» и «хакеров», в результате чего технические решения должны приниматься с учетом минимизации возможного ущерба от потенциальной зловредной деятельности. Даже если не рассматривать наличие злого умысла, то в любом случае, необходимо обезопасить себя от возможных ошибок в интегральных схемах и микропрограммном коде, на которые не обратят внимания специалисты энергетики при заказе оборудования цифровой подстанции. Также следует пересмотреть подходы к тестированию и испытанию элементов и систем цифровых подстанций, делая уклон на тестирование системообразующих и коммуникационных функций, так как на прикладной электроэнергетический уровень будет приходиться в среднем 1-5% от всего программного кода цифровой подстанции. В качестве аналогии, можно привести следующий пример. Традиционные цепи испытывают повышенным напряжением с целью проверки надежности изоляции, соответственно элементы цифровой подстанции нужно испытывать на устойчивость к кибернетической атаке.

Для начала рассмотрим подходы к обеспечению кибербезопасности на электроэнергетических объектах, предлагаемые в настоящее время:

- применение оборудования, прошедшего процедуры испытаний и получившего соответствующие сертификаты и экспертные заключения о его пригодности к выполнению заявленных функций;
- применение средств авторизации и контроля доступа;
- применение межсетевых экранов, и других подобных технологий (например, применение логических, т.е. «виртуальных» сетей – VLAN), разделяющих информационные потоки на логическом уровне;
- применение выделенных для технологических процессов сетей и каналов связи, т.е. средства физического разделения информационных потоков;
- ограничение на организационном и физическом уровне доступа посторонних лиц к электроэнергетическим объектам и элементам цифровой связи, серверам, контроллерам и т.п.

На первый взгляд, все перечисленные технологии и мероприятия должны обеспечить кибербезопасность электроэнергетических объектов, однако их реальная эффективность напрямую зависит от полноты и качества выполнения всех перечисленных мероприятий.

Рассмотрим также вопросы применения сертифицированного оборудования. В настоящее время существует практика и опыт выполнения подобных работ для традиционных элементов электроэнергетического оборудования. В случае цифровых подстанций принципиально важным моментом является то, чтобы сертификат соответствия выдавался не на модель оборудования в целом, не на серию изделий, а на конкретную конфигурацию «железа» и программного обеспечения (например, прошивку цифрового терминала РЗА). Иначе весь процесс испытаний и сертификации теряет всякий смысл: испытали одно, а эксплуатируется совсем другое. При этом необходимо обеспечить, чтобы сличение сертификата соответствия и фактического изделия, установленного на реальном электроэнергетическом объекте, происходило не на уровне маркировки изделия (бирки) – как это происходит сейчас, а необходимо, чтобы в сертификационном центре либо хранился сам испытуемый образец, либо хранилась копия программного обеспечения для центрального процессора и микропрограммного обеспечения для сигнальных и коммуникационных процессоров, вместе со схемами и фотографиями внутреннего устройства изделия. Тогда собственник оборудования, либо инжиниринговая компания получат возможность хотя бы минимальной проверки соответствия конкретного экземпляра изделия и сертификата соответствия, который предоставил завод-изготовитель.

В части возможностей средств авторизации, контроля доступа, межсетевых экранов и других подобных средств, можно отметить, что пример офисных операционных систем и браузеров, имеющих многомиллионные примеры использования, показывает, что ежемесячно обнаруживаются различные ошибки в программном обеспечении, в том числе влияющие на безопасность этого программного обеспечения. Безусловно, требования к промышленным системам намного строже, но чем обеспечена гарантия безошибочности специализированного программного обеспечения для цифровых подстанций? Небольшое число разработчиков, тестировщиков и пользователей (по сравнению с офисными системами) едва ли повышает качество программного обеспечения, особенно в области кибербезопасности. С большой вероятностью разработчики программного обеспечения для цифровых подстанций не являются специалистами в хакинге, соответственно едва ли они знают и применяют все возможные технологии, препятствующие взлому компьютерной платформы. С учетом вышесказанного, можно сформулировать требование к производителям оборудования и программного обеспечения для цифровых подстанций, в части необходимости предоставления сведений и подтверждений того, что разработка и тестирование велось с привлечением ведущих специалистов в области кибербезопасности, что были применены достаточные средства, гарантирующие отсутствие невыявленных ошибок, влияющих на безопасность и функционирование системы. Здесь можно привести аналогию с производителями традиционного электроэнергетического оборудования, которые подтверждают качество своей продукции наличием соответствующей производственной базы, испытательного и лабораторного оборудования, квалифицированного персонала.

Еще одна потенциальная угроза кибербезопасности электроэнергетических объектов проистекает из того, что сложная цифровая система имеет программное обеспечение не только для центрального процессора, на котором выполняются основные функции устройства или системы, но и микропрограммный код в коммуникационных процессорах и других процессорах, установленных в цифровых устройствах подстанций. Опасность состоит в том, что те же самые коммуникационные процессоры с одинаковым программным обеспечением могут присутствовать в большом числе устройств, соответственно случайная или преднамеренная ошибка в микропрограммном коде коммуникационного процессора может привести к полному отказу большой группы устройств цифровой подстанции, выполняющих, в том числе, взаиморезервируемые функции (например, функции основных и резервных защит). В случае работы разных устройств на общую информационную шину, потенциально возможна ситуация, когда некая комбинация данных в информационной шине станет катализатором отказа всех цифровых устройств, работающих на этой шине. Наиболее вероятна такая ситуация в случае с преднамеренным внесением «закладок» в микропрограммное обеспечение. Мировая

практика уже имеет случаи кибератак на электроэнергетические и энергетические объекты в разных странах мира, в том числе и широко обсуждаемые атаки на объекты атомной отрасли в Иране. Соответственно нельзя отвергать возможность повторения подобного в будущем в других государствах.

При осуществлении на практике какой-либо кибернетической угрозы, функциональные отказы систем управления цифровых подстанций могут привести к отключению или повреждению электроэнергетического оборудования. Вследствие этого возникают общие угрозы в снижении надежности и нарушении устойчивости, что в свою очередь является угрозой энергобезопасности целых регионов. Опасность вышеописанных угроз существенно возрастает, когда цифровые подстанции встраиваются в единые системы управления, например, в рамках реализации концепций ИЭС ААС и Smart Grid. Поэтому актуальность вопросов кибербезопасности при реализации вышеуказанных концепций возрастает многократно.

Рассматривая угрозы кибербезопасности для оценки важности мероприятий, в том числе дорогостоящих, по повышению кибербезопасности электроэнергетических объектов, важно отметить некоторые возможные мотивы к осуществлению различных кибератак. Во-первых, не следует забывать о военных угрозах. Ежегодно многие государства тратят миллиарды долларов на закупки вооружения и содержание многочисленных армий, при этом, безусловно, возникает большой соблазн нанести упреждающий удар по инфраструктуре противника (а электроэнергетика – это важнейшая инфраструктурная отрасль любой развитой экономики), не вовлекая в это собственно вооруженные силы. Во-вторых, не следует забывать, что крупнейшие электроэнергетические компании являются акционерными обществами (корпорациями), акции которых торгуются на биржевых площадках. Можно с уверенностью предположить, что акции компании, серьезно пострадавшей от массовой кибер-атаки, существенно упадут в цене, что делает их привлекательными для покупки потенциальными инвесторами. Учитывая многомиллиардную стоимость крупных электроэнергетических компаний, полученная таким образом выгода может исчисляться сотнями миллионов или даже миллиардами долларов. Всего лишь два приведенных выше примера, показывают, что потенциально возможен серьезный спрос на кибератаки объектов и систем электроэнергетики. Соответственно вопросам кибербезопасности должно быть уделено соответствующее внимание.

Для обеспечения кибербезопасности цифровых подстанций можно предложить следующие шаги:

- Необходимо исключать наличие в цифровой подстанции узлов, кибератака на которые может нарушить работу большого числа функций. Решение данной проблемы может заключаться в функциональной декомпозиции и физическом разделении информационных потоков.
- Необходимо исключить хакерский взлом важных элементов цифровой подстанции. Решение данной проблемы может заключаться в применении симплексных каналов выдачи информации, взамен дуплексных, с применением соответствующих коммуникационных протоколов.
- Необходимо исключить хакерский взлом таких элементов, как межсетевые экраны, особенно обеспечивающие выход в глобальные сети. Сегодня применяются программные межсетевые экраны, неправильная настройка которых (например, вследствие хакерской атаки) может предоставить злоумышленнику полный доступ к системам управления объекта, что недопустимо. Решение данной проблемы может заключаться в организации межсетевого разделения с использованием симплексных каналов, конвертацией цифровой информации в аналоговую, и затем обратно в цифровую.
- Необходимо функционально упрощать системы цифровых подстанций. Сегодня принято массово использовать при автоматизации подстанций стандартные технологии, например, Ethernet, протокол TCP/IP и т.п. В тоже время, не следует забывать об чрезмерной универсальности данных технологий, стандарты на которые сложны для понимания в виду наличия множества вариаций. Алгоритм программного обеспечения, реализующего стек протоколов TCP/IP [4] будет понятен единицам программистов, при

этом данные малопонятные элементы становятся типовыми для цифровой подстанции. Как результат, это может привести к тому, что персонал не будет понимать физики протекающих процессов, а это прямой путь к ослаблению кибербезопасности. Решение данной проблемы может заключаться в осознанном упрощении всех стандартных технологий до минимально требуемого уровня. Необходимо исключить все лишние вариации, а любое отклонение от заданного варианта должно рассматриваться как внештатная ситуация.

Авторы считают, что необходимо расширять дискуссии по вопросам кибербезопасности цифровых подстанций [5] в свете концепций ИЭС ААС и Smart Grid. Формировать коллективные экспертные мнения, которые необходимо доводить как до разработчиков оборудования и программного обеспечения, так и до субъектов электроэнергетики, надзорных и контролирующих органов.

С одной стороны, имеется необходимость в развитии технологий, в том числе цифровых, которые дают широчайшие возможности. С другой стороны, имеются угрозы надежности и даже энергобезопасности. Вместо поиска компромисса (как сочетание некоторого уровня новых технологий и некоторого уровня киберзащищенности), необходима гармонизация всех аспектов. Необходимо, чтобы новые цифровые технологии повышали, а не снижали кибербезопасность электроэнергетических объектов и систем.

3 ЗАКЛЮЧЕНИЕ

В данной статье сформулированы некоторые актуальные проблемы в области кибербезопасности электроэнергетических объектов и систем, что становится актуальным в связи с появлением принципиально новых объектов – цифровых подстанций. В свете возможности дальнейшей реализации концепций ИЭС ААС и Smart Grid проблема многократно обостряется.

В работе предложен ряд подходов, которые, по мнению авторов, позволят решить часть обозначенных проблем. Данная работа является постановочной и рассматривается авторами как повод к активизации дискуссии среди специалистов по данной тематике.

ЛИТЕРАТУРА

- [1] Горелик Т.Г., Кириенко О.В., Дони Н.А. Цифровая подстанция. Подходы к реализации // Сборник докладов XXI конференции "Релейная защита и автоматика энергосистем", Москва, 29-31 мая 2012, с. 10-17.
- [2] Фрейдман А.В. Stuxnet и промышленная безопасность // <http://www.phocus-scada.com/rus/pub/Stuxnet&IndustrialSecurity.html>
- [3] Анализ кода Stuxnet, сокращенный перевод на русский язык отчета Symantec: Nicolas Falliere, Liam O Murchu, and Eric Chien (Symantec), W32.Stuxnet Dossier, Ver 1.4 (February 2011) // <http://www.phocus-scada.com/rus/pub/Stuxnet-CodeAnalys-rus.pdf>
- [4] Стек TCP/IP // <http://www.protocols.ru/files/Protocols/TCP/IP.pdf>
- [5] Нудельман Г.С. О требованиях кибербезопасности систем РЗА при использовании МЭК 61850 // Сборник докладов XXI конференции "Релейная защита и автоматика энергосистем", Москва, 29-31 мая 2012, с. 10-17.