О киберфизической модели для исследований информационной безопасности в электроэнергетике.

Архангельский О.Д., ЗАО "РКСС", Волошин А.А., НИУ "МЭИ",
Иванов Ф.А., ЗАО "ЭнЛАБ",

Аннотация

Широкое внедрение информационных технологий и средств вычислительной техники на объектах электроэнергетики остро ставит вопрос обеспечения информационной безопасности и защищенности объектов топливно-энергетического комплекса (ТЭК). Однако оценка информационной безопасности объекта только с позиций анализа работы систем, входящих в состав информационно-телекоммуникационной инфраструктуры (ИТКИ) не может дать полного представления о реальных последствиях кибератак.

Для полноценного анализа и проведения оценки тяжести последствий необходимо анализировать различные сценарии нарушений в работе электроэнергетических систем (ЭЭС), вызванных кибератаками на ИТКИ и автоматизированные системы управления (АСУ). Для этого необходимо создание специализированных кибер – физических моделей (КФМ) энергосистем, в которых одновременно моделируются как работа АСУ и инфо-телекоммуникационной инфраструктуры, так и работа электрической части ЭЭС. Использование подобных КФМ позволяет оценить и проанализировать возможные последствия кибератак для различных объектов ТЭК (например, результатом кибератаки могут стать перерывы в электроснабжении потребителей, нарушение устойчивости работы ЭЭС, выход оборудования из строя и т.д.).

В ЗАО «Российская корпорация средств связи» (ЗАО РКСС) для этих целей создается уникальная КФМ, не имеющая аналогов в России. Отличительная особенность разработанной КФМ в том, что помимо выполненной на базе программно-аппаратного симулятора RTDS виртуальной модели первичного оборудования ЭЭС испытательный комплекс содержит также реальные устройства релейной защиты, интеллектуальные устройства и серверы АСУ ТП, объединенные в единую модель, имитирующую функционирование сложной электроэнергетической системы.

В настоящем докладе рассмотрены основные технические решения, использованные при создании КФМ, а также указаны особенности применения КФМ для исследований информационной безопасности.

Ключевые слова: кибер-физическая модель, симулятор энергосистем, кибербезопасность, информационные и телекоммуникационные системы управления.

Введение

В современных электроэнергетических системах (ЭЭС) системы сбора и передачи данных, оборудование связи, автоматизированные системы управления на различных уровнях иерархии оперативно – диспетчерского управления стали неотъемлемыми элементами ЭЭС. Современная система управления энергетикой построена на базе ИТКИ и АСУ, и все большее количество оборудования электрических подстанций имеет интерфейс для подключения к сетям связи [3]. Наряду с повышением эффективности оперативно-диспетчерского управления, активное внедрение информационных технологий и концепции удаленного управления на объектах ТЭК имеет и ряд недостатков: многие объекты электроэнергетики становятся уязвимыми для

злоумышленников, а возможные кибератаки на инфраструктуру таких объектов могут иметь серьезные последствия для городов и даже целых регионов [4].

Таким образом, в современном мире проблема кибер-преступности в целом и, в частности, кибератак на важные инфраструктурные объекты, становится все более актуальной. В связи с этим, в настоящее время в Российской Федерации особое внимание на государственном и корпоративном уровне уделяется информационной безопасности объектов ТЭК и отражению возможных кибератак.

Для предотвращения атак на инфраструктурные объекты и анализа векторов атак необходимо определить наиболее критичные (уязвимые) элементы системы и оценить тяжесть последствий от реализации возможной атаки. Тяжесть последствий потенциальных кибератак и их воздействие на устойчивость функционирования ЭЭС зависит, в том числе, от текущего режима работы энергосистемы: наличия резервов генерируемой и передаваемой по ЛЭП мощности, наличия резервных трансформаторов и питающих линий, а также от изменения топологии сети (т.е. производимых коммутаций) и возникновения повреждений оборудования. Очевидно, что осуществить проверку устойчивости ЭЭС для различных сценариев кибератак на реальном функционирующем силовом оборудовании не представляется возможным – как по организационным, так и по экономическим причинам. Вместо этого предлагается использовать метод моделирования ЭЭС в реальном времени с включенным в контур моделирования вторичным оборудованием (т.н. *hardware-in-the-loop* моделирование). Разрабатываемые в рамках такого подхода модели носят название *кибер-физических* [5]. Для создания подобных моделей вычислительный комплекс реального времени (Real Time Digital Simulator, RTDS) с программным обеспечением RSCAD подключается к реальным устройствам релейной защиты (или любым другим интеллектуальным устройствам «полевого» уровня) посредством аналоговых, дискретных и интерфейсных сигналов.

В настоящее время КФМ являются наиболее эффективным инструментом для проведения исследований в области информационной безопасности электроэнергетических систем и дают наиболее полные возможности для проведения моделирования и исследований. КФМ с использованием симулятора RTDS была продемонстрирована в сентябре 2016г. в г. Иннополис, в рамках конференции по кибербезопасности АСУ ТП [1]. С использованием данной КФМ также проходил финал турнира Capture The Flag (CTF), где экспертами исследовалось функционирование оборудования при различных несанкционированных воздействиях. Аналогичные турниры проводились и ранее, и их результаты стабильно неутешительные: имея возможность подключения к внутренней сети предприятия, условные хакеры несколько раз смогли вызвать ложные срабатывания силового оборудования, что в реальной ЭЭС может привести к тяжелым последствиям [2].

Успешное развитие систем моделирования реального времени побудило к созданию моделей, включающих в себя помимо РЗА также системы автоматического управления (АСУТП), системы сбора и передачи информации (ССПИ), и системы оперативно – диспетчерского управления верхнего уровня: SCADA, EMS–системы и т.д. Подобные дополненные *КФМ* позволяют проводить развернутые исследования взаимодействия оборудования подстанции и диспетчерского центра, изучать моделируемый участок ЭЭС

на предмет устойчивости к информационным атакам на различные информационные активы и т.д.

Созданная в ЗАО РКСС лаборатория на базе КФМ является первым российским комплексом, специально ориентированным на проведение научных исследований в области информационной безопасности объектов электроэнергетики. Использование в КФМ симулятора RTDS позволяет гибко наращивать возможности лаборатории и ее состав по мере появления новых задач и целей исследований. Разработанная КФМ состоит из следующих основных частей (см. Рис.1):

1. Автоматизированного рабочего места (АРМ), подключённого к локальной сети Ethernet, с установленным на нём специальным пакетом программ RSCAD, позволяющим создавать новые проекты, управлять и наблюдать за процессом моделирования;
2. Вычислительный комплекс RTDS, содержащий в своём составе процессорные платы, платы дискретного и аналогового ввода-вывода, а также различные интерфейсные платы;
3. Шкафы усилителей, предназначенных для усиления низкоуровневых аналоговых сигналов с платы цифро-аналогового преобразователя (ЦАП) симулятора RTDS. Каждый шкаф усилителей содержит различный набор блоков усиления, используемых для формирования входных сигналов тока и напряжения для тестируемых терминалов РЗА. Входные сигналы усиливаются до уровня, требуемого для нормальной работы терминалов РЗА;
4. Шкафов с исследуемым оборудованием РЗА, АСУ ТП и другими интеллектуальными устройствами «полевого» уровня.

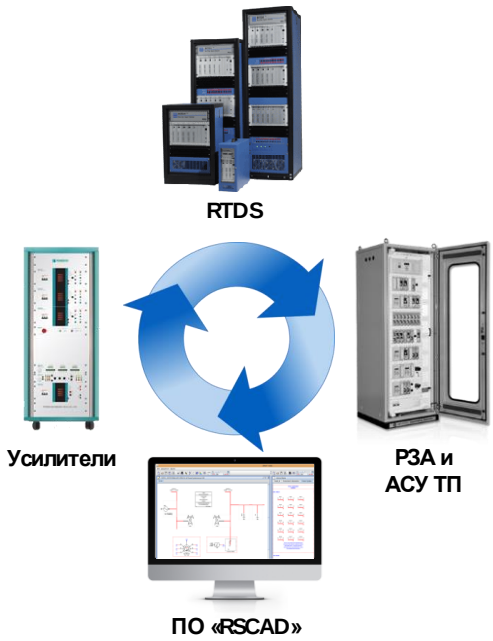

Рис. 1. Состав КФМ

Применение разработанной ЗАО РКСС кибер – физической модели позволяет качественно повысить уровень проводимых исследований информационной безопасности объектов ЭЭС за счет возможности имитации индивидуальных особенностей реальных

электрических сетей и энергообъектов, а также позволяет учесть при моделировании инфраструктурную избыточность, резервирование, работу систем противоаварийной автоматики, релейной защиты, различных вспомогательных и измерительных систем и т.д. Ниже представлены основные цели и задачи лаборатории ЗАО РКСС:

1. Разработка подходов и методов обнаружения кибератак, мер оперативного реагирования и управления инцидентами.
2. Исследование кибербезопасности подстанций и электрических сетей;
3. Анализ критических элементов подстанций.
4. Оценка защищенности объектов ЭЭС и их компонентов.
5. Анализ уязвимостей объектов электросетевой инфраструктуры, разработка моделей угроз для объектов электросетевого комплекса на основании проведенных тестовых и сценарных испытаний.
6. Проведение совместных с производителями РЗА и АСУ исследований оборудования с целью выявления наличия уязвимостей в указанном оборудовании.
7. Поддержка в разработке и дальнейшем развитии нормативной базы (национальных стандартов, руководств и «лучших практик») для обеспечения информационной безопасности объектов критической инфраструктуры.
8. Повышение квалификации по информационной безопасности.

Описание КФМ

Как уже было показано выше, в основу КФМ входит симулятор RTDS, позволяющий с помощью программного обеспечения RSCAD (см. Рис.2) проводить моделирование в реальном времени и взаимодействовать с устройствами релейной защиты и АСУ через аналоговые и дискретные сигналы, а также цифровые интерфейсы МЭК61850 (GOOSE, SV), PMU, MMS, 104, DNS, что актуально при моделировании «цифровых подстанций» и симуляции взаимодействия подстанции и диспетчерского центра.

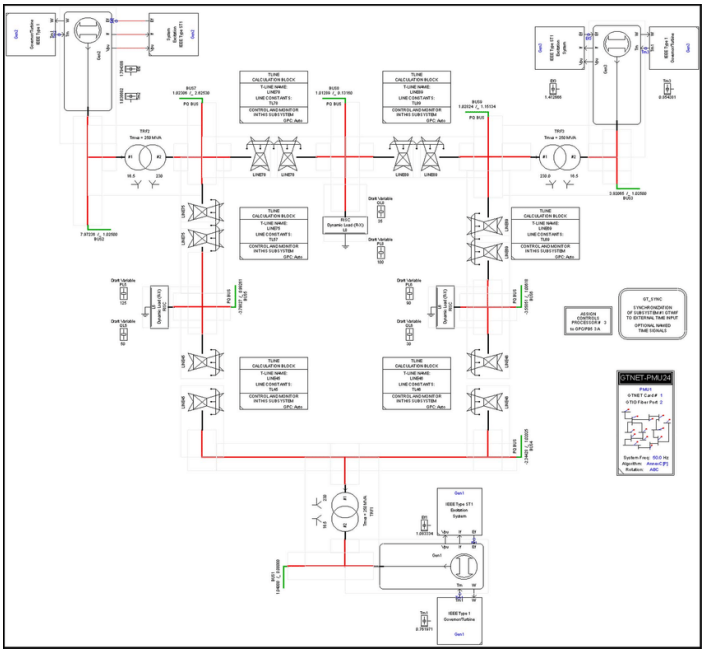

Рис.2 Пример модели: 9-ти узловая схема WSCC в ПО «RSCAD»

Логическую схему симулятора можно представить как несколько взаимодействующих между собой уровней, на каждом из которых находится определенное оборудование, программное обеспечение и т.д., соответствующее задачам данного уровня. В общем случае удобно использовать представление в виде четырех инфраструктурных уровней: (см. Рис. 3):

- уровень модели ЭЭС: моделируемая на вычислительном комплексе RTDS физическая инфраструктура электрических сетей, обеспечивающая передачу и распределение электрической энергии. Включает первичное и вторичное оборудование электрических станций и подстанций, а также линии электропередачи;
- коммуникационный уровень: информационно-коммуникационная инфраструктура, включающая оборудование связи подстанций и диспетчерских центров и обеспечивающая сбор данных с АСУ ТП и объектовых SCADA и передачу этой информации в диспетчерские системы верхнего уровня;
- уровень датчиков и контроллеров: интеллектуальные устройства (IEDs) «полевого» уровня, т.е. датчики, контроллеры присоединений и т.д. При этом, для реализации вторичной аппаратуры в КФМ используются как реальные устройства РЗА и АСУ, так и их виртуальные модели, созданные в программном обеспечении RSCAD;
- уровень приложений: на данном уровне представлены взаимодействующие между собой системы оперативно-диспетчерского и оперативно-технологического управления ЭЭС (включая ОУИК, SCADA, АСУ ТП и другие диспетчерские системы).

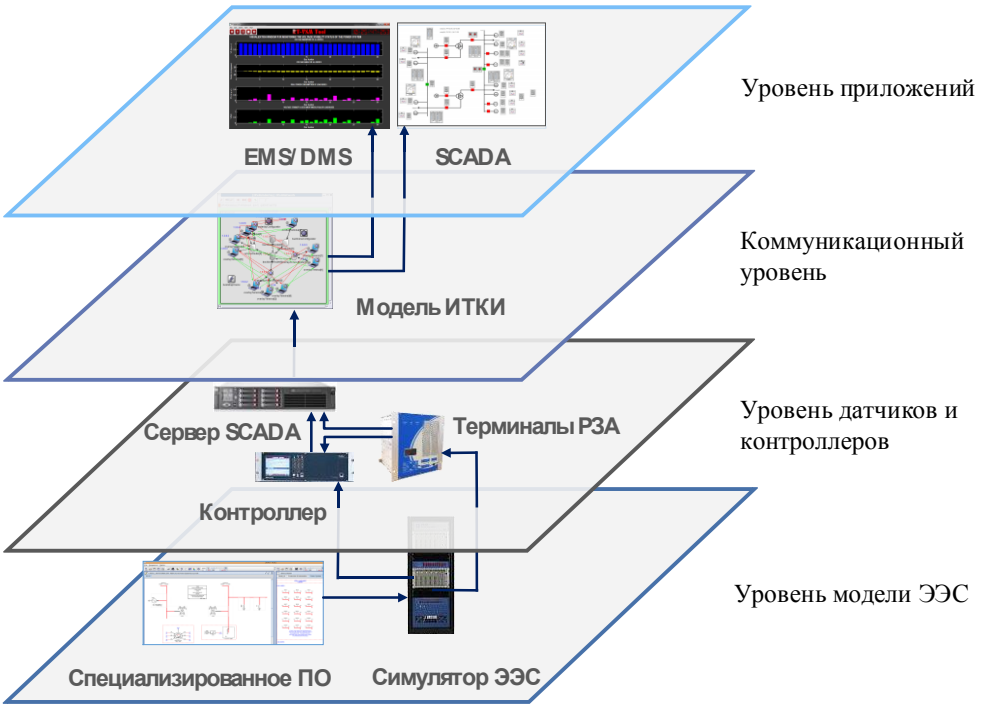

Рис. 3. Архитектура модели КФМ

Основным условием получения адекватной картины при моделировании является наличие моделей компонентов ЭЭС, максимально точно отражающих параметры реальных устройств. Библиотека RSCAD включает в себя все виды оборудования, используемого в ЭЭС, что позволяет успешно решать поставленные задачи.

При проведении испытаний КФМ позволяет решать следующие задачи:

1. Управление моделью ЭЭС в программно-аппаратном комплексе RTDS в режиме реального времени с реализацией информационного обмена с реальным оборудованием РЗА и АСУ ТП по протоколам: МЭК 61850 (GOOSE и SV), МЭК 60870-5-104, DNP;
2. Управление параметрами модели, автоматический перезапуск модели с новыми параметрами;
3. Управление параметрами устройств РЗА и коммутаторов локальной вычислительной сети лаборатории с использованием стандартных протоколов (МЭК 61850 (GOOSE, SV, MMS), DNP, 104, Telnet, SNMP);
4. Выполнение пользовательских сценариев проведения опытов на языке программирования Phyton, в том числе решение задач оптимизации параметров модели или испытуемого оборудования с применением генетических алгоритмов.
5. Сохранение результатов проведения опытов в базе данных;
6. Автоматическая генерация отчетов о проведении испытаний.

Разработанная КФМ является уникальной для России тестовой площадкой, позволяющей апробировать различные средства защиты информации, а в последствии проводить сертификационные испытания оборудования АСУ и интеллектуальных устройств.

В настоящее время можно выделить несколько основных направлений исследований, проводимых или планируемых к проведению в лаборатории ЗАО РКСС:

1. Проверка релейной защиты. Симулятор реального времени формирует сигналы, близкие к реальным сигналам ЭЭС. Наличие обратных связей обеспечивает взаимодействие проверяемого терминала релейной защиты с моделируемой ЭЭС, имеется возможность подключения нескольких устройств РЗА, для исследования их взаимодействия. В рамках моделирования различных систем возможно подключение устройств релейной защиты как к аналоговым источникам сигналов, так и по протоколу МЭК 61850.

2. Проверка систем управления. В рамках данного направления проводятся исследования корректности функционирования автоматизированных систем управления в различных условиях (в том числе, при деградации части функций системы в результате кибератаки). При этом в виртуальной модели указываются объекты управления, на которые может быть выдан управляющий сигнал. При этом, помимо коммутационного оборудования подстанций (выключателей, разъединителей и заземляющих ножей) к объектам управления могут быть отнесены и специализированные устройства, например возбудители, регуляторы и стабилизаторы генераторов, устройства управления для высоковольтных систем постоянного тока (HVDC), управляемые статические компенсаторы реактивной мощности (SVC),

управляемые через тиристоры последовательно включенные конденсаторы (TCSC) и статические синхронные компенсаторы (STATCOM).

3. Испытания устройств и систем синхронизированных векторных измерений (УСВИ и ССВИ) в реальном времени. В рамках разработанной модели могут проводиться испытания корректности функционирования систем векторных измерений (WAMS) при нарушении целостности или доступности информации, получаемой от интеллектуальных устройств. Кроме того, в разработанной КФМ существует возможность создания тестовых сигналов, синхронизированных по GPS, для проверки УСВИ на соответствие протоколу IEEE C37-118.

4. *Умные сети и распределенная генерация. Промышленный интернет вещей.* Исследование информационной безопасности и взаимодействия с ЭЭС интеллектуальных устройств, внедряемых в рамках реализации концепций «Умных сетей», «Распределенной генерации» и «Промышленного интернета вещей». *Для проведения подобных исследований в КФМ предусмотрена поддержка в*ысокоуровневых протоколов передачи данных: МЭК 61850, DNP3, IEEE 37.118, а в программном обеспечении «RSCAD» могут быть смоделированы различные источники энергии: газотурбинные установки, ветроустановки, солнечные панели, силовые электронные преобразователи.

Выводы

В связи с возросшей актуальностью проблемы информационной безопасности объектов топливно-энергетического комплекса в целом и электроэнергетики в частности, в ЗАО РКСС была создана тестовая площадка для исследования защищенности устройств РЗА и АСУ ТП и проведения исследований кибербезопасности объектов ЭЭС. Уникальность разработанного лабораторного комплекса в том, что помимо устройств релейной защиты в контур моделирования включено также оборудование и программное обеспечение АСУ ТП и другие интеллектуальные устройства и подсистемы. Таким образом, в рамках концепции полунатурного моделирования сложных ЭЭС, на стенде производится симуляция работы участка электрической сети с учетом функционирования различных автоматизированных и автоматических систем управления и интеллектуальных устройств. Это позволяет проводить всесторонние исследования информационной безопасности для данных систем, оценивать тяжесть возможных последствий кибератак на данные информационные ресурсы.

Ссылки

1. "Наша киберфизическая модель на конференции Кибербезопасность АСУ ТП 2016" http://ennlab.ru/rus/news/92
2. "Кто взломал электрическую подстанцию: разбор конкурса Digital Substation Takeover " https://www.phdays.ru/press/news/41185/
3. Организация телеуправления подстанциями без постоянного присутствия обслуживающего персонала. Комплексный подход / Федоров О.А., Небера А.А., Литвинов П.В., ЗАО «РТСофт» // С.5. - 4 CIGRE
4. SCADA Security in a Post Stuxnet World / Eric Byres, P. Eng // Byres Security Inc - 2007.
5. Khaitan S.K., J.D. McCalley “Cyber physical system approach for design of power grids” IEEE Power and Energy Society General Meeting, 2013;

Об авторах

Архангельский Олег Денисович окончил магистратуру НИУ «МЭИ», факультет «Институт Электроэнергетики», каф. «Электроэнергетические системы» в 2015 г. Направление 140400 «Электроэнергетика и электротехника». Профиль: Электроэнергетические системы, их режимы, устойчивость, надежность и качество электрической энергии; аспирант НИУ «МЭИ», факультет «Институт Электроэнергетики», каф. «Электроэнергетические системы». Направление: 13.06.01 Электро- и теплотехника, направленность (специальность): 05.14.02 Электрические станции и электроэнергетические системы. Место работы: ЗАО «Российская корпорация средств связи», Руководитель проектов.

Волошин Александр Александрович И.о. заведующего кафедрой релейной защиты и автоматизации энергосистем НИУ "МЭИ", к.т.н., ст. преп.

Иванов Федор Анатольевич родился в 1976 г. и в 2000 г. закончил "Чувашский государственный университет им. И.Н. Ульянова" по специальности "Автоматика и управление в технических системах". Занимался разработкой промышленных систем автоматики в ОАО "ВНИИР". С 2011 г. работает в должности заместителя технического директора ЗАО "ЭнЛАБ" и занимается технической поддержкой и продвижением программных (PSCAD) и программно-аппаратных комплексов (RTDS) для моделирования ЭС.