С.7-1. Человеческий фактор при обеспечении кибербезопасности объектов электроэнергетики

А.Б. ОСАК, Д.А. ПАНАСЕЦКИЙ, Е.Я. БУЗИНА
ИСЭМ 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, в результате чего весь функционал устройств релейной защиты, противоаварийной автоматики и автоматизированного диспетчерского управления сосредотачивается во взаимосвязанных компьютерных подсистемах энергообъекта. Имеется большое количество публикаций, посвященное общепринятому, на текущий момент, подходу к созданию цифровых подстанций, когда на основе стандарта МЭК-61850 создаются шины процессов и шины объектов.

Инфраструктурная важность электроэнергетики для существования, жизнеобеспечения и развития государства и общества, а также непрерывность и нераздельность процессов производства, передачи, распределения и потребления электрической энергии приводит к повышенной значимости задач по обеспечению безопасности, надежности и живучести электроэнергетических систем и их объединений, а также отдельных электроэнергетических объектов. Вопросы кибербезопасности современных электроэнергетических объектов, оснащенных цифровыми системами мониторинга, управления, релейной защиты и противоаварийной автоматики становятся все более актуальными в виду новизны проблемы [1, 3].

В большинстве публикаций и нормативных документах (включая стандарты МЭК, рекомендации СИГРЭ), посвященных вопросам кибербезопасности объектов электроэнергетики, основным способом ее обеспечения видится применение соответствующих технических средств, которые обеспечивают требуемую защиту от различных несанкционированных действий.

Авторы, не отрицая необходимость применения специальных технических средств обеспечивающих кибербезопасность, предлагают посмотреть на данную проблему с позиции человеческого фактора [4], так как именно человек (сотрудник энергопредприятия, сотрудник поставщика и подрядчика, или стороннее лицо) является основной причиной потенциальной киберугрозы.

В работе предлагается подход к анализу киберугроз, с классификацией возможных последствий и ущербов, с прослеживанием причинно-следственной связи по всей цепочке. Предлагается выделить группу киберугроз не связанных со злонамеренными действиями, а также группу киберугроз связанных со злонамеренными действиями отдельных лиц, конкурирующих бизнес-групп и даже враждебных действий некоторых стран. Учитывая тот факт, что заинтересованными сторонами в кибератаке могут быть, в том числе, государства, основным способом по недопущению кибератак со значимыми последствиями и ущербами, по мнению авторов, является применение специальных технических решений при проектировании цифровых систем. Данные технические решения должны на структурно-функциональном уровне исключить саму возможность успешной кибернетической атаки.

2 ОСНОВНАЯ ЧАСТЬ

2.1. Новые проблемы

В 2013 году, на фоне скандальных событий с Эдвардом Сноуденом, были озвучены многочисленные факты информационного слежения посредством цифровых технологий за государственными органами власти многих стран мира со стороны специальных служб США. По существу, данные факты можно квалифицировать, как непрерывные кибернетические атаки на государственные органы власти, причем данные атаки не были выявлены органами безопасности атакованных государств, а стали известны только благодаря шпионскому скандалу. С тех пор геополитическая обстановка в мире только накаляется.

Когда мы говорим о кибернетической безопасности, то часто возникает вопрос, не подвержены ли (сейчас или в будущем) данным атакам наши наиважнейшие инфраструктурные объекты, в том числе, объекты электроэнергетики? Возможно, не так страшно, если угроза состоит только лишь в несанкционированном мониторинге. Однако какие могут быть последствия в том случае, если существуют скрытые каналы несанкционированного управления?

2.2. Особенности цифровых подстанций

Первой ключевой особенностью, отличающей цифровую подстанцию от традиционной, является замена большинства физических аналоговых и дискретных связей (токовые цепи, цепи напряжения, оперативные цепи) цифровыми. При организации аналоговых связей для передачи одного сигнала ранее требовалась как минимум одна жила медного кабеля определенного сечения. При использовании цифрового кабеля по паре оптических волокон можно передавать тысячи и даже десятки тысяч различных сигналов, что при правильной организации позволяет существенно упростить кабельное хозяйство интеллектуальной цифровой подстанции.

Второй ключевой особенностью цифровой подстанции является то, что любое микропроцессорное устройство располагает вычислительным ресурсом. На современной подстанции располагаются десятки или сотни различных микропроцессоров, зачастую выполняющих однотипные функции. Степень загрузки микропроцессоров на разных устройствах разная, но в любом случае, как правило, имеется большое количество неиспользуемой вычислительной мощности. В традиционных подстанциях, функционал шкафа РЗА или ПА был ограничен количеством вмещаемых внутри него устройств вторичных коммутаций (клемм, реле, ключей, испытательных блоков и т.п.). В цифровой подстанции, имеется возможность одновременного выполнения на мощном современном микропроцессорном устройстве большего количества функций, чем было ранее.

И наконец, третьей ключевой особенностью цифровой подстанции является появление цифровых и оптических трансформаторов тока (ТТ) и напряжения (ТН). Данные устройства могут быть реализованы с использованием различных принципов, иметь различное конструктивное исполнение. Однако их общими свойствами являются повышенная точность не только в номинальном, но и в аварийных режимах, а также возможность преобразования аналоговых параметров в цифровую форму непосредственно в комплексе технических средств, относящихся к цифровому трансформатору тока или напряжения.

В функциональном плане цифровая подстанция является принципиально новым объектом с позиции систем управления. В ней обеспечивается глубокий мониторинг первичного оборудования и всех вторичных систем. Существенно упрощается процесс внедрения новых функций контроля и управления, так как для этого требуется только лишь установка программного обеспечения, и достаточный вычислительный ресурс (сервера, контроллеры, терминалы). При этом не потребуется организации аналоговых и дискретных цепей. С позиции концепции Smart Grid, цифровая подстанция – это эффективный электросетевой элемент, обладающий свойствами наблюдаемости, адаптивности и интеллекта. Тем не менее, создание цифровых подстанций в российских энергосистемах вызывает большое количество вопросов. Наиболее острые и не до конца решенные – это вопросы кибербезопасности.

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, функциональность, совместимость и взаимозаменяемость при относительно низкой цене. С этой точки зрения построение цифровой подстанции, безусловно, является эффективным мероприятием. С другой стороны, специалист-электроэнергетик не в состоянии глубоко вникнуть в аспекты реального функционирования таких кибернетических компонентов, более того, даже специалист-кибернетик не в состоянии досконально изучить функциональные схемы всех микропроцессоров и программного обеспечения. Поэтому следует обратить внимание на то, что неизбежным следствием развития цифровых и микропроцессорных технологий на объектах электроэнергетики является существенное усложнение внутренних алгоритмов работы элементов цифровых подстанций.

Таким образом, можно отметить, что при построении цифровых подстанций на основе стандарта МЭК 61850 возникает системное противоречие: по сути, предлагается существенно упростить физическую (аппаратную) часть цифровой подстанции за счет принципиального усложнения алгоритмической и программной частей. При этом ослабление кибербезопасности является неизбежным следствием увеличения объема системного и коммуникационного программного обеспечения, которое раньше выполняло вспомогательные функции, а теперь станет ключевым элементом.

2.3. Сравнение цифровых и традиционных подстанций с позиции надежности и живучести

Сопоставим задачи обеспечения надежности и способы их решения для традиционных и цифровых подстанций. Для традиционных подстанций существенных проблем с кибербезопасностью не возникает, поэтому для них будем рассматривать лишь общие вопросы надежности и живучести.

Ключевыми элементами, которые могут быть подвержены кибератаке с последующим нарушением функционирования цифровой подстанции являются:

- внешние цифровые каналы, по которым осуществляется технологическая и оперативная связь с другими энергообъектами и диспетчерскими пунктами;
- коммуникационные сети энергообъекта, включая коммутаторы и маршрутизаторы;
- шины процессов и шины объектов (в соответствии с МЭК-61850), которые в цифровой подстанции являются неотъемлемыми элементами любой функции РЗА, ПА, мониторинга и оперативного управления;
- цифровые устройства РЗА, ПА, управления и мониторинга электрооборудованием.

Таким образом, именно коммуникационные сети и каналы являются «узким местом» цифровой подстанции. Для сравнения отметим, что в традиционных подстанциях, таким «узким местом» являлись системы оперативного постоянного тока (СОПТ). Отказ СОПТ приводил к полной утрате управляемости энергообъекта. Все остальные подсистемы автоматического, автоматизированного или оперативного управления выполнялись достаточно независимыми друг от друга, поэтому отказ одной подсистемы не влиял на функционирование другой.

Классический подход для повышения надежности и живучести технической системы требует поиска возможных угроз (возмущающих факторов), и исследования влияния этих угроз на технологические процессы, т.е. оценивание устойчивости к ним. В качестве возможных угроз (возмущающих факторов) с позиции кибербезопасности для цифровых подстанций можно отметить следующие:

- кибератаки извне, через внешние цифровые каналы связи энергообъекта;

- невыявленные ошибки в программном обеспечении устройств цифровой подстанции;
- злонамеренные программные дефекты (закладки), встроенные в программное обеспечение микропроцессорных устройств цифровой подстанции, с целью управляемого вывода из строя системы;
- ошибки оперативного и эксплуатационного персонала энергообъекта.

Средствами повышения надежности и живучести являются:

- дублирование – установка нескольких одинаковых устройств;
- функциональное резервирование – реализация одинаковых или схожих функций с использованием разных физических принципов;
- декомпозиция – разделение различных функций между разными устройствами, физическое разнесение кабелей и устройств;
- упрощение – применение простых, понятных и однозначных алгоритмов управления.

При переходе от традиционных подстанций к цифровым на основе МЭК-61850, происходит отказ от следующих принципов:

- отказ от функционального резервирования, т.к. коммуникационные сети (включая коммутаторы и маршрутизаторы) работают на одном и том же принципе;
- отказ от декомпозиции, т.к. коммуникационные сети (включая коммутаторы и маршрутизаторы), обеспечивающие шины процессов и шины объектов, выполняют функции доставки информации до любых устройств мониторинга и управления;
- отказ от упрощения, т.к. алгоритмы передачи и обработки цифровой информации по коммуникационным сетям сложны.

Для обеспечения надежности и живучести цифровых подстанций применяют только:

- дублирование устройств;
- дублирование сетей и каналов связи;
- функциональное резервирование и декомпозицию исключительно на уровне электроэнергетических функций, но не на уровне цифровых технологий.

Коммуникационные сети и микропроцессорные устройства цифровых подстанций универсальны, и без существенной переделки могут решать любые информационные задачи, например, выполнять заведомо зловредные функции в процессе кибератаки, чего нельзя было сказать об устройствах на традиционных подстанциях (особенно на электромеханической базе).

2.4. Человеческий фактор при обеспечении кибербезопасности объектов электроэнергетики

Совершенствование технических и программных средств, выполняющих коммуникационные функции на цифровых подстанциях, а также применение специальных технических и программных средств, предназначенных для защиты от кибератак, снижает вероятность атаки извне и последствия от возможных невыявленных ошибок в программном обеспечении.

Ключевой проблемой является то, что одно и то же устройство или программное обеспечение может быть настроено так, чтобы обеспечивать кибербезопасность и недопускать кибератаки, а может быть настроено по-другому, т.е. способствовать кибератакам. Внешний вид устройств при этом не меняется, однако их функциональность в части кибербезопасности принципиально разная. Отличие исключительно в настройках, причем отличаться может незначительное число параметров из тысячи совпадающих. Неспециалист в вопросах кибербезопасности вообще не сможет выявить проблему путем каких-то периодических осмотров оборудования. Значит, требуется привлечение специально обученных специалистов, которые способны решать подобные задачи.

Соответственно, важнейшим требованием к специалисту по кибербезопасности является требование правильного и добросовестного выполнения своих обязанностей. Однако, учитывая масштаб последствий, а также то, что заинтересованными сторонами в кибератаке могут быть иностранные государства, на первый план выходят вопросы политической и бизнес лояльности, патриотизма, эффективности спецслужб и т.п. То есть вопросы, выходящие за рамки техники и энергетики. Если подобным образом, можно говорить о том, что любая цифровая подстанция должна превращаться в некий закрытый и секретный объект, наподобие военных и ядерных объектов, со всеми вытекающими затратами. Но готов ли электроэнергетический бизнес к такому?

Альтернативным путем является пересмотр структурной и функциональной схем цифровых подстанций таким образом, чтобы в принципе исключить многие из потенциально возможных киберугроз. Например, традиционные электромеханические реле, традиционные устройства вторичных коммутаций не подвержены кибератакам в виду отсутствия какой-либо цифровой части. Поэтому некоторое совмещение цифровых, аналоговых и механических устройств может являться простым и эффективным средством обеспечения кибербезопасности, причем полностью понятным электроэнергетикам.

2.5. Предложения по обеспечению кибербезопасности цифровых подстанций

Если все устройства РЗА, ПА, системы управления первичным оборудованием будут выполнены на цифровой базе и будут объединены в единую информационно-управляющую систему, то результатом кибератаки может быть полная потеря управляемости энергообъектом или заведомо ложное управление.

Если несколько смежных подстанций подвергнется целенаправленной кибератаке, то вполне возможны случаи полного обесточивания значительной группы потребителей (включая ответственных). Также возможны случаи повреждения дорогостоящего первичного оборудования вследствие неустраненного КЗ или длительной неустраненной перегрузки. При этом классические средства дальнего резервирования на смежных цифровых подстанциях могут быть также неработоспособны по все той же причине.

Как было отмечено выше, успешность кибератаки зависит не только от качества технических средств, но и от слабоуправляемых процессов, таких как лояльность и человеческий фактор. Поэтому одним из наиболее важных аспектов, который необходимо обеспечивать с позиции кибербезопасности цифровых подстанций, является то, чтобы успешная кибератака не приводила к повреждению дорогостоящего или сложно ремонтируемого оборудования. Соответственно необходимо хотя бы в минимальном объеме сохранять средства защиты и управления, выполненные без использования цифровых технологий, и не вовлеченные в сферу управления цифровых устройств.

В частности, газовые, дуговые и прочие подобные защиты оборудования могут легко быть построены на независимой от цифровых подсистем базе, и напрямую действовать на отключение выключателей, минуя цифровые системы управления. Сложностей с такой реализацией нет никаких, значительного числа медных кабелей это не потребует, зато надежность и живучесть энергообъекта повышается на порядок.

Применение цифровых технологий существенно расширяет возможности, может повышать быстродействие, чувствительность и селективность основных и резервных защит. Не хотелось бы жертвовать этими достоинствами в угоду защиты от гипотетических кибератак. Данное противоречие можно было бы решить путем реализации на цифровых подстанциях дополнительных степеней защит с большими выдержками времени, выполненных, возможно даже, на электромеханической базе. Например, установка классической МТЗ с заведомо большой выдержкой (больше, чем у традиционных резервных защит дальнего резервирования), отстроенной от термической стойкости оборудования, которая должна быть последним рубежом, защищающим оборудование от повреждения.

Важно также обеспечить независимые от цифровых подсистем элементы защиты и управления, независимым оперативным током, где сама СОПТ не должна управляться от централизованной цифровой системы управления.

Авторами предлагаются следующие мероприятия по повышению кибербезопасности цифровых подстанций и объектов электроэнергетики в целом:

– разделение информационных потоков различных подсистем на физически не связанные сегменты коммуникационных сетей передачи данных внутри подстанции, т.е. предлагается создание независимых друг от друга шин процессов и шин объектов для каждой функции автоматического или автоматизированного управления, требующей повышенной надежности;

- отказ от монотехнологичности в коммуникационных сетях передачи данных внутри подстанции (чтобы Ethernet и TCP/IP не были единственными коммуникационными технологиями цифровой подстанции);
- применение симплексных каналов с односторонней передачей информации там, где это достаточно для выполнения прикладной функции, например, односторонняя передача информации от цифрового ТТ (ТН) к устройствам РЗА, исключающая возможность кибератаки на сам ТТ (ТН) от неисправного устройства РЗА;
- создание выделенных сегментов коммуникационных сетей, использующихся для настройки и переконфигурирования микропроцессорных и коммуникационных устройств, причем в процессе эксплуатации данные сегменты должны быть нормально отключены (снято питание с коммуникационных устройств или разобраны разъемы);
- применение межсетевых экранов, разделяющих различные сегменты коммуникационных сетей на физическом (аналоговом) уровне, которые не должны допускать выполнение несанкционированных функций (сегодня межсетевые экраны реализуются на уровне программного обеспечения);
- применение специальных межсетевых экранов, предназначенных для передачи GOOSE сообщения между физически разделенными сегментами коммуникационных сетей с возможностью физического вывода из работы любого сигнала (аналог традиционного ключа/накладки для традиционной подстанции);
- применение для ответственных функций упрощенных узкоспециализированных протоколов обмена информации, которые не позволяют передавать несанкционированную информацию (в отличие от Ethernet и TCP/IP, которые поддерживают передачу любой информации).

Для реализации предлагаемых мероприятий необходима разработка и внедрение новых технологий, ранее не применявшихся для построения цифровых подстанций.

На организационном уровне необходимо принципиально переработать подходы к сертификации оборудования и лицензированию специалистов. С позиции кибербезопасности, функционал микропроцессорного устройства цифровой подстанции определяется исключительно его программным обеспечением. Соответственно сертификат соответствия должен быть на конкретную аппаратную версию и конкретную программную прошивку устройства. Чтобы это реализовать на практике, необходимо упросить организационно-бюрократическую сторону сертификации, сосредоточившись на проверке функций. Учитывая общую сложность цифровых технологий и применяемых алгоритмов цифровой коммуникации, необходимо обратить внимание на персональное лицензирование конкретных специалистов. Сейчас допуск на определенные виды работ выдается организации в целом, а необходимо этот допуск давать конкретным специалистам, без привязки к организации, тогда существенно повышается персональная ответственность специалиста, и снижается возможность административного давления. Следует отметить, что подобный способ лицензирования специалистов успешно применяется в США.

Авторы считают, что необходимо расширять дискуссии по вопросам кибербезопасности цифровых подстанций в свете концепций ИЭС ААС и Smart Grid [3]. 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 развития технологий, в том числе, цифровых, которые дают широчайшие возможности. С другой стороны, имеются угрозы надежности энергообъектов и даже энергобезопасности регионов и государств. Вместо поиска компромисса (как сочетание некоторого уровня новых технологий и некоторого уровня каберзащищенности), необходима гармонизация всех аспектов. Необходимо, чтобы новые цифровые технологии повышали, а не снижали кибербезопасность электроэнергетических объектов и систем. Авторы считают, что такое вполне осуществимо.

3 ЗАКЛЮЧЕНИЕ

В статье сформулированы некоторые актуальные проблемы в области кибербезопасности электроэнергетических объектов и систем, что становится важным в связи с появлением принципиально новых объектов – цифровых подстанций. В свете возможности дальнейшей реализации концепций ИЭС ААС и Smart Grid, значение обозначенных проблем существенно возрастет.

Авторами показывается, что наибольшую угрозу кибербезопасности для важных инфраструктурных систем, какой является электроэнергетическая отрасль, представляет собой человеческий фактор, причем главным образом среди специалистов, которые должны обеспечивать эту самую кибербезопасность.

Предлагается на цифровой подстанции выделять критические функции защит от повреждения оборудования, и реализовывать их не на цифровой базе, тем самым, исключая саму возможности кибератаки на эти критически важные защиты.

Предлагается на цифровой подстанции разделять информационные потоки на физическом уровне с целью исключения самой возможности распространения кибератаки на весь энергообъект в случае успешного взлома отдельных подсистем.

В работе предложен ряд подходов, которые, по мнению авторов, позволят решить часть обозначенных проблем. Данная работа, расширяя проблемы и уточняя предложения, ранее обозначенные в работе [2, 4], все-таки является постановочной и рассматривается нами 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] Осак А.Б, Панасецкий Д.А., Бузина Е.Я. Аспекты надежности и безопасности при проектировании цифровых подстанций // Сборник докладов международной конференции «Современные направления развития систем релейной защиты и автоматики энергосистем», Екатеринбург, 3 – 7 июня 2013 г.

[3] 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.

[4] Осак А.Б., Панасецкий Д.А., Бузина Е.Я. Кибербезопасность объектов электроэнергетики. Угрозы и возможные последствия. // Сборник докладов XXII конференции "Релейная защита и автоматика энергосистем", Москва, 27-29 мая 2014, с. 417-423.

С.7-2. Концепция построения комплекса кибербезопасности информационной инфраструктуры современных объектов электросетевого хозяйства

М.В. НИКАНДРОВ, М.В. БРАГУТА
ООО «Интеллектуальные Сети»,
ОАО «НТЦ ФСК ЕЭС»
Россия
nikandrov@igrids.ru , braguta_mv@ntc-power.ru

КЛЮЧЕВЫЕ СЛОВА

Информационная инфраструктура критически важных объектов, электросетевой комплекс РФ, информационная безопасность, кибератаки.

1 ВВЕДЕНИЕ

Повышение уровня автоматизации промышленных и системообразующих предприятий путем внедрения современных информационно-телекоммуникационных систем в технологические процессы обуславливает актуализацию вопросов безопасности информационной инфраструктуры критически важных объектов. Согласно официальной статистике за 2014 г. ФСБ России удалось пресечь 74 миллиона кибератак на государственные информационные системы [1]. Сменился характер инцидентов – повышается число «таргетированных атак», характеризуемых определенной целью и длительным периодом подготовки злоумышленников. Широкую известность целевых атак на информационную инфраструктуру промышленных объектов получил инцидент применения кибероружия «Stuxnet» против иранской ядерной программы. Используемые технологии при разработке кибероружия постоянно эволюционируют наряду с «точками» их применения: последние вирусные атаки («Energetic bear») разработаны с использованием новых методов заражения, таких как инфицирование инсталляционных пакетов SCADA систем на сайтах поставщиков программных решений, основной целью применения которых являются индустриальные сети.

Описанное выше подтверждается активной профильной деятельностью в области совершенствования законодательной и нормативной базы, а также принятой Концепцией государственной системы обнаружения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГС) [2]. В законопроект «О безопасности критической информационной инфраструктуры Российской Федерации» [3] включены требования о создании комплекса защиты информационной инфраструктуры критически важных объектов, к которым относятся объекты электросетевого хозяйства магистральных и распределительных электрических сетей. Необходимость гармонизации подходов, используемых при построении указанной ГС, и технологических особенностей промышленных информационно-технологических систем обуславливает критичность процесса детальной проработки способов защиты и выявления кибернетических атак на промышленных объектах, в том числе объектах электросетевого хозяйства единой национальной электрической сети.

В статье приведено общее описание предлагаемой авторами архитектуры комплексной организационно-технической системы обеспечения информационной безопасности объектов электросетевого хозяйства магистральных электрических сетей России (далее – Система).

2 ОБЪЕКТЫ АТАКИ

Несмотря на консервативность используемых технологий управления производственными процессами на объектах электросетевого хозяйства в настоящее время осуществляется переход от электромагнитных, аналоговых устройств к цифровым (микропроцессорным). Новые объекты характеризуются рядом особенностей:

- повышение концентрации микропроцессорных устройств в контуре технологического управления и наблюдения, потенциально подверженных внешним и внутренним угрозам;
- использование распределительных вычислительных сетей, включающих множество разнородных устройств, обуславливающих процесс формирования «благоприятной среды» для недекларированных потоков информации, а также ее утечки;
- необходимость передачи информации на верхние иерархические центры управления средствами корпоративных (технологических) вычислительных сетей;
- использование зарубежных «коробочных решений» средств защиты от вредоносного программного обеспечения непосредственно на промышленных объектах;
- наличие скрытых и сохранение стандартных паролей для конфигурирования цифровых устройств контура технологического управления.

Перечисленные особенности и факторы представляют из себя лишь вершину айсберга, являющего собой большое разнообразие мишеней для атаки с целью возможного несанкционированного захвата управления и получения конфиденциальной информации о состоянии объекта.

Результаты проведенных авторами экспериментальных исследований по кибератакам на образцы широко применяемых в РФ микропроцессорных устройств релейной защиты и автоматики (далее - МП РЗА) подтверждают описанные случаи уязвимости и угрозы. Экспериментальные исследования были проведены на терминалах МП РЗА, контролерах присоединений, серверах времени и на других устройствах вторичной коммутации. С использованием «классических» методов кибератак (DDoS, spoofing, fuzzing и т.д.) подтверждена возможность ограничения функционала микропроцессорных устройств, в отдельных случаях результатом эксперимента являлся полный отказ устройства.

Положительные результаты эксперимента подтверждают необходимость реализации комплексных мер по проверке уровня информационной безопасности наряду с функциональными испытаниями с учетом того, что МП РЗА является основным средством обеспечения технологической безопасности процесса передачи и распределения электрической энергии, и отказ устройств данного вида грозит большим масштабом последствий (ущербом).

Технологические требования к надежности и функциональности применяемых на объектах электросетевого хозяйства микропроцессорных устройств обуславливают необходимость классификации информационных активов по степени их влияния на производственные процессы и ущерба от отказа по причине киберинцидентов. В рамках проводимых исследований предложена классификация информационных активов (общее описание) в зависимости от уровня значимости и специфики электроэнергетики. За основу взяты рекомендации ФСТЭК России [4], в соответствии с которыми комплекс мер по защите информационной инфраструктуры АСУ ТП должен определяться исходя из уровня значимости и степени возможного ущерба, но при этом необходимо учитывать объем информационной инфраструктуры объекта.

К примеру, при анализе электрической подстанции, оснащенной системой защиты, построенной на базе электромеханических реле, нарушение работы которой повлечет за собой возникновения чрезвычайной ситуации федерального характера, необходимо присвоить данной системе высокий уровень значимости и первый класс защищенности (К1). В данном случае необходимо обеспечить полный комплекс мер защиты информационной инфраструктуры, но осуществить это практически невозможно, так как рассматриваемый объект характеризуется минимальной поверхностью атаки и неразвитой информационной инфраструктурой.

Общая классификация показана в таблице 1.

Особенность объекта	Класс защищенности
1) Объект построен на МП РЗА и контроллеров, оснащен полноценной АСУ ТП с возможностью дистанционного управления;	Первый класс (К1)

2) Работа объекта, влияющего на устойчивость ЕНЭС. 3) Нарушение работы объекта повлечет за собой возникновение чрезвычайной ситуации федерального или межрегионального характера или иные существенные негативные последствия.	
1) Объект построен на МП РЗА и контроллеров, оснащен полноценной АСУ ТП с возможностью дистанционного управления; 2) Работа объекта мало влияет на устойчивость ЕНЭС; 3) Нарушение работы объекта повлечет за собой возникновение чрезвычайной ситуации регионального характера или иные умеренные негативные последствия.	Второй класс (К2)
1) Объект построен на основе электромеханических и полупроводниковых систем РЗА, оснащен системой телемеханики без возможности дистанционного управления;	Второй класс (К2)
1) Нарушение работы объекта повлечет за собой возникновения чрезвычайной ситуации муниципального (локального) характера или возможны иные незначительные негативные последствия.	Третий класс (К3)

Табл. 1: Классификация объектов электросетевого хозяйства.

Для окончательного определения класса защищенности необходимо принимать решение по каждому объекту в отдельности.

3 АРХИТЕКТУРА СИСТЕМЫ

Комплексная Система должна включать в себя ряд организационных мероприятий и внедрение специализированных программно-технических средств. Структура Системы в обязательном порядке должна включать в себя следующие уровни:

- центральный уровень - корпоративный центр информационной безопасности (далее – Центр), встраиваемый в структуру ГС [5]. В задачи Центра должны входить мониторинг, обнаружение, предупреждение, ликвидация и прогнозирование ситуации в области обеспечения информационной безопасности объектов электросетевого хозяйства.
- объектовый уровень – программно-технические средства защиты и обнаружения кибернетических атак и нештатных компьютерных инцидентов. В задачи программно-технического обеспечения объектового уровня должны входить средства глубокого анализа сетевого трафика и анализа управляющих команд (промышленный DPI) внешних каналов объектовой связи, сигнализация и регистрация выявленных компьютерных инцидентов (кибератак).

4 ЗАКЛЮЧЕНИЕ

Изменение методов воздействия на технологическое и социальное развитие страны, использование современных технологий кибератак и кибервойн обуславливают острую необходимость проведения проактивных работ по формированию комплексной защиты информационной инфраструктуры объектов электросетевого хозяйства как критически важных объектов Российской Федерации. В статье проведено общее описание предлагаемой авторами архитектуры комплексной системы по обеспечению информационной безопасности объектов электросетевого хозяйства РФ. Ожидаемым результатом реализации предложенной архитектуры является обеспечение кибернетической защиты электрических подстанций, соответствующей уровню современных угроз и требованиям законодательства РФ.

ЛИТЕРАТУРА

[1] Обращение Президента РФ Путина В.В. «ФСБ в 2014 году пресекла 74 миллиона кибератак» [Электронный ресурс] // РИА-Новости/ URL: http://wap.ria.ru/defense_safety/20150326/1054622560.html. Дата обращения: 04.04.2015.

[2] Выписка из Концепции государственной системы обнаружения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (Концепция утверждена Президентом Российской Федерации 12 декабря 2014 г. № 1274).

[3] О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс] // Проект Федерального закона РФ. / URL: http://regulation.gov.ru/. Дата обращения: 04.04.2015 г.

[4] Приказ ФСТЭК России от 14.03.2014 от №31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природы среды» [Электронный ресурс]// ФСТЭК России. URL: fstec.ru. Дата обращения: 04.04.2015г.

[5] О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [Электронный ресурс]/ С.Н. Юдин // ФСБ России 2015. URL: ib-bank.ru/. Дата обращения 04.04.2015 г.

Actual trends in development of Power System Relay Protection and Automation
1–5 June 2015, Sochi (Russia)

S.7-3. Security Management for Substation Automation and Protection

C. BISALE, H-J. HERRMANN
Siemens AG
Germany
Chaitanya.b@siemens.com

KEYWORDS

Substation automation, password management, cyber security, integrity protection, centralized security management.

1 INTRODUCTION

Background

With the currently ongoing and increasing digitalization and automation of electrification aimed at achieving better system integration and efficiency, there has been a corresponding and unmistakable upward trend in the number and sophistication of cyber attacks that are targeted at the critical infrastructure of the energy and utilities sectors. Consequently, governmental and regulatory bodies have recognized the impending, real threats that such cyber attacks pose to a nation’s economy and security, and have constituted guidelines and strict governance measures to ensure that the power system operators take adequate steps to protect their infrastructure in a timely and responsible manner. Standardization bodies have also taken steps in tandem with the regulations to guide operators in establishing information security management systems (ISMS), based on standards such as ISO/IEC 27001 and 27019, to ensure secure operations, and to guide technology vendors in developing secure and interoperable substation automation and protection products and systems. Ultimately, the cyber security technologies and controls employed need to serve the primary interests of the operators, namely protect their business and capital by enabling smooth operations while at the same time mitigating the risks of cyber threats and ensuring compliance with cyber regulations.

Purpose of this paper

This paper offers details on the application and management of various cyber security controls and enabling technologies in digital substations. Beginning with the illustration of implemented security functions in modern protection and control devices, hereafter generically referred to as IEDs, this paper provides a bottom-up view to ensuring the overall operational security of an electric utility. Consequences for the communication infrastructure in a digital substation automation system (DSAS) and beyond from a cyber security perspective are covered. Ideas on migrating a legacy substation to a secure substation are presented. A discussion on addressing product interoperability in the area of cyber security by means of adopting standardization is presented. This paper concludes with a call for standardization and unification of the approaches required to deliver a cost-effective and efficient operational security to the DSAS operator.

2 BODY

2.1 Secure Products at the Core of Secure Substations

A depiction of a typical digital substation is offered in figure 1 along with some basic security controls in place. The management of the overall system security poses a multidimensional challenge for the utilities due to the geographically and topologically distributed yet connected and therefore vulnerable nature of digital substation networks. An orchestration of various cyber security controls and technologies is required to meet this challenge in the context of secure substation architectures. Whereas secure substation architectures provide the structural defense, the security controls provide behavioral/operational defense against cyber attacks.

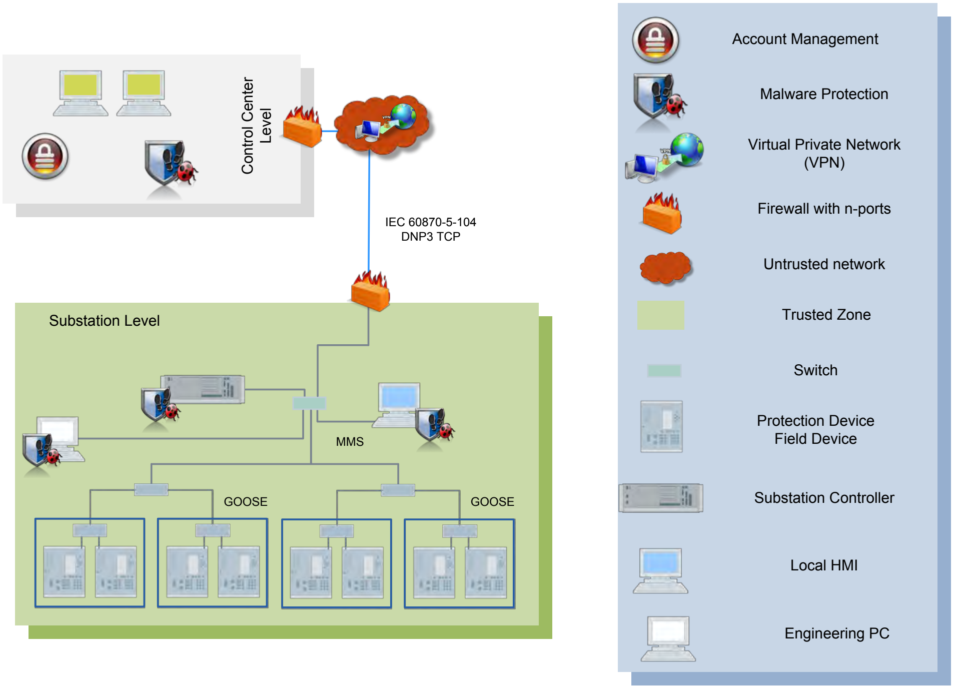


Figure 1: Typical Primary Digital Substation with Ethernet/IP-based Process Communication and (optional) site-to-site encryption

In Figure 2 the primary cyber security controls and technologies that need to be considered are listed – they are a distillation of the prevailing industry and regulatory standards that govern and guide cyber security implementation across the world. Although it lies outside the scope of this paper, the establishment of the physical security perimeter of the plant is a must, whereby physical access to a substation is permitted only to authorized personnel.

Regulatory guidelines such as the BDEW Whitepaper outline, among other aspects, the expectations of a secure product to a sufficiently concrete level so that vendors can implement these controls in conformance to the requirements, and the DSAS operator can verify the conformity statements as part of their ISMS governance activities to ensure the overall compatibility of the deployed products to their internal policies of both operational and regulatory nature.

2.2 User Authentication and Authorization

Once inside a substation, an operator normally views and controls the process automation using the substation-local human machine interface (HMI) software, which allows the viewing and modifying of the states of both primary substation equipment (e.g. circuit breaker, disconnector, etc) and secondary substation equipment (e.g. bay controller, protection device, etc) that control them. Therefore the HMI must support built-in access control and login mechanisms to allow and disallow all or specific functions based on the authorization level of the user that has logged in or has attempted to log in. As has been seen over recent years, some DSAS operators are establishing, or want to establish IT systems such as Microsoft Active Directory or other such X.500 directory service systems directly in the substations for being able to centrally manage user accounts and to couple substation automation products such as the HMI to use the centrally managed user accounting system for their access control purposes. This is one of many instances where the so-called Operational Technology (OT), meaning the HMI which is a domain-specific software and automation product, meets IT, meaning the Microsoft Active Directory Server, in the substation.

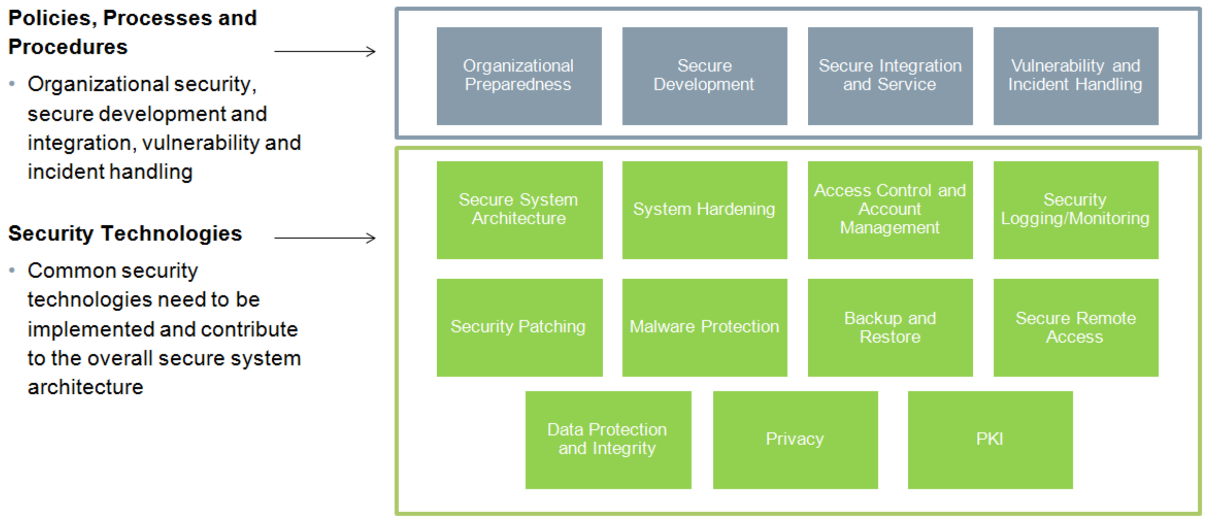

Policies, Processes and Procedures
• Organizational security, secure development and integration, vulnerability and incident handling
Security Technologies
• Common security technologies need to be implemented and contribute to the overall secure system architecture
Organizational Preparedness
Secure Development
Secure Integration and Service
Vulnerability and Incident Handling
Secure System Architecture
System Hardening
Access Control and Account Management
Security Logging/Monitoring
Security Patching
Malware Protection
Backup and Restore
Secure Remote Access
Data Protection and Integrity
Privacy
PKI

Figure 2: Cyber Security Controls and Technologies for a Digital Substation

Fine-grained access control management in IEDs is supported by the IEC 62351-8 standard "Role Based Access Control" (RBAC), which in addition to definition of standard roles and rights for digital substation and telecontrol systems, also describes the anchoring of roles in X.509 certificates so as to enable a public key infrastructure (PKI) based management of operator personnel and DSAS components (protection relays, substation controllers, HMI, ...), thereby supporting a critical aspect of operational security

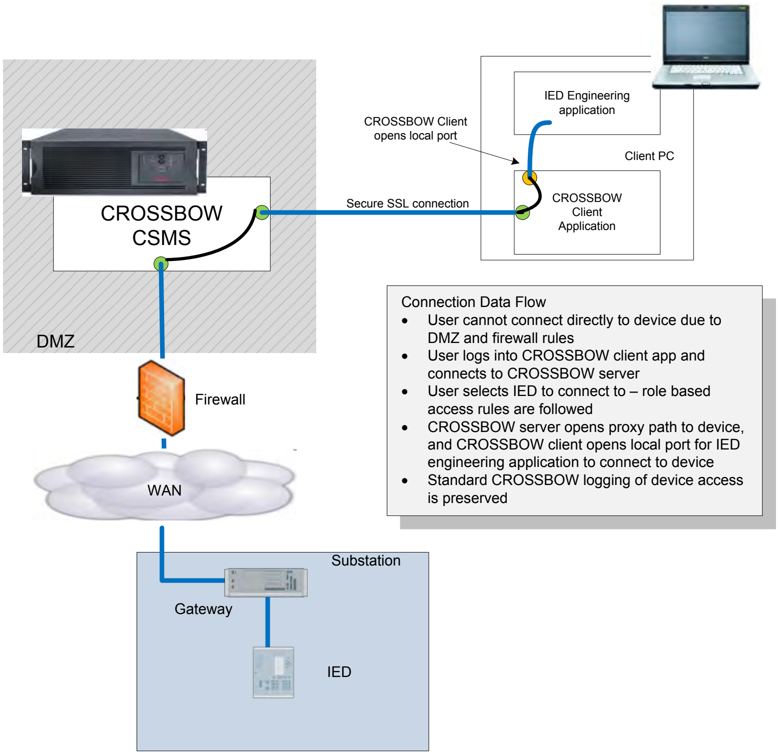
As of today, system-wide role-based access control (RBAC) is yet to be adopted as standard practice at the substation level, particularly in the bay level (e.g. protection relays). A prominent reason for this is the presence of legacy IEDs that are security-agnostic. A migratory step to apply secure remote access control in a consistent manner in legacy substations could be therefore to rely on a proprietary solution for the time being. Such centralized security management systems (CSMS) exist today (more features are described in the sections below) are capable of supporting pass-through connectivity between a remote client and the IED in the substation – see Figure 3 for an illustration of the same. Such a pass-through capability enables the CSMS to authenticate and authorize the operator trying to establish the remote connection and operate on the IED and also log the access for purposes of audit trail. Furthermore, such systems also support optional integration with central user management systems such as Active Directory, thereby making the migration to a standard, interoperable solution easier in the mid- to long-term.

2.3 Audit Trail

A closely related security control that substation automation systems must support is the security audit trail that keeps a secure log of all runtime activities performed by the logged on operator as well as the details of changes made to the configuration/engineering parameters of the HMI. In addition, a reliable timestamp for each activity must be logged.

2.4 Secure Time Synchronization

Due to the criticality of the integrity of the associated timestamps in the audit trail, and its criticality for the functional operations of an IED in general, substation automation gateways of today are, and should be able to use secure modes of time synchronization protocols such as the Network Time Protocol (NTP) to retrieve the current time from a central (remote) time server, normally at a control center, with server authentication and timestamp integrity support.


IED Engineering application
CROSSBOW Client opens local port
Client PC
CROSSBOW Client Application
CROSSBOW CSMS
Secure SSL connection
DMZ
Firewall
WAN
Substation
Gateway
IED

Connection Data Flow

- User cannot connect directly to device due to DMZ and firewall rules
- User logs into CROSSBOW client app and connects to CROSSBOW server
- User selects IED to connect to – role based access rules are followed
- CROSSBOW server opens proxy path to device, and CROSSBOW client opens local port for IED engineering application to connect to device
- Standard CROSSBOW logging of device access is preserved

Figure 3: An example for a migratory RBAC support scenario for legacy IED products by utilizing secure pass-through feature of a centralized security management system (CSMS)

2.5 Data Protection through Secure Communication

This security control is of high relevance to IEDs such as a substation gateway, which is closer to the unsecure wide-area network (WAN), and therefore more susceptible to network-based remote cyber attacks on process communication, than the bay-level IEDs such as protection devices, which typically communicate only within the substation and are not visible as network nodes outside the substation. So far the predominant choice of securing WAN-facing telecontrol communication has been to create virtual private networks (VPNs) based on IPSec (see Figure 1) to ensure confidentiality of the communication. While IPSec is simple to deploy, it has its limitations. Primarily, IPSec offers confidentiality and integrity but only a limited form of authentication which relies on shared secrets. It can support only site-to-site secure communication, or if the WAN-facing IED has IPSec built in, then end-to-site (site being the control center) secure communication. These configurations do not allow for ensuring the confidentiality or verifying the integrity of the originally transmitted data if the IPSec connection is terminated midway in the communication stretch (e.g. by an IPSec-capable router) and the unencrypted packets are sent by the terminating node potentially after manipulating and/or stealing the originally sent information.

A second significant restriction with IPSec is that its implementations from different network device providers are not guaranteed to interoperate with each other owing to the fact that the IPSec protocol has gone through several updates over time yielding several batches and maturity levels of implementations on the vendors' side.

A further point to note is that the predominant mode of deploying IPSec enabled devices is with pre-shared keys. Deploying IPSec with pre-shared keys is not complex and does not require a huge infrastructure to support it, but it has the disadvantage that the key can be relatively easily compromised due to mishandling. And if a pre-shared key is compromised at the control center level, then in order for a new uncompromised key to be applied, all the connected devices from all the connected substations need also to be updated so as to be able to connect to the control center with the new key. Although IPSec allows for certificate based mutual authentication between the communicating parties to take place, today's lack of availability of a public key infrastructure (PKI) that spans from the control center down to the substation facilities makes it virtually impossible for certificate based authentication of IPSec counterparts to be adopted.

In comparison, the much newer, mature, and utility sector-specific IEC 62351 set of standards covers the most commonly used process communication protocols for telecontrol and substation automation. When using IPSec the point terminating IPSec is most likely in a network facing the unsecure network (e.g. WAN), while the endpoint for IEC 62351 is often in a restricted environment with less communication options (like in a substation) thereby addressing end-to-end secure communication unlike IPSec, which usually offers site-to-site secure communication in the substation context.

The IEC 62351-3 standard provides the basis for secure communication by profiling the application of the Transport Layer Security (TLS) protocol for all TCP-based application layer (process communication) protocols. Building on top of this standard are a slew of other standards, for example the IEC 62351-4 for TLS-based encryption and authentication for IEC 61850-MMS, and the IEC 62351-5 for TLS-based encryption and authentication for IEC 60870-5-104 and DNP 3 TCP protocols that are used for substation-internal communication and/or telecontrol communication between a substation controller and the control center.

The trend in the utility industry in adopting the IEC 62351 set of standards for secure communication has been restricted to IEC 62351-5 largely because of the vulnerability of IEC 60870-5-104 or DNP 3 TCP protocols to cyber attacks owing to their potential traversal through the unsecure WAN (refer Figure 1) between the control center and the substation. The IEC 62351-4 standard, which defines secure IEC 61850-MMS communication has taken a back seat so far owing to the primary fact that MMS is not being used outside the scope of the substation network, and much less the Ethernet-based IEC 61850-GOOSE communication, which can be secured (message authentication only) based on IEC 62351-6.

But it is important to note here that the industry demand for vendor implementations of IEC 62351-4 based secure MMS is likely to rise thanks to new use cases and ideas where MMS is, or will be employed. Depending on the urgency of the required reaction to an extraordinary network condition such as surges detected by wide area monitoring networks based on phasor measurement units, or a weather forecast citing immediate bad weather, the control center might want to directly send an IEC61850-MMS based command to a protection relay in that area to engage a circuit breaker for localizing the instability, or alternatively alter the sensitivity thresholds of a protection algorithm for a specific period of time and then revert it back once the risk of instability has sufficiently subsided. While the possibilities that MMS provides does make such a use case feasible for implementation it is simply apparent that such a capability to control a protection device by entirely bypassing the substation gateway can be exploited by hackers to launch MMS-based attacks on the network by sending such commands to protection relays and causing electrical network instability. Such ideas for centralized adaptive protection of the network, combined with the application of IEC 61850-MMS as part of the decentralized energy resource (DER) integration is likely to push the application of secure MMS across the utility sector in the years to come.

2.6 Identity Management of IEDs using X.509 Certificates

With the foreseeable surge in the adoption of IEC 62351-4 (secure MMS) and IEC 62351-8 (RBAC) as illustrated in the earlier sections, the establishment of a PKI for management of X.509 based certificates becomes more of a prerequisite. In fact, utility operators should consider establishing a PKI not only for enabling end-to-end authentication supported across network segments by the IEC 62351 standards, but also to manage the limited site-to-site or end-to-site authentication with IPSec in a more secure and scalable manner than to use pre-shared keys. Figure 4 below highlights the advantages of using PKI-managed certificates over management of shared secrets such as with IPSec in an interconnected network.

A second reason for requiring certificate management is for the enrollment of IEDs into the substation. When secure communication becomes more prevalent at the substation-internal (e.g. bay) level then the proliferation of X.509 certificates for purposes of secure communication will cause an increase in the administration overhead involved in getting the certificates loaded into the IEDs, especially because the communication trust relationship will need to span from the control center to multiple individual subordinate substations, if not all. This process of updating a new device with certificates needs to be automated just as much as the process to renew the certificates of an existing set of devices due to any number of reasons. A PKI is usually designed to handle such standard certificate management use cases in an automated manner, and provides the basic infrastructure components such as certificate authorities (CAs) that sign the certificates, registration authorities (RAs) that verify the credentials of an IED before requesting a certificate for the IED from the CA, and a slew of cryptography protocol implementations for exchange of key materials, certificates and of course enrollment. The entire application of PKI in the context of power systems is being drafted in the IEC 62351-9 standard as of this writing.

Eventually, through the business push for secure MMS the establishment of PKI based on the 62351-9 standard will become commonplace, but a migration concept is currently required for the substations of today to enable this transition by helping substation operators to incrementally adopt certificate management at a local level and then eventually to establish a trust relationship with an overarching control center based on one organization-wide single spanning PKI owned optionally by the operator.

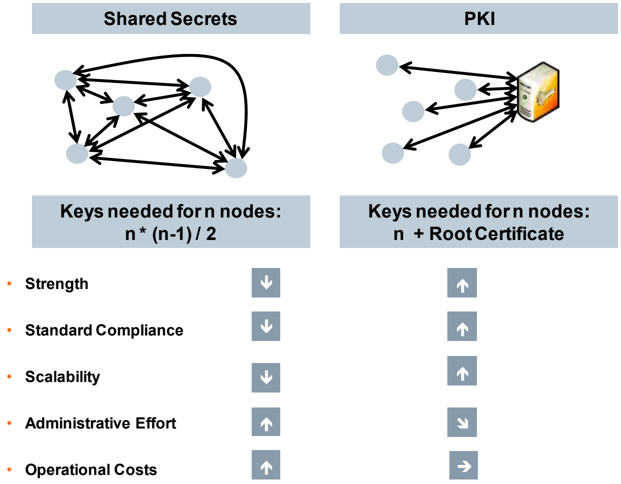


Figure 4: The benefits of PKI over Managing Shared Secrets

2.7 Password Management

For ensuring authorized access to IEDs even at the bay level for configuration purposes, IEDs such as protection relays should support at least the verification of a password for allowing the connection to be established. But given the sheer number of IEDs such as relays, and given the mandatory requirements of NERC-CIP (North American Reliability Corporation, Critical Infrastructure Protection) and BDEW-Whitepaper concerning the application of password policies (length, complexity, expiry timeframe) the task of managing passwords in IEDs will become economically unviable if carried out manually every few months as mandated. An automated password management system is therefore required.

A centralized security management system (CSMS) should be able to log into IEDs automatically, with the current user name and password. If a user/role management system is in place (whether a central one or IED-local), the CSMS itself should be provided the role of an Administrator for having the privileges for this task. The CSMS should be able to change the password to a specified or random password in conformance with password policy requirements of regulations or guidelines. By setting up a password policy using the CSMS, utilities will be able address the existing problem of managing and distributing their passwords for their IEDs over insecure media such as printouts of credentials in the hands of operations staff. The operators are no longer required to manually update the passwords of the geographically distributed DSAS components, because this is done automatically over the CSMS. This also means that for gaining access to an IED for example, either remotely or locally, the operator is first required to retrieve the current password by authenticating against the CSMS. The CSMS processes the user authentication by either integrating with a central user account management system like Microsoft Active Directory Server, or by directly hosting the user management services. Only upon verifying the operator’s identity does the CSMS provide the operator the current password, which it automatically set in the IED during the last update cycle. This approach therefore provides as a 2-factor authentication for accessing an IED, while also enabling centralized tracking of IED accesses, whether remotely or directly at the substation level.

2.8 Firmware and Configuration Version Monitoring of DSAS Components

Ensuring the integrity and change management of the deployed firmware and configuration settings across substations (or even locally at a substation) is also a requirement in regulations such as NERC-CIP and recommended in the BDEW-Whitepaper guideline. A CSMS depicted in the discussion above automates this task by maintaining a baseline of approved firmware versions and configurations of all supported DSAS components across substations in its central database server.

Once a configuration baseline has been established by the CSMS administrator for e.g. an IED, the CSMS should periodically read the device configuration and compare it to the baseline. It should be noted here that the verification of the integrity of the configuration changes is in the scope of the IED itself. The CSMS logs any discrepancy found and the same is reported to the CSMS supervisor. This usually occurs if an operator modifies the device configuration directly in the field, which is not uncommon practice. Once notified, the CSMS supervisor responds to such a discrepancy by examining the differences and finally approving the change (i.e. update the CSMS baseline) made to the device configuration in the field or by rejecting them (i.e. revert changes in device to baseline version, not necessarily using CSMS functionality).

Similarly, the CSMS supervisor can define baseline firmware versions in the CSMS server for the various deployed DSAS components and then set up the CSMS to periodically verify whether the deployment of the various firmware versions across the substations matches the centrally defined baseline. Firmware monitoring is handled in a manner similar to configuration monitoring as explained above.

2.9 Secure Logging of Events

In the center of securing all operations of a digital substation lies the systematic secure logging control. Without a high integrity, comprehensive, and structured log of security and functionally critical events occurring in the substation it is difficult to retrace the workings of due a cyber attack. All networking components, from routers, switches, CSMS instances, on the one hand to IEDs, HMI instances, substation controllers and remote terminal units (RTUs) on the other, need to participate in this central logging of security relevant events, so that operational staff can quickly spot anomalies in communication and/or functional behavior at a substation or beyond.

The Syslog centralized logging system is the most well-established implementation and is supported by most, if not all vendors of networking /IT equipment. The list of vendors is growing with IED vendors also adopting the Syslog approach. While a subset of such IEDs is also capable of directly participating in the centralized secure logging of events, some IEDs use the capability of communication standards such as IEC 61850-MMS to notify a higher level system such as a substation controller of any security events, which in turn can log the same to the central logging server such as Syslog. In any case, IEDs of today by and large should come with support for secure logging of events that cannot be tampered with, and are stored securely within the devices with restricted access to retrieve them.

A prominent approach to centralized logging and monitoring of a networked system is the application of the simple network management protocol (SNMP). The standard IEC 62351-7, “Network and System Management Date Object Models”, is currently in the process of being updated to an international standard. The standard applies_SNMP to power system operations and defines an SNMP management information base (MIB) for handling security events to be utilized for detecting possible security intrusions. With most modern IEDs supporting SNMP, some including the SNMP V3 protocol which supports various security models, it is foreseeable that IED vendors will extend their support IEC 62351-7 in the near future.

3 CONCLUSION

In Figure 5 a secure substation variant is laid out with the security controls discussed in this paper, which contrasts with typical substations of today where security is of minimal significance as depicted in Figure 1. Prevention and detection of unauthorized access to DSAS, administration of password policies in IEDs, periodical baseline checks for the deployed firmware/software versions, and detecting changes in deployed device configurations and software configurations, are among the many aspects of the cybersecurity challenge that are causing the utilities to shift their focus from device-level security to end-to-end operational security, as they upgrade their substations to reflect the needs of the markets.

The complex and challenging task of securing the interconnected grid with its heterogeneous components and technologies can be made centrally manageable as discussed in this paper, but emphasis should be laid by both power system operators and vendors on standardization and interoperability in all security related aspects in the years to come.

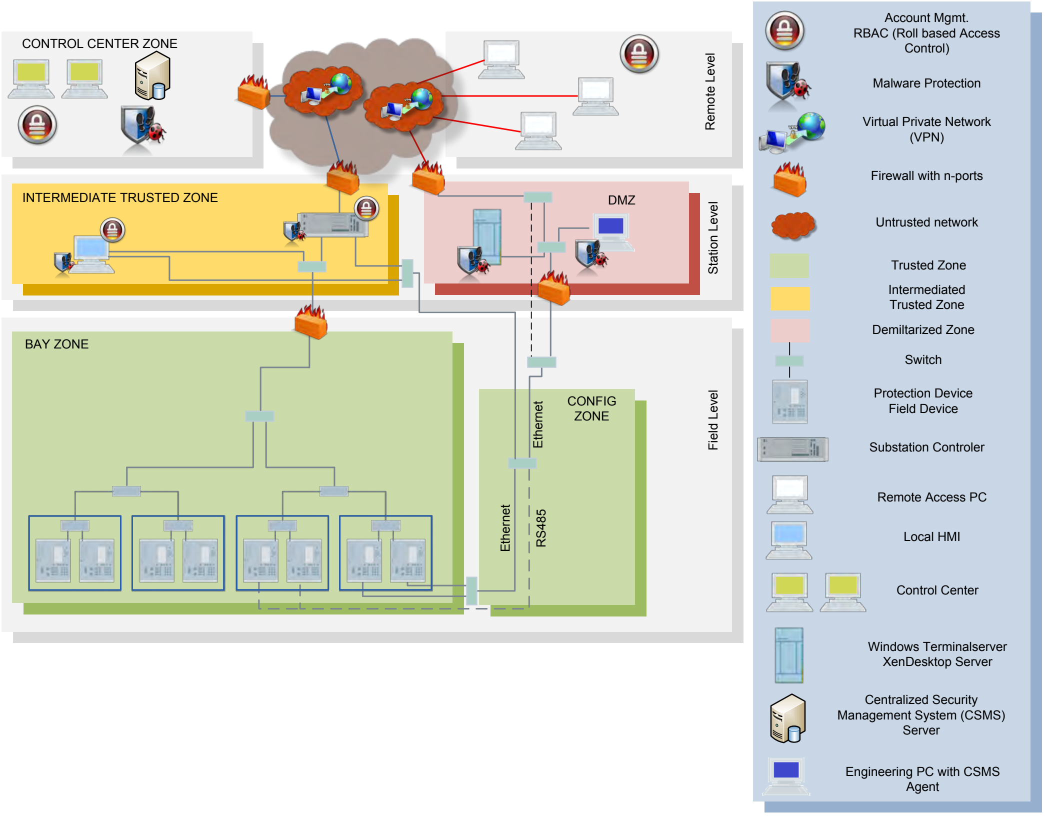

CONTROL CENTER ZONE
Remote Level
INTERMEDIATE TRUSTED ZONE
DMZ
Station Level
BAY ZONE
CONFIG ZONE
Ethernet
Ethernet
RS485
Field Level
Account Mgmt. RBAC (Roll based Access Control)
Malware Protection
Virtual Private Network (VPN)
Firewall with n-ports
Untrusted network
Trusted Zone
Intermediated Trusted Zone
Demilitarized Zone
Switch
Protection Device Field Device
Substation Controler
Remote Access PC
Local HMI
Control Center
Windows Terminalserver XenDesktop Server
Centralized Security Management System (CSMS) Server
Engineering PC with CSMS Agent

Figure 5: A Secure Substation Architecture Variant with Some of the Security Controls Implemented

REFERENCES

[1] NERC, North American Reliability Corporation, http://www.nerc.com/page.php?cid=2|20

[2] BDEW – Bundesverband Energie- und Wasserwirtschaft, Datensicherheit, http://www.bdew.de/bdew.nsf/id/DE_Datensicherheit

[3] ISO-IEC 62351, Part 1-11, http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=sea22.p&search=iecnumber&header=IEC&pubno=62351&part=&se

[4] RFC5246: The Transport Layer Security (TLS) Protocol Version 1.2, T.Dierks, E.Rescorla, August 2008, http://tools.ietf.org/html/rfc5246

[5] ISO TR 27019: Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002, March 2013

[6] ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management, June 2005 http://www.iso27001security.com/html/27002.html

[7] ISO 61850: Communication networks and systems for power utility automation

[8] IEC 60870-5-104: Telecontrol equipment and systems – Part 5-104:Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles, http://webstore.iec.ch/webstore/webstore.nsf/Artnum_PK/36194

[9] IEC 60870-5-7: Telecontrol Equipment and Systems Part 5-7: Security Extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols

[10] Syslog, industry standard for message logging, storage and analysis http://en.wikipedia.org/wiki/Syslog

Actual trends in development of Power System Relay Protection and Automation
1–5 June 2015, Sochi (Russia)

S.7-4. Cyber Security measures in Protection and Control IED's

KRISTER HAGMAN
ABB Power Systems
Sweden
krister.hagman@se.abb.com

KEYWORDS

Security, account management, security events

1 INTRODUCTION

The electric power grids and power systems are critical infrastructure parts of our modern society and are ascertained by high demands on reliability and stability. At the heart of these intelligent grids we find specialized IT systems, such as substation automation systems.

These systems are following standards and trends, as of which one of them is in particular Ethernet and TCP/IP based communication protocols. Evolving technologies like Ethernet and industry-specific standards such as IEC 61850 are enablers for information exchange that support not only higher reliability, but also important ensures interoperability between systems from different vendors

Key features to safe guard our grids are to enable support for authentication and authorization, auditability and logging as well as product and system hardening.

An easy solution to add and remove users that shall have or be revoked from having access is the implementation of a centralized account management in the substation automation system. This is a major benefit for the utilities that have to adhere to regulations. In the event of intrusion detection, finding unexpected usage patterns and for security forensics, the security logging mechanisms are a must. It has to be reliable, easily distributed and easily collected.

2 TRENDS

The last years trend in our industry have been to walk away from proprietary, vendor specific communication protocols and solutions to standardization and standards towards Ethernet and TCP/IP based solutions.

Main reason for this have been to get higher level of interoperability between different vendor's products, and in the end, to reduce the engineering cost and complexity for the Utilities. Given by the nature of the availability and ease of use of TCP/IP for almost everyone, the need for security gets elevated.

Another trend which can be seen is a high level of connectivity, meaning every device in our modern society have more or less a need of connectivity. This includes the power system as well as any other domain around us. The equipment needs to be configured, serviced, monitored and operated.

This is valid both from within close range of the system as well as far away from the same, remote operation.

Therefore standard communication infrastructure and high connectivity level forces us to take certain measures to safe guard our power system. We have to be able to control, monitor and protect our infrastructure.

3 SECURITY MEASURES

Reducing the exposure of the system is the first way of securing it, that can be done through physically (*physical perimeter*), firewalling (*blocking communication entry points*) and through white-listing (*allowed applications*). Independent if all of these are used or only one, the attack surface [1] must be known.

3.1 Hardening

To make a reliable and stable system the attack surface must be reduced. By knowing the attack surface, we know our exposure. The attack surface is reduced by only enabling the needed physical interfaces required, and also only to enable the required services needed per interface.

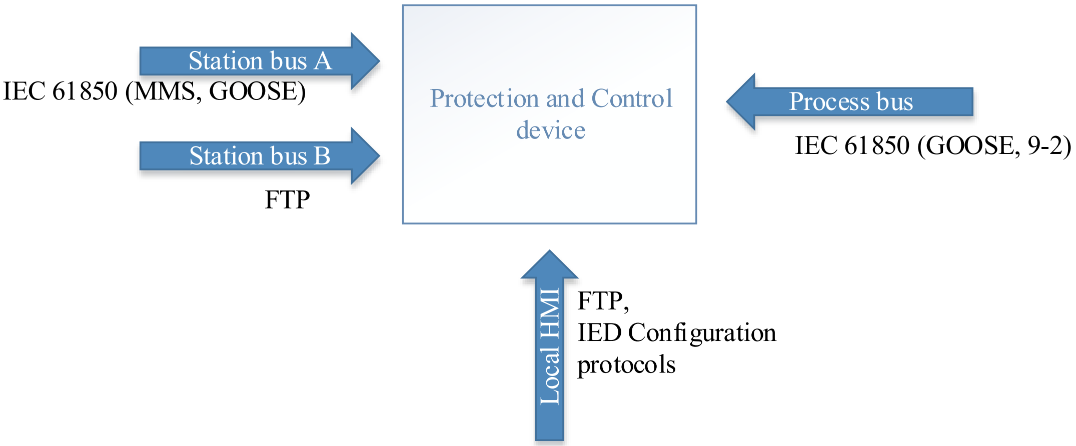


Figure 1: Communication Interfaces with enabled services

As seen in figure 1, only the required protocols per communication interface should be used. If e.g. FTP isn't needed on anything but *Station bus B* and *Local HMI*, then it shouldn't be enabled. This systematic results in a drastic reduction on the attack surface of our system, and on our exposure to bugs and vulnerabilities.

This can be visualized through the following matrix:

Protocol / Interface	*Station bus A*	*Station bus B*	*Process bus*	*Local HMI*
IEC 61850 – MMS	X			
IEC 61850 - GOOSE	X		X	
IEC 61850 – 9-2			X	
FTP		X		X
IED Configuration protocol				X

Table 1: Selection of protocols per interfaces

Reducing an exposure means directly reducing the device exposure for vulnerabilities that can be exploited by anyone unauthorized who wants to get control over the system.

The protocols selected to be run per interface must withstand improper usage, e.g. fuzzing, where unexpected packets of information (valid and invalid) are sent to the device to try to find vulnerabilities. Another vital feature is the one typically called *Denial of Service* (DoS) protection. Here the system have to withstand abnormal amount of data sent directly to the system as a method to prevent it from being able to communicate in a normal way. A DoS on a substation automation system can prevent e.g. control commands from being used, monitoring of measurements, GOOSE from being sent, and time synchronization to fail, etc.

To prevent these DoS attacks as well as having the ability to log the occurrence of them are two important measures that have to be taken in the power system.

3.2 Authorization

The second way in reducing exposure is to enable authorization mechanisms, i.e. the user have to provide proper credentials before being authorized to use the system. There are several ways to provide user credentials, but the most common one is using the combination of a user name and a password.

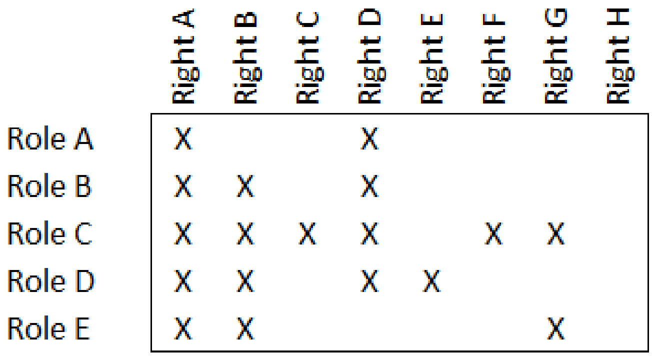
In the world of information systems, the usage of user name and password have long been debated and seen as not secure enough. This is also valid for the Power System area. As of today, most of our installations rely on physical perimeter protection only, and not authentication on each device in the system. What have been missing in our area are proper tools to aid the system owners to implement a working account management system. The tools have been insufficient, the devices have been too limited, hence the result, account management haven't been used.

The key to make this a success is the usage of a centralized account management system, like Active Directory from Microsoft. A system that enables centralized control over users, passwords, groups, policies etc.

These tools have now come to the Power System domain and with the enforcement of regulations like NERC CIP [2] there will be a quick change. The alternative would been to remove connectivity from the devices, which equals a step back in evolution.

With a central account management system, users can be added, removed, blocked, approved and monitored. As usual, the keyword is interoperability, meaning devices and systems from different vendors must work together. Another major factor is standardization where IEC 62351 is the key to success.

Once the centralized repository for users exists, the proper roles have to be given to the users. A user can have one to many roles, whereas each role represents a set of rights. IEC 62351-8 [3] have given us a pre-defined set of roles with a pre-defined set of rights. In comparison the standard defines which user roles shall have what user rights, as shown in figure 2.



	Right A	Right B	Right C	Right D	Right E	Right F	Right G	Right H
Role A	X			X				
Role B	X	X		X				
Role C	X	X	X	X		X	X	
Role D	X	X		X	X			
Role E	X	X					X	

Figure 2: Role to right mapping

In order to reduce the exposure for mistakes and vulnerabilities, we recommend to never use a role with more than necessary rights. The result will be a reduction of the risk of unintended failures from the user, e.g. usage an engineer role to change a configuration, not security administrator.

3.3 Authentication

Once we have the mechanism for authorize users in place we need to make sure that the users can be certain that they operate on the proper devices. We also need to make sure that the devices communicate with other proper devices. It is necessary to authenticate the different entities to each other, to not allow rogue devices or systems to act as if they were proper devices. Especially when using a centralized account management system, it is mandatory to ensure that only authenticated devices are allowed to retrieve user information from that system.

This is where certificates come into play as with certificates it can be verified that an authenticated system is talking to another authenticated system.

When both the centralized account management server as well as the clients using are authenticated, they can exchange information like user credentials, roles, rights and certificates.

Now we have a secure way to authorize users and allow them to change their passwords. If there wouldn't be a mutual authentication between the server and client, a rogue client could be used to enumerate all users in the central repository, and vice versa, if a rogue server is present, any user could be invented and given maximum rights which would circumvent the entire idea of authentication and authorization.

3.4 Auditability

After taking the steps of hardening, authorization and authentication, we have a system that is to a higher level more secure than the Power System we started with. Now the only thing missing is the visibility and ability to monitor what happens in the system. We are missing auditability. To be able to monitor the system we need the discrete actions in the system to be generated as events. These events are hereby called security events and are not be mixed with what we typically call process events.

Security events are used to indicate login, logout, forcing of values, changes in configurations, firmware changes, password changes, audit log access, etc.

They are important part of the regulations that Utilities have to adhere to. For instance, NERC CIP requires such events to be kept for a time of 90 days within a station. In parallel to the centralized account management, there typically is a centralized security event logger in the system. The responsibility of this system is to log all security events from all different parts of the system.

The central logger shall have a time correlated list of all the security events in the system. This is the place to audit when it comes to checking the system integrity. This is also the place for pattern recognition. To be able to see patterns and signs of abnormal behavior, data mining can be done on the central log. Things like scanning, password breaking attempts, nodes going online/offline etc. should be monitored and searched for. By observing the normal flow of events from a particular devices during normal operation, the system/users can learn to search for the differences in the patterns.

This pattern recognition is doing a similar task as an Intrusion Detection System (IDS) performs.

In the case of an event, a mal-operation in the power system or abnormal device/system behavior, the central logger is a good starting point for the forensics work. Since the events in the logs are time stamped, it should be possible to compare them with the process events and other time stamped events in the system. The central logger must be a trusted and reliable source of data. Tampering protection as well as read-traps, to log if someone reads the log, is normal protection

4 CONCLUSION

Since the trends are bringing normal IT technology into the area of Power Systems, we have to look for the same ways of protecting our systems as in the IT domain.

Earlier we have relied on physical perimeter protection and security-by-obscurity, i.e. each vendor have had their own proprietary protocols. Those days are over, now interoperability and regulated openness in the solutions are key.

The traditional approach “if the system is working do not touch it” has to be abandoned. It is no longer enough to judge the security and stability of a system by only looking at it as vulnerabilities can be laying below the surface. The only way to reduce the exposure of these vulnerabilities and mitigate the risk of attacks is to keep the system up to date.

By observing and measuring our systems, we build up knowledge of them, especially on the normal system states and behavior.

These security measures, i.e. *hardening, authentication, authorization,* and *auditing*, are applicable on all our systems independent of regulations on a particular market or region.

The final recommendation is to continue the work of pattern analysis and recognition as well as doing studies on mechanisms to keep a system up-to-date without risking reliability and dependability of the systems.

REFERENCES

[1] Stephen Northcutt, « The Attack Surface Problem », « http://www.sans.edu/research/security-laboratory/article/did-attack-surface

[2] NERC CIP, North American Electric Reliability Corporation, www.nerc.com

[3] IEC/TS 62351-8, Technical Specification, « Power systems management and associated information exchange – Data and communications security – Part 8 : Role-based access control »

Actual Trends in Development of Power System Relay Protection and Automation
1–5 June 2015, Sochi (Russia)

«SO UPS», JSC
Russian National Committee
ABS Electro

S.7-5. Closed Loop Design Processes Satisfy IEC Security and Dependability Requirements While Improving Commissioning and Maintenance

D. DOLEZILEK, F. AYELLO
Schweitzer Engineering Laboratories, Inc.
USA
dave_dolezilek@selinc.com

KEYWORDS

Protection, Automation, Commissioning, Maintenance, Modular, Design-for-Test, IEC 61850 Testing

1 INTRODUCTION

In the past, substation modernization efforts included several different stages of design and development teams completing their task and handing it off to the next team with little knowledge or influence beyond that transition. This resulted in the use of many different types of equipment, often without full compatibility or capability, which complicated system design and presented significant support challenges from an operation and maintenance perspective. Today, a new and innovative modular solution approach leverages the functionality available in intelligent electronic devices (IEDs), experience in efficient panel design, and awareness of substation installation methods to create complete protection, control, and monitoring (PCM) systems that are quickly and easily deployed. This solution creates not only a design fit for use, with all necessary features, but also fit for purpose, where the features are necessary and sufficient to satisfy the complete design.

The integrated design of the modular solution provides an innovative approach and a level of integration unparalleled in the industry to date. The entire control house, kiosks, or just the panels are engineered, designed, constructed, and tested off-site and then installed in the substation. This new solution is less expensive and more reliable due to the enhanced functionality of modern IEDs and the transparency of requirements between various teams. The modular solution delivers a wealth of power system information that provides users an increased understanding of power system asset status and operation. This information permits risk assessment and outage avoidance, reduces labor and outages for maintenance, and helps create a more competitive and reliable power system. Information from the system is used to monitor asset return on investment (ROI), identify and replace obsolete equipment, strategize effective use of resources and financial capital, and increase device and system productivity.

2 DESIGN OF MULTIFUNCTION IEDS

IEDs are often deployed months and years after their original development and must satisfy their intended purpose throughout their in-service lifespan, which is often longer than 25 years. Successful IED product development requires awareness of not only the first principles of power system operation but also how to best support installation, commissioning, and maintenance of the IED in the field. Functioning as a closed-loop system, feedback from the panel construction, PCM design, and field installation teams drives the development of features for interoperability and usability. International standards for performance and communications are included in the IED software and hardware design, which is then enhanced to be used to streamline manufacturing, assembly, testing, maintenance, and monitoring of IED in-service performance.

The use of digital messaging over a fiber cable to replace bundles of copper conductors provides significant wire savings and introduces the ability to monitor the health of the data connection. This practice of creating virtual wires via digital messages has been field-proven for more than a decade based on purpose-built digital communications standards created by National Institute of Standards and Technology-recognized standards-related organizations (SROs) and offered via a "reasonable and nondiscriminatory" license, such as MIRRORED BITS® communications. Also, protocols created by standards development organizations (SDOs), such as the IEEE and IEC, are useful. IEC 61850 Generic Object-Oriented Substation Event (GOOSE) messages have been used in the field for over a decade, and other standards are in use, such as IEEE C37.94.

Transparent communications among all groups lead to innovative successes, such as virtual wire supervision. With awareness of the fiber-optic behavior from the hardware design team and commissioning and maintenance suggestions from the construction and installation teams, IED designers use the connection health status to supervise the digital data path and differentiate between silence due to inactivity and silence due to a severed connection. Reliability is improved because the number of unsupervised components, processes, apparatus, and data paths is reduced. This approach vastly improves the value of the data by confirming the availability and reliability of the methods by which the data are collected and by alarming when a data path is broken. Studies show that many PCM system failures are due to mistakes and failures in the secondary system wiring. These problems are mitigated by virtual wiring.

Other features also monitor the ongoing performance of digital messaging. Awareness of the performance standards that communications-assisted PCM must meet at commissioning has led IED developers to create technologies that both meet and confirm satisfaction of these standards in real time and in service. International standards of performance are described in IEC 61850, IEC 60870, and IEC 60834, and the ramifications of incorrect operation are described by organizations such as the North American Electric Reliability Corporation (NERC).

Awareness of factory acceptance testing, site acceptance testing, commissioning, and maintenance requirements allows developers to implement international standards that support these tasks in addition to traditional PCM, supervisory control and data acquisition (SCADA), and automation. Awareness of the environments experienced by in-service devices and real-world conditions drives the design of hardware that can survive and excel in these environments.

3 IED HARDWARE DESIGN AND MANUFACTURING

The importance of reliability for device and system success is undeniable. IEDs must be designed and tested to verify that the device is suitable for the harsh environment of the substation, field kiosk, or pole-mounted cabinet, as demonstrated by the satisfaction of all applicable type tests and certifications.

To accurately track, measure, and improve reliability parameters, a wide array of techniques have been developed by device manufacturers and system designers. IEC 61850-3 defines quality metrics and makes frequent reference to IEC 60870-4, which specifies performance requirements for a telecontrol system, classifying these requirements according to properties that influence the performance of the system. IEC 61850-3 Section 4 describes internationally standardized requirements for the quality of substation PCM systems and includes the following scope:

> [It] details the quality requirements such as reliability, availability, maintainability, security, data integrity, and others that apply to the communications systems that are used for monitoring, configuration, and control of processes within the substation.

IEC 61850-3 Section 4 summarizes the design practices and reliability measures by prescribing the following quality metrics for comparison:

- Reliability measured as mean time between failures (MTBF).
- Device availability measured as a percentage of availability.
- System availability measured as a percentage of availability.

- Device maintainability measured as mean time to repair (MTTR).
- System maintainability measured as MTTR.

Awareness of the location and failure history of every device in service over its lifespan provides true observed measurements of quality, including mean time to failure (MTTF), mean time between removal (MTBR), and MTTR. This feedback and expectations from the commissioning and maintenance team drive world-class manufacturing practices, and testing of each IED unit is necessary to verify that every single device satisfies the hardware and software requirements in addition to reliability requirements. Hardware design and manufacturing that successfully meet quality expectations are demonstrated by IED environmental ratings and an extended manufacturer warranty. Awareness of the environmental stresses experienced by IEDs leads manufacturers to build their own components when satisfactory products, such as communications cables, IED power supplies, and contact output relays, are not available.

4 PANEL DESIGN AND CONSTRUCTION

Panel, control house, and field kiosk designs for functionality and manufacturability best practices lead to intuitive end-user-focused design and simple, efficient, repeatable assemblies that are quickly built and shipped globally. Operator preferences and best practices are used to create a design for optimized user interaction by placement of IEDs, test blocks, clocks, and computers so that they can be readily seen and used. Simplicity and consistency from panel to panel and station to station maintain operator familiarity with the interface during a crisis situation so that operators react quickly and correctly. Device terminations required for testing are positioned to make access safe and easy.

The use of digital messaging to replace copper wiring has had the most dramatic influence on the modernization of design and construction. Traditionally, copper is the primary interface between components in the yard and a relay that is centrally located within a control house. Evaluation of traditional in-service installations finds that there are typically 44 conductors between the field and a relay in a control house. Normally, several multiconductor cables are used; separate cables are typically installed for breaker status (trip/close) and current transformer (CT) and potential transformer (PT) secondaries.

Locating microprocessor-based relays in the yard significantly improves overall functionality, reduces size, and simplifies internal cabinet wiring, especially in the case of single-breaker bus arrangements. However, care must be taken to select IEDs that are designed for the harsh environment of outdoor installation, as demonstrated by stringent environmental ratings and long manufacturer warranties.

Even without moving the relay to the yard, digital communication of digital I/O greatly simplifies installations. Over 50 percent of the wires within the data path from the yard to the house are associated with circuit breaker control signals. The horizontal data paths for information exchange between components, labeled "wires" in Figure 1, represent pairs of copper communicating real-time status and control via analog signals. In this hybrid approach, the analog CT and PT wiring is retained, but the control wiring is replaced with a fiber-optic-based I/O transceiver module and communications cable, as shown in Figure 1.

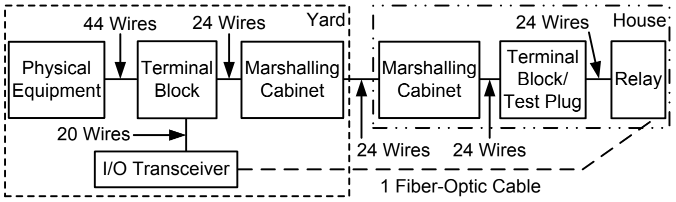


Figure 1: Hybrid project showing the amount of copper wire replaced with fiber-optic-based I/O module technology.

A switched Ethernet approach that replaces all copper conductors with virtual wires and supports communication among several devices is shown in Figure 2.

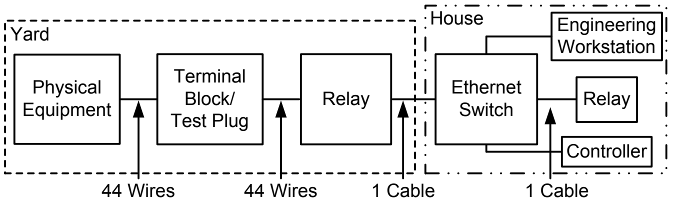


Figure 2: Ethernet-based relay installation with an Ethernet switch.

Awareness of PCM IED communications capabilities and on-site deployment needs from PCM design and construction teams drives best practices to include marshalling cabinets and fiber junction interfaces so that installation, factory acceptance testing, and commissioning of pretested systems go smoothly with minimal outage times.

5 PCM AND ICT DESIGN AND TEST

Station-specific PCM and information and control technology (ICT) designs and configurations demonstrate fitness for use and have appropriate and sufficient capabilities as illustrated via full functional tests of all protection schemes, communications networks, automation logic, SCADA interfaces, and monitoring in the safety of the factory. Pretesting the full application provides confidence in the design and assembly and reduces the complexity and amount of field work. This permits more accurate scheduling of on-site personnel and equipment. Station-specific designs and pretesting combine to further reduce the installation and commissioning effort because the site acceptance testing becomes an on-site repeat of the customer-focused factory acceptance testing. Factory acceptance testing and commissioning are supported by features developed in the IED and communications products that support efficient configuration and documentation. Also, reporting features built into the devices confirm correct and complete satisfaction of tests and automatically create test records for verification and archiving. Design accuracy is illustrated with appropriate ICT and communications-assisted interlocking and automation verification, test reports, internal IED diagnostics, and network communications digital messaging virtual wiring diagrams.

The communications standard IEC 61850-5 identifies fast messages that perform teleprotection and high-speed automation, such as trip, close, reclose, start, stop, block, unblock, trigger, release, and state change, with the expectation that the receiving IED will act immediately. IEC 61850-5 further describes a Type 1A fast message as the most important message that has the most demanding requirements and is used for tripping, interlocking, intertrips (direct transfer trip), and blocking. Type 1A has two performance classes. For Performance Class P1, the total transmission time is in the order of half a cycle and, therefore, 10 milliseconds is defined. For Performance Class P2/P3, the total transmission time is in the order of a quarter of a cycle and, therefore, 3 milliseconds is defined.

Collaboration between the IED design team and the PCM and ICT design team is essential for designing Ethernet network topologies and adequately delivering IEC 61850 GOOSE messages for teleprotection, interlocking, and high-speed automation.

Transparent and frequent communications among all the teams are most important at this step. Traditionally, panel, kiosk, and building assemblies were often completed based on drawing packages from a separate design team. Unfortunately, there are often issues that arise during the handoff between the construction team, with their specific expertise, and the installation team, with their different expertise and site knowledge. The new modular solution eliminates these issues through constant communications between teams during construction and then installation to mitigate unforeseen issues. Even more important is that this mode of personal communication continues throughout the commissioning process and also runs as a closed loop so installation provides feedback to improve design and construction.

6 SITE INSTALLATION AND COMMISSIONING

Site-specific testing and commissioning are simplified and documented via appropriate ICT and communications-assisted interlocking and automation verification, functional test reports, internal IED diagnostics, network message delivery logistics, and source-to-destination message transfer diagrams.

IEC 60834-1 is commonly used to evaluate point-to-point teleprotection. It defines dependability as the ability to receive each command message within the fixed actual transmission time defined by the application. Blocking and permissive schemes require a 99 percent success rate, and intertripping requires a 99.9 percent success rate of receipt of digital teleprotection messages. Failure is defined by the absence of the message at the receiving end or an excessive delay in delivery. These problems can cause a failure to trip or a delayed trip in an intertripping scheme or an unwanted operation in a blocking scheme. Therefore, a delay must still fall within the maximum allowable latency defined for the most stringent underlying applications that are dictated by the end user and is generally considered to be ≤ 20 milliseconds for permissive tripping and ≤ 30 milliseconds for direct trips.

IEC 61850-5 states that the overall message transfer time includes time used by Ethernet switches and other devices that are part of the complete network. It also states that testing and verification of the complete transfer time must be performed during site acceptance testing using the physical devices and network equipment.

Validation of the performance in the installed system also tests the primary equipment and its interfaces because the secondary system has previously been fully verified during the factory acceptance testing.

7 CONCLUSIONS

Collaborative learning from best practices developed over a decade of field-installed IED solutions provides compounding benefits of innovation as each iterative design improved on the last, leading to the present standards-based modular solutions.

Collaboration and frequent, uninhibited dialogue are essential among product software and hardware development, manufacturing, panel design and construction, PCM and ICT design and configuration, and site construction and installation teams.

Feedback including shared knowledge of field installation practices, global engineering processes, and in-service system requirements from experienced field service teams is essential via transparency among all teams. This information exchange ensures that each product, including IEDs, Ethernet switches, routers, computers, multiplexers, kiosks, panels, and complete control buildings, is designed to be fit for use and fit for purpose.

IED networks, once installed, must be tested and verified to correctly satisfy performance requirements, including digital message processing speed and delivery latency to support protection and automation applications. Network devices and IEDs that do not provide this information are not acceptable.

Actual Trends in Development of Power System Relay Protection and Automation
1–5 June 2015, Sochi (Russia)

S.7-6. Case Study: Increasing Reliability, Dependability, and Security of Digital Signals Via Redundancy and Supervision

P. FRANCO, G. ROCHA, D. DOLEZILEK
Schweitzer Engineering Laboratories, Inc.
USA
dave_dolezilek@selinc.com

KEYWORDS

Generic Object-Oriented Substation Event (GOOSE), time to live (TTL), message quality, digital signal supervisions.

1 INTRODUCTION

Electrical substation information and control technology (ICT) systems use a variety of topologies, networks, and protocols to communicate between multiple nodes. Typical electrical substation nodes include the following:

- Intelligent electronic devices (IEDs), such as protective relays, meters, and dedicated controllers.
- Local computers, programmable logic controllers, or programmable automation controllers (PACs), providing data concentration and automatic control.
- Local displays or human-machine interfaces (HMIs).
- Local-area network (LAN) devices, such as Ethernet switches, radios, and serial-to-Ethernet converters.
- Wide-area network (WAN) devices, such as time-division multiplexers and radios.

The LANs and WANs provide local and remote connections to support the following applications:

- Peer-to-peer interlocking and high-speed automation.
- Substation data concentration, automation, protocol conversion, and local operator HMI.
- Supervisory control and data acquisition (SCADA) masters located in control centers.
- Wide-area measurement and control (synchrophasor) systems.
- Remote engineering access and maintenance workstations.
- Event report gathering and analysis systems.

This paper presents methods for supervising signal exchange via digital messages. Case studies that provide examples of improvements to applications, such as logic selectivity, circuit breaker failure (50/62BF), and automatic line transfer (ALT) based on signal message supervision, are discussed.

2 SIGNALING METHODS FOR TELEPROTECTION APPLICATIONS

A hard-wired exchange of protection information uses an analog value at the receiver to indicate the status of the signal from the sender. Typically, an analog value set to zero indicates a status value of zero, and the maximum analog value represents a status value of one. This method creates a constant signal value at the receiver. However, if the signal wire is cut or disconnected, the receiving device cannot distinguish between this situation and a legitimate zero analog value. Digital messages convey the signal status each time they are received and, therefore, the signal exchange is not constant. Each time a digital message is received, the signal status is confirmed or a change of status is recognized. The receiver has no option but to assume that the signal status remains unchanged during the time between messages. However, the digital message exchange can be supervised, and the receiver will detect when the communications link is lost. MIRRORED BITS® communications publishes digital messages every 2 milliseconds over dedicated links, so the time between each signal confirmation is 2 milliseconds. A change of state is also detected within 2 milliseconds at the receiver. IEC 61850 GOOSE messages are configurable to be published at varying rates and are typically set to once per second over shared-bandwidth Ethernet networks. The time between signal confirmations at the receiver grows to once per second when GOOSE messages are used. A signal status change of state typically triggers an immediate GOOSE publication, so a change of state is also detected within 2 milliseconds at the receiver.

GOOSE messages are not published more rapidly so that the traffic on the shared-bandwidth Ethernet network is reduced. The consequence is that the time between confirmations is much longer, and the time to detect failed communications is much longer than with other digital messaging methods.

3 APPLICATION REDUNDANCY

3.1 Benefits of IEC 61850 Ethernet LAN

A great benefit of the IEC 61850 standard is point-to-point communication through IEC 61850 Generic Object-Oriented Substation Event (GOOSE) messages to exchange signal information among several IEDs. This signal exchange is used in protection, automation, and interlocking logic, enabling the development of a decentralized automation system distributed among several IEDs.

Improvement of substation operating conditions via automation of actions previously performed by operators improves system reliability, security, and availability, which directly reduces downtime periods. In addition to operational and economic aspects, the decision to adopt this substation philosophy, through the use of IEC 61850 communications protocols, is also based on the following benefits:

- High-speed communication via Ethernet packet exchange.
- Interoperability among equipment from different manufacturers.
- Significant reduction in the quantity of cables.
- Reduced likelihood of undetected cable failure due to signal supervision.
- Faster and more automatic commissioning.
- Lower possibility of obsolescence in the near future, ensuring the return of the investment made.
- Guarantee of easy expandability.

3.2 Typical Substation Automation System Network

A substation automation system (SAS) consists of protective relays, controllers, communications networks, gateways to make integration with a SCADA system easier, disturbance recorders, meters, synchronized phasor measurement units, local and remote engineering workstations, and a local HMI.

Communication with the control center and the HMI is usually accomplished via connections to a communications gateway. This gateway collects data from the IEDs via IEC 61850 manufacturing message specification (MMS) protocol, concentrates the data in one database, and then converts them into protocols that the SCADA and HMI machines expect, including DNP3, DNP3 LAN/WAN, IEC 60870-5-101, and IEC 61870-5-104. Other information, such as synchrophasor data, sequential event records, event reports, and settings, is collected via direct connections to the IEDs. Time synchronization data are broadcast to the IEDs via a separate IRIG-B network that continues to work even if the Ethernet network is compromised. This keeps data among the protective relays synchronized for forensic analysis. Standards are being developed now for accurate time synchronization over the Ethernet network, but they are not yet mature and do not work at all if the LAN fails [1]. An example distribution substation one-line diagram is shown in Figure 1a, and the corresponding architecture of the communications network of a distribution substation based on the IEC 61850 standard is shown in Figure 1b.

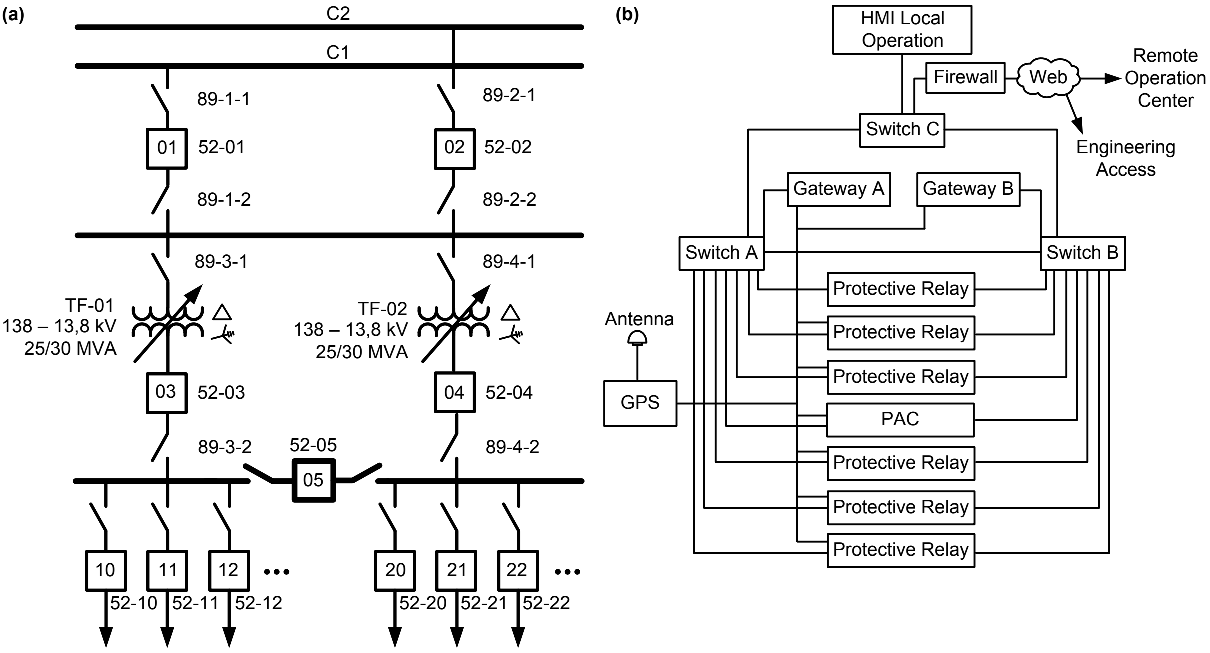


Figure 1: Typical substation one-line diagram (a) and data communications network (b)

3.3 Managing Active Connections Within a Protection LAN

With the use of protection systems that depend on information exchanged over communications networks, it becomes essential that the network be designed and monitored for dependability, reliability, and availability.

Ethernet technology allows a single active connection to each physical device identified by a media access control (MAC) address. Protection and control IEDs now support multiple physical Ethernet connections and have an internal switch to manage their use. The Ethernet switch function inside the IED switches between the internal logic connection and the external physical connections. Two external connections can be physically attached to LAN switches, with one as an active primary and the other as an inactive failover. The failover connection can be in hot-standby mode, ready to be enabled immediately after detection of a loss of functionality of the primary port. High-performance Ethernet requires that this internal switch function manage traffic between the internal logic connection and one external physical connection. When the external physical connection fails, the internal switch manages traffic between the internal logic connection and the failover hot-standby physical connection. In this fashion, GOOSE messages to and from this IED travel through the LAN with the best possible performance and with minimal impact on other IEDs. These direct connections support the appropriate speed and reliability required for protection and interlocking, as shown in Figure 2a, where Port A denotes primary and Port B denotes failover functionality.

The statuses of active connections are managed in the IEDs by link failure detection and failover. This works in conjunction with link supervision and activation within the LAN and is performed by the spanning tree algorithm (STA) within the switches (also referred to as bridges). The bridges within the spanning tree domain communicate with each other by broadcasting Ethernet packets that contain a special section devoted to carrying STA information. This portion of the packet is referred to as the bridge protocol data unit (BPDU). It contains LAN information that is used to determine which bridge controls the STA. This bridge, referred to as the root bridge, manages the active and hot-standby paths within the LAN. When a bridge starts up, it issues a BPDU in order to determine whether a root bridge has already been selected in the network. If no root bridge has been determined by pre-engineering, then the lowest bridge priority number of all of the bridges becomes the root bridge. Best engineering practices include design and engineering of the root bridge in advance in order to optimize LAN performance. The root bridge periodically transmits a BPDU to determine whether there have been any changes to the network topology and to inform other bridges of topology changes.

3.4 Low-Cost, Low-Performance Monitoring LAN

When IEDs are not performing protection or interlocking, some designers choose to sacrifice resilience and speed for cabling shortcuts. By having both physical Ethernet connections active simultaneously, all traffic passes in one physical port and back out the other. Traffic originating from, or directed to, the IED is managed between the physical connections and the internal logic connection via the IED switching function. In this mode, the IEDs can be cabled to one another in a ring or loop, as shown in Figure 2b. Although possible, this creates a lot of unnecessary processing burden on the IEDs by forcing traffic through them. It also creates delivery bottlenecks because cables and IEDs become saturated with unwanted messages that consume processor and cable bandwidth. Due to poor speed and resilience, this connection method is not used for protection IEDs but may be acceptable for monitoring and control IEDs. The speed to detect failure and activate an alternate traffic path is dramatically reduced, but the installation requires two fewer IED cables than the best practice method in Figure 2a.

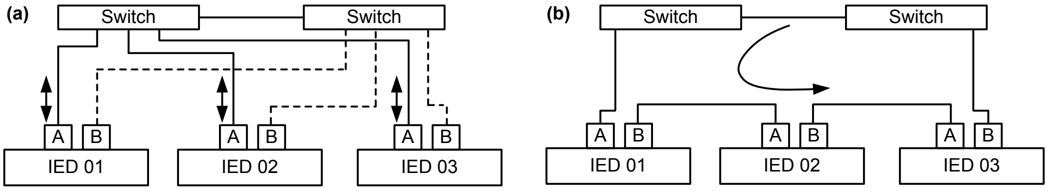


Figure 2: Primary and failover hot-standby connections (a) and ring architecture (b)

3.5 Packet Duplication Mislabeled as Redundancy

Though out of the scope of this paper, there are numerous LAN technologies to create and deliver duplicate Ethernet packets. These methods, such as Parallel Redundancy Protocol (PRP) and High-Availability Seamless Redundancy (HSR), actually do not provide redundancy but rather perform packet duplication [2].

3.6 Signal Redundancy Via IEC 61850 GOOSE Retransmission

GOOSE messages are delivered inside a LAN via a unique virtual LAN (VLAN) based on IEEE 802.1Q. Also, each IED is responsible for surviving message loss, duplication, delay, out-of-order delivery, and loss of connectivity in case the LAN does not function as expected.

IEC 61850-8-1 specifies that GOOSE behavior signal exchange via Type 1 or 1A fast messages must be published immediately after the signal status changes. This is referred to as a state change, or change of state. IEC 61850-8-1 also specifies a retransmission scheme to achieve a highly dependable level of signal delivery. These retransmissions are redundant publications of the GOOSE message, each with a different sequence number and each containing the signal change-of-state information. This mechanism provides redundant delivery of each signal change (in case one or more packets are lost in the network) in order to improve the resilience of interlocking and protection via digital messaging. Figure 3 shows this mechanism of retransmission of GOOSE messages. Once started, GOOSE messages are published constantly, containing a collection of data called a data set. During configuration, each GOOSE message is given a maximum time (MT) to wait between redundant message publications and the name of the data set to include in the message. The messages are published each time one of the data set elements changes or if the MT expires. After a data set element changes, a GOOSE message is published immediately and then published again after a short delay (often 4 milliseconds), represented by T1 in Figure 3. These redundant publications are repeated very often to increase the likelihood that all subscribers will receive them across the nondeterministic Ethernet network. The minimum time between publications (TBP) is a configuration setting in the publisher used to determine how quickly to publish the second and third GOOSE message after the signal change of state. After several publications, the TBP grows longer, as illustrated by T2 and T3 in Figure 3, until it reaches MT and is published as a steady state.

For each message, publishing IEDs create and include a time to live (TTL), calculated based on the TBP. The publishers calculate TTL to be multiples of TBP to prevent nuisance alarms caused by the frequent and small Ethernet network delays. TTL is 2(TBP) when TBP is equal to MT and 3(TBP) when TBP is any value other than MT. For the first few messages after a protection signal element in a data set changes state, the message is sent every 4 milliseconds, and then less rapidly. Each message includes the TTL, which forecasts the time delay before the next message will be published so that subscribers can monitor correct data flow.

When the next change of state occurs, a new message is created and published. The new data set event information is transmitted and repeated in the shortest TBP (T1), as shown in Figure 3. The retransmission time gradually increases from T2 to T3 and eventually settles at a stable retransmission time of TBP = MT.

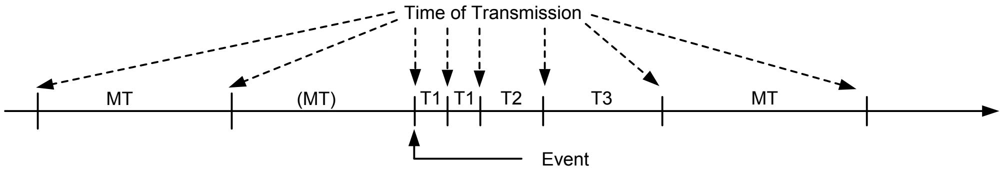


Figure 3: Example of changing time between message publications (from IEC 61850-5)

Subscribing IEDs constantly calculate time to wait (TTW) based on the TTL within each message. The subscriber considers data “stale” when the TTW expires and the IEDs have not received a new replacement message from the publisher.

If the subscribing IED detects expiration of the TTW, it assumes that the communication is lost and modifies its relay logic accordingly. The message redundant retransmission scheme is necessary to perform transmission from one to many and to allow each subscriber to know that the communications channel is healthy. However, depending on the choice of final stable retransmission time, it may not be sufficient to guarantee the reliability of mission-critical tasks.

3.7 IED Communications Supervision and Status

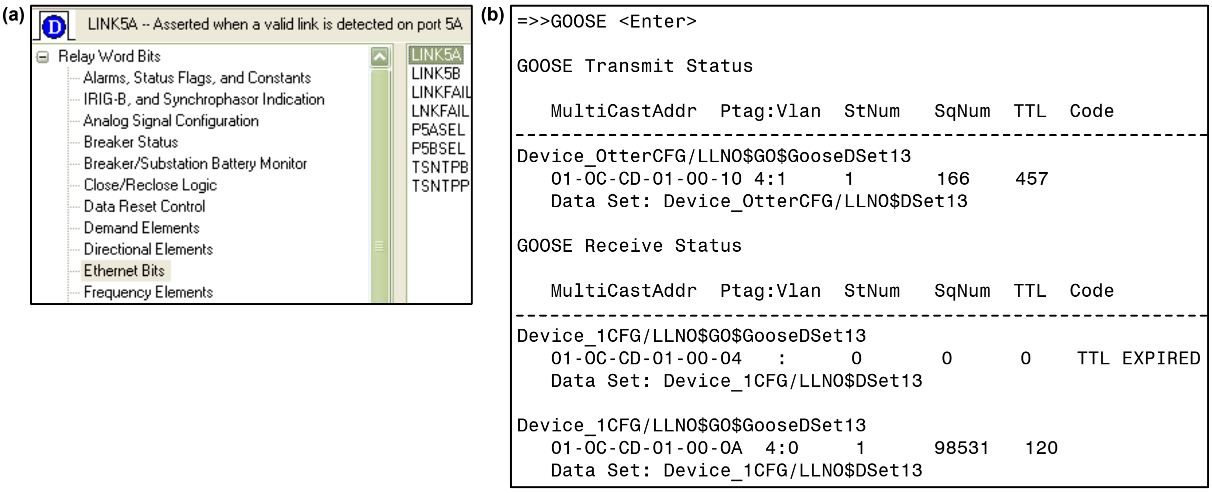
Protection, monitoring, and control IEDs have internal binary variables, as illustrated in Figure 4a, that identify and monitor communications parameters. In the screenshot of a software engineering tool shown in Figure 4a, an engineer has selected and highlighted the status value LINK5A, which is asserted when Ethernet Port 5A has a valid LAN link status. These binary variables are used in internal logic to dynamically modify algorithms and are published to SCADA systems and HMIs to provide network status information. Alarms based on these statuses are used to dispatch maintenance teams for actions at the communications network in order to correct defective situations in the network. This supervision and alarming increases the availability and reliability of the substation Ethernet network, which in turn increases the availability and reliability of the protection and control system accordingly.

3.8 Subscriber IED Supervision of GOOSE Performance

The commissioning and maintenance of traditional IEDs using hard-wired copper conductors to convey signals is done with multimeters and oscilloscopes. In automation systems using signaling via digital messages based on the IEC 61850 standard, traditional maintenance and commissioning tools are replaced with tools developed by IED manufacturers. Figure 4b shows an example of an IED GOOSE report that displays the status and configuration of published and subscribed GOOSE messages. This report supports the monitoring of which messages the IED is transmitting and receiving and whether there is some failure in the network that hinders the communication among the IEDs. This feature helps the technical team identify connection and settings errors by displaying the active configuration, including the following:

- *MultiCastAddr* indicates the MAC multicast address of the GOOSE message.
- *Ptag* indicates the message priority level.
- *Vlan* identifies the IEEE 802.1Q VLAN configured for the message.
- *Code* indicates the type of errors and failures in the network or in the message, if any.

Error codes include *out of sequence* (OOS) when one or more packets are not delivered and the sequence number of the next received packet is not consecutive. If the delay between messages becomes large, the TTL is set to *expired* because the link is considered disabled. Other errors include *message corrupted*, *configuration changes*, *commissioning needed*, and *test mode*.



LINK5A -- Asserted when a valid link is detected on port 5A

```
=>>GOOSE <Enter>

GOOSE Transmit Status

   MultiCastAddr  Ptag:Vlan  StNum   SqNum  TTL  Code
-----------------------------------------------------------
Device_OtterCFG/LLNO$GO$GooseDSet13
   01-0C-CD-01-00-10 4:1     1       166    457
   Data Set: Device_OtterCFG/LLNO$DSet13

GOOSE Receive Status

   MultiCastAddr  Ptag:Vlan  StNum   SqNum  TTL  Code
-----------------------------------------------------------
Device_1CFG/LLNO$GO$GooseDSet13
   01-0C-CD-01-00-04   :      0       0      0    TTL EXPIRED
   Data Set: Device_1CFG/LLNO$DSet13

Device_1CFG/LLNO$GO$GooseDSet13
   01-0C-CD-01-00-0A  4:0     1      98531   120
   Data Set: Device_1CFG/LLNO$DSet13
```

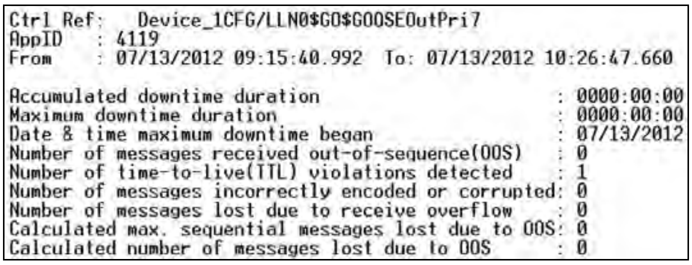
Figure 4: Engineering tool display of available internal IED Ethernet supervisory status (a) and an internal IED GOOSE report (b)

Figure 5 illustrates an IED report that details the availability and the quality of an individual GOOSE subscription. These values help technicians to understand, diagnose, and troubleshoot any potential issues with each individual GOOSE exchange. Technicians can see records of when the exchange failed and for how long, as well as when GOOSE messages are dropped or received out of sequence. These data also reveal the frequency, time, and duration of LAN failures.

3.9 IED GOOSE Message Quality Supervision

The major reason for failures in the protection and automation schemes of traditional systems is the inability to monitor the integrity of the metallic cable that transfers the signal information between the IEDs.

When, instead, the system uses digital GOOSE messages to convey signal status, any communications failure between the IEDs is monitored in real time as message quality. This status is used within the IEDs to perform blocking and/or change protection and automation logic to prevent incorrect performances.



```
Ctrl Ref:   Device_1CFG/LLN0$GO$GOOSEOutPri7
AppID   : 4119
From    : 07/13/2012 09:15:40.992  To: 07/13/2012 10:26:47.660

Accumulated downtime duration                    : 0000:00:00
Maximum downtime duration                        : 0000:00:00
Date & time maximum downtime began               : 07/13/2012
Number of messages received out-of-sequence(OOS)  : 0
Number of time-to-live(TTL) violations detected   : 1
Number of messages incorrectly encoded or corrupted: 0
Number of messages lost due to receive overflow   : 0
Calculated max. sequential messages lost due to OOS: 0
Calculated number of messages lost due to OOS     : 0
```

Figure 5: GOOSE message subscription statistics

Supervision is performed constantly, even when there is no change in the value of any variable inside the data set. This is possible because the GOOSE message is transmitted periodically at the MT as a heartbeat function. If the subscriber IED detects that the GOOSE message has not been received within the expected timeframe, the message quality variable is set to *failed*. Therefore, each subscriber calculates its own message quality for each GOOSE subscription.

Figure 6 illustrates the use of message quality within a transformer relay subscribing to a feeder relay. The feeder relay data set includes a block signal when it detects the fault and attempts to trip the feeder breaker. The feeder relay data set also includes a breaker failure indication when the trip output is unsuccessful. The transformer relay detects the fault current locally and trips immediately upon receiving breaker failure indication. When the transformer relay either receives a block signal from the feeder relay or detects loss of communications from the feeder relay, it delays tripping for 100 milliseconds. This delay allows the feeder breaker to clear the fault. If, however, communications with the feeder are normal and the relay does not detect the fault, the transformer relay immediately trips.

The typical logic example in Figure 6 shows how important immediate detection of message quality failure is to the protection of the transformer and the bus. As mentioned previously, message quality fails when the TTW expires and the relay has not received a new replacement message from the publisher. An accurate TTW is based on accurate TTL values calculated and published within each GOOSE message. Calculation of message quality is most critical immediately after a signal status change of state. This is also when the redundant GOOSE messages are published in the burst of retransmissions. TTW expires at 3(TTL) and message quality is set to *failed*.

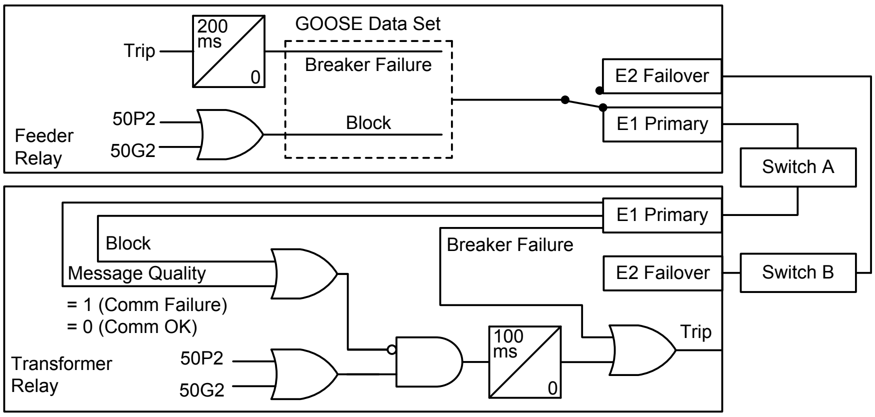


Figure 6: Use of GOOSE message quality status in IED logic

As an example, consider IED1, which calculates TTW based on the actual TTL for a retransmission burst of 4, 4, and 8 milliseconds after the initial signal change-of-state message. IED2 never calculates TTL, but rather uses a fixed value of 500 milliseconds. IED3 never calculates TTL, but rather uses a fixed value of 2,000 milliseconds. When GOOSE exchange fails immediately following the first message with a signal change of state after a fault, the three IEDs have a very different detection of failure. Message quality for the immediately failed exchange with IED1 is set after 12 milliseconds. Message quality for the immediately failed exchange with IED2 is set after 1,500 milliseconds, and message quality for the immediately failed exchange with IED3 is set after 6,000 milliseconds. Therefore, logic operations are blind to failed communications with IED2 for 1.5 seconds and IED3 for 6 seconds, creating unwanted and unsafe conditions.

3.10 The Use of Message Quality Within Protection Schemes

Protection and automation engineers seek the best methods to design secure logic schemes. With the use of IEC 61850 communications for protection and automation applications, best known methods now include the use of message quality supervision within protection signaling via GOOSE messages. In each example, the message quality logic input is calculated within the relay performing the logic based on the criteria listed previously for each GOOSE subscription.

Typical logic applications in a protection and control system for the substation illustrated in Figure 1a include logic selectivity, circuit breaker failure (50/62BF) and ALT. The value of supervision of message quality within logic schemes is demonstrated in the following examples.

3.10.1 Logic Selectivity

Logic selectivity enables fast and secure real-time changes to the logic so that it adapts to changes in the substation infrastructure, communications network, and protection requirements. Figure 7 illustrates logic in the relay protecting Breaker 52-03, which monitors the status from any of the feeder relays (10, 11, and 12). If none of these downstream feeder relays have a protection pickup and all have normal communications, the torque control (67P1TC) is set. Torque control equations control the operation of various levels of overcurrent elements. For example, the Level 1 phase-instantaneous and definite-time overcurrent elements (67P1/67P1T) are only enabled when feeder relays are communicating normally and report no faults indicated by 67P1TC = 1. In Figure 8, when this is the case, 67P1TC = 1 is set, and then 67P1/67P1T follows 50P1 (which has been set to be fast and sensitive) to immediately trigger. If the tie breaker (52-05) is closed, this logic also includes Feeders 20, 21, and 22. If communications to any feeder relay are lost, the selectivity logic is not set because it is unknown if that relay is attempting a protective trip. In this case, if the upstream breaker relay sees fault current but has lost communications to one or more of the feeder relays, 67P1TC is not set and the trip equation waits for the 51S1T time-coordinated trigger. Figure 8 illustrates the 52-03 breaker relay trip logic being conditioned by torque control (selectivity) or relying on coordination timers.

3.10.2 Circuit Breaker Failure

The circuit breaker failure scheme shown in Figure 9 runs in each feeder breaker relay and reacts to the detected failure of a circuit breaker trip failure to operate (breaker failure), indicated as BFTRIP1. This defect is mitigated by sending a trip signal to the appropriate relay protecting and controlling a circuit breaker upstream. Figure 9 illustrates logic in the relay controlling feeder Breaker 52-10, which is subscribing to GOOSE messages from other relays. Once the relay for 52-10 detects local breaker failure *and* has normal communications from the relay controlling 52-03 calculated as good message quality with a status value of zero, it sends a BF initiated trip for 52-03 (50/62BF 52-03). If the relay for 52-10 detects local breaker failure *and* communications have been lost from the relay controlling 52-03 and calculated as failed message quality with a status value of one, it sends a BF initiated trip for both 52-01 (50/62BF 52-01) and 52-02 (50/62BF 52-02). If the relay for 52-10 detects local breaker failure, Breaker 52-02 is closed, *and* communications are normal from the relay controlling Breaker 52-05, the relay sends a BF initiated trip for 52-05 (50/62BF 52-05). If the relay for 52-10 detects local breaker failure *and* communications have been lost from the relay controlling 52-05, it sends a BF initiated trip for 52-04 (50/62BF 52-04). The logic in Figure 9 shows the use of communications supervision in the relay for 52-10 when forwarding the 50/62BF signal to the circuit breakers upstream in order to mitigate the communications failures, thus ensuring the correct and safe operation of the system.

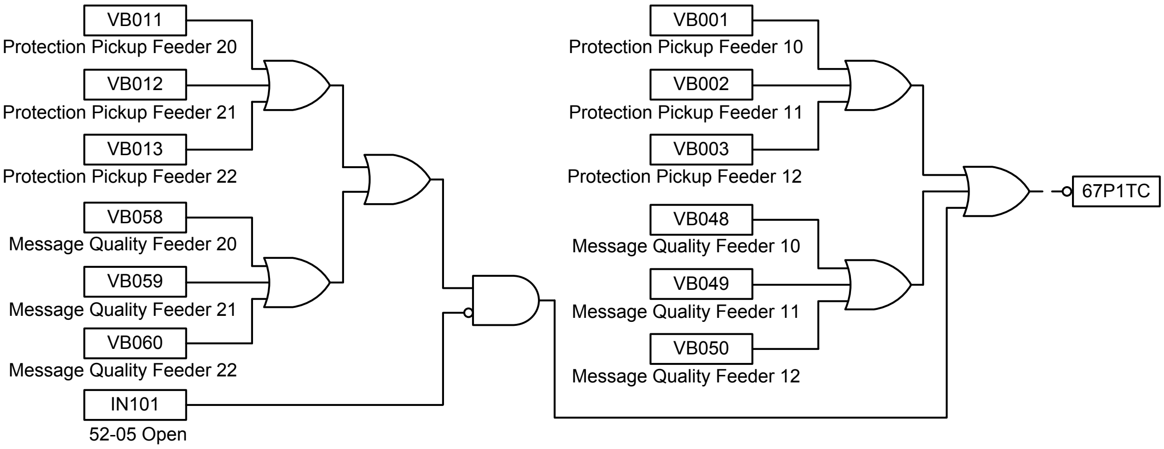

VB011
Protection Pickup Feeder 20
VB012
Protection Pickup Feeder 21
VB013
Protection Pickup Feeder 22
VB058
Message Quality Feeder 20
VB059
Message Quality Feeder 21
VB060
Message Quality Feeder 22
IN101
52-05 Open
VB001
Protection Pickup Feeder 10
VB002
Protection Pickup Feeder 11
VB003
Protection Pickup Feeder 12
VB048
Message Quality Feeder 10
VB049
Message Quality Feeder 11
VB050
Message Quality Feeder 12
67P1TC

Figure 7: Selectivity logic in Breaker 52-03 relay

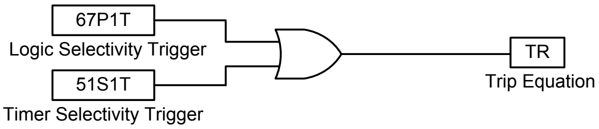


Figure 8: Logic in Breaker 52-03 relay chooses coordination timer trigger only if 67P1T selectivity trigger is not set

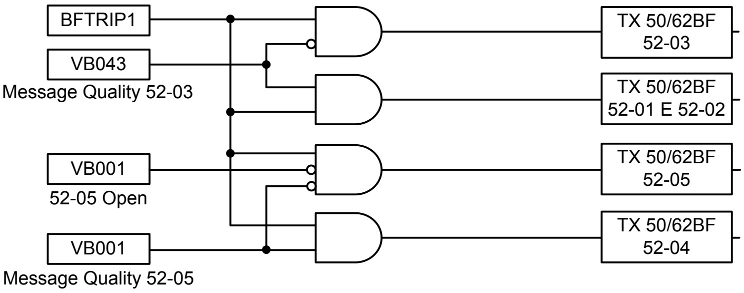


Figure 9: Circuit breaker failure scheme

3.10.3 Automatic Line Transfer

The transfer between alternate lines is done automatically via the relays exchanging interlock signals within GOOSE messages. The line in operation is shut down and supply is reestablished to consumers through the automatic transfer to the backup line.

The relays protecting the feeds into the substation monitor the voltage of the line in operation (Figure 10a). Absence of voltage on the active feed (C1) indicates Line 1 – Dead (Figure 10a) and presence on the other line (C2) indicates Line 2 – Live. The ALT logic (Figure 10b) confirms correct operation of C2 and that the switches on either side of Breaker 52-02 are closed (Figure 10b). This triggers the start of the ALT by setting ALT Start = 1 after the automation sequence timer expires.

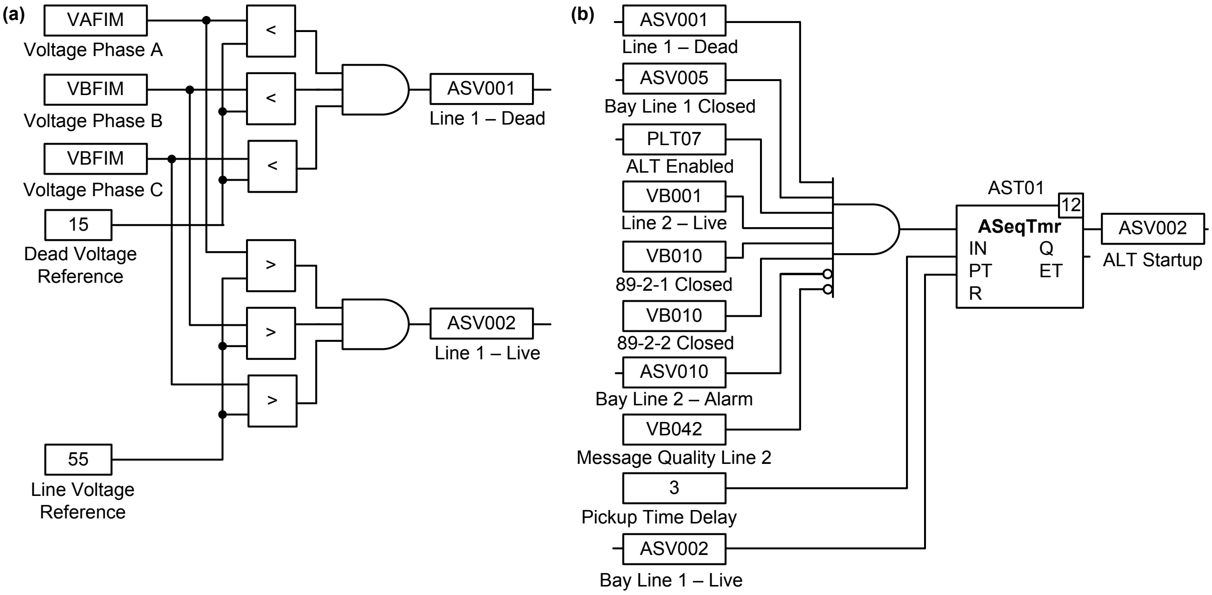


Figure 10: Voltage monitoring (a) and ALT startup (b)

4 CONCLUSION

The protocols within the IEC 61850 standard have become an efficient method of communicating between IEDs to transmit information about statuses, measurements, interlocks, and protection signals. Correct design of a protection and automation system based on IEC 61850 protocols requires correct engineering of the Ethernet LAN for speed, reliability, dependability, and availability. The mission-critical nature of digital protection applications also requires a much higher level of dependability, security, and Ethernet network availability for delivery of the GOOSE packets. At the IED level, correct operation of peer-to-peer communications must be supervised and communications failures, once detected, must trigger blocking and/or change protection and automation schemes to prevent incorrect performances. These GOOSE subscription defects are communicated to operators at the HMI and SCADA systems as alarms. These alarms are also sent to technicians so that communications errors can be immediately found and corrected. The IED diagnostic reports support troubleshooting, diagnostics, and preventive maintenance.

REFERENCES

[1] S. T. Watt, S. Achanta, H. Abubakari, and E. Sagen, “Understanding and Applying Precision Time Protocol,” proceedings of the 2014 Power and Energy Automation Conference, Spokane, WA, March 2014.

[2] S. Chelluri, D. Dolezilek, J. Dearien, and A. Kalra, “Understanding and Validating Ethernet Networks for Mission-Critical Protection, Automation, and Control Applications,” March 2014. Available: http://www.selinc.com.