УДК

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ВСТРОЕННЫХ В МУЛЬТИПЛЕКСОРЫ ДОСТУПА МОДУЛЕЙ ПЕРЕДАЧИ СИГНАЛОВ КОМАНД РЕЛЕЙНОЙ ЗАЩИТЫ И ПРОТИВОАВАРИЙНОЙ АВТОМАТИКИ

В.А. Харламов, к.т.н., начальник отдела оборудования ЗАО «Юнител Инжиниринг»

Системы релейной защиты и автоматики (РЗА) в значительной степени обеспечивают сохранение устойчивой работы Единой Национальной Электрической Сети (ЕНЭС) и снижение ущерба при повреждении сетевого электрооборудования. Устройства и системы противоаварийной автоматики (ПА) обеспечивают сохранение устойчивой работы ЕНЭС, локализацию и предотвращение развития системных аварий, обеспечение синхронной работы отдельных частей ЕЭС России в послеаварийных режимах.

В системах РЗА и ПА широко используется передача сигналов команд и управляющих воздействий, осуществляемая с помощью устройств передачи аварийных сигналов и команд (УПАСК). Неправильная работа УПАСК может привести не только к отключению одной линии электропередачи (ЛЭП), но и к серьезным системным авариям. Поэтому к УПАСК предъявляются очень высокие требования к вероятности пропуска принимаемой команды (надежности), вероятности приема ложной команды (безопасности) и времени передачи команд [1]. Правильная работа УПАСК определяется не только заложенными в них при разработке алгоритмами обработки сигналов, качеством проектных решений и выполнения пуско-наладочных работ, но и организацией их эксплуатации и технического обслуживания.

Традиционно в электроэнергетике для передачи сигналов команд РЗ и ПА используются УПАСК, которые работают по каналам высокочастотной (ВЧ) связи, организованным по фазным проводам ЛЭП. Это обусловлено тем, что ЛЭП связывают те объекты, между которыми необходима передача команд РЗ и ПА, их высокой надежностью и минимальным временем устранения их неисправностей. В настоявшее время в российской электроэнергетике все более широко используются цифровые системы передачи информации (ЦСПИ) для организации телефонных каналов диспетчерской и технологической связи, каналов передачи данных корпоративных информационных систем, телемеханики, автоматизированных информационно-измерительных систем коммерческого учета электроэнергии (АИИС КУЭ), автоматизированных систем управления технологическими процессами (АСУ ТП), организации видеоконференций и видеонаблюдения. В последнее десятилетие ЦСПИ начали активно использоваться для передачи сигналов команд РЗ и ПА. В процентном отношении число УПАСК, работающих по ЦСПИ, постоянно растет по сравнению с числом УПАСК, работающих по ВЧ каналам.

В России наибольшее распространение получили мультиплексоры доступа со встроенными интерфейсными модулями передачи команд РЗ и ПА, являющимися по сути дела встроенными в мультиплексоры УПАСК. Это обусловлено тем, что еще десять лет назад встроенные в мультиплексоры УПАСК являлись существенно более дешевым, по сравнению с другими, решением для передачи сигналов команд РЗ и ПА через ЦСПИ. На данный момент времени в российской электроэнергетике используются в основном мультиплексоры доступа со встроенными УПАСК зарубежных производителей: FOX515 с модулями TEBIT компании ABB и PCM30U-OCH с модулями PBS компании TTC Marconi.

За прошедшее десятилетие накоплен большой опыт эксплуатации мультиплексоров со встроенными в них УПАСК, который выявил целый ряд серьезных проблем:

- невозможность полного разделения зон ответственности и обслуживания между службами РЗА и ПА и службами средств диспетчерского и технологического управления (СДТУ) в мультиплексоре доступа со встроенными УПАСК;
- сложность обеспечения информационной безопасности (ИБ) встроенных УПАСК;
- реализация встроенных УПАСК часто не соответствует отраслевым стандартам и дополнительным требованиям российской электроэнергетики и принятым в ней нормам эксплуатации, не обеспечивает их интеграцию в АСУ ТП объектов;
- необходимость отключения питания мультиплексора доступа при проведении технического обслуживания встроенных УПАСК;
- несовместимость между собой встроенных УПАСК в мультиплексорах доступа разных производителей.

Мультиплексоры доступа ЦСПИ находятся в зоне ответственности и обслуживания служб СДТУ. При установке в них встроенных УПАСК в мультиплексорах появляются устройства, о специфике функциональности и параметров которых специалисты служб СДТУ не имеют полной информации. Если осуществлять обслуживание встроенных УПАСК только службами СДТУ, то на них ложится полная ответственность за их ложную работу, которая возможна по целому ряду причин, например, из-за возникновения наведенных напряжений на длинных сигнальных кабелях, идущих от устройств РЗА и ПА, из-за неправильного заземления их оплетки. В случае возникновения технологических нарушений, связанных с работой встроенных УПАСК, службы СДТУ должны привлекаться к их расследованию, хотя они могут быть вызваны причинами, о которых ее специалисты имеют мало понятия, т.к. они относятся к специфике работы служб РЗА и ПА.

Поэтому существует необходимость привлечения служб РЗА и ПА к обслуживанию встроенных УПАСК и разделению зон ответственности, как это показано на рис.1.

Но такому совместному обслуживанию мультиплексоров доступа мешает то, что управляющее программное обеспечение (ПО) общее как для УПАСК, так и для связной функциональности, и часто без отдельных паролей на разную функциональность. В результате при совместном обслуживании службами РЗА и ПА и службами СДТУ мультиплексоров со встроенными УПАСК могут возникнуть следующие проблемы:

- сотрудники служб РЗА и ПА могут изменить параметры мультиплексоров, что может нарушить функционирование, как части, так и всех каналов в ЦСПИ;
- сотрудники служб СДТУ могут изменить параметры встроенных УПАСК, что может привести не только к нарушению его работы, но к серьезным технологическим нарушениям (например, поменять местами выходы команд разного назначения, что может быть обнаружено не сразу, а лишь только при расследовании технологического нарушения).

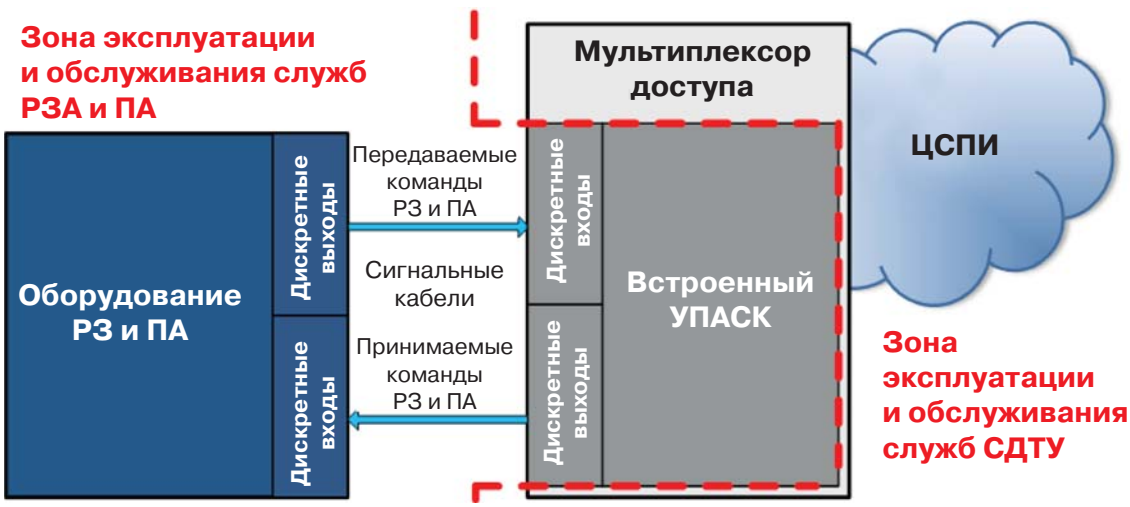

Рис.1. Разделение зон эксплуатации и обслуживания в мультиплексоре доступа со встроенным УПАСК

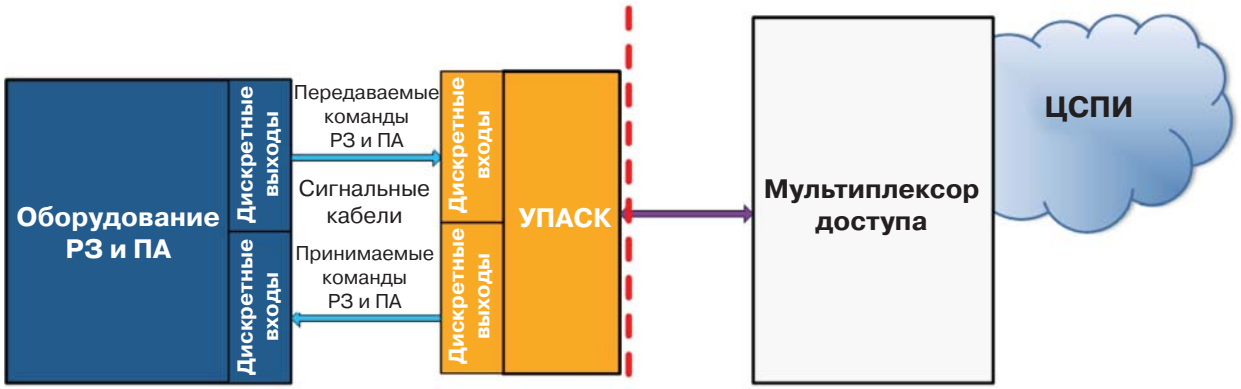

Рис.2. Разделение зон эксплуатации и обслуживания при вынесенном из мультиплексора доступа УПАСК

Пытаясь решить указанную проблему, в ОАО «ФСК ЕЭС» часто на одном объекте устанавливают два мультиплексора доступа: один для служб СДТУ, а другой для служб РЗА и ПА [2, 3]. Но очевидно, что полного разделения зон ответственности и обслуживания между данными службами можно достигнуть только выносом УПАСК из состава мультиплексора (рис.2). При этом УПАСК подключается к мультиплексору доступа по стандартному, желательно оптическому, цифровому интерфейсу.

Еще пятнадцать лет назад казалось, что вопросы ИБ имеют отношение только к государственным и финансовым структурам, а в электроэнергетике они не актуальны. Сегодня задача обеспечения ИБ остро стоит и в ней. Возможны различные мотивы для осуществления кибератак. Например, многие государства тратят огромные суммы денег на покупку вооружения и содержание армий. У них может возникнуть желание нанести упреждающий удар по инфраструктуре противника, важнейшей частью которой безусловно является электроэнергетика, без привлечения традиционных вооруженных сил. Или, крупные электроэнергетические компании являются акционерными обществами, акции которых представлены на биржах. Можно предположить, что акции компании, серьезно пострадавшей от кибератаки, приведшей к массовым серьезным технологическим нарушениям и последующему ущербу из-за недоотпуска электроэнергии, существенно упадут в цене, что делает их привлекательными для покупки потенциальными инвесторами. Это привело к разработке и утверждению отраслевых стандартов по ИБ в ОАО «ФСК ЕЭС» [4].

Учитывая, что от правильной работы УПАСК зависит устойчивая и безаварийная работа всей энергосистемы в целом, то встроенные в мультиплексоры УПАСК являются очень привлекательной для кибератак мишенью. Еще большую привлекательность обуславливает то, что получив несанкционированный доступ к одному из мультиплексоров доступа в сети, через ее каналы управления можно поразить все УПАСК, находящиеся на разных объектах энергосистемы. Поэтому к УПАСК сейчас предъявляются требования по обеспечению их ИБ [5].

Обеспечить ИБ встроенных в мультиплексоры УПАСК сложно по ряду причин [6]:

- УПАСК встроены в мультиплексоры, которые первоначально разработаны для операторов связи с использованием операционных систем (ОС) Unix/Linux, QNX, pSOSystem и т.д. часто устаревших версий с известными уязвимостями;
- управляющее ПО для мультиплексоров реализовано на базе ОС Windows или Unix/Linux с использованием для подключения к оборудованию по Ethernet широко распространенных и обладающих уязвимостями протоколов Telnet и SNMP и позволяет работать не только с локальным мультиплексором, но и со всеми мультиплексорами в ЦСПИ.

Следует отметить, что постоянно обнаруживаются новые уязвимости, срок устранения которых часто составляет более одного года, а иногда устранить их вовсе не возможно. Поэтому потенциально встроенные УПАСК могут быть поражены как локально, так и дистанционно, как немедленно, так и отложено.

Вынос УПАСК из мультиплексоров (рис.2) и принятие специальных мер [6] позволяют решить проблемы обеспечения ИБ. В любом случае, несанкционированный доступ через ЦСПИ к вынесенно-

му УПАСК будет блокирован (естественно при отсутствии подключения к портам управления УПАСК через ЦСПИ).

В тоже время реализация встроенных в мультиплексоры УПАСК зарубежных производителей имеет целый ряд недостатков:

- несоответствие параметров дискретных входов передачи команд РЗ и ПА российским отраслевым стандартам [5, 7];
- регистраторы событий обладают возможностью редактирования, что затрудняет или делает невозможным объективное расследование технологических нарушений;
- отсутствие контактов аварийной сигнализации и подтверждения передачи и приема команд РЗ и ПА, что делает невозможным вывод информации об авариях и срабатываниях встроенных УПАСК в системы центральной сигнализации объектов;
- отсутствие интеграции в АСУ ТП объектов по используемым для устройств РЗА и ПА стандартным протоколам, например, ГОСТ Р МЭК 60870-5-101, зарубежные производители предлагают использовать для этих целей протокол SNMP, предназначенный для систем управления сетями связи и часто имеющий проблемы с обеспечением ИБ;
- отсутствие светодиодной индикации с фиксацией передачи и приема сигналов команд РЗ и ПА с ручным сбросом для дежурного персонала объектов.

Возможной причиной этого может быть то, что УПАСК встраивались в уже разработанные для операторов связи мультиплексоры доступа и обеспечить в них требуемую функциональность, устранив указанные выше недостатки, технически невозможно.

Устранить часть приведенных выше недостатков встроенных УПАСК можно использованием панели контроля и управления с системой регистрации ПКУ СР24, разработанной и производимой ЗАО «Юнител Инжиниринг» в России, а именно:

- привести в соответствие параметров дискретных входов передачи команд РЗ и ПА российским отраслевым стандартам [5, 7];
- обеспечить фиксацию информации о прохождении команд РЗ и ПА в не редактируемых энергонезависимых регистраторах событий;
- вывести информацию о прохождении команд РЗ и ПА в системы центральной сигнализации и в АСУ ТП объектов;
- обеспечить светодиодную индикацию передачи и приема сигналов команд РЗ и ПА с фиксацией и ручным сбросом.

Но даже с использованием ПКУ СР24 остаются нерешенными проблемы фиксации аварийной сигнализации встроенных УПАСК в не редактируемых регистраторах событий и ее вывода в системы центральной сигнализации и в АСУ ТП объектов.

Согласно правилам технического обслуживания (ТО) устройств РЗА [8] при проведении периодического профилактического контроля и профилактического восстановления требуется проводить измерение сопротивления и испытание электрической прочности изоляции дискретных входов и выходов команд РЗ и ПА встроенных УПАСК, т. к. на них присутствует оперативный ток. Проблема состоит в том, что данные испытания проводятся при снятом напряжении питании оборудования. Выключение питания мультиплексора доступа приведет к потере не только каналов передачи команд РЗ и ПА, но и всех других организованных через него каналов, в том числе РЗА, например, каналов дифференциальных защит линий. Кроме того, требуется согласование сроков проведения ТО встроенных УПАСК между службами РЗА и ПА и службами СДТУ.

Вынос УПАСК из мультиплексоров (рис.2) решает указанные выше проблемы проведения их ТО, т. к. снятие напряжения питания с вынесенного из мультиплексора УПАСК никак не нарушает работоспособность других каналов.

Встроенные УПАСК разных производителей не совместимы между собой на канальном уровне (рис. 3). Такая ситуация требует использования при построении ЦСПИ мультиплексоров доступа одного и того же производителя для организации передачи команд РЗ и ПА, что в конечном счете способствует монополизации российского рынка и завышении цен зарубежными производителями.

Проведенные рядом компаний, в том числе и ЗАО «Юнител Инжиниринг», испытания показали совместимость на канальном уровне интерфейсов E1 мультиплексоров доступа разных производителей

Рис.3. Несовместимость встроенных УПАСК разных производителей

Рис. 4. УПАСК, подключаемые к интерфейсам Е1 мультиплексоров доступа разных производителей

Рис.5. УПАСК, подключаемые к интерфейсам Е1 мультиплексора доступа и транспортного мультиплексора

(другие цифровые интерфейсы не всегда совместимы на канальном уровне). Поэтому в ЦСПИ с использованием мультиплексоров доступа разных производителей каналы РЗА и ПА можно организовывать с использованием интерфейсов Е1 (рис. 4). Кроме того, если в ЦСПИ используются транспортные мультиплексоры STM-4 и выше, УПАСК можно подключать напрямую к их интерфейсам Е1 (рис. 5). Исключение мультиплексора доступа повышает надежность канала передачи команд РЗ и ПА через ЦСПИ.

Таким образом, использование УПАСК, подключаемых к оборудованию ЦСПИ по интерфейсам Е1, не требует использования мультиплексоров доступа одного производителя для организации передачи сигналов команд РЗ и ПА.

Вынос УПАСК из состава мультиплексоров доступа устраняет присущие встроенным УПАСК проблемы. Кроме того, вынос УПАСК из мультиплексоров и использование линейки оборудования ПКУС, разработанной и производимой ЗАО «Юнител Инжиниринг» в России, позволяет снизить требуемое число мультиплексоров доступа в ЦСПИ [2, 3] при организации каналов РЗА и ПА, что снижает стоимость ее реализации и эксплуатации.

Список литературы

1. IEC 60834-1, Teleprotection equipment of power systems – Performance and testing – Part 1: Command systems.

2. В.А. Харламов, Реализация цифровых каналов технологической связи для РЗА и ПА. — Воздушные линии, 2013, № 2, с. 53–58.

3. В.А. Харламов, Эффективная организация цифровых каналов связи для РЗА и ПА. — Электроэнергия. Передача и распределение, май-июнь 2013, № 3 (18), с. 90–91.

4. СТО 56947007-29.240.01.147-2013... СТО 56947007-29.240.01.147-2013, «Система обеспечения информационной безопасности ОАО «ФСК ЕЭС», Приложения 1...11 к Приказ ОАО «ФСК ЕЭС» от 24.06.2013 № 378.

5. СТО 56947007-33.040.20.123-2012 «Аттестационные требования к устройствам противоаварийной автоматики».

6. С.Е. Романов, В.А. Харламов, Каналы технологического управления. Универсальность и безопасность. — Релейщик, июнь 2013, № 1, с. 19–21.

7. СТО 56947007-29.120.40.102-2011 «Методические указания по инженерным расчетам в системах оперативного постоянного тока для предотвращения неправильной работы дискретных входов микропроцессорных устройств релейной защиты и автоматики, при замыканиях на землю в цепях оперативного постоянного тока подстанций ЕНЭС».

8. СТО 56947007-33.040.20.141-2012 «Правила технического обслуживания устройств релейной защиты, автоматики, дистанционного управления и сигнализации подстанций 110–750 кВ».