УДК 621.316

ЦЕНТРАЛЬНЫЙ СЕРВЕР РЕЛЕЙНОЙ ЗАЩИТЫ И АВТОМАТИКИ

Р.Г. МУСТАФИН

Казанский государственный энергетический университет

Рассматриваются некоторые проблемы центрального сервера релейной защиты и автоматики подстанции. Проводится сравнение надежности набора терминалов релейной защиты и центрального сервера релейной защиты и автоматики подстанции.

Ключевые слова: подстанция, терминал релейной защиты и автоматики, сервер, надежность.

Введение

В качестве объекта защиты выберем подстанцию, защита которой может быть выполнена в двух вариантах: с использованием набора микропроцессорных терминалов релейной защиты и автоматики (далее – терминалы) или с использованием центрального сервера релейной защиты и автоматики (далее – сервер).

Предметом рассмотрения является сравнительный анализ вероятностей отказов защиты подстанции (не отключение защитой повреждения, короткого замыкания на линии) при использовании терминалов или сервера.

При сравнении этих двух вариантов будем рассматривать только вероятность отказов терминалов или сервера, без учета вероятности отказов других элементов: измерительных трансформаторов, линий связи, выключателей.

Для читателей будет интересно узнать мнения видных деятелей энергетики, высказанные по идеям данной статьи, которые собраны в конце статьи, ссылки в статье оформлены как [ГВИ 1].

Концепция сервера родилась не на пустом месте, она является прямым продолжением непрерывного роста числа функций одного элемента защиты: [ГВИ 1].

На базе электромеханических реле одна защита состояла из нескольких реле: тока, времени, промежуточных, указательных, и др. [ГВИ 2].

На базе полупроводниковых реле одна защита, как правило, уже состояла из одного реле [ГВИ 3].

- Переход к микропроцессорной базе привел к бурному росту уже числа защит в одном терминале (десятки защит), одновременном выполнении функций автоматики в том же терминале.
- Соответственно логическим продолжением данной тенденции является концепция сервера, на котором располагаются все защиты подстанции. Подобная концепция имеет своих сторонников [1, 2].

Некоторые особенности центрального сервера релейной защиты и автоматики

Для сравнительного анализа вероятностей отказов защиты подстанции при использовании терминалов или сервера нам потребуется простейшая схема подстанции (рис.1). И для начала рассмотрим аналоговую подстанцию: аналоговые измерительные трансформаторы, медные кабели, терминалы (на каждый объект защиты – по своему одному или несколько терминалов).

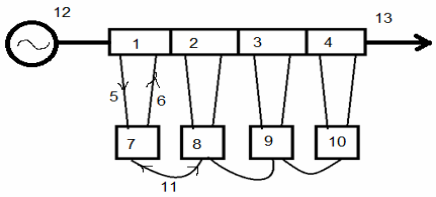

Рис. 1. Простейшая схема подстанции. Объекты защиты (*1–4*) расположены на одной линии тока, связаны линиями связи *5,6* с терминалами (*7–10*), которые также связаны друг с другом линиями связи *11*. Питание подстанции одностороннее *12*, потребители *13*

Переход к цифровой подстанции, стандарт МЭК 61850 (цифровые измерительные трансформаторы, оптоволоконные кабели) мало меняет конфигурацию системы защиты: оставляя тот же самый набор терминалов [ГВИ 4]. При этом могут добавляться шина процесса *14* и станционная шина *15*, которые объединяют все сигналы в одну шину (рис. 2).

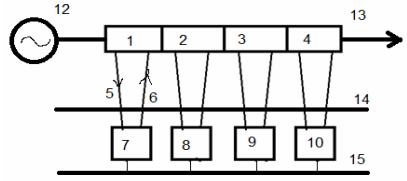

Рис. 2. Простейшая схема цифровой подстанции. Шина процесса *14* и станционная шина *15*

Релейная защита формирует особые требования по пропускной способности к шине процесса *14* и станционной шине *15*:

- При 80 выборок (измерений тока и напряжения в цифровых измерительных трансформаторах) в секунду каждая сигнальная линия *5* создает в шине процесса *14* информационный поток 5–6 Мбит/с. При большом числе сигнальных линий *5* может потребоваться логическая сегментация шины процесса *14* [3].
- Станционная шина *15* должна выдерживать повышенные информационные нагрузки – «Информационный шторм» * [4].

Центральный сервер релейной защиты и автоматики

Цифровая подстанция создает хорошие предпосылки для концепции сервера:

- Цифровые входные и выходные сигналы у терминалов.
- Все терминалы различаются только программным обеспечением, все программы (со всех терминалов) можно разместить в одном сервере *16* (Рис. 3).

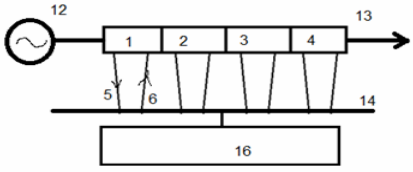

Рис. 3. Простейшая схема цифровой подстанции. Центральный сервер релейной защиты и автоматики *16*

При наличии сервера связь отдельных защит осуществляется внутри сервера, поэтому отпадает необходимость в станционной шине *15* (здесь и далее подчеркнем преимущества сервера перед терминалами).

«Такая концентрация имеет только один плюс: снижение стоимости РЗ. Основным ее недостатком является снижение надежности РЗ» [5]. То есть основной проблемой, которую должны решить разработчики концепции сервера – проблема надежности [ГВИ 5].

---

* СТО 56947007 – 25.040.40.112-2011 Типовая программа и методика программно-технического комплекса автоматизированной системы управления технологическими процессами (ПТК АСУ ТП) и микропроцессорного комплекса системы сбора и передачи информации (МПК ССПИ) подстанции в режиме повышенной информационной нагрузки «шторм» / Стандарт организации ОАО «ФСК ЕЭС», 2011.

Сравнение двух конфигураций – набор терминалов и сервер

Резервирование – основной способ повышения надежности работы устройств. [ГВИ 6]. Пусть вероятность отказа устройства (например в течении одного года) *P* гораздо меньше единицы. Тогда при работе двух устройств на одну задачу [ГВИ 7] вероятность одновременного отказа двух устройств есть произведение вероятностей отказа каждого устройства. Например: Если $P=10^{-2}$, то вероятность одновременного отказа двух устройств равна $P*P=10^{-4}$, то есть надежность работы при резервировании значительно возрастает. В релейной защите используют как резервирование для повышения надежности срабатывания защиты (отключения выключателя), так и резервирование для уменьшения излишнего срабатывания защит.

Применяют два способа ближнего резервирования:

- В пределах подстанции резервирование одного терминала релейной защиты другим (отличным по функциям, и защищающим данный или другой объект) терминалом.
- Два или несколько одинаковых терминалов релейной защиты (защищающих один объект и работающими на один выключатель) резервируют друг друга. Такое резервирование также применяется в релейной защите при особых требованиях к надежности.
- С резервированием одинаковыми терминалами, работающими на один выключатель, связана мажоритарная система (система голосований)*: если терминалы выдают разные управляющие команды – какую из них исполнить? Для разных задач могут быть разные сценарии мажоритарной системы. Например: для повышения надежности срабатывания защиты (отключения выключателя), так и для уменьшения излишнего срабатывания защит может быть применена система «2 из 4» (Рис. 4).

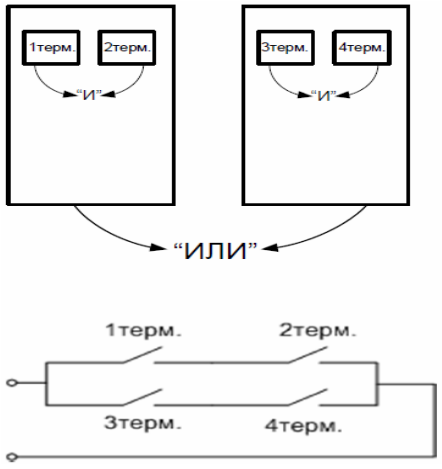

Рис. 4. Система состоит из двух шкафов*. Каждый шкаф состоит из двух функционально однотипных терминалов с выполнением выходных воздействий по схеме «И» для минимизации ложного срабатывания [ГВИ 7], ведущего к отключению, при отказе единичного элемента. Шкафы работают по схеме «или» (по схеме «два из четырех»)

---

* РД ЭО 1.1.2.28.0807-2009 Устройства релейной защиты и электроавтоматики атомных электростанций. Общие технические требования. ОАО «ВНИИАЭС». 2010: "Для исключения или минимизации отключения или разгрузки энергоблока АЭС в результате ложного срабатывания УРЗА из-за повреждения или отказа единичного элемента допускается применение для построения логических цепей принципа мажорирования ... Применение принципа мажорирования указывается в техническом задании на проектирование УРЗА конкретного энергоблока АЭС. После внесения в ТЗ выбираются принципы построения 2/3 или 2/4 в зависимости от первичной схемы и требований заказчика ... и проведенных расчетов по надежности вариантов схем».

---

* Шкафы ШЭЭ 22Х АИ фирмы ЭКРА

Соответственно для повышения надежности работы сервера также можно применить резервирование: несколько одинаковых серверов (*16*, *17*, *18*) получают одну и ту же информацию и защищают одни и те же объекты (Рис. 5).

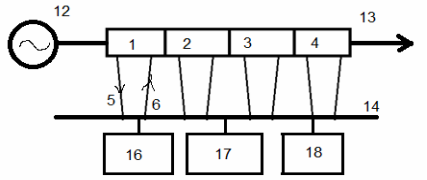

Рис. 5. Несколько одинаковых серверов (*16*, *17*, *18*) получают одну и ту же информацию и защищают одни и те же объекты (1-4)

При наличии трех серверов (Рис.5), кроме повышения надежности, система получает дополнительные преимущества [ГВИ 8]:

- Автоматическое обнаружение поврежденного сервера: у поврежденного сервера управляющие сигналы будут отличны от сигналов двух исправных серверов.
- Появляется возможность резервирования всех элементов: для этого каждый сервер должен быть снабжен собственной линией связи, измерительными трансформаторами, выключателем [ГВИ 9].
- Появляется возможность «горячей» замены серверов, настройки, параметрирования серверов: без остановки работы защит.

При отказах одного или нескольких серверов необходима перестройка режима работы мажоритарной системы, например [ГВИ 10]:

- В нормальном режиме «1 из 3». При этом система защищена от полного отказа (остановки) двух серверов.
- В нормальном режиме «2 из 3». При этом система защищена от полного отказа (остановки) одного сервера и защищена от неправильной работы (выдачи ложной команды на отключение) одного сервера.
- При отказе одного сервера – «1 из 2». При этом система защищена от полного отказа одного сервера.
- При отказе двух серверов – «1 из 1».

Стоит напомнить, что полный отказ сервера обычно обнаруживает «Сторожевой таймер» (контрольный таймер, англ. *Watchdogtimer*) — аппаратно реализованная схема контроля за зависанием системы [ГВИ 11].

Шина процесса *14* при наличии сервера теряет актуальность: все защиты имеют возможность обмениваться информацией внутри серверов *16*, *17*, *18*. Кроме того, единственная шина процесса *14* (без резервирования) понижает надежность системы. Поэтому целесообразна сегментация шины процесса *14*, например (Рис. 6): разбиение на отдельные сегменты (*19–22*) по числу объектов защиты (*1–4*). При этом каждый сегмент (*19–22*) соединен с каждым из серверов (*16*, *17*, *18*).

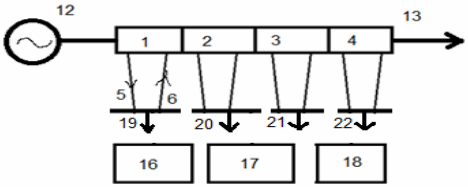

Рис. 6. Несколько одинаковых серверов (*16*, *17*, *18*), каждый сервер получает информацию и выдает команды управления, связан со всеми сегментами (*19-22*)

Сравнительная надежность набора терминалов - и центрального сервера

На рис.1 рассмотрена конфигурация, когда защиты стоят на одной линии, назовем ее *последовательной*. Для рассмотрения нам потребуется еще одна конфигурация терминалов:

параллельная, когда от одной шины отходят несколько линий, при этом каждая линия защищена одним терминалом (рис.7) [ГВИ 12].

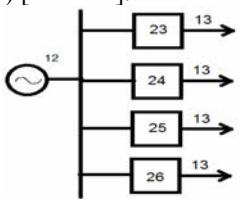

Рис.7. Простейшая схема подстанции. Объекты защиты вместе с терминалами защиты (*23*-*26*) защищают линии *13*

При этом схемы рис.1 и рис.7 имеют принципиальное различие: на схеме рис.1 имеется ближнее резервирование, на схеме рис.7 резервирования нет. Благодаря резервированию схема рис.1 более защищена, отметим особую роль терминала *7* (и повреждений на отрезке 1-2): для него нет ближнего резервирования, и один этот терминал во многом определяет вероятность отказа подстанции [ГВИ 13].

Для возможности сравнения двух конфигураций сделаем допущение: вероятности P отказа терминалов и центрального сервера одинаковы. Нам также потребуется ввести вероятность X повреждения (например короткого замыкания) на линии электропередачи. Для последовательной схемы это будет вероятность появления повреждения на участках (*1*-*2*, *2*-*3*, *3*-*4*, *4*-линия), для параллельной схемы это будет вероятность появления повреждения на линиях *13*, с защитами *23*, *24*, *25*, *26*. При сравнении терминалов и сервера применим следующий метод: выделим вероятности, линейные по X (при этом мы считаем, что $X<<1$), тогда сравнивая две системы мы можем X не учитывать (сократить).

Параллельная схема

Начнем с параллельной схемы (Рис.7), как самой простой. Вероятность отказа защиты от повреждения на одной линии равна $P*X$, соответственно вероятность того, что отказ защиты данной линии не приведет к отказу всей защиты равна $(1-P*X)$. Поскольку все линии *13* независимы, поэтому вероятность того, что ни одна из защит n линий не приведет к отказу всей защиты равна $(1-P*X)^n$. Откуда легко получаем вероятность Y отказа защиты:

$$Y = (1 - (1 - P*X)^n)$$

Линейная часть $Y \approx n*P*X$, соответственно $Y \sim n*P$ (для Рис.7 $n=4$).

Последовательная схема

Здесь рассмотрение более сложное, поскольку есть зависимость от того, в каком месте (на рис. 1 это участки *1*-*2*, *2*-*3*, *3*-*4*, *4*-линия) произошло повреждение, и какой из терминалов (на рис.1 это терминалы *1*, *2*, *3*, *4*) отказал. Отказ защиты системы происходит когда несколько последовательно расположенных терминалов, начиная с терминала *1* (рис. 1) откажут (например терминалы *1*; *1* и *2*; *1*, *2* и *3*; *1*, *2*, *3* и *4*). Поэтому рассмотрим все четыре случая.

Отказал терминал *1*, терминал *2* работает, остальные терминалы для нас не важны, поскольку второй терминал их резервирует, вероятность такого события $P*(1-P)$. Система рухнет, если повреждение обязательно есть на участке *1*-*2*, поскольку если на этом участке нет повреждения, тогда остальные целые терминалы штатно отключат повреждения на линии. Поэтому участок *1*-*2* даст вклад X в вероятность отказа защиты. Остальные участки никакого вклада не дадут, поскольку для каждого участка будет две возможности: X и $(1-X)$, которые при сложении дадут *1* (понятно почему: поскольку есть или нет повреждений на данных участках не влияет на систему). В результате получаем

$$Y=X*P*(1-P).$$

Отказали терминалы *1* и *2*, терминал *3* работает, остальные терминалы для нас не важны, вероятность такого события $P^2*(1-P)$. В этом случае важны повреждения на участках *1*-*2* и *2*-*3*, которые дадут три слагаемых: $X(1-X)$, $(1-X)X$ и XX, после сложения получим: $X(2-X)$. Соответственно

$$Y= X(2-X)*P^2*(1-P).$$

Отказали терминалы *1*, *2* и *3*, терминал *4* работает, вероятность такого события $P^3*(1-P)$. В этом случае важны повреждения на участках *1-2*, *2-3* и *3-4*, которые дадут семь слагаемых, после сложения которых получим: $X(3-3X+X^2)$. Соответственно

$$Y=X(3-3X+X^2)*P^3*(1-P).$$

Отказали терминалы *1*, *2*, *3* и *4*, вероятность такого события P^4. В этом случае важны повреждения на всех участках, которые дадут 15 слагаемых, после сложения которых получим: $X(3-6X+4X^2-X^3)$. Соответственно

$$Y=X(3-6X+4X^2-X^3)*P^4.$$

Сложив все четыре случая и выделив линейные части, получим:

$Y\approx X*(P+P^2+P^3)$, соответственно $Y\sim(P+P^2+P^3)$.

Ложное срабатывание

Кроме отказа терминала возможно ложное срабатывание терминала: когда в отсутствии повреждения на линии терминал выдаст команду на отключение выключателя. Обозначим вероятность такого события как *Z*. Тогда для четырех терминалов (для обоих схем) полная вероятность ложного срабатывания будет равна $(1-(1-Z)^4) = 4Z-6Z^2+4Z^3-Z^4$. Заметим некую разницу в «стоимости» ложного срабатывания для разных схем: если в последовательной схеме (рис.1) каждый терминал отключает всех потребителей, то в параллельной схеме (рис.7) один терминал отключает только одну линию [ГВИ 13].

Центральный сервер

Для одного сервера *16* (рис.3) ничего считать не надо: вероятность *P* отказа, и вероятность ложного срабатывания *Z* (просто для терминала и сервера мы их приравняли [ГВИ 14]). Поскольку сервер управляет всеми защитами, то при отказе сервера любое повреждение на линии приведет к отказу защиты, и вероятность такого события $(1 - (1-X)^4)$. Соответственно вероятность отказа защиты $Y=P*(1 - (1-X)^4)$. Линейная часть $Y\approx 4*P*X$, соответственно $Y\sim 4*P$.

Для трех серверов *16*, *17*, *18* (рис.5) возможны разные сценарии мажоритарной системы, рассмотрим два сценария: «1 из 3» (когда выключатель будет отключен, если хотя бы один сервер выдаст команду на отключение) и «2 из 3» (когда выключатель будет отключен, когда два любых сервера одновременно выдадут команду на отключение).

Рассмотрим сценарий «1 из 3». Для отказа защиты необходимо, чтобы одновременно отказали все три сервера. Соответственно вероятность отказа защиты $Y= P^3*(1 - (1-X)^4)$. Линейная часть $Y\approx 4*P^3*X$, соответственно $Y\sim 4*P^3$. Вероятность ложного срабатывания равна $(1-(1-Z)^3)=3Z-3Z^2+Z^3$.

Рассмотрим сценарий «2 из 3». Для отказа защиты необходимо, чтобы одновременно отказали два сервера, и таких комбинаций три, и одна комбинация когда отказали все три сервера: $Y=(3*P^2*(1-P)+P^3)*(1-(1-X)^4)$. Линейная часть $Y\approx(12*P^2*(1-P)+4P^3)*X$, соответственно $Y\sim 12*P^2*(1-P)+4P^3=12*P^2-8P^3$. Для ложного срабатывания необходимо, чтобы ложную команду одновременно выдали два сервера, и таких комбинаций три: $3*Z^2$, или все три сервера Z^3, сложив получим: $3*Z^2+ Z^3$.

Сравнение набора терминалов - и центрального сервера

Соберем все полученные формулы в одну таблицу.

Вероятности	Последовательная схема	Параллельная схема	Сервер		
			«1 из 1»	«1 из 3»	«2 из 3»
Отказ защиты	$P+P^2+P^3$	$4*P$	$4*P$	$4*P^3$	$12*P^2-8P^3$
Ложное срабатывание	$4Z-6Z^2+4Z^3-Z^4$	$4Z-6Z^2+4Z^3-Z^4$	Z	$3Z-3Z^2+Z^3$	$3*Z^2+ Z^3$

Из этой таблицы можно сделать простые выводы (которые впрочем, очевидны, и которые можно было сделать и без сложного рассмотрения):

- Даже один сервер почти не отличается по надежности от набора терминалов.
- Система из трех серверов значительно превосходит набор терминалов по надежности (пропорционально P^3 или P^2 для серверов, вместо P * для терминалов).

• Система из трех серверов при схеме «2 из 3» значительно превосходит набор терминалов по вероятности ложного срабатывания (пропорционально Z^2 для серверов, вместо Z для терминалов).

Таким образом, центральный сервер релейной защиты и автоматики имеет уникальные свойства, такие как отсутствие станционной и технологических шин. Кроме того, система из нескольких серверов будет иметь большую (по сравнению с набором терминалов) надежность как по отказам, так и по ложным срабатываниям, позволит автоматически обнаруживать поврежденный сервер, позволит заменять и настраивать сервера без остановки защит. В результате концепция сервера может применяться для защиты цифровой подстанции в некоторых особых случаях.

Замечания по тексту статьи от Гуревич. В.И., к.т.н., Центральная лаборатория Электрической компании Израиля:

[ГВИ 1] В данной статье по умолчанию принимается, что эта концепция верна. На самом деле верность этой концепции не доказана. По нашему мнению, такая концепция является отрицательной и приводит к резкому снижению надежности РЗ, поскольку отказ терминала с ограниченным количеством функций приводит к отказу лишь нескольких функций РЗ, а при выходе из строя терминала (сервера), на котором сконцентрированы все функции РЗ, защищаемый объект остается вообще без защиты.

[ГВИ 2] Это не совсем так. Имеются комбинированные электромеханические защиты, выполняющие функции целого вида защит (например, электромеханическое реле дистанционной защиты линии типа *LZ*-31).

[ГВИ 3] Это не так. Полупроводниковые реле, за очень редким исключением, лишь повторяли функции электромеханических реле, а сложные защиты составлялись из набора отдельных реле.

[ГВИ 4] Стандарт МЭК 61850 описывает лишь протокол связи, а не концепцию построения цифровой подстанции. Целесообразность широкого применения цифровых ТТ и ТН далеко не однозначна [7]. В настоящее время уже переходят от относительно дорогой оптоэлектронной системы к более дешевой и менее надежной сетевой (*Ethernet*).

[ГВИ 5] Проблема сформулирована не верно. Автор не ставил перед собой задачу повысить надежность существующей подстанции. Автор ставит задачу повышения надежности при одновременном существенном снижении стоимости существующей подстанции, поскольку целью перехода от существующей концепции подстанции к рассматриваемой в статье концепции – концепции сервера – является именно снижение стоимости подстанции. В статье же рассматриваются только вопросы надежности без учета стоимости.

[ГВИ 6] Надежность в технике – это понятие очень широкое и комплексное. Резервирование – это всего лишь один из многочисленных способов повышения надежности, а вовсе не основной из них.

[ГВИ 7] Это справедливо лишь для частного случая последовательного соединения устройств, тогда как в релейной защите устройства функционально соединяют параллельно, а не последовательно.

[ГВИ 8] А какова будет стоимость этих трех серверов по сравнению со стоимостью существующей сегодня микропроцессорной РЗ, если учесть, что концепция перехода на серверы связана исключительно со стремлением снизить стоимость существующей сегодня релейной защиты подстанции? Если применять три сервера, то где же экономия? А если нет экономии, то зачем вообще переходить на концепцию сервера?

---

* На Рис.1 отрезки *1-2*, *2-3*, *3-4* и *4*-линия могут быть сильно неравнозначны по вероятности повреждения: вероятность повреждения на отрезке *4*-линия может быть значительно выше (по сравнению с другими отрезками). Тогда, очевидно, в последовательной схеме основной вклад в отказ защиты даст член P^4 (то есть четыре ступени ближнего резервирования!) и для сравнения по надежности потребуется больше трех серверов. Если ступней резервирования у терминалов два, то уже три сервера сравняются с терминалами по надежности (при схеме «2 из 3»).

[ГВИ 9] То есть, речь идет, фактически, о строительстве трех отдельных подстанций, вместо одной!

[ГВИ 10] И кто же это будет делать на работающих серверах?

[ГВИ 11] Сторожевой таймер (*watchdog*) и система самодиагностики имеются в составе каждого отдельно взятого терминала. Неправильное действие этого элемента вследствие его повреждения может привести к блокированию всех функций сервера

[ГВИ 12] На самом деле «защиты НЕ стоят на одной линии» и «каждая линия НЕ защищена одним терминалом». Реальная структура РЗ намного сложнее.

[ГВИ 13] Подстанции строятся таким образом, что отказ в срабатывании одного терминала не влечет за собой отказ целой подстанции и отключение всех потребителей.

[ГВИ 14] На каком основании делается такое допущение? Ведь, во-первых, центральный сервер намного сложнее одиночного терминала, а, следовательно, вероятность сбоев в его работе будет намного выше. Во-вторых, из-за более сложного программного обеспечения и пользовательского интерфейса значительно больше вероятность ошибок персонала при конфигурации и периодических проверках функций центрального сервера по сравнению с одиночным терминалом (а ведь «человеческий фактор» - причина неправильных действий РЗ в 50 – 70 % случаев). В-третьих, последствия от отказа в работе одиночного терминала с ограниченным количеством функций и центрального сервера с полным набором всех функций РЗ целой подстанции - совершенно различны. Как же можно приравнивать их надежность без учета всех этих обстоятельств?

Автор благодарит Григорян Тамару Анатольевну, к.ф.м.н., доцента кафедры ВМ КГЭУ за полезные обсуждения, а также Гуревича Владимира Игоревича, почетного профессора, к.т.н., ведущего специалиста Центральной лаборатории Электрической компании Израиля за подробный анализ статьи.

Summary

Some problems of the central server of relay protection and automation examined. The reliability of terminals of relay protection is compared with the reliability of central server.

Keywords: substation, terminal of relay protection and automation, server, reliability.

Литература.

1. Волошин А.А., Арцишевский Я.Л, Максимов Б.К. // Релейщик. 2012. №2. С.32-33.

2. Патенты РФ № 2468407 от 17.06.2011, № 2014121512 от 22.05.2014, № 2014121514 от 22.05.2014.

3. Соколов Г.А. Особенности реализации системы РЗиА цифровой подстанции на примере использования цифровой ДЗШ. Цифровая подстанция. // Апрель 2014. С. 30 – 33.

4. Шевцов М.В. Передача дискретных сигналов между УРЗА по цифровым каналам связи. // Релейщик. 2009, №1. С.60-63.

5. Гуревич В.И. Микропроцессорные реле защиты. Устройство, проблемы, перспективы. М.: Инфра-Инженерия, 2011. 336 с.

6. Гуревич В.И. Уязвимости микропроцессорных реле защиты. Проблемы и решения. М.: Инфра-Инженерия, 2014. 256 с.

7. Гуревич В.И. Оптические трансформаторы тока: нужно быть реалистами. // Электрические сети и системы. 2010. № 4. С. 73 - 76.

Поступила в редакцию ***23 марта 2015 г.***

Мустафин Рамиль Гамилович **–** канд. физ.-мат. наук, доцент кафедры «Релейная защита и автоматизация элекроэнергетических систем» (РЗА) Казанского государственного энергетического университета (КГЭУ).