УДК 621.311:681.5
DOI: 10.17586/0021-3454-2015-58-12-999-1007

МЕТОДИКА ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ SCADA-СИСТЕМ

Зо Е Чжо

Национальный исследовательский университет „МИЭТ“, 124489, Москва, Россия
E-mail: kyawzawye.47@gmail.com

Проанализированы возможности повышения достоверности информации, получаемой с помощью автоматизированных систем контроля и управления в энергетике. Обоснована необходимость совмещения процедур ввода информации, поступившей от датчика, и кодирования сообщения. Предложены новые принципы кодирования, сочетающие впервые синтезированный биимпульсный условно корреляционный код с циклическим кодом. Такой подход обеспечивает высокий уровень достоверности, характеризующийся вероятностью появления необнаруживаемых искажений в канале ввода—вывода информационных сигналов $\approx 10^{-14}$, это значение на 2—3 порядка лучше требований нормативных документов. Разработанный метод позволяет одновременно с опросом состояния датчиков диагностировать неисправность цепи связи с датчиком, т.е. фиксировать наличие короткого замыкания или разрыва цепи.

Ключевые слова: *достоверность, автоматизирование, SCADA, энергетика, комбинация сигналов, телесигнализации, диспетчерское управление.*

Введение. Автоматизированные системы диспетчерского контроля и управления (SCADA-системы) широко используются для управления технологическими процессами в таких отраслях промышленности, как электроэнергетика всех уровней (от центрального диспетчерского управления едиными энергосистемами до сельских электрических сетей); электрифицированный железнодорожный транспорт; нефте- и газотранспортные системы; промышленные предприятия; аэропорты, морские и железнодорожные терминалы; коммунальное хозяйство городов и др. [1, 2]. Электроэнергетика в настоящее время является базовой отраслью, ставящей все новые теоретические и практические задачи, решение которых с помощью SCADA-систем возможно лишь при усовершенствовании структуры, а также основных информационных характеристик: достоверности, быстродействия, помехоустойчивости.

Следует отметить, что значительная часть информационно-управляющих комплексов выполняется в виде набора „готовых“ компонентов — универсальных программируемых логических контроллеров (ПЛК). Широко распространены комплексы на ПЛК ввода—вывода дискретных и аналоговых сигналов, производимые компаниями — Allen Bradley, GE-Fanuc, Schneider Electric, Octagon system и др. Основу базовых ПЛК составляют „неинтеллектуальные“ модули циклического ввода—вывода дискретных и аналоговых сигналов и модули интерфейсных связей. Аппаратура и программы обработки, проверки достоверности, привязки информации к меткам времени находятся в центральном процессоре [3—5]. Однако во всех системах на базе ПЛК не выполняются требования стандартов о разделении выполнения команд технических устройств на этапы и использовании пауз между этапами для контроля (по цепям обратной связи) отсутствия искажений. В результате уровень достоверности (вероятность выполнения искаженной команды — составляет не 10^{-14}—10^{-16}, а 10^{-6}—10^{-8}) на шесть-восемь порядков хуже указанного в стандартах для систем высшей категории качества. Кроме того, каждый крупный производитель разрабатывает и использует в системах свой протокол обмена информацией [6]. Все это сокращает возможности SCADA-систем. Выходом из создавшегося положения могла бы стать разработка международного стандарта, регламентирующего информационный обмен в SCADA-системах [7].

Для SCADA-систем, ориентированных на использование современных цифровых каналов связи, ФСО и ФСК России в качестве базового выбран протокол IEC 60870-5-101 (104) по ГОСТ Р МЭК 870-5-101 (104). Так как базовый протокол должен учитывать множество вариантов его использования, потери в эффективности информационных обменов и достоверности информации в SCADA-системам неизбежны. Целью настоящей статьи является анализ наиболее важной характеристики SCADA-систем — достоверности полученной с их помощью информации.

Анализ параметров систем на базе стандарта IEC 61850. Важной составляющей повышения достоверности информационных обменов в SCADA является диагностика работоспособности системы. Рассмотрим принцип проведения диагностики работоспособности элементов и системы телемеханики в целом, который введен во вторую редакцию стандарта — IEC 61850-10 (Conformance Testing) [8]. Не предусматривается проведение процедур тестирования и диагностики в реальном масштабе времени. Необходимость отключения рабочего режима системы для перехода в режим диагностики может привести к потере важной информации, т.е. указанная в [8] методика диагностики не может быть применена в системах, в которых режим реального времени не может быть отключен даже на незначительное время.

Важно также подчеркнуть, что при проведении диагностики в соответствии с указанным стандартом реальные датчики положения объектов и исполнительные механизмы заменяются эмуляторами. В результате самые важные для диагностики и самые ненадежные элементы системы телемеханики исключаются из процедуры контроля.

Соглашаясь с предлагаемым стандартом выполнения диагностики, многие авторы публикаций, содержащих анализ параметров систем телемеханики на базе IEC 61850, предлагают показатель надежности определять по сроку службы компонентов системы и по наработке на отказ. При таком подходе в расчет вводятся только обнаруживаемые отказы; за пределами анализа оказываются необнаруживаемые отказы, являющиеся главной причиной приема некорректных сигналов состояния оборудования, а также причиной выполнения искаженных команд управления.

При проведении системного анализа достоверности и надежности предпочтительно ориентироваться на требования к указанным параметрам в стандарте IEC 60870-4 [9]. По этому стандарту надежность SCADA-систем должна определяться наработкой на обнаруживаемый и необнаруживаемый отказ (до отказа или между отказами) для одного канала каждой выполняемой функции, а достоверность информации — вероятностью появления необнаруживаемого отказа в трассе, начиная от источника и заканчивая приемником. Указанная интерпретация основных показателей систем диспетчерского управления, в частности, предполагает, что при расчете достоверности канала телеуправления необходимо учитывать вероятность появления необнаруживаемого отказа формирователя команды, т.е. элементов пульта или ПЭВМ диспетчера, элементов передачи, приема и вывода сигнала управления, включая контакты выходных (промежуточных) реле[*].

Показатели надежности каналов телесигнализации и телеуправления определяются временем наработки на отказ не менее 17 000 часов, а достоверности каналов телеуправления и телесигнализации — вероятностью появления необнаруживаемого отказа не более 10^{-14} и 10^{-12} соответственно. Так как применение IEC 61850 позволяет решать более сложные задачи, естественно предположить, что к обеспечению надежности и достоверности следует подходить более жестко — использовать для оценки надежности показатель наработки на отказ не менее 20 000 часов, а для достоверности телеуправления и телесигнализации — вероятность не обнаруживаемого отказа не более 10^{-15} и 10^{-13} соответственно.

[*] ГОСТ 26.205-88. Комплексы и устройства телемеханики. Общие технические условия.

Модель канала телесигнализации. Проведем анализ мер, обеспечивающих достижение требуемого показателя достоверности информации для самых важных каналов системы диспетчерского управления — телесигнализации и телеуправления. Рассмотрим модель канала телесигнализации, представленную на рис. 1.

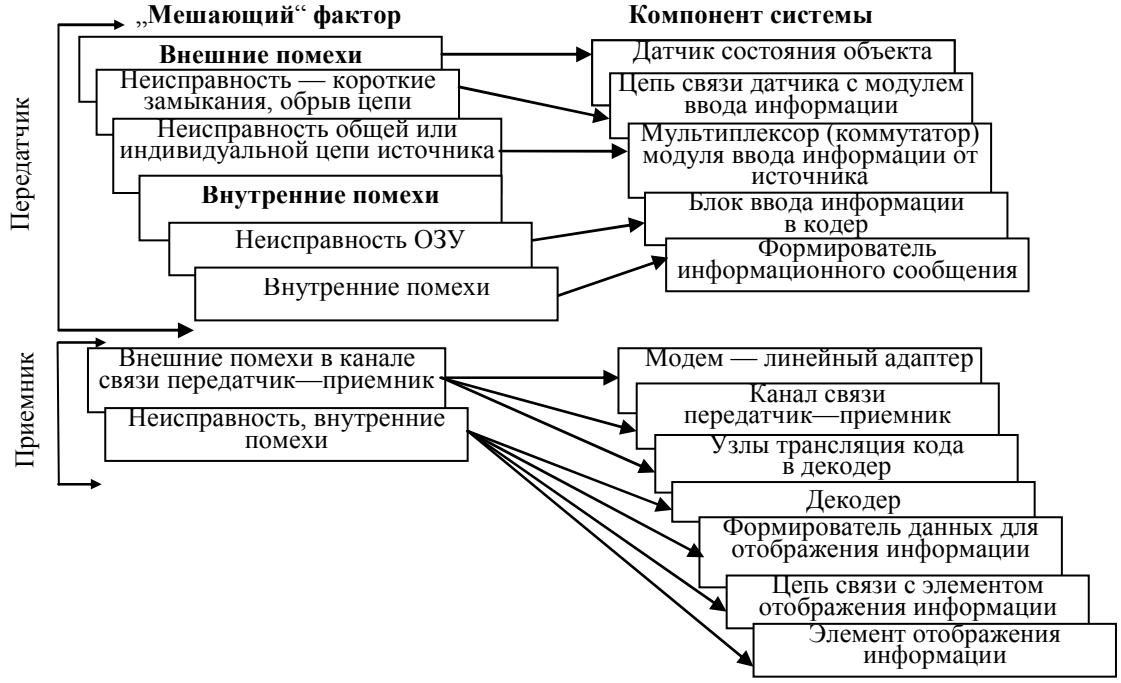

Рис. 1

Датчики телесигналов состояния объектов (ТС) обычно размещаются в зоне действия электромагнитных помех электрических подстанций. В связи с широкой полосой частот флуктуационных помех или „белого шума“ для защиты от помех применяют не фильтрацию, а стробирование. В таком случае вероятность искажения сигнала от датчика при стробировании $P_{\text{и.с}}$ составит:

$$P_{\text{и.с}} = P_1 P_{\text{о}}, \tag{1}$$

где P_1 — вероятность возникновения помехи, искажающей сигнал датчика; $P_{\text{о}}$ — вероятность опроса состояния датчика во время действия помехи.

Тогда

$$P_{\text{и.с}} = P_1 \frac{T_{\text{с}}}{T_{\text{о}}}, \tag{2}$$

где $T_{\text{с}}$ — длительность сигнала стробирования; $T_{\text{о}}$ — период опроса датчиков.

Обычно применяют: $T_{\text{с}} = 5 \cdot 10^{-6}$ с , $T_{\text{о}} = 10^{-2}$ с. Тогда при $P_1 = 10^{-4}$ получим $P_{\text{и.с}} = 5 \cdot 10^{-7}$.

Как видно, использование только метода стробирования не обеспечивает требуемого уровня достоверности информации. Для повышения помехозащищенности может быть использовано повторное стробирование сигнала от датчика с интервалом времени, превышающим возможную длительность сигнала помехи, однако это приводит к ухудшению динамических характеристик функциональных устройств.

С помощью „мощных“ помехозащитных кодов можно обнаружить практически все возможные помехи в канале связи.

Однако попытка борьбы с помехами только в канале связи не может обеспечить достоверный прием данных, если уже в кодер поступает информация с необнаруженными искажениями. Более того, к указанным выше возможным причинам ввода недостоверной информации следует добавить: необнаруживаемые искажения данных во внутренней магистрали SCADA-систем; необнаруживаемые искажения из-за воздействия помех, сбоев и неисправностей аппаратуры на участке трассы вывода данных.

Наряду с использованием „мощных“ помехозащитных кодов для повышения достоверности информации используются каналы обратной связи. Наибольшее распространение получили системы с каналом информационной (ИОС) и решающей (РОС) обратной связи. Важно подчеркнуть, что искажения информации в системе с каналом обратной связи не будут обнаружены, если произойдет двойное искажение одного и того же сигнала в информационных посылках, передаваемых по прямому и обратному каналам.

Например, при длине посылки в L двоичных сигналов и вероятности однократного искажения информации помехами в канале связи P_1 вероятность необнаруженного искажения информации в системе с обратным каналом составит:

$$P_{\text{н.иОК}} = L P_1^2 . \qquad (3)$$

При L =100 бит и P_1 =10^{-4} вероятность необнаруженного искажения информации в системе с обратным каналом равна $10^2 \cdot 10^{-8} = 10^{-6}$, что значительно превышает предельно допустимые значения, оговоренные стандартом для современных SCADA-систем. Так, регламентируемые значения для каналов ввода—вывода дискретных сигналов (телесигнализации) и команд управления лежат в пределах 10^{-8}—10^{-10} и 10^{-11}—10^{-14} соответственно.

Уменьшения $P_{\text{н.иОК}}$ можно добиться, если осуществить более чем однократную передачу данных по прямому и (или) обратному каналам, однако это приводит к еще большим снижению эффективности использования канала связи и усложнению аппаратуры устройств ввода и вывода.

Наиболее эффективно для обнаружения искажений создать условия, при которых каждое устройство трассы доставки телесигнала от датчика к приемнику будет протестировано „в динамике“, т.е. будет проверена его адекватная реакция на сигнал „1“ и „0“.

Предлагается использовать метод обнаружения искажений и повышения достоверности информации, который основан на совмещении процедур ввода и кодирования информации. Кодирование ведется с использованием биимпульсного условно корреляционного кода (БУКК), при этом не только обеспечивается достоверность идентификации состояния объекта, но и обнаруживаются и идентифицируются неисправности (обрыв или короткое замыкание) цепей связи контроллера с датчиками ТС. Метод исключает необходимость проведения отдельных процедур кодирования и тестирования (диагностики) [6, 10].

На рис. 2 приведен фрагмент схемы формирования БУКК.

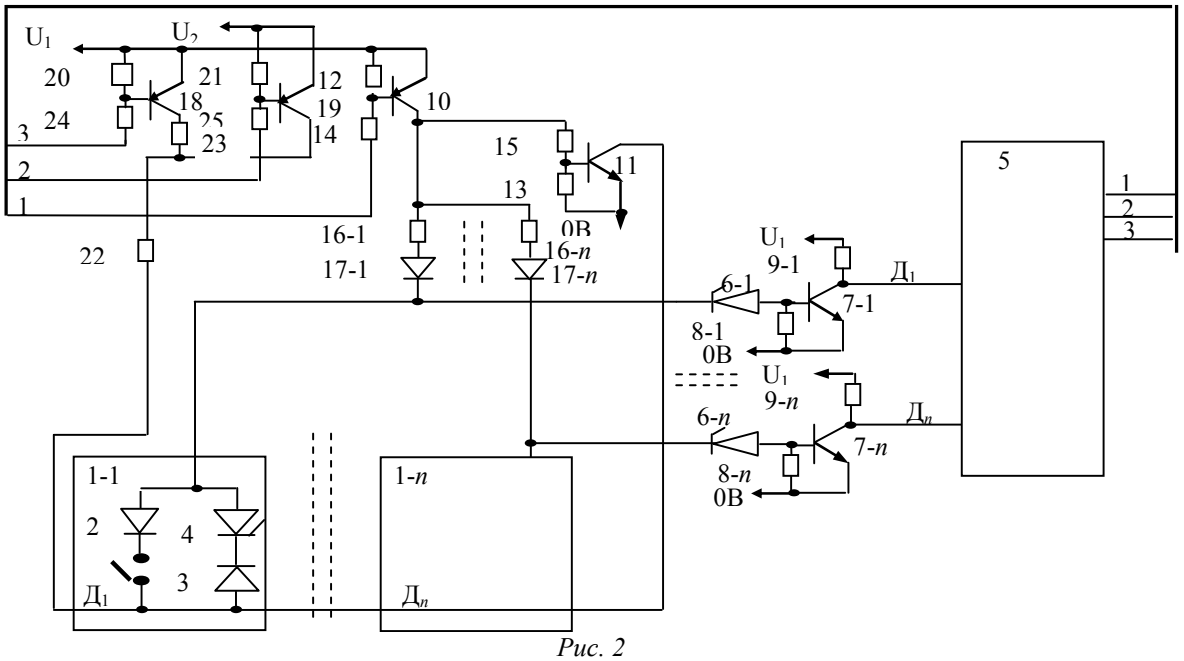

Рис. 2

Для N датчиков используются индивидуальные узлы 1-1, …, 1-n, в которые кроме контактов датчиков ($Д_1$, …, $Д_n$) введены диоды *2* и *3* и стабилитрон *4*. Контроллер ввода данных *5* воспринимает сигналы от формирователей, включающих ограничивающие стабилитроны *6*, усилители *7* и согласующие резисторы *8* и *9*. Контроллер *5* выполняет опрос состояния датчиков ТС в два этапа, формируя сигналы на выходах *1—3*. На первом этапе формируется сигнал на выходе *1*, которым переводятся в рабочее состояние усилители *10* и *11*, а на втором — усилитель *18* или *19* — в зависимости от результата, полученного на первом этапе. Если контакт датчика замкнут, сигнал от усилителя *10* проходит через цепь — резистор *16*, диоды *17* и *2*, контакт датчика — и замыкается на шину 0В через усилитель *11*. В результате сигнал на вход *7* не проходит, а контроллер *5* фиксирует на первом этапе сигнал с уровнем „1“ и формирует на втором этапе сигнал на выходе *2*. Уровень сигнала от *19* выше суммы ограничителей на стабилитронах *4* и *6*. В результате сигнал от *19* проходит через диод *3* и стабилитроны *4* и *5* на вход *7*. Контроллер *5* фиксирует уровень сигнала „0“. Таким образом, при замкнутом контакте датчика контроллер *5* формирует биимпульсную корреляционную пару сигналов „1“ и „0“.

Если контакт датчика разомкнут, на первом этапе опроса сигнал от узла *1* проходит на вход формирователя *7*, а контроллер *5* фиксирует сигнал с уровнем „0“. В этом случае на втором этапе опроса состояния датчика рабочий сигнал от *5* формируется на выходе *3*. Сигнал от контроллера переводит в рабочее состояние усилитель *18*. Уровень сигнала от усилителя *18* меньше суммы пороговых напряжений стабилитронов *4* и *6*. Поэтому сигнал на вход *7* не поступает, а контроллер *5* фиксирует сигнал с уровнем „1“. Таким образом, при замкнутом контакте датчика контроллер *5* формирует биимпульсную корреляционную пару сигналов „0“ и „1“.

Важно подчеркнуть, что предложенный метод позволяет одновременно с опросом состояния датчиков диагностировать неисправность цепи связи с датчиком, т.е. фиксировать наличие короткого замыкания или разрыва цепи.

Легко проверить, что при наличии короткого замыкания цепи связи с датчиком контроллер зафиксирует биимпульсную пару сигналов „0“ и „0“, а при разрыве цепи связи с датчиком — „1“ и „1“. На рис. 3 показаны комбинации сигналов, формируемых по предложенной методике. (В связи с тем что при неисправности цепи связи с датчиком корреляция между парой сигналов нарушается, формируемый код назван условно корреляционным).

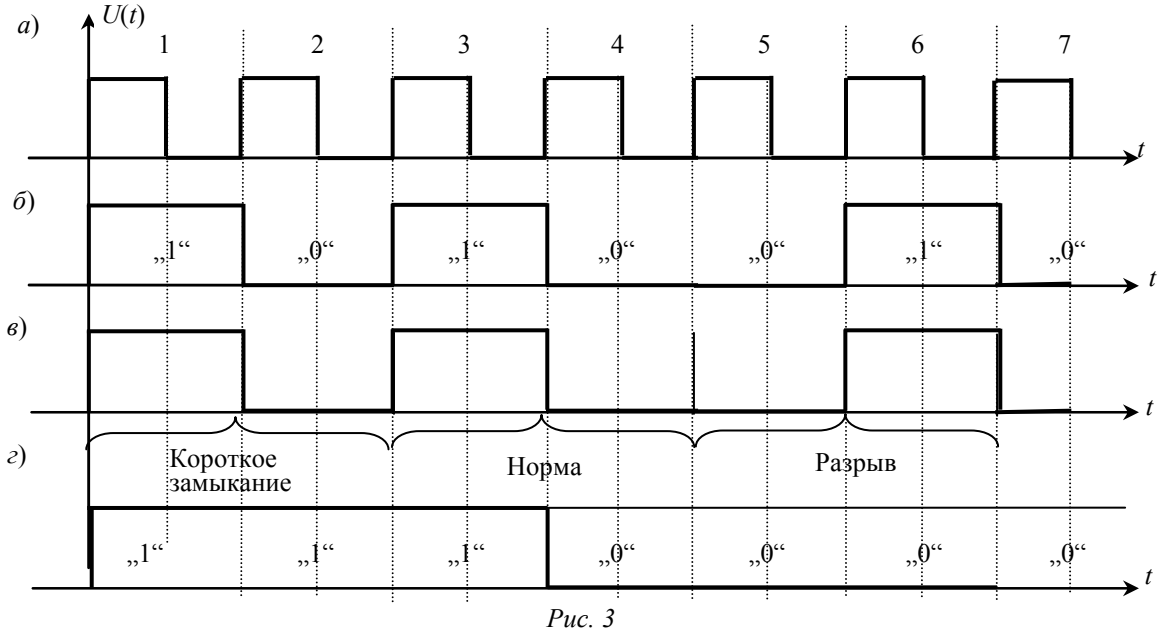

Рис. 3

Важно, что в разработанном способе кодирования инверсия второго бита пары — „условная“, она зависит от результата диагностики цепей связи с датчиками. Бит инвертируется, когда при динамическом контроле не обнаружено искажений. Только в этом случае

биимпульсный код принимает вид „10“ или „01“. При обнаружении искажений пара сигналов кода превращается в комбинацию „11“ (короткое замыкание) или „00“ (разрыв цепи связи с датчиком), давая возможность за счет двух „неразрешенных“ комбинаций определить место и вид искажения [6, 10—13].

На рис. 3, *а* приведены сигналы генератора тактовых импульсов, которыми задают последовательность кодирования. Состояние (положение) одного датчика телесигнализации преобразуют в код в двух смежных тактах, для кодирования состояния всех n датчиков используется $2n$ тактов. Традиционный способ кодирования иллюстрируется рис. 3, *б*. На каждом нечетном такте формируется первый сигнал биимпульсного кода, например, при замкнутом состояния датчика — „1“, а при разомкнутом — „0“. На каждом четном такте формируют второй сигнал кода, инвертируя сигналы нечетных тактов. Биимпульсные коды и информационное сообщение в целом не видоизменяются, если, как показано на рис. 3, *в*, например, возникает короткое замыкание в цепи связи кодера с первым датчиком или оборвется цепь связи с третьим датчиком. В результате переданное информационное сообщение окажется недостоверным. Из рис. 3, *г* видно, что для биимпульсного условно корреляционного кода при обнаружении искажений код превращается в „11“ (короткое замыкание) или в „00“ (разрыв цепи связи с датчиками). Таким образом, предложенный способ кодирования позволяет не только обнаружить неисправность, но и локализовать номер датчика и тип обнаруженной неисправности.

Методика расчета достоверности телесигнализации. Определим достоверность информации ТС при использовании предложенного метода.

При расчете достоверности, т.е. вероятности появления необнаруживаемого искажения информации, учитываются параметры всех узлов трассы доставки данных от датчика до приемника — элемента отображения (например, монитора компьютера АРМ диспетчера).

Оценим численное значение достоверности информации для случая формирования модулем

— БУКК, который в неизменном виде вводится в информационную часть сообщения;

— компонентов рабочего цикла, включая дополнительные компоненты, повышающие помехозащитные свойства информационного сообщения в целом.

Расчет достоверности канала ТС проведем при следующих начальных условиях, определяющих структуру рабочего цикла (информационной части сообщения):

n_1 — код идентификации адреса контролируемого объекта — два байта;

n_2 — код идентификации типа информационного сообщения — два байта;

n_3 — информационное поле — от 0 до 64 байт,

n_4 — поле защиты, контрольная последовательность кода — два байта.

Считая искажение каждого компонента информационного сообщения независимым, определим вероятность искажения всего сообщения как сумму вероятностей для отдельных составляющих:

$$P_{\text{н.иТС}} = P_{\text{ввТС}} + P_{\text{аТС}} + P_{\text{тТС}} + P_{\text{зТС}}, \qquad (4)$$

где $P_{\text{ввТС}}$ — необнаруживаемые искажения при вводе и одновременном кодировании для образования БУКК; $P_{\text{аТС}}$ — вероятность появления необнаруживаемого искажения кода идентификации адреса контрольной последовательности; $P_{\text{тТС}}$ — вероятность появления необнаруживаемого искажения кода идентификации типа сообщения; $P_{\text{зТС}}$ — вероятность появления необнаруживаемого искажения контрольной последовательности кода.

Вероятность появления необнаруживаемого искажения информации при вводе и одновременном кодировании:

$$P_{\text{ввТС}} = n_{\text{ТС}} P_{0/1} P_{\text{и.с}}^2 (1 - P_{\text{и.с}})^{n_{\text{ТС}}-2}, \qquad (5)$$

где $P_{0/1}$ — условная вероятность такого воздействия помехи при повторном искажении вводимого дискретного сигнала, которое противоположно воздействию при первичном искажении; $n_{\text{ТС}}$ — число разрядов кода, равное числу датчиков ТС

$$P_{\text{и.с}}^2 = P_1^2 \left(\frac{T_{\text{с}}}{T_{\text{ц.о}}} \right)^2 . \tag{6}$$

В формуле (5) введен множитель $n_{\text{ТС}}$, а не число сочетаний двойных искажений, так как для БУКК контроль пар сигналов проводится по отдельности.

При $(1 - P_{\text{и.с}})^{n_{\text{ТС}}-2} \to 1$ получим

$$P_{\text{ввТС}} = n_{\text{ТС}} P_1^2 P_{0/1} \left(\frac{T_{\text{с}}}{T_{\text{ц.о}}} \right)^2 . \tag{7}$$

Использование двухбайтной контрольной последовательности обеспечивает получение кодового расстояния ≥4. Поэтому при наложении контрольной последовательности на $P_{\text{ввТС}}$ получим

$$P_{\text{ввТС1}} = \left(n_{\text{ТС}} P_1^2 P_{0/1} \left(\frac{T_{\text{с}}}{T_{\text{ц.о}}} \right)^2 \right)^4 C_n^4 . \tag{8}$$

Учитывая длину кодов идентификации адреса контрольной последовательности, типа информационного сообщения и контрольной последовательности циклического кода, получим показатель

$$P_{\text{аТС}} + P_{\text{тТС}} + P_{\text{зТС}} = P_1^4 \left(C_{16}^4 + C_{16}^4 + C_{16}^4 \right), \tag{9}$$

тогда

$$P_{\text{н.иТС}} = \left(n_{\text{ТС}} P_1^2 P_{0/1} \left(\frac{T_{\text{с}}}{T_{\text{ц.о}}} \right)^2 \right)^4 C_n^4 + P_1^4 \left(C_{16}^4 + C_{16}^4 + C_{16}^4 \right). \tag{10}$$

Подставив в (10) числовые значения: $P_1 = 10^{-4}$, $n_{\text{ТС}} = 32$, $T_{\text{с}} = 5 \cdot 10^{-6}$ с, $T_{\text{ц.с}} = 10^{-2}$ с, $P_{0/1} = 0{,}5$, получим $P_{\text{н.иТС}} \approx 5 \cdot 10^{-13}$.

Результирующее значение вероятности появления необнаруживаемых искажений удовлетворяет наиболее жестким требованиям стандарта, причем оно практически полностью определяется вероятностью искажения дополнительных компонентов информационного сообщения, что делает актуальным использование более защищенных кодов идентификации адреса контролируемого объекта и типа сообщения.

Выводы. Применение предложенного принципа кодирования телесигнализации позволяет обеспечить требуемый высокий уровень достоверности $\sim 10^{-13}$ информации, получаемой с помощью автоматизированных систем диспетчерского контроля и управления в энергетике. Полученный показатель на несколько порядков превосходит требования стандартов и параметры, обеспечиваемые лучшими аналогами. Для реализации описанной методики в сервисы протокола IEC 61850 необходимо ввести возможность передачи сигнала состояния объекта двумя битами и описания функции ТС всеми четырьмя рабочими комбинациями, отображающими данные одного объекта контроля („включен“ — „отключен“ — „короткое замыкание цепи связи с датчиком“ — „обрыв цепи связи с датчиком“).

СПИСОК ЛИТЕРАТУРЫ

1. *Wan Jusoh W.N.S.E., Mat Hanafiah M.A., Ghani M.R.A., Raman S. H.* Remote terminal unit (RTU) hardware design and implementation efficient in different application // Proc. of the 7th Intern. Power Engineering and Optimization Conf. 2013. P. 570—573. DOI: 10.1109/PEOCO.2013.6564612.

2. *Monedero I., Biscarri F., León C., Guerrero J. I., González R., Pérez-Lombard L.* Decision system based on neural networks to optimize the energy efficiency of a petrochemical plant // Expert Systems with Applications. 2012. Vol. 39, Is. 10. P. 9860—9867.

3. *Allwood G., Wild G., Hinckley S.* Programmable logic controller optical fibre sensor interface module // Proc. of SPIE. The Intern. Society for Optical Engineering. 2011. DOI: 10.1117/12.903235.

4. *Sehgal S., Acharya V.* Effect of PLC and SCADA in boosting the working of elevator system // IEEE Students' Conf. on Electrical, Electronics and Computer Science, SCEECS 2014. Bhopal, 1—2 March 2014.

5. *Tinham B*. New directions // Plant Engineer. 2014. P. 16—17.

6. *Чжо Зо Е, Тайк Аунг Чжо, Баин А. М., Касимов Р. А*. Методика повышения эффективности межмодульных информационных обменов в автоматизированных системах управления объектами энергетики // Вести высших учебных заведений Черноземья. 2013. Т. 31, № 1. С. 49—53.

7. *Чжо Зо Е, Баин А. М., Касимов Р. А*. Методика снижения интенсивности информационных потоков интегрированных информационно-управляющих систем в энергетике // Оборонный комплекс — научно-техническому прогрессу России. 2013. № 3. С. 33—37.

8. *Li G.-J., Zhang D., Deng Q.-C., Hu L.* Design and implement of conformance test system for sub-station based on IEC61850-9-2 LE // Dianli Xitong Baohu yu Kongzhi/Power System Protection and Control. 2010. Vol. 38, Is. 6. P. 115—118.

9. *Brunner C.* Iec 61850 for power system communication // Proc. of IEEE/PES *Transmission and Distribution Conference and Exposition*. Chicago, 2008. P. 1—6.

10. *Баин А. М.* Новые теоретические подходы к созданию многофункциональных систем управления в энергетике повышенной достоверности // Фундаментальные исследования. 2014. № 3. С. 701—705.

11. *Чжо Зо Е, Баин А. М., Касимов Р. А., Гринченко Э. А*. Методика формирования рабочих циклов при проведении информационных обменов и управлении распределенными энергообъектами // Оборонный комплекс — научно-техническому прогрессу России. 2013. № 4. С. 18—23.

12. *Чжо Зо Е, Пайе Тэйн Наинг*. Автоматизированная система управления технологическими процессами в газовых потоках // Научное обозрение. 2013. № 7. С. 65—69.

13. *Лисов О. И., Чжо Зо Е, Пайе Тэйн Наинг*. Методика оптимизации управления технологическими процессами распределенных систем // Изв. вузов. Приборостроение. 2014. Т. 57, № 3. С. 26—30.

Сведения об авторе

Зо Е Чжо — канд. техн. наук, докторант; Национальный исследовательский университет „МИЭТ“, кафедра информатики и программного обеспечения вычислительных систем;
E-mail: kyawzawye.47@gmail.com

Рекомендована кафедрой информатики и программного обеспечения вычислительных систем

Поступила в редакцию 29.03.15 г.

Ссылка для цитирования: *Чжо Зо Е* Методика повышения достоверности SCADA-систем // Изв. вузов. Приборостроение. 2015. Т. 58, № 12. С. 999—1007.

A METHOD TO INCREASE SCADA-SYSTEM RELIABILITY

Zaw Ye Kyaw

National Research University of Electronic Technology, 124489, Moscow, Russia
E-mail: kyawzawye.47@gmail.com

Possibilities of increasing reliability of information obtained with the use of automated monitoring and control systems in energy production industry are qnalyzed. The necessity of coupling the procedures of information input from a sensor with message encoding is justified. New principles of coding combining two-pulse conditional correlation code first synthesized by the author, with a cyclic code are proposed. The proposed approach is reported to ensure a high level of reliability with the probability of non-detectable distortion in input-output data signals channel of ~10^{-14} which is 2-3 orders of magnitude better than the regulatory requirements. The developed method makes it possible to diagnose the fault circuit communication with the sensor, i.e., to detect a short circuit or open circuit, simultaneously with the sensor status survey.

Keywords: reliability, automated, SCADA, energy, signal combination, remote signaling, supervisory control.

Data on author

Zaw Ye Kyaw — PhD, Doctoral Student; National Research University of Electronic Technology, Department of Information and Software Computing Systems;
E-mail: kyawzawye.47@gmail.com

For citation: *Kyaw Zaw Ye* A method to increase SCADA-system reliability // Izvestiya Vysshikh Uchebnykh Zavedeniy. Priborostroenie. 2015. Vol. 58, N 12. P. 999—1007 (in Russian).

DOI: 10.17586/0021-3454-2015-58-12-999-1007