



КОММУНИКАЦИОННЫЕ ПРОТОКОЛЫ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ

Е.С. Рогова (АО «ТРЭИ»)

Российская промышленность активно развивается, и производство программируемых логических контроллеров (ПЛК) не является исключением. Как известно, основные производители зарубежных ПЛК ушли из России, и у многих производителей появилась задача замены иностранного оборудования. Российский рынок может предложить отечественные ПЛК, но проблема заключается в том, что в России практически нет ПЛК, сертифицированных в соответствии с требованиями стандартов функциональной безопасности в лабораториях, имеющих мировой авторитет, таких как TÜV SÜD Rail GmbH, Exida и др. Кроме того, сейчас сертификация в таких лабораториях невозможна из-за санкций. В связи с этим, многие производители ПЛК обращаются в российские компании по сертификации, которые гарантируют прохождение добровольной сертификации в течение нескольких недель. Заказчики ПЛК, видя наличие сертификата, подтверждающего соответствие уровням SIL 1-3 (УПБ 1-3), уверены в соответствии приобретаемого оборудования необходимым требованиям. К сожалению, на текущий момент это часто не так, и необходимо обладать определёнными знаниями, чтобы выявить эти несоответствия. В данной статье разбирается одна из важнейших составляющих функциональной безопасности ПЛК – коммуникационные протоколы для обмена данными, связанными с безопасностью. В статье показывается разница между стандартными протоколами и протоколами функциональной безопасности; разбирается обмен данными в приборных системах безопасности в промышленной автоматизации; рассматривается соответствие протоколов обмена данными требованиям функциональной безопасности на основании качественного и количественного анализа коммуникационных ошибок.

Ключевые слова: коммуникационный протокол, коммуникационный уровень безопасности, программируемый логический контроллер, уровень полноты безопасности, SIL, коммуникационные меры безопасности, МЭК 61784-3, МЭК 61508.

Введение

В соответствии с ГОСТ Р МЭК 61508, функциональная безопасность (ФБ) – это «часть общей безопасности, обусловленная применением управляемого оборудования и системы управления УО, и зависящая от правильности функционирования Э/Э/ПЭ систем, связанных с безопасностью, и других средств по снижению риска»¹. Дискретным уровнем соответствия оборудования требованиям функциональной безопасности является Уровень

Полноты Безопасности (УПБ/SIL). До введения санкций некоторые российские компании прошли сертификацию по ФБ в международных лабораториях. Например, компания АО «ТРЭИ» успешно прошла ресертификацию своей продукции на соответствие уровню SIL 3 в 2017 г. в TÜV SÜD Rail GmbH. В настоящее время всё больше производителей ПЛК демонстрируют наличие сертификата, полученного в российских компаниях по сертификации, на соответствие определённому уровню УПБ/SIL.

¹ ГОСТ Р МЭК 61508-4-2012 (IEC 61508-4: 2010). Национальный стандарт РФ. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 4. Термины и определения // Федеральное агентство по техническому регулированию и метрологии. М.: Стандартинформ, 2014.

При просмотре документации на некоторые контроллеры с таким сертификатом возникают вопросы по реальному соответствию продукции требованиям того или иного уровня SIL/УПБ. Формальная выдача сертификата на соответствие уровням SIL 1-3 (УПБ 1-3), безусловно, не является доказательством безопасности продукции (не говоря уже о SIL 4/ УПБ 4). Такие «пробелы» в безопасности обнаруживаются при изучении как самих сертификатов, выданных некоторыми российскими сертификационными компаниями, так и подтверждающих документов (например, руководство по функциональной безопасности). Формальный подход к выдаче сертификатов включает, но не ограничивается следующими примерами:

- выдача сертификата уровня SIL 3 на ПЛК, которые при данном уровне диагностики и толерантности к отказам могут достичь только уровня SIL2;
- выдача сертификата уровня SIL 3 на ПЛК, где в руководстве по функциональной безопасности на модули ввода/вывода и на мастер-модули указаны нереалистично заниженные значения показателей безопасности — PFD_{AVG}/PFH , которые просто невозможно достичь, имея представление о реальной архитектуре и комплектующих ПЛК;
- выдача сертификата уровня SIL2-SIL3 на ПЛК, где в руководстве по функциональной безопасности указаны стандартные протоколы обмена данными, но эти протоколы не могут использоваться для передачи данных, связанных с безопасностью.

Можно приводить и другие примеры, но вопросы полного соответствия ПЛК стандартам функциональной безопасности (то есть соответствия системного уровня, аппаратной и программной частей, менеджмента ФБ) не являются целью данной статьи. В данной статье предлагается проанализировать только часть возможного несоответствия требованиям ФБ, а именно, коммуникационные протоколы передачи данных в промышленной автоматизации для использования в приборных системах безопасности (ПСБ).

Например, производитель ПЛК №1 заявляет о соответствии уровню SIL 3 и описывает следующие протоколы обмена: встроенные интерфейсы по протоколам ГОСТ Р МЭК 60870-5-101 (Master/Slave), ГОСТ Р МЭК 60870-5-104 (Master/Slave), Modbus RTU (Master/Slave), Modbus TCP (Master/Slave). Производитель ПЛК №2 заявляет о соответствии уровню SIL 2 и описывает обмен данными по Modbus RTU. Производитель ПЛК №3 заявляет о соответствии уровню SIL 2 и сообщает об использовании следующих протоколов передачи данных: Modbus TCP, Modbus RTU, IEC 60870-5-104, OPC UA, Powerlink.

Ни один из протоколов, упомянутых в приведенных примерах, не является протоколом, разрешенным для передачи данных, связанных с безопасностью. Разберем далее, почему же данные протоколы нельзя применять для передачи данных, связанных с безопасностью, какие особенные требования у коммуникационных протоколов

безопасности, какими бывают коммуникационные ошибки, и зачем проводить качественный и количественный анализ коммуникационных ошибок.

Коммуникационные протоколы в промышленной автоматизации

В промышленной автоматизации используются различные протоколы данных, они отличаются по разным параметрам, начиная от назначения протокола до реализации коммуникационных уровней модели OSI [1]. Семь уровней модели OSI представлены на рис. 1 снизу вверх: 1) физический; 2) канальный; 3) сетевой; 4) транспортный; 5) сеансовый; 6) представления; 7) прикладной. Согласно ГОСТ Р МЭК 61784-3, КУБ — это «коммуникационный уровень выше прикладного уровня, включающий все необходимые меры для обеспечения безопасной передачи информации в соответствии с требованиями МЭК 61508»².

К протоколам нижнего уровня относятся сетевые соединения/интерфейсы: например, RS-485/232 (физический) или Ethernet и CAN (физический и канальный). На основе таких протоколов нижнего уровня, как RS-485, CAN, Ethernet строится большинство коммуникационных протоколов верхнего уровня, широко используемых в промышленной автоматизации. Среди них есть и стандартные протоколы передачи данных, и коммуникационные протоколы безопасности. Большинство протоколов группируется по семействам коммуникационных профилей CPF (Communication profile family), согласно IEC 61784-1-0, которые могут включать один или несколько коммуникационных профилей. Профили помогают корректно установить соответствие требованиям стандартов и «избежать распространения альтернативных реализаций, которые ограничили бы их использование, ясность и понимание»³.

Существует множество стандартных коммуникационных протоколов уровня приложения, относящихся к тем или иным коммуникационным профилям, которые можно использовать для передачи данных, не связанных с безопасностью. Например, протоколы «запрос-ответ» семейства CPF15 - Modbus TCP и Modbus RTU на основе мастер-слейв модели [2] подходят для широкого спектра приложений распределенного ввода/вывода, включая сбор данных, управление, мониторинг процессов, а также тестирование и измерения. Физический уровень Modbus RTU — это RS-485, а Modbus TCP — Ethernet.

Широко известные протоколы семейства CPF 3 Profibus и Profinet также активно используются в автоматизации. Физический уровень Profibus — это MBP (Manchester Encoded Bus Powered) или RS-485, а Profinet — Ethernet. Оба протокола используются для связи контроллеров систем управления с датчиками и исполнительными механизмами, а также для обмена с вышестоящими системами, а Profinet дополнительно используется в системах реального времени [3].

² ГОСТ Р МЭК 61784-3-2015 (IEC 61784-3: 2010). Национальный стандарт РФ. Промышленные сети. Профили. Часть 3. Функциональная безопасность полевых шин. Общие правила и определения профилей. М.: Стандартинформ, 2016.

³ IEC 61784-1-0: 2023. Industrial networks - Profiles - Part 1-0: Fieldbus profiles - General concepts and terminology // Edition 1.0. International Electrotechnical Commission. TC 65/SC 65C. 2023-03-24.

Коммуникационный уровень безопасности (КУБ/SCL)
7. Прикладной (Application)
6. Представления (Presentation)
5. Сеансовый (Session)
4. Транспортный (Transport)
3. Сетевой (Network)
2. Канальный (Data Link)
1. Физический (Physical)

Рис. 1. Уровни OSI модели

Некоторые протоколы нельзя отнести к тому или иному семейству профилей (CPF): например, протокол MQTT, широко применяющийся в области Internet of Things (IoT) или протокол CANopen, который также не относится к какому-либо семейству CPF.

Стандартные протоколы обмена используются в автоматизации только при отсутствии требований безопасности. Если же такие требования есть, необходимо использовать сертифицированные протоколы безопасности, разрабатывать свои протоколы ФБ или надстраивать КУБ на уже существующий уровень приложения в стандартном протоколе, если это возможно. Ниже приведены некоторые примеры коммуникационных протоколов безопасности.

Протокол CIP Safety из семейства CPF 2 был создан для передачи данных, связанных с безопасностью, через EtherNet/IP или DeviceNet [3]. Основанный на протоколе CIP (Common Industrial Protocol), протокол CIP Safety использует механизм производитель-потребитель для обмена данными между безопасными узлами.

Протокол Profisafe (CPF 3) на основе Ethernet используется для передачи данных, связанных с безопасностью (между модулями ПЛК, для межконтроллерного обмена, обмена данными с датчиками/актуаторами) в мастер-слейв системах.

Протокол Safety over EtherCAT (FSoE) из семейства профилей CPF 12 оптимизирован для применения в мастер-слейв системах реального времени. Физический уровень FSoE – Ethernet. Возможна инкапсуляция нескольких коммуникационных профилей.

При использовании любых коммуникационных протоколов безопасности необходимо проверять наличие и актуальность сертификатов на соответствие тому или иному уровню SIL, а при необходимости сделать верхнеуровневую оценку соответствия требованиям ФБ самостоятельно. К сожалению, при использовании западных коммуникационных протоколов безопасности в условиях санкций возникает проблема приобретения, периодического обновления программного обеспечения, а также предоставления

документации. Именно поэтому производитель отечественного ПЛК может выбрать самостоятельную разработку протокола, как это сделано, например, в контроллерах ПАЗ серии TREI-5B-04 SAFE. Для этого, помимо всего прочего, необходимо понимать, как в системах промышленной автоматизации происходит обмен данными, связанными с безопасностью.

Обмен данными в системах промышленной автоматизации

Традиционно в автоматизации определяются три основных уровня: сенсоры/датчики, логические устройства (например, ПЛК), исполнительные механизмы. Информация с датчиков поступает для обработки в логических устройствах, которые вырабатывают управляющее воздействие. В ПЛК передача данных, связанных с безопасностью (то есть данных, при нарушениях в передаче которых нарушается функция безопасности), может происходить между модулями ввода/вывода и процессорным модулем ПЛК или, например, между процессорными модулями, обеспечивая межконтроллерный обмен.

Рассмотрим пример системы SIL 3: данные о превышении уровня жидкости в резервуаре поступают с двух датчиков на резервированные модули дискретного ввода (DI); мастер-модуль выдает управляющее воздействие «Закрыть задвижку»; команда на закрытие задвижки передается в модуль дискретного вывода (DO), с которого сигнал поступает на саму задвижку. Однако между мастер-модулем и модулем вывода произошло искажение данных в сообщении, передающем команду на закрытие задвижки. Это искажение не было детектировано в модуле DO из-за низкой эффективности выбранного CRC⁴ полинома, и команда в искаженном виде передается на задвижку, которая в итоге не закрывается, а остается открытой (рис. 2), нарушая функцию безопасности. Задача коммуникационного уровня безопасности – это реализация мер безопасности, которые будут детектировать или предотвращать различные коммуникационные ошибки. Безусловно, даже при наличии КУБ коммуникационные ошибки возможны, но они будут сведены к минимуму, допустимому при том или ином уровне SIL. На рис. 2 стрелками показаны логические соединения, по которым передаются данные, связанные с безопасностью. На одно логическое соединение в стандарте IEC 61784-3 рекомендуется не превышать 1% от максимально допустимых значений PFH/PFD_{AVG}.

При рассмотрении функции безопасности необходимо также учитывать время реакции функции безопасности: если функция безопасности будет выполнена вне допустимого интервала времени, это эквивалентно невыполнению функции безопасности⁵.

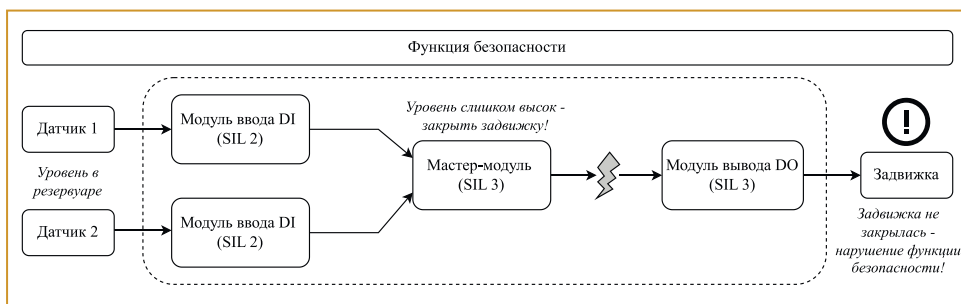


Рис. 2. Пример передачи данных в системе SIL 3

⁴ CRC (Cyclic Redundancy Check) – циклический контроль избыточности.

⁵ IEC 61784-3: 2021. Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions // Edition 4.0. International Electrotechnical Commission. TC 65/SC 65C, 2021-02-16.

В некоторых системах скорость передачи и время реакции или ответа зависят от числа участников. Если скорость передачи и время реакции или ответа связаны с безопасностью, может возникнуть необходимость ограничить число участников. Для примера, рассмотренного на рис. 2, время реакции (ВР) функции безопасности может рассчитываться следующим образом:

$$BP_{\text{Функция Безопасности}} = \max(BP_{\text{Датчик 1}}, BP_{\text{Датчик 2}}) + BP_{\text{Модуль ввода DI}} + BP_{\text{Сеть}} + BP_{\text{Мастер-модуль}} + BP_{\text{Сеть}} + P_{\text{Модуль ввода DO}} + BP_{\text{Задвижка}} \quad (1)$$

При этом, время реакции сети ($BP_{\text{Сеть}}$) может рассчитываться отдельно, а может быть учтено в соответствующих модулях контроллера, но не может быть проигнорировано.

Модели коммуникационных каналов

Согласно ГОСТ Р МЭК 61508-2, методы и средства, необходимые для обеспечения требуемой меры отказов (такой как остаточная интенсивность отказов) коммуникационного процесса, должны быть реализованы с использованием двух возможных подходов: белого или черного канала (рис. 3). При этом белый коммуникационный канал (вместе со всеми компонентами внутри канала) должен быть спроектирован и реализован в соответствии с требованиями стандартов ГОСТ Р МЭК 61508 и ГОСТ Р МЭК 61784-3 или ГОСТ Р МЭК 62280⁶. Примером протокола, использующего модель белого канала, является стандарт CANopen Safety⁷. Черный же коммуникационный канал допускает, чтобы части канала, за исключением концов черного канала, не были разработаны/не проходили подтверждение в соответствии с ГОСТ Р МЭК 61508. В этом случае, согласно IEC 61508-2, меры, необходимые для обеспечения обработки отказа коммуникационного процесса, должны быть реализованы в Э/Э/ПЭ подсистемах или элементах, связанных с безопасностью, которые взаимодействуют с коммуникационным каналом в соответствии с МЭК 61784-3 или МЭК 62280.

Таким образом, модель черного канала допускает применение обычных «небезопасных» сетевых устройств (свитчей, коммутаторов), через которые без изменения проходят данные безопасности, так как любые ошибки, которые могут возникнуть, в том числе и при прохождении данных через такие устройства, будут детектированы на концах черного канала. Этот принцип лежит в основе всех коммуникационных протоколов безопасности, чьи коммуникационные профили определены в стандартах серии IEC 61784. Внутри черного канала безопасное сообщение должно проходить без изменений

от начальной до конечной точки, и только на конце черного канала сообщение открывается и проверяется на ошибки. Принцип черного канала работает только в том случае, когда оба конца канала соответствуют описанным требованиям и реализуют обработку коммуникационных ошибок. Согласно IEC 61508-2, выбирая модель белого канала, необходимо удостовериться, что все устройства внутри белого канала (включая любые сетевые устройства) должны быть «безопасными». Интенсивности отказов всех устройств внутри белого канала, безусловно, должны быть учтены при расчете показателей безопасности (MTTF, PFD_{AVG}, PFH) контура приборной системы безопасности.

Анализ коммуникационных ошибок

Анализ ошибок коммуникационного уровня безопасности может быть качественным и количественным. Этап качественного анализа обязателен: без него не имеет смысла начинать количественный анализ.

Качественный анализ

Качественный анализ заключается в анализе типов коммуникационных ошибок, которые могут возникнуть в КУБ того или иного протокола, и в сопоставлении мер безопасности этим коммуникационным ошибкам. На одну коммуникационную ошибку должна быть реализована хотя бы одна мера безопасности, которая может эту ошибку детектировать или предотвращать: для каждого протокола составляется своя матрица коммуникационных ошибок (табл. 1). На этапе количественного анализа может оказаться, что полнота мер безопасности не достаточна, и необходимо либо добавить, либо изменить уже существующие меры безопасности. При этом важно понимать, что такая работа проводится на коммуникационном уровне безопасности. Например, есть CRC, закрывающая фрейм на канальном уровне протокола, но по требованиям стандарта МЭК 61784-3 необходимо обеспечить целостность кадра безопасности также и на уровне КУБ.

Согласно IEC 61784-3, под ошибками искажения понимаются ошибки целостности данных, передаваемых в сообщении. Обычно ошибки искажения вызваны

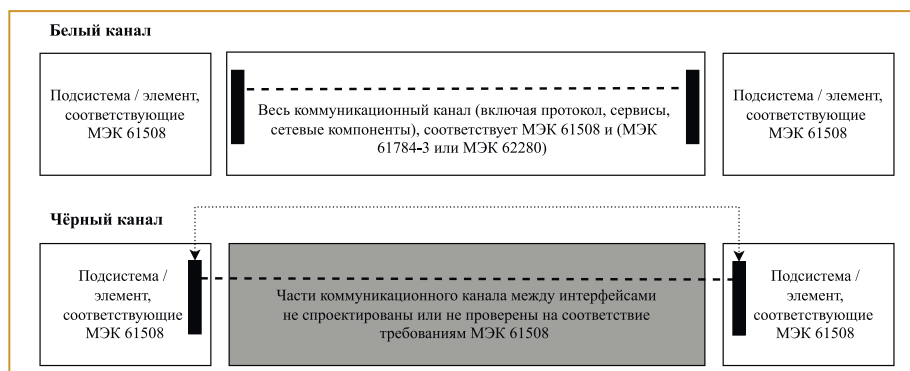


Рис. 3. Модели каналов передачи данных, связанных с безопасностью, согласно IEC 61508-2 (ГОСТ Р МЭК 61508-2)

⁶ ГОСТ Р МЭК 61508-2-2012 (IEC 61508-2: 2010). Национальный стандарт РФ. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч.2. Требования к системам // Федеральное агентство по техническому регулированию и метрологии. М.: Стандартинформ, 2014.

⁷ EN 50325-5. Industrial communications subsystem based on ISO 11898 (CAN) for controller-device interfaces - Part 5: Functional safety communication based on EN 50325-4. European standard, July 2010.

Таблица 1. Пример матрицы коммуникационных ошибок

Коммуникационные ошибки	Меры безопасности							
	Номер последовательности	Метка времени	Ожидание по времени	Аутентификация связи	Ответное сообщение	Обеспечение целостности данных	Резервирование с перекрестным сравнением	Различные системы обеспечения целостности данных
Искажение						x	x	
Непреднамеренное повторение	x	x					x	
Неверная последовательность	x	x					x	
Потеря	x						x	
Недопустимая задержка		x	x					
Внесение (вставка)	x	x		x			x	
Подмена («маскарад»)				x				x
Адресация				x				

ошибками в среде передачи или помехами. Непреднамеренное повторение — это ошибочное повторение сообщений. При неверной последовательности сообщения безопасности из определенного источника следуют в ненадлежащем порядке, нарушая предварительно определенную последовательность. При потере сообщение или подтверждение не получено. Недопустимая задержка выражается в том, что время прибытия сообщения выходит за пределы разрешенного периода ожидания (таймаута). Такие ошибки происходят обычно из-за ошибок в среде передачи, перегруженных линий передачи, помех или из-за задержки в активных сетевых элементах (коммутаторах, маршрутизаторах и т.д.). Внесение (вставка) вызвана неисправностью или помехами, из-за которых получено сообщение, относящееся к неожиданному или неизвестному источнику. Если из-за неисправности или помех сообщение от источника, не связанного с безопасностью, интерпретируется таким образом, что оно воспринимается как от действительного источника, связанного с безопасностью, это подмена («маскарад»). Таким образом, данные, не связанные с безопасностью, будут получены участником, связанным с безопасностью, который затем будет рассматривать их как связанные с безопасностью. Неверная адресация означает, что сообщение, связанное с безопасностью, доставляется неправильно участнику, связанному с безопасностью, который затем воспринимает полученные данные, как предназначенные именно ему (IEC 61784-3).

Отметим, что меры детектирования коммуникационных ошибок, описанных выше, могут быть разными для разных протоколов. Тем не менее, необходимо понимать, что, например, добавление CRC никак не поможет детектировать потерю или задержку сообщения, а номер последовательности бессилён против ошибок адресации. Резервирование с побитным перекрестным сравнением способно детектировать большое число коммуникационных ошибок.

Однако не всегда возможно надстроить коммуникационный уровень безопасности. Существуют протоколы, в которых нельзя реализовать требуемый набор мер безопасности даже на качественном уровне или такая реализация приведет к нежелательным последствиям. В качестве примера можно взять протокол MQTT, в котором

не предусмотрено ожидание по времени для каждого фрейма, а также требуются дополнительные меры по организации правильной последовательности фреймов, что сильно сказывается на производительности. Если в протоколе отсутствует детектирование каких-либо коммуникационных ошибок, это значит, что требования безопасности нарушены.

Количественный анализ

Количественный анализ коммуникационных ошибок в разрабатываемой системе ПЛК проводится согласно требованиям ГОСТ Р МЭК 61784-3 или ГОСТ Р МЭК 62280 (МЭК 61508-2, п. 7.4.11.2). В данной статье представлен обзор количественного анализа согласно ГОСТ Р МЭК 61784-3, который заключается в оценке интенсивности остаточной коммуникационной ошибки.

При расчете контура безопасности рекомендуется, чтобы общая остаточная ошибка для одного логического соединения не превышала 1 % от предельно допустимого значения PFH/PFD_{AVG} . Максимально разрешенные величины общей интенсивности остаточных коммуникационных ошибок на одно логическое соединение функции безопасности приведены в табл. 2. При этом в IEC 61784-3 сказано, что итоговые значения PFH/PFD_{AVG} для каждого устройства безопасности должны включать PFH/PFD_{AVG} логического соединения функции безопасности. При соблюдении «правила одного процента» данный вклад может быть пренебрежимо мал. Однако требования к расчету интенсивностей остаточных ошибок ужесточились в четвертом издании стандарта IEC 61784-3 (2021), и некоторые известные зарубежные производители были вынуждены вносить изменения в уже разработанные ими протоколы безопасности.

Согласно стандарту IEC 61784-3, общая интенсивность остаточной ошибки коммуникационного канала безопасности на одно логическое соединение состоит из четырех слагаемых:

$$\lambda_{SC} = RR_I + RR_T + RR_M + RR_A, \tag{2}$$

где RR_I — интенсивность остаточной ошибки целостности, RR_T — интенсивность остаточной ошибки своевременности, RR_M — интенсивность остаточной ошибки маскарада, RR_A — интенсивность остаточной ошибки

Таблица 2. Соотношение между уровнем SIL и величиной λ_{SC} (IEC 61784-3)

SIL (УПБ)	PFH, [ч ⁻¹]	Максимально разрешенная величина остаточной ошибки на одно логическое соединение функции безопасности (λ_{SC} , [ч ⁻¹])
4	$< 10^{-8}$	$< 10^{-10}$
3	$< 10^{-7}$	$< 10^{-9}$
2	$< 10^{-6}$	$< 10^{-8}$
1	$< 10^{-5}$	$< 10^{-7}$

подлинности, λ_{SC} – общая интенсивность остаточной ошибки (в час) коммуникационного канала безопасности на одно логическое соединение.

В четвертом издании стандарта IEC 61784-3 остро поставлен вопрос расчета RR_I . Формула для расчета в предыдущем издании IEC 61784-3 была пересмотрена. Использование формулы из предыдущего издания стандарта может стать причиной серьезной недооценки величины RR_I и, как результат, ложного соответствия требованиям того или иного УПБ. В четвертом издании коэффициент распределения кода A , предлагается находить посредством компьютерной симуляции или с помощью математического анализа, что и является основной сложностью. Также в четвертом издании стандарта IEC 61784-3 возникают требования по расчету интенсивностей остаточных ошибок своевременности RR_T , подлинности RR_A и маскировки RR_M , которых не было в предыдущем издании. Если общая интенсивность остаточной ошибки не соответствует требованиям SIL, то возникает необходимость улучшения эффективности коммуникационных мер безопасности: это может быть, например, выбор другого полинома CRC, увеличение битности номера последовательности и др.

В стандартных протоколах обмена данными нет требований безопасности, и даже если на качественном уровне все необходимые коммуникационные меры безопасности присутствуют, то на количественном уровне полноты этих мер может быть недостаточно. Именно поэтому в руководстве по безопасности на ПЛК должен быть указан коммуникационный протокол безопасности, его КУБ, качественный анализ и результаты количественного анализа коммуникационных ошибок. Если этого нет в руководстве по ФБ, то необходимо запросить документ, в котором необходимая информация присутствует. Это может быть спецификация коммуникационного уровня безопасности протокола или выдержка из него. Если производитель ПЛК не имеет данной информации, то, скорее всего, используется стандартный протокол передачи данных, и о соответствии требованиям безопасности говорить не приходится.

Заключение

Коммуникационные протоколы должны удовлетворять требованиям ФБ при их использовании с целью передачи данных, связанных с безопасностью. В статье была показана разница между стандартными протоколами

и протоколами безопасности, представлен пример передачи данных в контуре безопасности, рассмотрены качественный анализ и общие требования к количественному анализу коммуникационного уровня безопасности. Показано, что стандартные протоколы передачи данных нельзя применять в приборных системах безопасности для обмена данными, связанными с безопасностью. При этом, на основе стандартного протокола бывает возможно надстроить коммуникационный уровень безопасности, доказав качественно и количественно соответствие требованиям безопасности в отношении предотвращения и детектирования коммуникационных ошибок.

Проектантам систем безопасности и заказчикам ПЛК для систем ПАЗ важно знать, что наличие сертификата SIL1-3, к сожалению, не всегда означает соответствие продукта требованиям функциональной безопасности. В данной статье описаны пункты, на которые нужно обращать внимание в части коммуникационных протоколов при обмене данными, связанными с безопасностью, а также указана информация, которая должна быть предоставлена производителем в руководстве по безопасности или в других документах по запросу. ПЛК с сертификатом SIL1-3 не может использовать Modbus, Profinet и другие стандартные коммуникационные протоколы для обмена данными, связанными с безопасностью. Автор призывает сделать переход на российские ПЛК безопасным не только на бумаге, но и в действительности, и обратить внимание на функциональную безопасность, ведь эти ПЛК будут использоваться на заводах, фабриках, электростанциях и других объектах автоматизации в России.

Данная работа может быть продолжена в направлении количественной оценки интенсивности остаточных коммуникационных ошибок, а именно, в части сравнения результатов симуляции с аналитическими результатами, полученными путем применения упрощенной формулы вычисления интенсивности остаточных ошибок целостности.

Список литературы

1. Zimmerman H. OSI reference model - the ISO model of architecture for Open Systems Interconnection // Invited paper. IEEE Transactions on Communications. Vol. com-28, No. 4, April 1980.
2. Тимаев А.А. Промышленные сети. Уч. пособие. Екатеринбург. Издательство Уральского университета, 2020.
3. Industrial Ethernet Facts. System comparison. The 5 major technologies. 2nd Edition. Issue 2, February 2013.

Рогова Елена Сергеевна – канд. техн. наук, инженер по функциональной безопасности, АО «ТРЭИ». E-mail: e.rogova88@gmail.com