

## КОЛИЧЕСТВЕННЫЙ АНАЛИЗ ОШИБОК В КОММУНИКАЦИОННЫХ ПРОТОКОЛАХ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

А.С. Рогов, Е.С. Рогова (ООО "ФАНКСЭЙФЕТИ")

В четвертом издании международного стандарта IEC 61784-3:2021 по функциональной безопасности полевых шин внесены существенные изменения в методику анализа коммуникационных ошибок: добавлены требования количественной оценки ошибок своевременности, подлинности и маскировки, а также доказательства эффективности применяемых CRC-полиномов путем точного расчета вероятности остаточных ошибок целостности данных. Эти изменения потребовали корректировки расчета интенсивности остаточных ошибок и пересмотра многих зарубежных протоколов функциональной безопасности, так как прежние подходы давали заниженные (оптимистичные) оценки коммуникационных ошибок, что приводило к ложному соответствию требованиям функциональной безопасности. Действующий российский стандарт ГОСТ Р МЭК 61784-3-2015 основан на устаревшем втором издании IEC 61784-3:2010 и не учитывает ключевые изменения четвертого издания. В статье анализируются необходимость и причины появления новых требований четвертого издания, демонстрируется возможность практической реализации обновленных расчетов интенсивности остаточных ошибок с помощью разработанного авторами статьи программного обеспечения. Результаты исследования подтверждают необходимость скорейшего обновления национального стандарта в соответствии с актуальными международными требованиями.

Ключевые слова: функциональная безопасность, коммуникационный протокол, коммуникационный уровень безопасности, уровень полноты безопасности, коммуникационные меры безопасности, CRC-полиномы, АСУТП.

### ВВЕДЕНИЕ

Международный стандарт IEC 61784-3 регламентирует принципы обеспечения функциональной безопасности при передаче данных на основе подхода, представленного в комплексе стандартов IEC 61508 (ГОСТ Р МЭК 61508) [1, 2, 3]. В нем рассматриваются безопасная передача данных, коммуникационные уровни безопасности, возможные коммуникационные ошибки и методы их детектирования и предотвращения. Стандарт также определяет коммуникационные профили, удовлетворяющие требованиям функциональной безопасности (FSCP, Functional Safety Communication Profiles).

В промышленной автоматизации помимо производителей оборудования (например, программируемых логических контроллеров), коммуникационные протоколы

функциональной безопасности интересуют также проектантов систем безопасности и системных интеграторов, так как от времени реакции протокола и корректности определенного значения  $PFD_{avg}/PFH$  сетевой составляющей зависит, будет ли выполнена функция безопасности ПСБ (приборной системы безопасности) или нет. Отметим, что простое добавление циклического избыточного кода CRC (Cyclic Redundancy Check) к передаваемым данным не делает протокол безопасным, как думают некоторые разработчики и инженеры АСУТП. Протоколы функциональной безопасности (ФБ) отличаются от стандартных протоколов, прежде всего, наличием так называемого коммуникационного уровня безопасности (КУБ/SCL), в котором реализуются требуемые коммуникационные меры безопасности. Отсутствие КУБ или отсутствие полноты реализованных мер безопасности в КУБ сказывается на безопасности

## ОСНОВНЫЕ ИЗМЕНЕНИЯ В ЧЕТВЕРТОМ ИЗДАНИИ IEC 61784-3

данных, передаваемых посредством протокола, что в конечном счете является причиной несрабатывания функции безопасности из-за недетектированных коммуникационных ошибок. Основные коммуникационные ошибки определяются в стандарте ГОСТ Р МЭК 61784-3 (IEC 61784-3): это ошибки искажения данных, непреднамеренного повторения, неверной последовательности, потери, недопустимой задержки, внесения (вставки), подмены (маскарада) и адресации [1, 2, 3].

Работу над стандартом IEC 61784-3 ведет рабочая группа IEC TC 65/SC65C WG12. На сайте IEC представлены издания стандарта IEC 61784-3 в хронологическом порядке с момента выпуска первого издания IEC 61784-3 в 2007 г. (таблица).

Четвертое издание стандарта было выпущено в феврале 2021 г., однако до сих пор не переведено на русский язык и не адаптировано в России. На момент публикации данной статьи в России действует ГОСТ Р МЭК 61784-3-2015 [2], который соответствует второму изданию IEC 61784-3:2010 [3]. Разница между вторым и четвертым изданиями IEC 61784-3 заключается не только в некоторых деталях по проведению качественного анализа коммуникационных ошибок, но и в существенных изменениях, касающихся количественного анализа коммуникационных ошибок.

В первых двух изданиях стандарта IEC 61784-3 количественно рассматривались исключительно ошибки целостности. Скорректированная расширенная модель оценки (TADI) была введена в качестве справочного приложения в третьем издании, которое было выпущено в мае 2016 г. Именно тогда было предложено в качестве рекомендаций, не обязательных к выполнению, включать в количественный анализ коммуникационных ошибок все ошибки из расширенной модели TADI. Однако обязательной для количественной оценки коммуникационных ошибок расширенная модель TADI стала только в четвертом издании IEC 61784-3, которое было опубликовано в феврале 2021 г. Работа над стандартом ведется и сейчас: например, в апреле 2024 г. были выпущены поправки (IEC 61784-3:2021+AMD1:2024 CSV), которые планируется включить в пятое издание стандарта.

В следующих разделах статьи рассматриваются основные нововведения четвертого издания IEC 61784-3, связанные с количественным анализом коммуникационных ошибок, а также демонстрируется практическая реализуемость количественного анализа.

### Модель TADI

С введением модели TADI общая интенсивность остаточных коммуникационных ошибок (определяемая в IEC 61784-3 как «статистическая интенсивность, с которой меры безопасности КУБ не обнаруживают ошибки» [1]) была дополнена новыми количественными составляющими. Помимо интенсивности остаточных ошибок целостности данных  $RR_I$ , определенной еще во втором издании, модель включает:

$RR_T$  — интенсивность остаточных ошибок своевременности;

$RR_A$  — интенсивность остаточных ошибок подлинности;

$RR_M$  — интенсивность остаточных ошибок маскарада.

Общая интенсивность остаточных ошибок  $\lambda_{SC}$  рассчитывается как сумма всех компонентов:

$$\lambda_{SC} = RR_I + RR_T + RR_A + RR_M. \quad (1)$$

И своевременность (T, timeliness), и подлинность (A, authenticity), и целостность данных (DI, data integrity) — это общие свойства безопасности, которые требуют детектирования соответствующих коммуникационных ошибок (рис. 1).

Своевременность (T) требует детектирования недопустимой задержки, непреднамеренного повторения, неправильной последовательности и потери сообщений. В четвертом издании приводится пример вычисления интенсивности остаточной ошибки своевременности  $RR_T$ . Для ее вычисления, помимо прочего, необходимо знать такие показатели, как толерантность к ошибкам (то есть сколько раз подряд произойдет коммуникационная ошибка прежде чем КУБ перейдет в безопасное состояние), число запоминающих устройств (устройств, хранящих сообщения в памяти), и др. Таким образом, по причине высокого значения  $RR_T$  могут возникнуть определенные ограничения на число коммутаторов внутри черного канала, чего не было во втором издании стандарта. Также значение  $RR_T$  зависит от разрядности номера последовательности как меры по детектированию ошибок своевременности. Если во втором издании было достаточно качественного наличия номера последовательности, то в четвертом издании учитывается также число

Таблица. Издания стандарта IEC 61784-3 [5]

Издание	Дата	Публикация	Статус	
4	4.1	2024-04-19	IEC 61784-3:2021+AMD1:2024 CSV	Действует
	4.0	2024-04-19	IEC 61784-3:2021/AMD1:2024	Действует
	<b>4.0</b>	<b>2021-02-16</b>	<b>IEC 61784-3:2021</b>	<b>Действует</b>
3	3.1	2017-08-04	IEC 61784-3:2016+AMD1:2017 CSV	Пересмотрен
	3.0	2017-08-04	IEC 61784-3:2016/AMD1:2017	Пересмотрен
	3.0	2016-05-13	IEC 61784-3:2016	Пересмотрен
	3.0	2016-05-13	IEC 61784-3:2016 RLV	Пересмотрен
2	<b>2.0</b>	<b>2010-06-29</b>	<b>IEC 61784-3:2010</b>	<b>Пересмотрен</b>
1	1.0	2007-12-14	IEC 61784-3:2007	Пересмотрен

бит этого поля в сообщении с безопасными данными.

Подлинность (A) требует детектирования ошибок адресации и вставки. Таким образом, приемник сообщений должен принимать только те данные безопасности, которые получены от аутентифицированного (подлинного) источника сообщений. Аутентификация предотвращает обработку данных безопасности из сообщения, которое не предназначено для данного получателя. В случае передачи A-кода явным образом, битовые ошибки в полученном коде аутентификации уже учитываются при расчете остаточных ошибок целостности. В результате  $RR_A$  часто (где это применимо) имеет значение 0.

Не смотря на то, что ошибки маскарата (подмены) не включены в TADI модель, они включены в количественную оценку интенсивности остаточных ошибок. Ошибки маскарата возникают в том случае, когда из-за сбоя или помехи сообщение от источника, не связанного с безопасностью, воспринимается относящимся к безопасности участником как сообщение от источника, связанного с безопасностью [1]. В целом, небезопасные сообщения с высокой вероятностью будут обнаружены КУБ, поскольку они должны соответствовать всем предварительным условиям (своевременность, подлинность и целостность данных). Именно поэтому при расчете общей интенсивности остаточных коммуникационных ошибок маскарата зачастую дает пренебрежимо малый вклад. По этой же причине под расширенной моделью оценки часто понимают только ошибки T, A, DI (собственно, TADI модель), не называя явным образом ошибки маскарата.

Расчет интенсивностей остаточных ошибок своевременности, подлинности и маскарата обычно выполняется путем подстановки параметров коммуникационного протокола и характеристик черного канала в соответствующие формулы стандарта [1]. Однако разработчики часто сталкиваются со значительными сложностями при вычислении интенсивности остаточных ошибок целостности, что обуславливает необходимость отдельного рассмотрения данного вопроса в настоящей работе.

Для обеспечения целостности данных (DI) необходимо обнаружение искажения данных. Среди методов контроля целостности данных широкое распространение в промышленных протоколах получил циклический избыточный код (CRC). Его популярность обусловлена высокой надежностью, эффективностью и относительной простотой программно-аппаратной реализации. Эффективность контроля целостности данных может быть повышена за счет

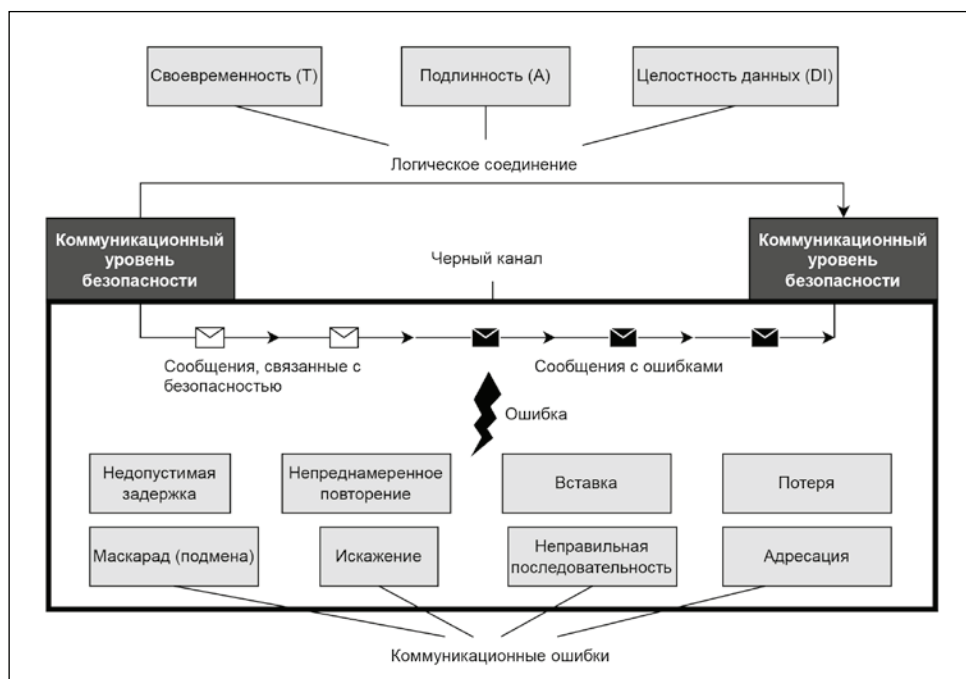


Рис. 1. Коммуникационные ошибки в черном канале согласно модели TADI

применения дополнительных мер, таких как: дублирование с побитовым перекрестным сравнением, передача сообщений с повторением, подтверждение приема с возвратом исходных данных и др. Требования стандарта к оценке интенсивности остаточных ошибок целостности  $RR_I$  претерпели существенные изменения в четвертом издании и рассмотрены ниже.

#### Выбор CRC-полинома и оценка остаточной ошибки целостности

Согласно действующему четвертому изданию международного стандарта IEC 61784-3:2021 [1], вклад интенсивности остаточной ошибки целостности  $RR_I$  в интенсивность общей коммуникационной остаточной ошибки  $\lambda_{SC}$  равен:

$$RR_I = RP_I \times \nu \times RP_{FSCP_I}, \quad (2)$$

где  $RP_I$  — вероятность остаточной (то есть необнаруженной) ошибки целостности,  $\nu$  — максимальное число безопасных сообщений, проверенных принимающим КУБ за 1 час (частота передачи безопасных сообщений),  $RP_{FSCP_I}$  — вероятность остаточной ошибки для других мер целостности (при наличии таковых), уникальных для FSCP [1].

И второе (IEC 61784-3:2010 / ГОСТ Р МЭК 61784-3-2015) [2, 3], и четвертое издание стандарта IEC 61784-3:2021 [1] приводят общую формулу расчета вероятности остаточной ошибки целостности данных  $RP_I = R_{CRC}$  для методов обнаружения ошибок на основе CRC в двоичном симметричном канале (binary symmetric channel, BSC):

$$R_{CRC}(P_e) = \sum_{i=1}^n A_i \times P_e^i \times (1 - P_e)^{n-i}, \quad (3)$$

где  $A_i$  — коэффициент распределения кода (определяемый либо компьютерной симуляцией, либо математическим

анализом для всех значений  $i=1, 2, \dots, n$ );  $n$  — число бит в кодовом блоке, включая сигнатуру CRC;  $P_e$  — вероятность битовой ошибки, то есть вероятность получения бита с неверным значением.  $R_{CRC}$  — вероятность того, что на пути передачи данных в коммуникационном канале произошла (хотя бы одна) битовая ошибка и она не была обнаружена получателем средствами используемого полинома CRC. Расчет  $R_{CRC}$  по формуле (3) сводится к вычислению коэффициентов  $A_i$  ( $i=1, 2, \dots, n$ ). Коэффициент распределения кода  $A_i$  определяется как число кодовых слов длиной  $n$ , вес Хэмминга которых равен  $i$  для используемого CRC-полинома. Иными словами,  $A_i$  равен числу кодовых слов, содержащих ровно  $i$  единичных («1») бит. Таким образом, для непосредственного вычисления  $A_i$  необходимо перебрать  $2^k$  кодовых слов, где  $k$  — число информационных бит в кодовом блоке (без сигнатуры CRC). С увеличением размера передаваемой информации  $k$  такая процедура становится практически нереализуемой: например, при  $k=1000$  бит необходимо проверить  $2^{1000} \approx 10^{300}$  кодовых слов.

Однако во втором издании (IEC 61784-3:2010 / ГОСТ Р МЭК 61784-3-2015) [2, 3] показано, что для определенного класса так называемых «правильных»<sup>1</sup> ("proper") CRC-полиномов применима аппроксимация коэффициента распределения кода  $A_i$  с весовым коэффициентом  $2^{-r}$ , так что величина  $R_{CRC}$  может быть вычислена приближенно:

$$R_{CRC}(P_e) \approx 2^{-r} \sum_{k=d_{min}}^n \binom{n}{k} P_e^k (1 - P_e)^{n-k}, \quad (4)$$

где  $r$  — число бит CRC, добавленных к сообщению в качестве CRC-сигнатуры для обнаружения ошибок;  $d_{min}$  — минимальное расстояние Хэмминга для кодового блока длины  $n$  бит и полинома CRC (CRC обнаруживает до  $(d_{min} - 1)$  ошибок). Также объясняется, что данная аппроксимация может дать меньшие (оптимистичные) значения вероятности возникновения остаточных ошибок, чем точные вычисления (3). Однако для высокой вероятности битовых ошибок  $P_e$  (значение, близкое к 0,5) наихудшим значением будет  $2^{-r}$ . Второе издание настоятельно рекомендует применять именно «правильные» полиномы. «Правильный» CRC-полином — это такой полином, для которого  $R_{CRC}(P_e)$  растет монотонно с ростом  $P_e$  для  $0 < P_e < 0,5$  [6]. При этом проверять полином на правильность необходимо для всех используемых в коммуникационном протоколе размеров кодового блока  $n$ : если полином является правильным для заданной длины данных  $n$ , он может оказаться неправильным для других длин (как меньших, так и больших). Проверка полиномов на правильность является отдельной аналитической задачей, требующей от инженеров соответствующей математической подготовки [6]. Рекомендации по проверке полиномов на правильность второе издание стандарта не приводит.

<sup>1</sup> Стандарт IEC 61784-3 оперирует терминами "proper/improper polynomial", которые в русскоязычном издании ГОСТ Р МЭК 61784-3-2015 были переведены как «образующий/не образующий полином». Авторы настоящего исследования полагают, что такой перевод может вызывать терминологическую путаницу, и в дальнейшем изложении используют более семантически точные эквиваленты «правильный/неправильный полином».

Таким образом, во втором издании требуется, чтобы разработчики коммуникационных протоколов безопасности рассчитывали интенсивность остаточных ошибок целостности. Однако в нём приведены методы расчёта только для узкого подкласса CRC-полиномов. Кроме того, отсутствие универсальных методов расчета интенсивности для произвольных CRC-полиномов может спровоцировать некорректное применение аппроксимационной формулы (4), включая ее использование для «неправильных» полиномов.

В четвертом издании IEC 61784-3 [1] формула (4) была удалена, поскольку коэффициенты распределения кода  $A_i$  в любом случае должны быть рассчитаны для подтверждения правильности CRC-полинома, и аппроксимационная формула может давать излишне оптимистичные результаты. Соответственно, была также исключена рекомендация использовать «правильные» полиномы. Четвертое издание обязывает проводить точный расчет  $R_{CRC}$  по формуле (3) для всех используемых в протоколе размеров кодовых блоков  $n$ , а также приводит ссылки на методы расчета. В следующем разделе показано, что точный расчет  $R_{CRC}$  реализуем на практике.

Важной частью оценки интенсивности остаточной ошибки целостности  $RR_I$  является выбор значения вероятности битовой ошибки  $P_e$ , для которого будет вычислена величина вероятности остаточной ошибки целостности  $RP_I = R_{CRC}(P_e)$ . И второе, и четвертое издание стандарта определяют верхнюю границу ( $10^{-2}$ , если не обосновано применение меньшего значения) диапазона вероятности битовой ошибки, внутри которого следует оценивать эффективность используемых методов обнаружения ошибок целостности. Однако, если второе издание предписывает выполнять оценку  $R_{CRC}$  при значении  $P_e$ , равным  $10^{-2}$ , то согласно четвертому изданию необходимо убедиться, что требуемый уровень вероятности остаточной ошибки целостности достигнут при всех значениях  $P_e$  вплоть до  $10^{-2}$ . Такое различие в требованиях связано с тем, что второе издание предполагает применение «правильных» CRC-полиномов, для которых  $R_{CRC}$  растет монотонно с ростом  $P_e$  и, следовательно, имеет максимум в крайней точке  $P_e = 10^{-2}$  диапазона значений  $P_e \leq 10^{-2}$ . Четвертое издание не исключает применение «неправильных» CRC-полиномов, для которых функция  $R_{CRC}(P_e)$  не является монотонно растущей и может иметь максимум во внутренней точке  $P_e < 10^{-2}$  диапазона значений  $P_e \leq 10^{-2}$ . В стандарте также приводятся результаты исследований, согласно которым для анализа поведения функции  $R_{CRC}(P_e)$  в качестве нижней границы  $P_e$  достаточно взять значение  $2/n$ . По этой причине в четвертом издании требуется вычислять  $R_{CRC}$  в множественных точках  $P_e$  в диапазоне  $[2/n; 0,01]$  (по крайней мере, в точках  $2/n, 4/n, 8/n$  и так далее до 0,01). Например, CRC-полином 0x1f1922815 является «правильным» для  $n=512$  и «неправильным» для  $n=2048$  и  $n=12000$  бит (рис.2). Следовательно, для оценки  $RR_I$  для  $n=512$  следует использовать значение  $R_{CRC}$  при  $P_e=0,01$ , а для  $n=2048$  и  $n=12000$  — максимальные значения  $R_{CRC}$  в диапазоне

$[2/n; 0,01]$  (соответствующие значения отмечены маркерами-точками на рис.2).

Таким образом, четвертое издание в отличие от второго предоставляет полные методические указания по оценке остаточной ошибки целостности для любых видов CRC-полиномов, не оставляя места для неоднозначных трактовок и ошибок в оценке уровня полноты безопасности (УПБ) систем с коммуникационными протоколами функциональной безопасности.

**Упрощенный пример оценки интенсивности остаточных ошибок**

Рассмотрим пример простейшего безопасного сообщения без меток времени и сообщений синхронизации (рис.3). Предположим, что данные пересылаются между двумя устройствами уровня SIL 3, и соответствующая функция безопасности имеет назначенный уровень SIL 3.

Размер сообщения, включая CRC,  $n=128$  бит. Так как  $2/n > 0,01$ , то достаточно найти значение  $R_{CRC}$  в точке  $P_e=0,01$ . Согласно справочному Приложению Н из четвертого издания IEC 61784-3 [1], при  $P_e=0,01$  величина  $R_{CRC}$  достигает значения  $R_{CRC} \approx 1,33 \times 10^{-14}$ . Предположим, что максимальное число безопасных сообщений в час равно  $\nu=36000$  (10 безопасных сообщений в секунду). Тогда, применяя (2), получаем  $RR_T \approx 4,8 \times 10^{-10}$  [ч<sup>-1</sup>].

Согласно IEC 61784-3, в данном случае адресация явная и  $RR_A=0$ .

Интенсивность остаточной ошибки своевременности при условии, что номер последовательности 32-х битный, а КУБ переходит в безопасное состояние только после детектирования третьей коммуникационной ошибки, и в системе есть четыре запоминающих элемента, равна  $RR_T \approx 2,8 \times 10^{-12}$  [ч<sup>-1</sup>], где частота появления некорректных последовательностей безопасных сообщений на один запоминающий элемент равна  $10^{-3}$  [ч<sup>-1</sup>] согласно IEC 61784-3:2021 [1].

Остаточная ошибка маскировки  $RR_M$  в данном примере пренебрежимо мала. Если взять, например, 32 устройства, которые потенциально могут высылать замаскированные пакеты с частотой  $10^{-3}$  [ч<sup>-1</sup>] на одно устройство согласно IEC 61784-3: 2021 [1], то так как длина адресного поля 16 бит, номер последовательности - 32 бита, а CRC - 32 бита,  $RR_M \approx 2,6 \times 10^{-26}$  [ч<sup>-1</sup>].

В итоге:  $\lambda_{SC} = RR_T + RR_T + RR_M + RR_A \approx 4,8 \times 10^{-10}$  [ч<sup>-1</sup>], что соответствует требуемому уровню SIL 3.

Однако предположим, что КУБ разрабатывался в соответствии со вторым изданием, то есть в соответствии с ГОСТ Р МЭК 61784-3-2015 [2], в котором отсутствовали требования к количественной оценке ошибок своевременности, и номер последовательности был 16-битный. Тогда  $RR_T \approx 1,8 \times 10^{-7}$  [ч<sup>-1</sup>]. В итоге:  $\lambda_{SC} = RR_T + RR_T + RR_M + RR_A \approx 1,8 \times 10^{-7}$  [ч<sup>-1</sup>], что не соответствует требуемому уровню SIL 3.

Как показано в Приложении Н четвертого издания IEC 61784-3: 2021 [1], для более длинных сообщений (например, 1056 бит) полином 0x1f1922815 становится неправильным, и значение  $R_{CRC}$  превышает оценку  $2^{-r} = 2^{-32}$ . Таким образом, при расчете согласно формуле (4) из второго издания будут получены заниженные (оптимистичные) значения интенсивности остаточных ошибок.

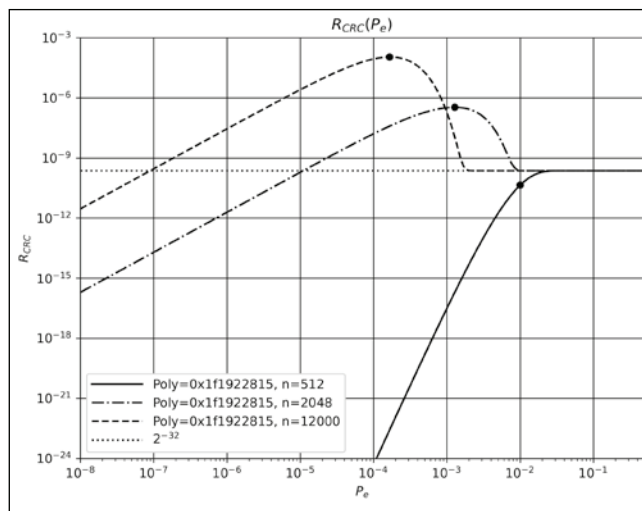


Рис.2. Вероятность остаточной ошибки целостности  $R_{CRC}$  для CRC-полинома 0x1f1922815 при разных значениях  $P_e$  и  $n$ . Маркерами-точками отмечены значения  $R_{CRC}$  для оценки  $RR_i$

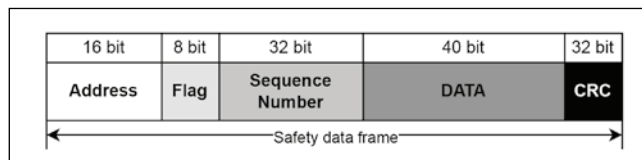


Рис.3. Пример структуры безопасного сообщения, где Address – поле адреса, однозначно определяющего получателя; Flag – поле, необходимое для распознавания типа безопасного сообщения; Sequence Number – номер последовательности; DATA – безопасные данные; CRC – контрольная сумма CRC32 (полином 0x1f1922815), закрывающая все безопасное сообщение

**ТОЧНЫЙ РАСЧЕТ ВЕРОЯТНОСТИ ОСТАТОЧНОЙ ОШИБКИ ЦЕЛОСТНОСТИ**

Четвертое издание стандарта приводит в справочном приложении вычисленные значения вероятностей остаточных ошибок целостности  $R_{CRC}$  для нескольких значений  $n$  и  $P_e$  для двух популярных CRC-полиномов: CRC32 (0x1f1922815) и CRC16 (0x14eab). Однако разнообразие используемых на практике CRC-полиномов и размеров передаваемых данных существенно ограничивает применимость этих справочных значений, что делает необходимым выполнение индивидуальных расчетов для каждого конкретного случая.

Как было показано выше, точный расчет  $R_{CRC}$  по формуле (3) сводится к нахождению коэффициентов  $A_i$  ( $i=1,2,\dots,n$ ), для непосредственного вычисления которых необходимо перебрать  $2^k$  кодовых слов. Сложность такой вычислительной задачи растет экспоненциально с ростом размера передаваемой информации  $k$ . Для современных коммуникационных протоколов с  $k > 1000$  бит такая процедура становится практически нереализуемой. Однако, используя тождества Мак-Вильямс [7], коэффициенты распределения кода  $A_i$  могут быть вычислены через коэффициенты распределения двойственного (“dual”) кода  $B_i$ , и формула для  $R_{CRC}$  примет вид [8]:

$$R_{CRC}(P_e) = 2^{-(n-k)} \sum_{i=0}^n B_i (1 - 2P_e)^i - (1 - P_e)^n. \quad (5)$$

Двойственный код содержит  $2^p = 2^{n-k}$  кодовых слов, где  $p = n - k$  — размер CRC-сигнатуры в битах. Таким образом, для нахождения  $R_{CRC}$  достаточно вычислить  $B_i$ , перебрав  $2^p = 2^{n-k}$  кодовых слов двойственного кода, и воспользоваться формулой (5). Авторами статьи было разработано программное обеспечение (ПО), реализующее данный метод вычисления. Разработанное ПО позволяет рассчитывать  $R_{CRC}$  для всех распространенных длин CRC-полиномов: от 8- и 16-битных (используемых во встраиваемых системах) до 32-битных (применяемых в промышленных Ethernet-сетях). При этом для выполнения расчетов достаточно современного инженерного компьютера: метод не требует применения высокопроизводительных вычислительных систем или специализированного оборудования. На рис. 2 показаны результаты вычисления вероятности остаточной ошибки целостности  $R_{CRC}$  для CRC-полинома 0x1f1922815 при разных значениях  $P_e$  и  $n$ . Вычисленные значения  $R_{CRC}$  совпадают с приведенными в справочном приложении четвертого издания стандарта ( $n=512$  и  $n=2048$ ). Стандарт приводит значения  $R_{CRC}$  для CRC-полинома 0x1f1922815 для значений  $n$ : 64, 128, 512, 1056, 1536, 2048 бит. В случае применения отличных или больших значений  $n$  ( $n > 2048$ ) в коммуникационном протоколе разработчикам необходимо проводить вычисления. Для демонстрации эффективности используемого вычислительного метода в применении к Ethernet-сетям, были проведены вычисления  $R_{CRC}$  для размера кодового блока  $n=12000$  бит, что соответствует максимальному размеру 1500 байт полезного блока данных (Maximum Transmission Unit, MTU) в сети Ethernet (рис. 2). Из рис. 2 также видно, что некорректное применение аппроксимационной формулы (4) и оценки  $2^{-r}$  для «неправильных» полиномов приводит к недопустимому занижению значения  $R_{CRC}$  и, следовательно, интенсивности остаточных ошибок. Так, для  $n=2048$  оценка дает  $R_{CRC} \approx 2^{-r} = 2^{-32} \approx 2,3 \times 10^{-10}$ , в то время как согласно точному расчету  $\max[R_{CRC}] \approx 3,4 \times 10^{-7}$ . Разница в три порядка для величины интенсивности остаточных ошибок критична для определения соответствия уровню SIL ( $\lambda_{SC} < 10^{-9}$  для SIL3 и  $\lambda_{SC} < 10^{-7}$  для SIL1).

Таким образом, точный расчет вероятности остаточной ошибки целостности необходим и может быть реализован на практике.

#### ЗАКЛЮЧЕНИЕ

В статье показано, как изменились требования к количественному анализу ошибок в коммуникационных протоколах функциональной безопасности при переходе от второго к четвертому изданию международного стандарта IEC 61784-3. В представленных результатах исследования продемонстрировано, что применение устаревшей методики второго издания приводит к заниженным оценкам интенсивности остаточных ошибок, что может вызывать

ошибочное соответствие заявленному уровню полноты безопасности.

В России ситуация осложняется тем, что действующий ГОСТ Р МЭК 61784-3-2015 по-прежнему основан на устаревшем издании IEC 61784-3:2010 и не учитывает критически важные для безопасности нововведения. Проведенный в статье анализ подтвердил, что современные требования, несмотря на их повышенную математическую сложность, необходимы для обеспечения должного уровня безопасности промышленных систем. Практическая реализуемость этих требований демонстрируется точным расчетом вероятности остаточных ошибок целостности, выполненным с помощью разработанного авторами статьи программного обеспечения, успешно применяемого на практике.

Результаты проведенного исследования убедительно свидетельствуют о необходимости безотлагательно обновления национального стандарта в соответствии с современными международными нормами. Отсутствие актуальной нормативной базы создает существенные риски эксплуатации промышленных систем с фактическим уровнем полноты безопасности, не соответствующим декларируемым показателям.

#### Список литературы

1. 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.
2. ГОСТ Р МЭК 61784-3-2015 (IEC 61784-3: 2010). Национальный стандарт РФ. Промышленные сети. Профили. Ч. 3. Функциональная безопасность полевых шин. Общие правила и определения профилей. // М.: Стандартинформ, 2016.
3. IEC 61784-3:2010. Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions // Edition 2.0. International Electrotechnical Commission. TC 65/SC 65C, 2010-06-29.
4. Рогова Е.С. Коммуникационные протоколы функциональной безопасности в промышленной автоматизации // Автоматизация в промышленности. 2024. №7. С. 3-8.
5. Webstore of International Electrotechnical Commission. IEC 61784-3:2021. URL: <https://webstore.iec.ch/en/publication/62095>
6. Leung-Yan-Cheong S., E. Barnes and Friedman D. On Some Properties of the Undetected Error Probability of Linear Codes (Corresp.) // IEEE Transactions on Information Theory 25, no. 1 (January 1979): 110–12.
7. Macwilliams, Jessie. A Theorem on the Distribution of Weights in a Systematic Code // The Bell System Technical Journal 42, no. 1 (January 1963): 79–94.
8. Fujiwara T., Kasami T., Kitai A., and Lin Shu. On the Undetected Error Probability for Shortened Hamming Codes // IEEE Transactions on Communications 33, no. 6 (June 1985): 570–74.

Рогов Андрей Сергеевич — канд. техн. наук, генеральный директор, Рогова Елена Сергеевна — канд. техн. наук, ведущий специалист по функциональной безопасности, ООО "ФАНКСЭЙФЕТИ".  
E-mail: [andrei.rogov@func-safety.ru](mailto:andrei.rogov@func-safety.ru)