FuncSafety

Оценка интенсивности остаточных ошибок в коммуникационных протоколах функциональной безопасности

Рогова Елена, ведущий специалист по функциональной безопасности, к.т.н.

Рогов Андрей, генеральный директор, к.т.н.

09.10.2025

© 2025 ООО «ФанкСэйфети»

Стандарты и коммуникационные протоколы ФБ

FuncSafety

Примеры стандартных протоколов:
Modbus TCP, Modbus RTU, Profibus, Profinet, Ethernet/IP, CANOpen, MQTT

Примеры протоколов ФБ:
CIP Safety, openSAFETY, PROFISafe, Safety over EtherCAT (FSoE)

ГОСТ Р МЭК 61784-3: КУБ (SCL) – это «коммуникационный уровень выше прикладного уровня, включающий все необходимые меры для обеспечения безопасной передачи информации в соответствии с требованиями МЭК 61508»

ГОСТ Р МЭК 61508

- **ГОСТ Р МЭК 61784-3**
- ГОСТ Р МЭК 62280

- В России действует **2-е издание** IEC 61784-3: 2010 (т.е. ГОСТ Р МЭК 61784-3-2015)
- В мире действует **4-е издание** IEC 61784-3: 2021

© 2025 ООО «ФанкСэйфети»

Анализ коммуникационных ошибок

1) Качественно: реализовать меры безопасности для детектирования коммуникационных ошибок (искажения, непреднамеренного повторения, недопустимой задержки, неверной последовательности, неправильной адресации, вставки, подмены, потери)

2) Количественно: вычислить величину интенсивности остаточной ошибки

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

Правило:
$\lambda_{SC}^{*} \leq 1\%$ PFH

**статистическая интенсивность, с которой меры безопасности, реализованные в КУБ протокола, не могут детектировать ошибки*

© 2025 ООО «ФанкСэйфети»

Качественный анализ коммуникационных ошибок

FuncSafety

Коммуникационные ошибки	Меры безопасности							
	Номер последовательности	Метка времени	Ожидание по времени	Аутентификация связи	Ответное сообщение	Обеспечение целостности данных	Резервирование с перекрёстным 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				

© 2025 ООО «ФанкСэйфети»

Различия в анализе коммуникационных ошибок №1

FuncSafety

Во втором издании IEC 61784-3 (т.е. ГОСТ Р МЭК 61784-3-2015) количественно учитываются только ошибки целостности данных, т.е. $\lambda_{SL} = RR_I$

В четвёртом издании IEC 61784-3: 2021 общая интенсивность остаточной ошибки коммуникационного канала безопасности на одно логическое соединение:

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

1

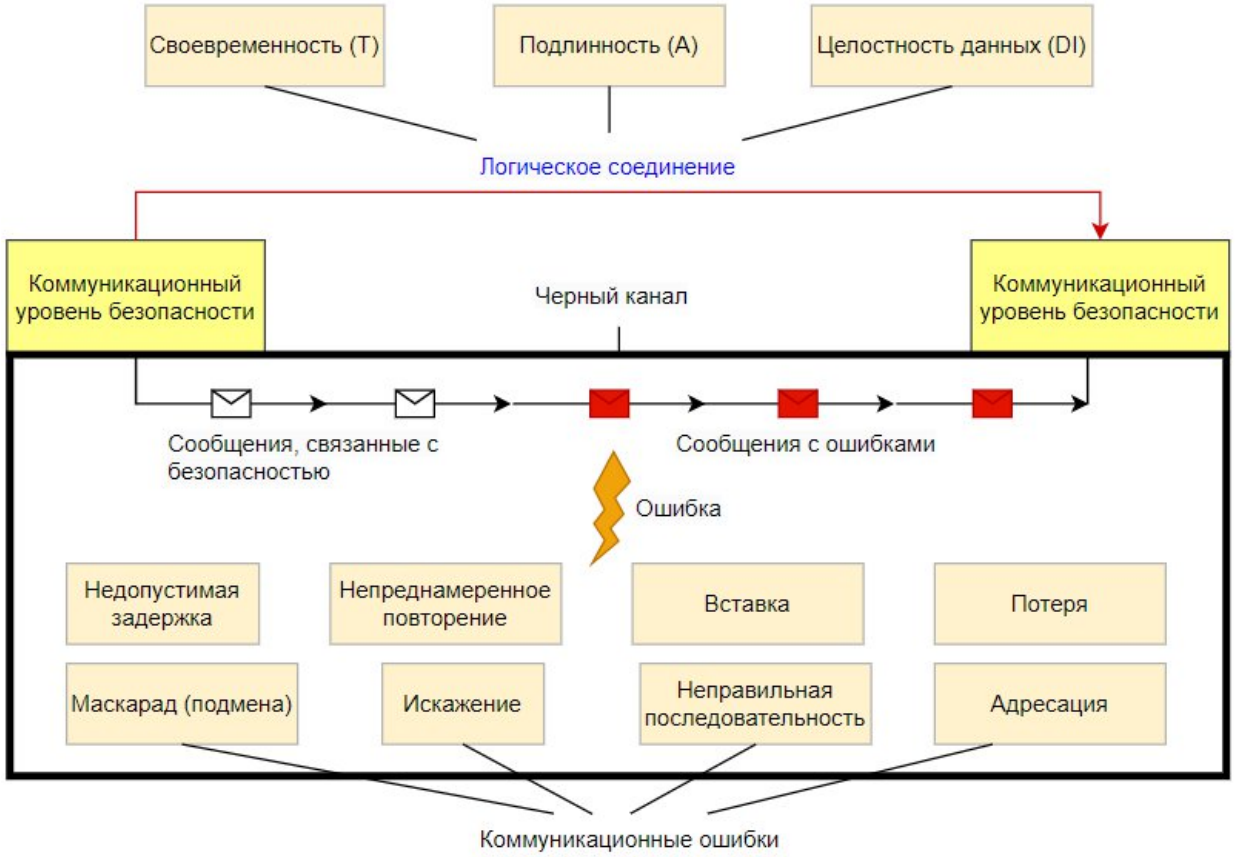
RR_I - Интенсивность остаточной ошибки целостности
RR_T - Интенсивность остаточной ошибки своевременности
RR_M - Интенсивность остаточной ошибки маскарада
RR_A - Интенсивность остаточной ошибки подлинности
λ_{SC} - Общая интенсивность остаточной ошибки (в час) коммуникационного канала безопасности на одно логическое соединение

Модель TADI

T- Timeliness (своевременность)
A - Authenticity (подлинность)
DI - Data Integrity (целостность данных)

TADI-модель (Timeliness, Authenticity and Data Integrity):

- 3-е издание IEC 61784-3: справочно
- 4-е издание IEC 61784-3 (2021 г): **обязательно**



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

© 2025 ООО «ФанкСэйфети»

Различия в анализе коммуникационных ошибок №2

FuncSafety

Расчет интенсивности остаточной ошибки целостности RR_I

Интенсивность остаточной ошибки целостности для методов на основе CRC:

$$RR_I = R_{CRC} \times v$$

R_{CRC} — вероятность остаточной (*необнаруженной*) ошибки целостности данных средствами CRC,
v — частота передачи сообщений (1/час).

Как вычислять R_{CRC} ?

- 2-е издание IEC 61784-3: 2010 (=ГОСТ Р МЭК 61784-3-2015):
  использовать «правильные» CRC-полиномы и оценку

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

- 4-е издание IEC 61784-3: 2021 (нет ГОСТа)
  использовать точную формулу, для любых CRC-полиномов

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

2

© 2025 ООО «ФанкСэйфети»

CRC-полиномы: «правильные» и «неправильные»

FuncSafety

Путаница терминов в переводе:

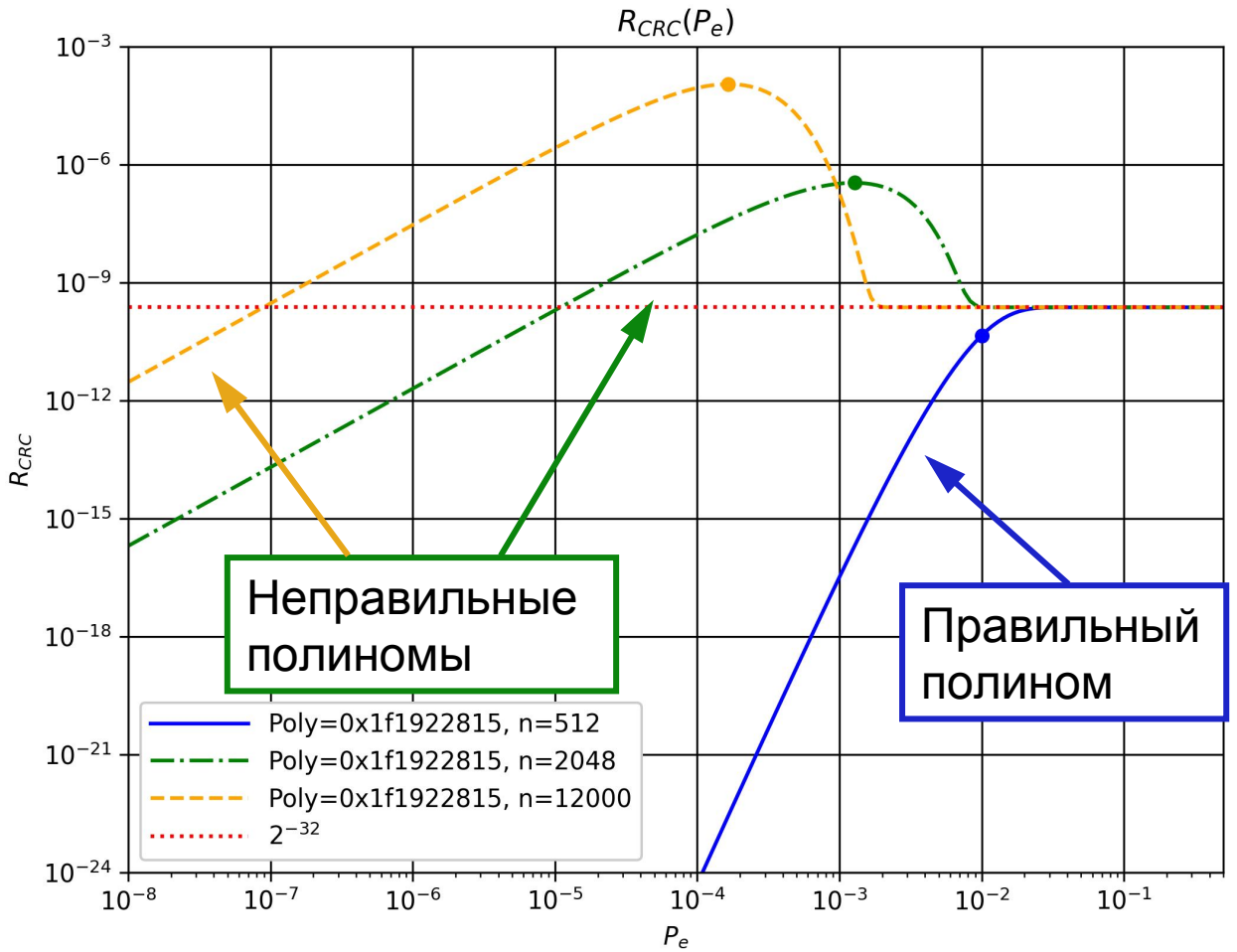
- IEC 61784-3 => ГОСТ Р МЭК 61784-3:
  "proper polynomial" => «образующий полином»;
  "improper polynomial" => «необразующий полином»
- "proper polynomial" ≠ «образующий полином» !!!
- Используем перевод дословно:
  "proper polynomial" => «правильный полином»;
  "improper polynomial" => «неправильный полином»

«Правильный» CRC-полином:

- полином, для которого $R_{CRC}(P_e)$ растет монотонно с ростом P_e для $0 \le P_e \le 0.5$
- Оценка 2-го издания верна только для «правильных» полиномов !!!

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

- Чтобы определить «правильность» нужен точный расчет !!!



Рогов А.С., Рогова Е.С. Количественный анализ ошибок в коммуникационных протоколах функциональной безопасности // Автоматизация в промышленности. - 2025. - №7. - С. 3-8

© 2025 ООО «ФанкСэйфети»

Количественный анализ: точный расчет ошибки целостности

- Точный расчет. Прямой метод («*в лоб*»):

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

  A_i — «коэффициент распределения кода» — число кодовых слов, вес Хэмминга которых (число бит «1») равен *i* ;
  P_e — вероятность битовой ошибки.
- Сложность: для вычисления A_i необходимо перебрать 2^k кодовых слов (k — число информационных бит сообщения).
- Нереализуемо на классическом компьютере!
  Для $k = 1000$ бит необходимо проверить $2^{1000} \approx 10^{300}$ кодовых слов!

© 2025 ООО «ФанкСэйфети»

Количественный анализ: точный расчет ошибки целостности

- Точный расчет. Альтернативный метод («*дуальный код*»):

  $R_{CRC}(P_e) = 2^{-r} \sum_{i=0}^{n} B_i(1-2P_e)^i - (1-P_e)^n$, где

  B_i — коэффициент распределения *дуального кода*.
- Сложность: необходимо перебрать 2^r кодовых слов *дуального кода* ($r = n - k$ — размер CRC, бит).
- Реализуемо на настольном компьютере!
  для $r = 32$ бит (CRC-32) необходимо проверить $2^{32} < 10^{10}$ кодовых слов

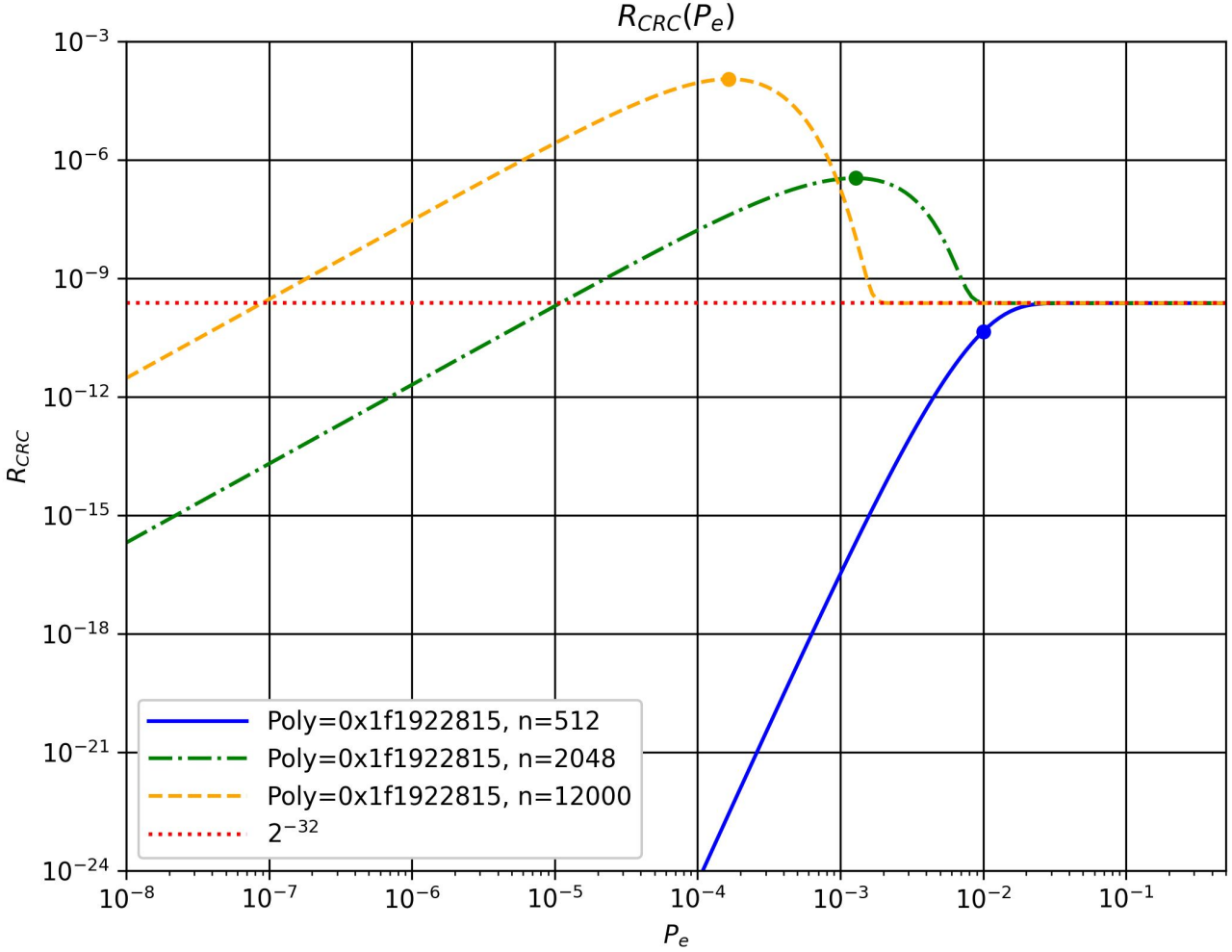
Рогов А.С., Рогова Е.С. Количественный анализ ошибок в коммуникационных протоколах функциональной безопасности // Автоматизация в промышленности. - 2025. - №7. - С. 3-8

© 2025 ООО «ФанкСэйфети»

Расчет интенсивности остаточной ошибки целостности RR_I

FuncSafety

Вероятность остаточной ошибки целостности $R_{CRC}\,(P_e)$ для CRC-полинома 0x1f1922815 для $n = 512, 2048, 12000$ бит (1500 байт). Маркеры-точки: значения R_{CRC} для оценки RR_I.



Интенсивность остаточной ошибки целостности:

$$RR_I = R_{CRC} \times v$$

v — частота передачи сообщений (1/час)

Выбор значения P_e для расчета $R_{CRC}\,(P_e)$

- 2-е издание («правильные» полиномы):

$$R_{CRC} = R_{CRC}\left(P_e = 10^{-2}\right)$$

- 4-е издание (любые полиномы):

$$R_{CRC} = max\{R_{CRC}\left(P_e \le 10^{-2}\right)\}$$

(максимум на отрезке)

Рогов А.С., Рогова Е.С. Количественный анализ ошибок в коммуникационных протоколах функциональной безопасности // Автоматизация в промышленности. - 2025. - №7. - С. 3-8

© 2025 ООО «ФанкСэйфети»

Программа по расчёту остаточной ошибки целостности

FuncSafety

Калькулятор вероятности остаточной ошибки целостности данных (Rcrc)

https://func-safety.ru/crc-calc/

Полином:

CRC-16-IEC61784 (0x4EAB)

Длина сообщения (без CRC), бит:

368

Вероятность битовой ошибки:

10^{-2} (1%)

Вероятность остаточной ошибки целостности (Rcrc):

2.9261350482540755e-4

Вычислить

Вычисление завершено 100%

© 2025 ООО "ФанкСэйфети"

https://func-safety.ru/

FuncSafety

СПАСИБО!

ООО «ФанкСэйфети»

- ✓ Подготовка к сертификации по стандартам ФБ
- ✓ Оценка функциональной безопасности, аудит ФБ
- ✓ FMEA, FMEDA анализ сложных систем "под ключ"
- ✓ Разработка КУБ коммуникационных протоколов. Расчёт интенсивности остаточных ошибок
- ✓ Расчёт надёжности
- ✓ Повышение ФБ компетенций специалистов, задействованных в Ваших проектах
- ✓ В штате сертифицированные TÜV SÜD инженеры и эксперт по ФБ

8(800)222-89-85
info@func-safety.ru