



# ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ И «ИНДУСТРИЯ 4.0». ЧАСТЬ 2

ТОМ МИНИ (TOM MEANY)  
ПЕРЕВОД: МИХАИЛ РУССКИХ  
tau68@rambler.ru

Во второй части статьи продолжим рассматривать особенности функциональной безопасности в рамках «Индустрии 4.0»: требования к сетям, безопасности, роботам/коботам, программному обеспечению и полупроводниковым приборам, используемым для реализации этих функций безопасности.

## ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ И СЕТЬ

Система функциональной безопасности, как правило, состоит из подсистемы датчиков, логической подсистемы и подсистемы вывода. Эти три элемента объединяются для реализации функции безопасности, и именно к ней в целом применяются требования SIL, PFH, SFF и HFT. Поэтому связь между данными подсистемами непосредственно влияет на безопасность. Для обеспечения требований функциональной безопасности МЭК 61508 ссылаются на стандарт промышленной шины МЭК 61784-3. К ним относятся меры по устранению источников случайных и систематических ошибок.

Обобщенно опасности, относящиеся к сетевой связи, которые необходимо учитывать, представлены в таблице, где приведены такие

стандарты, как МЭК 61784, EN 50159 и МЭК 62280 [1].

Каждая строка таблицы должна содержать как минимум одну защиту. Более подробная информация о конкретной защите приведена в стандартах МЭК 61784-3 [2] и МЭК 62280-1/EN 50159 [3]. Например, с нарушением целостности (искажением) данных можно бороться, используя циклический избыточный код (CRC) с алгоритмом Хэмминга, зависящим от ожидаемой частоты ошибок по битам, требований SIL и количества передаваемых битов в 1 ч.

Требования дополнительно усложняются тем фактом, что, по мнению специалистов, в промышленной среде безопасные и небезопасные данные лучше передавать в одной сети.

МЭК 61508-2:2010 предлагает два варианта. Первый вариант — под-

ход создания белого канала, когда весь канал связи разработан в соответствии с МЭК 61508. Второй вариант — подход создания черного канала, в соответствии с которым не делается никаких предположений о рабочих характеристиках канала связи, а обеспечение безопасности предусматривается специальным уровнем каждого защитного устройства. Этот уровень безопасности обеспечивает защиту от угроз благодаря набору различных защит, дополняющих защиты базового стандарта промышленной шины и способных, например, предполагать использование другого CRC-кода, что позволяет обнаружить нарушения целостности битовой последовательности. Подход к созданию черного канала является гораздо более распространенным. Одним из примеров может служить PROFIsafe, который представляет

собой уровень безопасности, располагающийся поверх протоколов PROFIBUS или PROFINET.

**ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ И ЗАЩИЩЕННОСТЬ**

Интересно, что во многих языках «безопасность» (safety) и «защищенность» (security) описываются одним и тем же словом. Тем не менее в сфере производства эти термины охватывают различные вопросы, которые иногда могут вступать в противоречие друг с другом. Одно из определений безопасности заключается в том, что обеспечение безопасности позволяет предотвратить нанесение вреда в результате непреднамеренных действий, тогда как понятие защищенности предполагает, что обеспечение защищенности позволяет предотвратить нанесение вреда в результате преднамеренных действий. К общим чертам обоих понятий можно отнести то, что безопасность и защищенность должны рассматриваться на уровне архитектуры, в противном случае в дальнейшем их очень трудно реализовать в системе. Но эти два понятия вступают в противоречие в том плане, что стандартная реакция безопасности на неожиданное событие заключается в отключении системы, и такую особенность хакеры могут использовать посредством атак типа «отказ в обслуживании», а это в свою очередь относится к тому, что должна пресечь защита. К функциям защищенности, как правило, относятся пароли для аутентификации, но вы действительно захотите замедлить реакцию системы безопасности, пока кто-то вводит пароль, или заблокировать пользователя, если пароль введен неверно три раза?

Вторая редакция МЭК 61508 от 2010 г. практически не содержит требований к защищенности. В ней лишь говорится, что защищенность должна быть предусмотрена, и дается отсылка ко все еще не выпущенной серии стандартов МЭК 62443. Кроме того, в настоящее время разрабатываются конкретные стандарты, предусматривающие взаимосвязи между функциональной безопасностью и защищенностью в таких областях, как промышленное оборудование и атомная энергетика.

По аналогии с уровнями SIL в МЭК 61508 и МЭК 62443 определены уровни защищенности SL 1–4. Система,

которая соответствует SL 1, защищена от ошибочных действий обычного пользователя, тогда как система, которая соответствует SL 4, может иметь защиту от взлома, спонсируемого другими государствами. Однако непосредственного соответствия между SIL и SL не существует.

В МЭК 62443 наряду с МЭК 62443-4-2 приведены семь фундаментальных требований (FR) для обеспечения рекомендаций относительно того, что необходимо каждому фундаментальному требованию для достижения конкретного уровня SL. К этим требованиям относятся:

- Управление идентификацией и аутентификацией (IAC).
- Контроль использования (UC).
- Целостность системы (SI).
- Конфиденциальность данных (DC).
- Ограничение потока данных (RDF).
- Своевременный отклик на события (TRE).
- Доступность ресурсов (RA).

SL 1 может затем быть представлен как вектор защиты вида (1, 1, 1, 1, 1, 1), где каждый элемент в векторе соответствует одному из семи фундаментальных требований. Учитывая, что SL 1 обеспечивает защиту от случайных атак, такой уровень является минимальным требованием для приложения безопасности, где необходимо учитывать предсказуемое неправильное использование [4]. Можно утверждать, что подходящий вектор для приложений безопасно-

сти с уровнем SIL выше SIL 1 равен (N1, N2, N3, 1, 1, N6, 1) [4], в котором признается, что конфиденциальности данных, ограничению потока данных и доступности ресурсов свойственен ограниченный интерес в рамках промышленных приложений функциональной безопасности. Тем не менее нет четкой корреляции между значениями для N1, N2, N3 и N6 в зависимости от уровня SIL (2, 3 или 4).

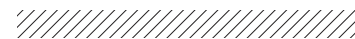
Ключевой момент, о котором следует помнить, заключается в том, что, хотя не все системы безопасности имеют требования к функциональной безопасности, защищенность должна предусматриваться для всех систем, связанных с безопасностью.

**ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ И РОБОТЫ**

ИСО 10218 [5] является стандартом, в котором приведены требования безопасности для промышленных роботов, в том числе и роботов. Он охватывает вопросы безопасной остановки, обучения, управления скоростью и контроля разделения элементов, а также ограничения мощности и силы. В пункте 5.4.2 стандарта ИСО 10218-1:2011 приводится требование о том, чтобы связанные с безопасностью части системы управления были спроектированы в соответствии с уровнем эффективности защиты = D с категорией конструкции 3, как определено в ИСО 13849-1:2006, или SIL 2 с уровнем отказоустойчивости аппа-

**ТАБЛИЦА. УГРОЗЫ И ЗАЩИТЫ В СЕТИ**

| Угрозы                           | Защиты                   |                 |                |   |                          |                         |                  |                          |
|----------------------------------|--------------------------|-----------------|----------------|---|--------------------------|-------------------------|------------------|--------------------------|
|                                  | Номер последовательности | Временная метка | Время ожидания | Идентификаторы источника и точки назначения | Сообщение обратной связи | Процедура идентификации | Код безопасности | Криптографические методы |
| Непреднамеренный повтор          | X                        | X               |                |   |                          |                         |                  |                          |
| Потеря данных                    | X                        |                 |                |   |                          |                         |                  |                          |
| Появление неизвестного сообщения | X                        |                 |                | X   | X                        | X                       |                  |                          |
| Ошибочная последовательность     | X                        | X               |                |   |                          |                         |                  |                          |
| Искажение данных                 |                          |                 |                |   |                          |                         | X                | X                        |
| Недопустимая задержка            |                          | X               | X              |   |                          |                         |                  |                          |
| Подмена                          |                          |                 |                |   | X                        | X                       |                  | X                        |



ратного обеспечения 1, как определено в МЭК 62061:2005. По сути, это означает создание по крайней мере 2-канальной системы безопасности с диагностическим охватом не менее 60% для каждого канала. Оба стандарта (ИСО 13849 и МЭК 62061) ссылаются на МЭК 61508-3 в вопросах относительно требований к программному обеспечению.

В стандарте ИСО 10218 не учтены автономные наземные транспортные средства, и хотя беспилотные автомобили рассматриваются в стандарте ИСО 26262, промышленное использование транспортных средств является особым случаем в сфере автомобилестроения и имеет гораздо более ограниченную область применения. Сфера действия директивы по промышленному оборудованию включает автономные наземные транспортные средства, и, учитывая отсутствие конкретного стандарта, пока будут применяться нормативы общего стандарта МЭК 61508.

Хотя для стационарных роботов сеть, скорее всего, будет основана на Ethernet, для автономных наземных транспортных средств она станет беспроводной, вследствие чего понадобится обеспечивать дополнительные требования к безопасности.

### ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Подробные требования для реализации высококачественного программного обеспечения в основном одинаковы, независимо от того, обеспечиваете ли вы безопасность или реализуете защиту. Например, программная ошибка, допущенная программистом, может привести к сбою системы, если возникнет соответствующая последовательность обстоятельств, приводящая к этой ошибке. Трудно судить о возможности такого исхода, но в некоторых стандартах функциональной безопасности говорится, что вероятность этого события должна рассматриваться как 100% [6]. Тем не менее может казаться разумным тот факт, что безошибочная программа с вероятностью 99,99% не приведет к про-

блемам с безопасностью в нормальных условиях, все же хакер будет стремиться к выявлению уязвимости в 0,01%. Поэтому устранение систематических ошибок так же важно для обеспечения защищенности, как и для обеспечения функциональной безопасности. Однако совершенному на 100% программному обеспечению, связанному с безопасностью, действительно могут быть присущи серьезные проблемы в плане защищенности.

В прошлом в системах безопасности запрещалось использование программного обеспечения, поскольку оно считалось непригодным для проверки из-за большого количества различных состояний. В новых стандартах приводится модель жизненного цикла, которая, если ее придерживаться, позволяет обеспечить безопасность, потому что методы, приведенные в этих стандартах, созданы для разработки безопасных систем в прошлом. Программное обеспечение по своей сути является привлекательным средством, поскольку оно позволяет преобразовать стандартный механизм в специфический (рис. 1). Однако эта универсальность также становится одной из его слабых сторон.

В документах, таких как ESDA-312 [7], говорится, что многие методы из МЭК 61508 могут использоваться для удовлетворения требований промышленной безопасности. В результате такого процесса будет создана соответствующая рабочим продуктам документация, которую можно применять для демонстрации достижения безопасности.

К этим методам относится проверка проекта, наличие стандарта написания кода, планирование использования инструментов, проверка на уровне отдельных элементов системы, отслеживание требований, независимая проверка и оценка. Хотя программное обеспечение не подвержено износу, аппаратное обеспечение, на котором оно работает, может выйти из строя, и это нужно предусмотреть в программном обеспечении. Для промышленных механизмов и роботов применение избыточных архитектур, таких как категория 3 или категория 4 из ИСО 13849, сокращает потребность в реализации диагностики на уровне микросхемы, но ужесточает требование к нали-

чию разнообразного программного обеспечения.

### ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ И МИКРОСХЕМЫ

В работе интеллектуальных систем очень важную роль играют микросхемы. Они позволяют создавать средства для отслеживания предметов в контейнере, а не самого контейнера, отслеживания положения рук робота, а не только самого робота в целом, отслеживания состояния даже малозначимых механизмов, а также обработки данных для того, чтобы в облако передавалась только полезная информация. Новые микросхемы управления двигателем могут повысить его КПД и продлить срок службы аккумуляторной батареи.

В данном случае микросхемы представляют собой «мозг», а компоненты, особенно применяемые в периферийных устройствах, обеспечивающие интеллектуальные функции, должны быть компактными и маломощными. Они также предоставляют методы для работы с датчиками, например радаром, лазером, датчиком магнитного поля, камерой или ультразвуковым датчиком. Они могут измерять скорость и положение, а благодаря новым технологиям, таким как AMR (анизотропное магнитосопротивление), датчики способны определять скорость и положение вала двигателя без использования внешних механических компонентов. При применении в сетях микросхемы реализуют как физический интерфейс, так и уровни MAC (управления доступом к среде). В беспроводных сетях эта реализация может быть выполнена на одной микросхеме.

Аналогичным образом микросхемы могут обеспечивать безопасность с помощью PUF (физически неклонировуемых функций), криптографических ускорителей и механизмов обнаружения несанкционированного доступа. Учитывая современный уровень интеграции, все, что раньше представляло собой требования на уровне системы, теперь во многих случаях становится требованиями на уровне микросхемы.

Тем не менее в существующих стандартах промышленной функциональной безопасности мало учитывается роль микросхем, а в стандартах обеспечения безопасности и того меньше.

**РИС. 1. ▽**  
Ключевое преимущество программного обеспечения



Для автомобильной промышленности стандарт ИСО 26262-11:2018 является отличным информационным ресурсом, и большая его часть пригодна для случаев использования микросхем, в том числе и в промышленности. Во второй редакции МЭК 61508 представлена модель жизненного цикла специализированных микросхем (ASIC), которая практически идентична модели для программного обеспечения. Фактически вопрос относительно того, является код языка описания аппаратного обеспечения (HDL), такой как Verilog, программным или просто описывает аппаратное обеспечение, весьма интересен. В приложении Е к МЭК 61508-2:2010 приводятся требования к обеспечению резервирования на кристалле при использовании одного куска кремния, но в данном случае рассматриваются только цифровые цепи и случай дублирования, при этом не предусматривается разнородное резервирование и использование аналоговых или смешанных цепей. Информативное приложение F к МЭК 61508-2:2010 чрезвычайно полезно, поскольку в нем приводится список мер, которые необходимо предпринять во время разработки микросхемы, чтобы избежать появления систематических ошибок. В нем указаны требования для каждого уровня SIL, но опять-таки только для цифровых цепей, а об аналоговых или смешанных цепях нет никаких упоминаний.

Высокий уровень интеграции микросхемы может быть как преимуществом, так и недостатком. Отдельные транзисторы микросхемы обладают очень высокой надежностью по сравнению с отдельными компонентами, причем наиболее ненадежными элементами микросхемы часто становятся контакты. Например, если для прогнозирования надежности используется стандарт Siemens SN 29500, то микросхема, содержащая 500 000 транзисторов, будет иметь показатель FIT (отказы за время) 70, но это число возрастет лишь до 80, если количество транзисторов увеличится в 10 раз до 5 млн штук. Если используются две микросхемы и каждая содержит 500 000 транзисторов, то показатель FIT будет равен 70 для каждой, что в общей сложности составит FIT 140. Таким образом, лучше использовать одну микросхему с показателем FIT 80 вместо двух с FIT 140, к тому же это выгоднее и по другим причинам,

таким как экономия занимаемой на печатной плате области, сокращение количества дорожек, уменьшение числа внешних пассивных компонентов, а также меньший размер встроенных в микросхемы антенн по сравнению с размером печатных антенн, что позволяет минимизировать электромагнитные помехи. Недостаток в данном случае заключается в том, что для сложной микросхемы довольно трудно определить режимы отказа. Простота — это друг безопасности, и весьма вероятно, что два отдельных микроконтроллера будут считаться более простыми, чем микросхема, содержащая два микроконтроллера. В приложении Е к МЭК 61508-2:2010 приводятся некоторые рекомендации на этот счет. Однако в большинстве стандартов безопасности  $\beta$  (вероятность сбоя каналов в одно и то же время и по одной и той же причине) менее 10% считается очень хорошим показателем.

Производители микросхем могут помочь своим заказчикам, разрабатывающим оборудование для обеспечения безопасности и защиты, предоставляя сертифицированные компоненты, руководства по безопасности или паспорта безопасности для выпущенных компонентов, встроенных в микросхемы аппаратных ускорителей, как внешних, так и встроенных в микросхемы диагностических функций, а также средств для разделения критического и некритического

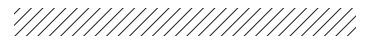
(с точки зрения безопасности и защиты) программного обеспечения. Эти функции обеспечения безопасности и защищенности должны быть разработаны в самом начале процесса проектирования. Попытка добавления этих функций после разработки микросхемы приведет к повышению сложности системы и необходимости использования дополнительных компонентов.

Существует несколько вариантов разработки микросхем для применения в функционально безопасных системах. В стандарте не указано требование использовать только совместимые микросхемы — в данном случае отмечено лишь, что разработчики модулей или систем должны сами убедиться, что выбранная микросхема подходит для их системы. Наличие независимого руководства по безопасности является одним из критериев применимости микросхемы, но не единственным вариантом.

К другим вариантам относятся:

- Разработка микросхемы полностью в соответствии с МЭК 61508 с внешней оценкой и руководством по обеспечению безопасности.
- Разработка микросхемы полностью в соответствии с МЭК 61508 без внешней оценки, но с руководством по безопасности.
- Разработка микросхемы в соответствии со стандартным процессом,





предусмотренным в полупроводниковых компаниях, но с публикацией паспорта безопасности.

- Разработка микросхемы в соответствии со стандартным процессом полупроводниковых компаний.

**Примечание.** Для компонентов, не разработанных в соответствии с МЭК 61508, руководство по безопасности может называться паспортом безопасности или аналогичным термином, чтобы избежать путаницы. Содержание и формат в обоих случаях будут одинаковыми.

Первый вариант является наиболее дорогостоящим для производителя полупроводниковых микросхем, но и максимально полезным для разработчиков модулей или систем. Наличие такого компонента, для которого вариант применения, показанный в рамках концепции безопасности для микросхем, совпадает с применением в системе, снижает риск возникновения проблем, связанных с внешней оценкой модуля или системы. Доля дополнительных проектных работ, обеспечивающих реализацию функции безопасности SIL 2, может составлять порядка 20% и более. Все дополнительные работы могут составлять и больший процент, хотя производители полупроводниковых компонентов, как правило,

уже предполагают строгий процесс разработки даже без учета функциональной безопасности.

Второй вариант позволяет сэкономить на внешней оценке, но все остальное остается таким же, как и для первого варианта. Этот вариант может оказаться подходящим, если заказчики все равно будут проводить внешнюю сертификацию модуля/системы, а микросхема станет важной частью такой системы.

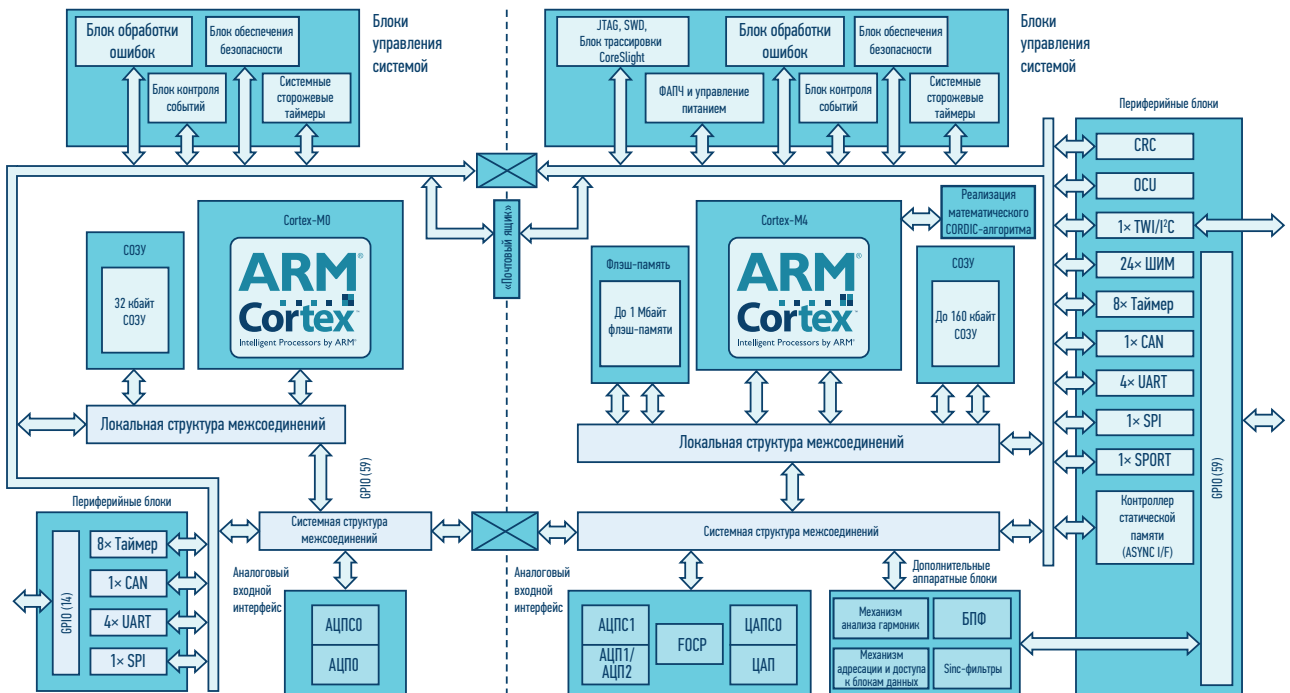
Третий вариант предпочтителен для уже выпущенных микросхем, когда имеющийся паспорт безопасности может предоставить разработчику модуля или системы дополнительную информацию, необходимую для обеспечения безопасности на более высоких уровнях. К этой информации относятся подробности фактического используемого процесса разработки, показатели FIT для микросхемы, подробная диагностическая информация и свидетельство о сертификации производственных площадок в соответствии с ИСО 9001.

Впрочем, четвертый вариант останется наиболее распространенным способом разработки микросхем. При использовании таких компонентов для создания безопасных модулей или систем понадобятся дополнительные компоненты и затраты на проектирование

модуля/системы, поскольку данные компоненты не будут иметь необходимых функций диагностики, необходимых для двухканальной архитектуры. Кроме того, интервалы диагностических тестов при использовании этих компонентов, как правило, будут неоптимальными, а количество годных устройств окажется меньше, поскольку будет невозможно определить, какой из потенциально неисправных элементов вышел из строя, что напрямую влияет на количество годных устройств. При отсутствии паспорта безопасности разработчику модуля/системы также придется делать осторожные допущения, рассматривая микросхему как черный ящик. Это может снизить заявленные показатели надежности.

Для того чтобы упростить реализацию функциональной безопасности, производители микросхем могут разработать собственную интерпретацию стандарта МЭК 61508. В Analog Devices имеется внутренняя спецификация компании, называемая ADI61508, которая является интерпретацией стандарта МЭК 61508, применяемой для разработки микросхем (рис. 2). Все семь частей МЭК 61508 интерпретированы в одном документе, причем биты именно стандарта МЭК 61508 не име-

**РИС. 2. ▼**  
Процессор серии ADSP-CM4 1x от ADI с множеством функций безопасности и защит



ют отношения к микросхеме, тогда как остальные биты спецификации применяются к микросхемам.

Независимо от того, какие стандарты системного уровня используются при разработке, микросхемы создаются в соответствии с МЭК 61508, за исключением одного случая — автомобильная электроника, когда для разработки микросхем и программного обеспечения применяется ИСО 26262.

## ЗАКЛЮЧЕНИЕ

В промышленности в целом и в рамках «Индустрии 4.0» в частности широко используются различные стандарты функциональной безопасности, основанные на документе МЭК 61508. К ним относятся стандарты разработки программного и аппаратного обеспечения, сетей, систем безопасности и робототехнических средств. Однако в настоящее время распространение информации ведется по нескольким стандартам, а «Индустрия 4.0» имеет уникальные особенности, связанные с постоянными изменениями, необходимыми в силу универсальности данной

концепции. Может случиться так, что в будущем появится единый сфокусированный стандарт для «Индустрии 4.0», который упростит соответствие требованиям и будет содержать интерпретацию основных стандартов безопасности. Возможно, он получит название «Безопасность 4.0» или «Умная безопасность». Аналогичным образом, в стандарте МЭК 61508 требуется привести больше информации, связанной с разработкой микросхем, чтобы обеспечить достаточную безопасность. В дальнейшем перспективные возможности «Индустрии 4.0» станут реальностью, а задачи, стоящие перед ней, удастся решить, и тогда будет очень интересно наблюдать полученный результат.

Функциональная безопасность может многое предложить «Индустрии 4.0», не только потому, что она является неотъемлемым элементом фабрик будущего, но и потому, что предоставляет методы, позволяющие повысить надежность, отказоустойчивость, степень резервирования и улучшить диагностические возможности. ●

## ЛИТЕРАТУРА

1. МЭК 62880. «Железные дороги. Системы связи, сигнализации и обработки данных. Часть 1. Экстренная связь в закрытых системах передачи». Международная электротехническая комиссия, 2017.
2. МЭК 61784-3. «Промышленные сети. Профили. Часть 3. Функциональная безопасность промышленных шин. Общие правила и определения профилей». Международная электротехническая комиссия, 2016.
3. EN 50159. «Железные дороги. Системы связи, сигнализации и обработки данных. Часть 1. Экстренная связь в закрытых системах передачи». Европейский комитет электротехнической стандартизации, сентябрь 2010.
4. Бранд Й. Какое отношение имеет уровень защищенности к уровню полноты безопасности? 8-й Европейский конгресс по встраиваемому программному обеспечению и системам реального времени (ERTS), 2016.
5. ИСО 10218-1. «Роботы манипуляционные промышленные. Требования к технике безопасности. Часть 1. Роботы». Международная организация по стандартизации, 2011.
6. Хоббс К. Встраиваемые программные системы для систем с особыми требованиями к безопасности. Auerback Publications, 2015.
7. Институт соответствия требованиям безопасности международной ассоциации автоматизации (ISA). EDSA-312. «Обеспечение безопасности встраиваемых устройств. Оценка безопасности разработки программного обеспечения». Международная электротехническая комиссия, 2016.