ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58538— 2019

СИСТЕМЫ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ И ИНТЕГРАЦИЯ

Спецификация требований к организации информационного взаимодействия

Издание официальное

Москва
Стандартинформ
2019

Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «НИИ экономики связи и информатики «Интерэкомс» (ООО «НИИ «Интерэкомс»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 100 «Стратегический и инновационный менеджмент»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 сентября 2019 г. № 717-ст

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Настоящий стандарт устанавливает базовые требования к функциональной совместимости (далее — IFRS-спецификации), а также методологию, гарантирующую потребителям, что произведенные различными компаниями продукты (как в настоящее время, так и в будущем) смогут совместно функционировать без потери заложенного в них функционала.

Достижение целей функциональной совместимости требует обязательного выполнения следующих трех этапов стандартизации (см. рисунок 1), обеспечивающих интеграцию, начиная от приборных разъемов и заканчивая базовыми системными функциями, а именно:

- сосуществование — этап, на котором различные системы могут функционировать в одной и той же среде, не препятствуя работе друг друга;
- взаимодействие — этап, на котором различные технологии объединяются для «сквозной» передачи данных. Это, прежде всего, относится к техническому решению, относящемуся к разъемам, протоколам, шлюзам и т. п.;
- функциональная совместимость (интероперабельность) — этап, на котором различные функции приложений могут согласованным образом использовать общую информацию. Это требует как взаимодействия структурных элементов между собой, так и их сосуществования, а также введения новых бизнес-правил, процессов и требований информационной безопасности, которые позволят объединять различные приложения.

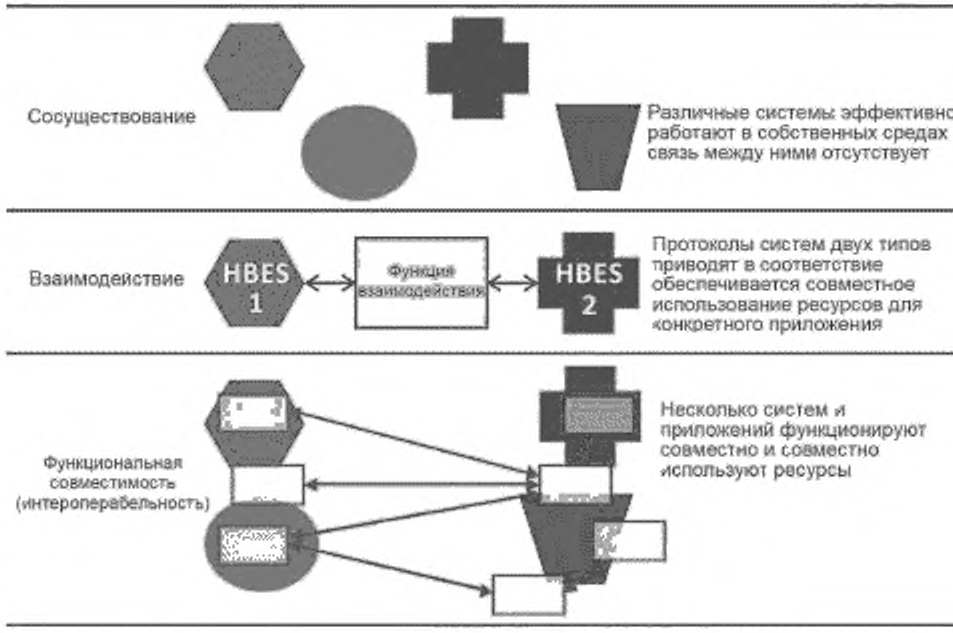

Рисунок 1 — Этапы стандартизации, обеспечивающие интеграцию продуктов между собой

IFRS-спецификации относятся к третьему из указанных выше этапов и содержат базовый набор правил, позволяющих обеспечивать функциональную совместимость продуктов, на которые распространяются различные стандарты и которые используются в какой-либо установке или оборудовании.

Настоящий стандарт охватывает четыре высокоуровневые функциональные операции: обнаружение, конфигурирование, эксплуатацию (функционирование) и управление. При этом определяется общий набор требований, которые при их соблюдении и выполнении этапов сосуществования и взаимодействия систем будут обеспечивать их функциональную совместимость.

В настоящем стандарте не рассматривается вопрос сосуществования или взаимодействия систем на основе технологических стандартов.

Функциональная совместимость также должна предусматриваться соответствующими ассоциациями коммерческих предприятий, однако в большинстве случаев она ограничивается приобретением клиентами продуктов только у членов конкретного объединения. Настоящий стандарт не исключает необходимость и ценность подобных объединений, но акцентирует внимание на возможности приобретения клиентами продуктов/услуг у конкурирующих объединений при сохранении их функциональной совместимости. Ожидается, что расширение рынка произойдет для тех объединений, которые будут соответствовать требованиям настоящего стандарта, поскольку клиенты будут приобретать их продукты с большей свободой выбора и уверенностью в том, что они будут функционировать должным образом.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ И ИНТЕГРАЦИЯ

Спецификация требований к организации информационного взаимодействия

Industrial automation systems and integration.
Requirement specification for organization of interoperability

Дата введения — 2020—01—01

1 Область применения

Настоящий стандарт содержит требования к функциональной совместимости (интероперабельности), определенные с учетом семиуровневой базовой эталонной модели взаимодействия открытых систем, четырьмя основными этапами интероперабельности и пятью типами взаимодействия.

Настоящий стандарт содержит также методологию, предназначенную для подтверждения соответствия требованиям, связанным с заявленным уровнем функциональной совместимости устройств в электронных системах для жилых домов и общественных зданий (далее — в HBES-системах/HES-системах).

Настоящий стандарт распространяется на установки одного и того же HBES-типа (или же установки двух и более разнородных HBES-типов). В HBES-установках одного и того же типа допускается использовать любые функциональные возможности для их обслуживания, применения и использования топологии систем связи. Ограничения на технологии формирования соединений между разнородными HBES-установками в настоящем стандарте отсутствуют.

Область действия настоящего стандарта распространяется на подсоединение устройств к различным сервисам связи для «сквозного» межсетевого обмена информацией между ними, на процессы обнаружения, посредством которых устройства могут распознавать друг друга и конфигурироваться для установления связи, а также на общие аспекты управления и работы с приложениями.

Настоящий стандарт также устанавливает требования к функциональной совместимости, которая требуется для устройств, обеспечивающих работу конкретных приложений, например, отвечающих за управление обогревом/освещением зданий, управление энергопотреблением и т. д. Требования к функциональной совместимости, определенные в настоящем стандарте, необходимы, но недостаточны для функциональной совместимости приложений, поскольку в ней не определены ни порядок проведения измерений, ни алгоритмы (которые получают, обрабатывают или реагируют на них), ни порядок взаимодействия между пользователями, поставщиками услуг и HBES-приложениями. За это определение несут ответственность эксперты и организации, которые специализируются в конкретных областях применения приложений.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:

ГОСТ Р ИСО/МЭК 9646 Информационная технология. Взаимосвязь открытых систем. Методология и основы аттестационного тестирования

Издание официальное

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 Определения, связанные с безопасностью

3.1.1 **управление доступом (контроль доступа)** (access control): Предотвращение несанкционированного использования ресурсов, обеспечение возможности санкционированного доступа и предупреждение несанкционированного доступа к данным (при управлении доступом должны быть определены процессы, которые могут выполнять элементы системы).

Примечание 1 — Подобный контроль становится особенно важным, когда для доступа к какому-либо ресурсу требуется несколько объектов/систем. В этих случаях (и особенно — в тех случаях, когда безопасность информации является проблемной), возможно, должны устанавливаться различные уровни прав доступа, которые будут зависеть от приоритета доступа к приложению и характера ресурса. Разрешение и возможность использования объекта для определенной цели — запроса информации от объекта, изменения значений его параметров (или изменения его состояния).

Примечание 2 — В тех случаях, когда для реализации одной или нескольких конкретных целей нескольким сервисам или приложениям требуется доступ к объекту, необходимо определять уровни доступа, включая определение основного владельца прав доступа (возможно — владельца объекта).

Пример — Доступ к информации с правом считывания общего параметра; разрешение на включение/выключение, т. е. выполнение определенных операций.

3.1.2 **права доступа** (access rights): Разрешение и возможность использования объекта для определенной цели — запроса информации от него, изменения значений параметров или изменения его состояния.

Примечание — В тех случаях, когда для реализации одной или нескольких конкретных целей ряд сервисов или приложений требуют доступа к объекту, необходимо определять уровни доступа, включая определение основного владельца прав доступа (возможно — владельца объекта).

Пример — Доступ с правом считывания информации об общем параметре; разрешение на включение/или выключение, т. е. выполнение определенных операций.

3.1.3 **аутентификация** (authentication): Процесс надежного установления подлинности объектов путем защищенного сопоставления предъявленного и хранящегося идентификатора объекта.

Примечание — Подтверждение предъявляемой идентификационной информации пользователя может выполняться путем проверки некоторых секретных сведений, ключа или свойства, связанных с этим пользователем, например, пароля, SSL-ключа, секретного PGP-ключа или подписи руки.

3.1.4 **авторизация** (authorization): Решение о разрешении пользователю не выполнять никаких операций над объектом (запретить доступ), или выполнять над объектом операции одного или нескольких типов (разрешить доступ).

Примечание — Подобное разрешение может даваться путем сопоставления утвержденных прав доступа пользователя с запрошенной пользователем операции (операций) для объекта, например, считывания информации и изменения определенного содержимого объекта.

3.1.5 **конфиденциальность** (confidentiality): Свойство, позволяющее не предоставлять или не раскрывать информацию неавторизованным физическим лицам, организациям или процессам.

3.1.6 **отказ от обслуживания (несанкционированное блокирование доступа к информации)** (denial of service): Предотвращение авторизованного доступа к ресурсам или отсрочка критических по времени операций (нежелательных или вредоносных сообщений, которые могут приводить к неправильному функционированию сетевых ресурсов).

3.1.7 **перехват информации (прослушивание)** (eavesdropping): Ситуация, при которой неавторизованный пользователь прослушивает передаваемые сообщения, к которым у него не должно быть доступа. При этом информация остается неизмененной, однако ее конфиденциальность оказывается поставленной под сомнение.

Пример — Перехват номеров кредитных карт или секретной информации, т. е. перехват любой информации на линии связи, который может делать информацию полезной для оператора перехвата сообщений (см. термин «конфиденциальность»).

3.1.8 **шифрование** (encryption): Процесс маскировки данных для скрытия их содержания.

Примечание — В контексте сетевой безопасности шифрование обычно выполняют путем применения к данным любого из нескольких установленных математических алгоритмов, разработанных специально для целей шифрования.

3.1.9 **информационная безопасность** (information security): Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

Пример — Использование ключа для шифрования или обнаружение несанкционированного доступа; разрешение доступа для считывания/записи информационных объектов; файлы регистрации сетевых событий для изменения данных.

3.1.10 **целостность (информации)** (integrity): Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

3.1.11 **неотказуемость** (non-repudiation): Сервис, обеспечивающий подтверждение целостности и происхождения данных (неразрывно друг от друга) любой из участвующих сторон.

Пример — Цифровая подпись может служить доказательством, предотвращающим отказ, поскольку эта подпись связывает сообщение с его отправителем.

3.1.12 **физическая безопасность** (physical security): Правила и системы, вводимые для обеспечения защиты непосредственного (физического) доступа к помещению или устройствам от реальных угроз.

Пример — Открывающиеся и закрывающиеся двери, обеспечивающие прохождение через них инвалидной коляски и отвечающие стандартам на подобные спецсредства.

3.1.13 **приоритет** (priority): Относительное упорядочение, придаваемое процессу/операции по отношению к другим процессам (операциям).

Пример — Жизненно важные процессы могут обладать более высоким приоритетом по отношению к другим пользовательским процессам.

3.1.14 **конфиденциальность (защита информации от несанкционированного доступа)** (privacy): Защита информации, которая может быть реализована путем отслеживания операций в сети (см. термин «прослушивание»).

3.1.15 **атака повторного воспроизведения сообщений** (replay attack): Перехват и запись сообщений для их отправки в более поздние сроки с тем, чтобы их получатель, не осознавая этого, считал, что фиктивный трафик является законным.

3.1.16 **непризнание участия** (repudiation): Отрицание одним из субъектов информационного обмена причастности ко всему сообщению или к его частям.

3.1.17 **защищенность** (safety): Состояние уверенности в том, что при определенных условиях какой-либо агент не будет оказывать неблагоприятных воздействий.

Примечание — Поскольку исполнительный элемент все больше отдаляется от основного устройства или операции, объем операций, которые могут приводить к возникновению опасных состояний, будет возрастать. Эта проблема может усугубляться при наличии двух и более исполнительных элементов в каком-либо устройстве (или участвующих в операциях).

3.1.18 **безопасность** (security): Правила и методики, устанавливаемые владельцами, которые призваны обеспечивать контроль за использованием их собственности другими владельцами.

Пример — Автовладельцам, которым выделены машиноместа, разрешено открывать гаражные ворота, а всем другим автовладельцам — запрещено.

3.1.19 **требования безопасности** (security requirements): Цель, задача и критерии успеха, относящиеся к приложению или сервису.

Примечание — Настоящий стандарт определяет требования к безопасности, связанные с уровнями функциональной совместимости и охватывающие как физическую, так и информационную безопасность. Эти требования должны сочетаться с требованиями защиты и с другими факторами, такими как разрешение и приоритет доступа, обнаружения, конфигурирования и управления.

3.1.20 **валидация** (validation): Процесс определения того, пригодны ли продукт или услуга для удовлетворительного выполнения назначенных им функций.

3.1.21 **верификация** (verification): (в области криптографии) Акт проверки подлинности цифровой подписи путем обработки данных с помощью специальных математических операций, предоставленных отправителем с целью выяснения того, соответствуют ли эти данные ожидаемому результату.

Примечание — Если информация, предоставляемая отправителем, дает ожидаемый результат, то подпись считается действительной, поскольку оценка правильного ответа требует использования секретных данных, известных только отправителю. Верификация позволяет удостоверяться в том, что информация была отправлена именно подписавшим ее отправителем и что эта информация (сообщение) впоследствии кем-либо не была изменена.

3.2 Определения, связанные с процессами

3.2.1 **объект** (object): Представление информации в виде структур данных и операций над ними, реализованных в аппаратных средствах, программном обеспечении или данных, встроенных в поток, на которые можно ссылаться и которые с использованием какого-либо взаимодействия могут быть получены с помощью каких-либо процессов, других объектов и пользователей.

3.2.2 **приложение** (application): Совокупность функций, которые способны оказывать поддающееся измерению воздействие на физические объекты и которые используются для достижения целей, соответствующих тем или иным функциональным возможностям приложения.

Примечание — Этот термин также применяют для ссылки на технологию, систему или продукт. Приложение может состоять из нескольких элементов/объектов/сущностей, действующих совместно с целью предоставления какой-либо услуги/продукта. Приложение может использовать определенные элементы системы/технологии для создания приложения. Приложение может быть программой, которая предоставляет определенный сервис в компьютерной, процессорной или (домашней) системе.

Пример — Устройства в «умном» доме работают совместно для выполнения приложения, связанного с регулированием потребления энергии, которое владелец «умного» дома использует для снижения потребления электроэнергии. При этом никаких дополнительных услуг не требуется.

3.2.3 **конфигурация** (configuration): Набор параметров состояния объекта или устройства.

Пример — Устройство может подсоединяться к приложению с помощью определенного сетевого адреса, а его объекты могут регистрироваться объектами в других устройствах.

3.2.4 **процесс конфигурирования** (configuration process): Конфигурирование параметров объекта (объектов) или приложений, выполняемое с помощью средств конфигурирования и других операций, которые могут быть автоматическими и управляться другими сервисами и/или приложениями.

Пример — Объединение объектов одного устройства с объектами в других устройствах.

3.2.5 **обнаружение** (discovery): Процесс, позволяющий пользователям, приложениям, объектам и устройствам в системах обнаруживать новые элементы и определять то, что они собой представляют.

Примечание — Объекты могут предоставлять и указывать свои параметры или реагировать на широковещательную передачу для получения информации об определенных типах объектов.

Пример — Набор сетевых протоколов UPnP.

3.2.6 **процесс обнаружения** (discovery process): Процесс выполнения операций по обнаружению.

3.2.7 **межплатформенное программное обеспечение** (middleware): Общий термин для обозначения функций, формирующих инфраструктуру связи, являющуюся частью распределенной системы, в которой используются приложения.

Примечание — Межплатформенное программное обеспечение можно использовать для функциональной совместимости и согласования данных, предоставленных объектом в соответствии с конкретной спецификацией на домашнюю систему, с требованиями других систем.

Пример 1 — Функциональность IP-маршрутизации домашнего шлюза к ISP-службам позволяет межплатформенному программному обеспечению соединяться с интернет-провайдером с целью регистрации локальных устройств, получения доступа к интернет-сервисам и маршрутизации IP-пакетов между локальными и внешними процессами.

Пример 2 — Смарт-система измерений/учета позволяет использовать межплатформенное программное обеспечение для установления подлинности загруженных в него прикладных объектов, прежде чем разрешать использовать им свои сервисы связи для реализации определенных прикладных функций.

3.2.8 **операции** (operations): Сервисные средства поддержки приложений, запрашиваемые объектами в системе, которые совместно реализуют какую-либо функцию.

3.2.9 **управление системой (системный менеджмент)** (system management): Сервисные средства поддержки приложений, запрашиваемые объектами в системе, которые не связаны с выполняемыми приложениями.

Примечание — Примерами могут служить сбор статистических данных, диагностирование неисправностей, инсталляция модифицированного встроенного и компьютерного программного обеспечения.

3.3 Определения, связанные с функциональной совместимостью

3.3.1 **сосуществование** (coexistence): Объекты и приложения, существующие в одной и той же операционной среде и не конфликтующие между собой.

Примечание — Функции этих объектов и приложений могут (или не могут) быть связанными или зависимыми друг от друга.

Пример — Сервис безопасности отслеживает события, происходящие в доме, с помощью интеллектуального прибора учета электроэнергии, передавая показания по Zigbee-каналу на домашний шлюз безопасности. Из-за напряженного трафика между другими устройствами, подсоединенными к Zigbee-каналу (например, с блоком дисплея потребителя), этот прибор временами бывает слишком перегружен для передачи событий, связанных с безопасностью, поэтому может возникать задержка в сообщении о проникновении в дом. При этом системы/приложения нельзя считать сосуществующими.

3.3.2 **функциональная совместимость (интероперабельность)** (interoperability): Способность двух или более сетей, систем, устройств, приложений или компонентов обмениваться информацией и, при этом, использовать полученную информацию.

3.3.3 **(межсетевое) взаимодействие** (interworking): Возможность обмениваться информацией между сервисами/устройствами, обладающими различными функциональными возможностями и/или с различными источниками происхождения, с целью обеспечения функциональной совместимости.

Пример — Домашний шлюз к ISP-сервисам обеспечивает взаимодействие между сетью Ethernet и WiFi-средой в доме, а также с ADSL-средой вне дома, с целью поддержки маршрутизации IP-пакетов для взаимодействия между объектами-приложениями в доме (с помощью IP-протокола) и другими объектами-приложениями.

3.3.4 **открытый стандарт** (open standard): Общедоступный документ, утвержденный уполномоченными международными органами по стандартизации, в котором определены архитектура, функции, протоколы и критерии соответствия характеристик систем связи.

3.3.5 **единая архитектура программы брокера объектных запросов** (CORBA): Система для распределенной обработки, определенная рабочей группой OMG по управлению OMI-объектами.

3.3.6 **язык формализованного описания** (Formal Description Language, FDL): Машинно-обрабатываемые и формально определенные синтаксис и семантика для выражения абстрактных свойств системы.

3.3.7 **декларация о соответствии реализации** (Implementation Conformance Statement, ICS): Заключение, выдаваемое поставщиком реализации или системы, утверждающее их соответствие данной спецификации (с указанием, какие функциональные возможности реализованы).

Примечание — ICS-декларация может принимать следующие формы: ICS-протокола, ICS-заключения, зависящего от профиля, ICS-заключения для информационных объектов и др.

3.3.8 **ICS-проформа** (ICS proforma): Документ в виде опросника (анкеты), который после завершения реализации или системы становится ICS-заключением.

3.3.9 **ICS-протокол** (Protocol ICS, PICS): ICS-заключение для реализации или системы, утверждающее о соответствии данной спецификации на протокол.

3.3.10 **декларация о соответствии реализации функциональной совместимости** (Interoperability ICS): ICS-декларация для реализации или системы, утверждающая о соответствии IFRS-требованиям.

3.3.11 **рабочая группа по управлению объектами** (Object Management Group, OMG): Промышленный консорциум, который устанавливает стандарты на распределенные объектно-ориентированные системы, на моделирование программ, систем и бизнес-процессов, а также на стандарты, основанные на моделях.

3.3.12 **подтверждение** (acknowledgement): Сообщение, формируемое в ответ на полученное сообщение и подтверждающее его прием или отклонение.

Примечание 1 — Подтверждение приема сообщения или положительное квитирование могут свидетельствовать о получении сообщения. Кроме того, оно может подтверждать принятие операции и успешность ее выполнения.

Примечание 2 — Отклонение сообщения или отрицательное квитирование могут свидетельствовать о том, что получатель не смог принять сообщение (или же не смог выполнить операцию, запрошенную в сообщении). При этом может указываться причина отклонения, а после завершения выполнения команды могут возвращаться параметры измененной конфигурации.

Пример — Механизм открывания дверей подтверждает, что он получил команду на их открытие, но не подтверждает, что он действовал в соответствии с этой командой.

3.3.13 **режим адресации сообщений любому устройству группы** (anycast): Режим связи, при котором сообщение передается в групповом режиме адресации и от объектов, получивших исходное сообщение, ожидаются ответные сообщения.

Примечание — Данный режим часто используют для выявления функциональных возможностей устройств или объектов системы.

3.3.14 **режим многоадресной адресации сообщений** (broadcast): Режим связи, при котором сообщение адресуется всем объектам системы.

Примечание — Этот режим характеризуется единственной операцией передачи сообщения, которая используется для распространения информации между всеми объектами-получателями системы.

Пример — Произошло возгорание, открывайте все двери!

3.3.15 **режим выполнения операции типа «не реже одного раза»** (at least once): Семантики выполнения, при которых операция, запрашиваемая объектом (или после исполнения которой), может выполняться еще один или несколько раз.

Примечание — Подобные семантики также называют «идемпотентностью». Периодическое выполнение операции не приводит к нестабильности состояния. При этом заявителю всегда сообщается, если операция была выполнена успешно.

Пример — Включение освещения, которое может потребоваться сразу нескольким пользователям или приложениям.

3.3.16 **режим выполнения операции типа «не более одного раза»** (at most once): Семантики выполнения, при которых операция, запрашиваемая объектом (или после исполнения которой), может либо вообще не выполняться, либо выполняться еще только один раз.

Примечание — Операция не сможет выполняться более одного раза без перехода объекта в нестабильное состояние и без информирования заявителя (объекта) о том, что запрашиваемая операция была выполнена успешно.

Пример — Добавление промежутка времени в график работы терморегулятора отопления. Если этот промежуток находится в пределах существующего временного интервала того же типа (например, включение/выключение отопления), то операция выполняться не будет.

3.3.17 **элементарность, атомарность** (atomicity): Возможность разделения операций (или последовательности операций) на несколько субопераций.

Примечание — Последовательность операций называется «элементарной», если ее невозможно прервать или разделить на более дробные последовательности субопераций.

3.3.18 **согласованность** (consistency): Состояние параметров, которые изменились в результате выполнения какой-либо операции (или последовательности операций), и должны находиться в диапазоне отклонений, указанном в приложении.

Примечание — Последнее особенно важно в системах, в которых несколько приложений совместно используют функциональные возможности объектов и их сервисов. При этом никакой элемент одного приложения не может устанавливать состояние параметра объекта на значение, которое будет неприемлемым для элемента другого приложения.

Пример — Диспетчер энергоснабжения отключил какое-либо электрооборудование, однако жилец дома, который ранее включил его, продолжает считать, что это электрооборудование все еще включено. В этом случае жильцу (или устройству, которое контролирует состояние электрооборудования в интересах жильца) необходимо отправить соответствующее уведомление.

3.3.19 **долговечность** (durability): Сохранение результатов выполнения каких-либо операций и работоспособности системы (и ее элементов) при возникновении неисправностей (отказов) в ней.

Пример — Тариф, загруженный в смарт-систему измерений (учета), будет сохраняться в этой системе даже во время прерывания электропитания.

3.3.20 **режим выполнения операции типа «только один раз»** (exactly once): Семантики выполнения, при которых операция, запрашиваемая объектом (или после исполнения которой), может выполняться еще только один раз.

Примечание — Эти семантики являются исключительно строгими, и во многих системах реализован двухфазовый подход, в соответствии с которым любая сторона может отменять (возвращать) операцию до тех пор, пока запрашивающая сторона не укажет ответчику (респондеру) на необходимость выполнения этой операции. Даже после этого элементы системы могут не функционировать, причем фаза их восстановления будет инициироваться после восстановления соответствующего сервиса.

Пример — Сделайте предварительный заказ, снимите 10 долларов США с моего банковского счета в коммерческом центре.

3.3.21 **семантики выполнения операций** (execution semantics): Определяют конечный результат выполнения операций, запрашиваемых объектом (или операций над объектом).

Примечание — При этом важным является именно конечный результат операции, а не процессе ее выполнения, который приводит к полученному результату. Из-за отказа (неработоспособности) какого-либо элемента в информационной цепочке между запрашивающей стороной (инициатором запроса) и респондером в выполнении какой-либо операции могут возникать периодические прерывания (сбои), о которых в процессе выполнения этой операции может сообщаться обеим сторонам.

3.3.22 **многоадресная передача сообщений** (multicast): Режим связи, при котором сообщение адресуется всем объектам, которые подписали соглашение на использование закрепленных за ними адресов.

3.3.23 **дистанционный режим работы, дистанционное управление** (remote operation): Режим взаимодействия, в котором используется модель типа «Команда/Ответное сообщение об исполнении».

Примечание — Модель дистанционного управления представлена в четырех вариантах: без получения подтверждения (ответного сообщения), с получением подтверждения (ответного сообщения); синхронный (блокировка инициатора запроса до получения ответного сообщения) и асинхронный (передача ответного сообщения производится с небольшой задержкой).

3.3.24 **режим управления без получения подтверждения** (unacknowledged): Вариант модели дистанционного управления, при котором в ответ на полученное сообщение никакое подтверждение (ответное сообщение) не формируется.

3.3.25 **одноадресная передача сообщений** (unicast): Режим связи, при котором сообщение адресуется единственному объекту, который подписал соглашение на использование закрепленного за ним адреса.

Примечание — Взаимодействия в модели типа «Команда/Ответное сообщение об исполнении» часто реализуются с использованием одноадресных сообщений.

Пример — Контроллер комфорт-системы запрашивает установленный в кухне датчик о температуре на ней.

3.4 Сокращения

В настоящем стандарте использованы следующие сокращения:

AC — переменный ток (alternating current);

ACID — элементарность (атомарность) (A), согласованность (C), изолированность (I), долговечность (D) — это свойства взаимодействий, включая одновременное и совместное использование ресурсов нескольких распределенных объектов (atomic, consistent, isolated, durable);

ADSL — асимметричная цифровая абонентская линия связи (asymmetric DSL);

API — интерфейс прикладного программирования (application programming interface);

APP — прикладной, представительский, транспортный и сеансовый уровни, характерные для настоящего стандарта (application, presentation, transport and session layers, specific to this technical specification);

AS — автономная система (autonomous system);

ASN.1 — абстрактная синтаксическая нотация, версия 1 (abstract syntax notation one);

ATM — асинхронный режим передачи данных (asynchronous transfer mode);

CDU — потребительский модуль индикации (дисплей) (consumer display unit);

DLC — управление каналом передачи данных (DLC-протокол) (data link control);

DLNA — альянс цифровых сетей для дома (digital living network alliance);

DOS — отказ от обслуживания (denial of service);

DSL — цифровая абонентская линия связи (DSL-протокол) (digital subscriber link);

DVB — цифровой широковещательный видеосигнал (цифровое телевидение) (digital video broadcast);

ETSI — европейский институт телекоммуникационных стандартов (european telecommunications standards institute);

FDL — язык формализованного описания (formal description language);

GPRS — пакетная радиосвязь общего пользования (general packet radio service);

GSM — глобальный стандарт цифровой мобильной сотовой связи (groupe special mobile, global system for mobiles);

HAN — домашняя локальная сеть (home area network);

HBES — электронные системы для жилых домов и общественных зданий (home and building electronic system);

HDMI — мультимедийный интерфейс высокого разрешения (HDMI-спецификация) (high-definition multimedia interface);

HES — домашние электронные системы (home electronic systems);

HSPA — высокоскоростная пакетная передача данных (high speed packet access);

HTTPS — протокол защищенной передачи гипертекстовой информации (hypertext transfer protocol-secure);

ICT — информационно-коммуникационные технологии (information and communications technologies);

IEC — международная электротехническая комиссия (international electrotechnical commission);

IEEE — институт инженеров электротехники и электроники (institute of electrical and electronics engineers);

IFRS — спецификация на базовые требования к функциональной совместимости (interoperability framework requirements specification);

IICS — декларация о соответствии реализации функциональной совместимости (interoperability implementation conformance statement);

IP — интернет-протокол (internet protocol);

IR — инфракрасный (infra-red);

IS — международный стандарт (international standard);

ISO — Международная организация по стандартизации (International standards organisation);

ISP — интернет-провайдер (internet service provider);

ITU-T — сектор стандартизации электросвязи Международного союза электросвязи (international telecommunications union-telecommunications);

LAN — локальная вычислительная сеть (local area network);

MAC — управление доступом к среде передачи или к каналу связи (medium access control);

MAC — код проверки подлинности сообщения (message authentication code);

Mbps — мегабит в секунду (megabit per second);

NWK — сеть (уровень эталонной модели взаимодействия открытых систем (OSI-RM)) (network (layer of the osi-rm));

OMG — группа по управлению объектами (OMG-стандарт) (object management group);

OSI — взаимодействие открытых систем (OSI-стандарт) (open system interconnection);

OSI-RM — эталонная модель взаимодействия открытых систем (reference model (for osi));

PC — персональный компьютер (ПК) (personal computer);

PDU — протокольные блоки данных (protocol data unit);

PGP — программа защиты сообщений с шифрованием («надежная конфиденциальность») (pretty good privacy);

PHY — физический уровень OSI-RM (physical (layer of the osi-rm));

PICS — заявка о соответствии реализации протоколу (protocol implementation conformance statement);

PIN — персональный идентификационный номер (personal identification number);

PIXIT — дополнительные данные о реализации протокола (protocol implementation extra information for testers);

PLC — технология связи по линиям электропередачи (powerline communications);

PPPoATM — протокол двухточечной связи (передачи) в ATM-режиме (point-to-point protocol over atm);

PSTN — коммутируемая телефонная сеть общего пользования (public switched telephone network);

QoS — качество сервиса (quality of service);

RJ45 — телекоммуникационное гнездо № 45, стандартизированное как TIA/EIA-568-B и используемое в телефонии и системах связи (registered jack no. 45 — standardised as tia/eia-568-b, used for telephony and communications applications);

RPC — дистанционный вызов процедур (remote procedure call);

RPC IDL — язык описания интерфейса для RPC (rpc interface definition language);

RS 232 — стандарт на последовательное соединение между терминальным оборудованием и терминальным оборудованием канала передачи данных. Стандартом ITU-T является V.24 (recommended standard 232, a standard for serial connection between a data terminal equipment and a data circuit-terminating equipment. the itu-t standard is v.24.);

SDU — блок служебных данных (service data unit);

SLA — соглашение об уровне обслуживания (service level agreement);

SLR — требования к уровню обслуживания (service level requirement);

SMS — служба коротких сообщений (short message service);

SSL — уровень защищенных разъемов (SSL-протокол) (secure socket layer);

STB — ресивер цифрового телевидения (STB-декодер) (set top box);

TCP — протокол управления передачей данных (TCP-протокол) (transmission control protocol);

TRS — транспортный уровень OSI-RM (transport (layer of the osi-rm));

TS — техническая спецификация (technical specification);

UPnP — универсальный разъем (режим) Plug and Play (universal plug and play);

USB — универсальная последовательная шина (universal serial bus);

VC — виртуальная схема (канал) (virtual circuit);

VP — виртуальный путь (virtual path);

WAN — глобальная вычислительная сеть (wide area network);

WiFi — беспроводный интернет, соответствующий IEEE 802.11 (wireless fidelity, ieee 802.11);

WiMAX — телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств (worldwide interoperability for microwave access);

XML — расширяемый язык разметки (extensible markup language).

4 Принципы функциональной совместимости

4.1 Функциональные этапы

4.1.1 Общие положения

В данном разделе описаны этапы обнаружения, конфигурирования, эксплуатации (функционирования) и управления, которые более подробно рассмотрены в А.3.

4.1.2 Этап обнаружения

Поддержка этапа обнаружения является фундаментальным требованием, обеспечивающим функциональную совместимость в системах с динамической структурой, в частности — предусмотренных настоящим стандартом, согласно которому, устройства/сервисы будут инсталлированы профессионально, или напрямую — конечными пользователями (причем эти устройства и сервисы со временем могут изменяться).

4.1.3 Этап конфигурирования

По завершению процесса обнаружения объекты в системе будут обладать отображением структуры всех объектов, с которыми им предстоит взаимодействовать для запуска того или иного приложения. Настоящий стандарт не ограничивает форму, содержание или местоположение указанной структуры, а также средства, с помощью которых она сформирована.

Основная операция при конфигурировании — это установление связи (или привязки) между объектами, которые должны взаимодействовать. В некоторых системах эта привязка может осуществляться на последнем подэтапе обнаружения и может оставаться постоянной на протяжении всего срока службы системы, периодически обновляться или ликвидироваться. Один объект может создавать несколько связей с другими объектами, если его функциональные возможности должны многократно использоваться несколькими приложениями.

Привязка может допускаться или запрещаться в зависимости от используемой политики безопасности или контроля доступа. Прежде чем объект будет выполнять какую-либо операцию (или возвращать информацию), он может потребовать ввод пароля доступа от другого объекта, который намерен с ним взаимодействовать. Для выполнения привязки объект также может инициировать последовательность взаимодействий со своими владельцами и пользователями. В процессе привязки и в рамках требований к системе безопасности между объектами может осуществляться и обмен ключами.

Этап конфигурирования также может включать передачу информации от одного объекта другим, что позволяет им взаимодействовать и с другими объектами. Например, в приложении для освещения, использующем средства электропередачи, переключатели и источники света не имеют естественной привязки: вполне вероятно, что любой переключатель может выявлять все источники света в установке, и наоборот. Объект-менеджер может взаимодействовать с жильцами дома для установления связей между переключателями и источниками света. Сразу же после построения схемы освещения пары «переключатель/источник света» смогут получать информацию о существовании друг друга и соответственно — выполнять их привязки. Этот пример содержит много исходных допущений относительно архитектуры, функций и протоколов для системы освещения, которые, однако, в других ситуациях могут оказаться неприменимыми.

4.1.4 Этап эксплуатации (функционирования)

После выполнения этапа конфигурирования система и ее приложения будут переходить на этап эксплуатации, на котором взаимодействия между объектами будут реализовывать функции приложения и обеспечивать достижение общей цели.

В результате выполнения этих функций и алгоритмов их реализации будут формироваться общие последовательности взаимодействий. Реальные изменения будут происходить в среде, в которой действуют приложения, причем эти изменения будут инициироваться показаниями датчиков, которые в свою очередь могут изменяться под воздействиями, инициируемыми данными приложениями.

4.1.5 Этап управления

Этап управления — это этап, который выполняется параллельно, но в количественном отношении он может отличаться от работы системы в стандартном режиме. Наличие этого этапа позволяет специально выделенным объектам (процессам) управления получать привилегированную информацию относительно системы, ее компонентов и их состояния. Объекты управления могут имитировать поведение системы, выполнять дистанционную диагностику и считывать данные с регистров, которые обычно недоступны для непривилегированных пользователей. Они также могут выполнять переустановку локальных или глобальных систем, перезапуск процессов обнаружения/конфигурирования, а также принудительный перевод системы в определенные состояния.

Уровень безопасности, необходимый для ввода этих объектов в систему и разрешения на их взаимодействие с системой, намного превышает уровень безопасности, требуемый на других этапах.

4.2 Уровни функциональной совместимости

Цель классификации функциональной совместимости по уровням состоит в выборе уровня, доступного установщикам приложений, поставщикам услуг и пользователям, а также в отражении динамического характера систем на соответствующих уровнях. Уровень 0 не предоставляет подобного выбора, поскольку он относится к автономной системе одного и того же поставщика, которая обладает фиксированным набором функций и не может обеспечивать совместную работу с другими системами. При повышении уровня функциональной совместимости область выбора функций расширяется. системы могут сосуществовать, быть взаимосвязанными, а их приложения — объединяться. В конечном счете, этими системами пользователи могут оперировать и управлять (как локально, так и дистанционно), используя при этом продукты от большого числа поставщиков и большое число технологий межсетевого взаимодействия.

Уровни 0 — 3 функциональной совместимости являются репрезентативными для состояния HBES-домена в системах, которые проектируются и разрабатываются для определенной цели. Разработчики этих систем при выработке своих технических решений могут использовать четко заданную иерархию требований к системе, конечному пользователю и бизнесу в целом с набором известных технических требований. В настоящем стандарте не сформулированы требования к соответствию для подобных систем, поскольку настоящий стандарт основан на положениях о функциональной совместимости, сформулированных поставщиками и установщиками приложений (в т. ч. содержащихся и в международных стандартах). Классификация по уровням функциональной совместимости используется в качестве неофициальной при анализе ее возможностей.

Для ныне предлагаемых приложений (а также для перспективных открытых систем) ситуация является полностью «прозрачной» из-за отсутствия набора всеобъемлющих, общих, открытых пользовательских требований, из которых вытекают системные/технические решения и требования к функциональной совместимости, которая должна поддерживаться на протяжении всего жизненного цикла системы, сохраняя при этом изменения, дополнения и обновления, предлагая «обратную» функциональную совместимость. Уровни 4—6 функциональной совместимости относятся к системам, которые отвечают этому требованию. В настоящем стандарте определены также требования к функциональной совместимости для систем, которые претендуют на соответствие Уровням 4—6.

Таблица 1 — Уровни функциональной совместимости

Уровень 0		Одиночная система со структурой, определяемой поставщиком и сформированной с помощью устройств, которые используют одну и ту же HBES-спецификацию и локально определяют функциональную совместимость, проверенную поставщиком для одного или нескольких доменов приложений. При этом уверенность в сосуществовании объектов/приложений отсутствует
Уровень 1		Система Уровня 0, функционирующая в одном или нескольких доменах приложений. При этом необходима верификация сосуществования объектов/приложений
Уровень 2		Системы с несколькими Уровнями 1, которые взаимодействуют между собой для обмена информацией и функционально совместимы в различных доменах приложений и, с учетом различных спецификаций, верифицированы поставщиками с использованием спецификаций на соответствие, согласованных с помощью каждой из используемых HBES-спецификаций
Уровень 3		Аналогичен Уровню 2, за исключением того, что функциональная совместимость проверяется на соответствие международным стандартам, которые распространяются на используемые в системе HBES-спецификации
Соответствие IFRS-Спецификации	Уровень 4	Аналогичен Уровню 3, но на котором приложения/устройства соответствуют IFRS-спецификациям по функциональным возможностям и допускают установку, управление и внесение изменений квалифицированным установщиком в процессе функционирования системы
	Уровень 5	Аналогичен Уровню 4, но на котором все изменения в приложениях/устройствах будут выполняться автоматически
	Уровень 6	Аналогичен Уровню 5, но при наличии дистанционного управления, диагностики и обслуживания (автоматической установки, эксплуатации и технической поддержки)

В таблице 1 приведено общее описание уровней функциональной совместимости, а их подробное описание, идентифицирующие мотивационные сценарии/варианты и примеры использования со всеми их различиями, приведены в А.4 и далее.

5 Условия соответствия

5.1 Требования соответствия к функциональной совместимости

5.1.1 Общие положения

Настоящий стандарт применим к системам/устройствам, для которых необходима функциональная совместимость на Уровнях 4, 5 и 6, однако для систем/устройств на Уровнях 0—3 какие-либо требования отсутствуют.

Ниже рассмотрены следующие общие требования к соответствию на Уровнях 4, 5 и 6.

5.1.2 Идентификатор объекта

Любой объект в системе должен обладать собственным идентификатором, который позволяет объекту однозначно отличаться от других объектов этой же системы с точки зрения его функциональности и местоположения, причем объект должен рассматриваться системой связи как член группы и включаться в режим многоадресной и широковещательной рассылки.

Идентификаторы могут выбираться проектировщиками и разработчиками системы, причем в различных HBES-спецификациях они могут обладать различными форматами и семантиками. Произвольность при выборе идентификаторов может создавать риск их несовместимости, и этот фактор является основным источником нарушений функциональной совместимости, поскольку объекты могут становиться недоступными для системы связи, а их функции — недоступными для приложений.

Соответствие настоящему стандарту требует детального выбора идентификаторов и увязки между различными схемами HBES-идентификации.

Подробные требования к идентификатору приведены в 5.2.1.

5.1.3 Описание объекта

Любой идентифицируемый объект должен (при условии наличия прав доступа к нему) предоставлять сервисам/приложениям какой-либо системы (а также сервисам/приложениям, не принадлежащим

этой системе) свою спецификацию, информацию о состоянии (статусе) объекта и другую запрашиваемую информацию.

Установив функциональную совместимость на уровне идентификатора, далее следует определить конкретные требования к функциям, чтобы сделать их доступными. HBES-спецификации содержат определения функций, связанных с объектами с точки зрения основных и структурированных типов данных. Кроме того, разработчики могут свободно определять собственные объекты и расширять функциональные возможности тех объектов, которые уже находятся в каталоге. Нарушения функциональной совместимости могут возникать в тех случаях, когда реализации объектов либо не соответствуют описаниям, либо при ненадлежащем документировании расширений. В различных HBES-спецификациях базовые и структурированные типы данных определены по-разному.

Соответствие настоящему стандарту требует описания состава и функциональности объектов, включая контроль доступа и другие требования безопасности, а также увязки между взаимодействующими объектами, определенными в различных HBES-спецификациях.

Подробные требования к состоянию (статусу) объекта см. 5.2.2 и ниже.

5.1.4 Обнаружение объекта

Любая система, спецификация или протокол должны обладать средствами инициализации процесса обнаружения объектов в системе (определения их местоположения, их идентификации и описания), в том числе сервисами/приложениями, внешними по отношению к этой системе.

Подробные требования к этапу обнаружения приведены в 5.2.3.

На Уровне 4 процесс обнаружения инициализируется средствами, которые не интегрированы в систему (например, управляющим приложением) и используются профессиональными установщиками приложений. На Уровне 5 процесс обнаружения автоматически инициализируется системой, а на Уровне 6 — может инициализироваться сущностью, установленной удаленно по отношению к системе.

5.1.5 Конфигурирование объекта

Любой обнаруживаемый объект может (при условии наличия прав доступа к нему) конфигурироваться с помощью сервисов/приложений системы (а также сервисов/приложений, не принадлежащих этой системе) или с помощью протокола, к которому они относятся.

Подробные требования к процессу конфигурирования приведены в 5.2.4.

На Уровне 4 процесс конфигурирования является необязательным и может инициироваться средствами связи, которые не интегрированы в систему (например, управляющим приложением), и используются профессиональными установщиками приложений. На Уровне 5 процесс конфигурирования автоматически инициализируется системой и в общем случае требует от пользователя разрешения на внесение изменений в конфигурацию. На Уровне 6 этот процесс может инициализироваться сущностью, которая устанавливается дистанционно по отношению к системе и, как правило, требует от пользователя разрешения на внесение изменений в конфигурацию.

5.1.6 Эксплуатация объекта

Любой конфигурируемый объект может использоваться сервисами/приложениями системы (а также сервисами/приложениями, не принадлежащими этой системе), или протоколом, к которому они относятся.

Подробные требования к функционированию объекта приведены в 5.2.5.

5.1.7 Управление объектом

Любой обнаруживаемый объект может (при условии наличия прав доступа к нему) управляться сервисами/приложениями системы (а также сервисами/приложениями, не принадлежащими этой системе).

Подробные требования к управлению объектом приведены в 5.2.6. Возможности управления объектом относятся только к Уровню 6.

5.1.8 Требования безопасности и доступ к объекту

Перед выполнением каких-либо операций сервисом/приложением необходимо установить наличие разрешения на эти операции.

Правила, относящиеся к безопасности информации, ее защите и приоритету, необходимо соблюдать как на уровне объектов, так и на уровне модели приложений (необходимо подтверждение соответствия действующим в этой области Международным стандартам), однако их функционирование и взаимодействие выходят за рамки рассмотрения настоящего стандарта.

Подробные требования безопасности, доступа и защиты объекта приведены в 5.2.7.

5.2 Частные условия соответствия

5.2.1 Требования к описанию идентификатора объекта

Требование настоящего стандарта на Уровнях 4, 5 и 6 состоит в том, что любой объект (устройство, оборудование, система, приложение или сервис) необходимо идентифицировать в пространстве (пространствах) имен всей системы и ее подсистем. Требование уникальности идентификатора зависит от режима доступа, например, при одноадресной передаче данных (1-1; в этом случае идентификатор должен быть уникальным в пространстве имен, из которого он извлекается), при групповой передаче данных (1-m; в этом случае идентификатор используется для идентификации одного или нескольких (m) объектов) или при многоадресной передаче данных (1 — все объекты; в этом случае используется идентификатор, предназначенный для адресации всех объектов). В некоторых случаях идентификаторы можно использовать взаимозаменяемо как имена или адреса (см. ниже).

Объекты, соответствующие данному частному условию, должны предоставлять:

- Имя (имена) для их использования внешними объектами, которые способны использовать интерфейсы, предлагаемые этим объектом. Средства, с помощью которых это имя будет выводиться, не регламентируются настоящим стандартом;
- Тип данных (путем указания идентификатора). Средство, с помощью которого этот тип будет выдаваться, а также его семантика (например, код продукта или название абстрактной спецификации на тип данных);
- Местоположение в системе — путем указания одного или нескольких сетевых адресов; номера того адреса, который может поддерживаться; режимов передачи данных (с одноадресной адресацией, с адресацией любому устройству группы или с многоадресной адресацией); средства и основополагающие HBES-спецификации, с помощью которых они будут выдаваться;
- Дескриптор/метка или другие средства обращения к объекту в течение всего срока службы в операционной системе (при его использовании);
- Другие постоянные идентификаторы, например, серийный номер.

5.2.2 Требования к функциональному описанию объекта

5.2.2.1 Общие положения

В соответствии с настоящим стандартом необходимый объем информации об объектах всегда должен быть доступен. За исключением случаев, когда четко не оговорено иное, к Уровням 4, 5 и 6 должны применяться следующие частные требования.

5.2.2.2 Классификация объектов

Объект должен предоставлять достаточный объем информации для возможности его использования другими объектами, включая информацию об аспектах безопасности, защиты и возможности доступа. Минимальная информация об объекте должна содержать его основное назначение, целевой домен приложения и текстовое описание, а также может включать средства связи, оценку качества, гарантию качества и другую дополнительную информацию (на усмотрение изготовителя). Описание должно представляться в форме удобочитаемого текста.

В следующих подпунктах для описания поддерживаемых интерфейсов (типов данных, операций и атрибутов) следует использовать один из Международных стандартных формализованных языков описания (FDL).

Операции должны определяться сигнатурой функции, включая входные, выходные и входные/выходные данные и возвращаемые данные-результаты, а также определять принимаемые входные данные и данные, сформированные на выходе. Атрибуты могут включать в себя время на прием (ответ) запрашиваемой операции; скорость, с которой допускается запрос операции; ограничения на доступ к считыванию/записи информации; идентификаторы, используемые в протокольных блоках данных (PDU) для выделения (разграничения) полей, из которых они составлены, а также другую информацию, которую можно считать достаточной для обеспечения функциональной совместимости. Допустимые FDL-языки — это языки ASN.1, XML (при этом необходимо указывать стандартные OMG-схемы), Corba IDL, ISO RPC IDL, JSON, SENML. В тех случаях, когда тот или иной язык не позволяет работать с обязательной информацией, в описании следует указывать синтаксис, который можно использовать для описания этой информации. Кроме того, подобное описание должно содержать все необходимые данные в виде комментариев в тексте.

5.2.2.3 Функциональный интерфейс объекта

Объект должен предоставлять описание типа своих данных, операций и атрибутов, с использованием одного из Международных стандартных формализованных языков описания (FDL).

5.2.2.4 Интерфейс для обнаружения объекта

Объект должен предоставлять описание типов своих данных, операций и атрибутов, поддерживающих процесс его обнаружения, конкретные аспекты которого рассмотрены в 5.2.3.

5.2.2.5 Интерфейс для конфигурирования объекта

Объект должен предоставлять описание своих типов данных, операций и атрибутов, поддерживающих процесс его конфигурирования. Соответствие этому требованию является необязательным на Уровне 4, но обязательным — на Уровнях 5 и 6.

5.2.2.6 Интерфейс для управления объектом

Объект должен предоставлять описание своих типов данных, операций и атрибутов, поддерживающих процесс управления им. Соответствие этому требованию является необязательным на Уровне 4, но обязательным — на Уровнях 5 и 6.

5.2.3 Требования к процессу обнаружения

5.2.3.1 Общие положения

Необходимо определить средства, с помощью которых описывающая объект информация будет извлекаться из функционального интерфейса объекта и предоставляться в качестве входных/выходных параметров с целью выявления функций интерфейса, включая синтаксис и семантику информации, зашифрованной в операциях обнаружения, причем этот синтаксис/семантику следует выбирать из одного из перечисленных выше FDL-языков.

5.2.3.2 Описания объекта: самоописание и описание объектов, подлежащих обнаружению

Объект, участвующий в процессе обнаружения, должен указывать информацию о нем самом, а также информацию, передаваемую тем объектам, которые намерены его обнаруживать. Кроме того, он должен указать число связей с запрашивающими объектами, которые данный объект будет поддерживать.

Объект, участвующий в процессе обнаружения, должен указывать объекты (посредством ссылки на их самоописания, см. 5.2.2), которые намерены его обнаруживать, а также ограничения, накладываемые на процесс обнаружения. Кроме того, он должен указывать число связей с обнаруженными объектами, которые данный объект будет поддерживать.

5.2.3.3 Режим связи

Объект должен указывать режим связи, используемый для передачи сообщений, которые связаны с процессом обнаружения (режим многоадресной передачи, режим с адресацией любому устройству группы или режим одноадресной передачи).

5.2.3.4 Процесс обнаружения

Объект должен указывать модель и протокол взаимодействия, которые он будет использовать для реализации процесса обнаружения и/или для реагирования на взаимодействия при обнаружении. Объект также должен указывать время ожидания на получение ответных сообщений; скорость, с которой будут обеспечиваться взаимодействия; ошибки, которые могут возникать, операцию, выполняемую после получения сообщений об ошибках/отказах и любые другие ограничения на усмотрение поставщика.

5.2.3.5 Область обнаружения

Объект, который ограничивает область обнаружения, должен указывать размеры этого ограничения по времени, пространству и по логическим аспектам. Объект в шлюзе, участвующий в процессах обнаружения, должен указывать ограничения, применимые к области обнаружения, а также любые другие дополнительные ограничения.

5.2.3.6 Безопасность и конфиденциальность

См. 5.2.7.

5.2.4 Требования к процессу конфигурирования

5.2.4.1 Общие положения

За исключением случаев, когда иное однозначно не оговорено, следующие подпункты применимы к Уровням 4, 5 и 6.

5.2.4.2 Привязки

Объект, участвующий в процессе конфигурирования, должен указывать число привязок/связей с запрашивающими объектами, которые он будет поддерживать.

Объект, участвующий в процессе конфигурирования, должен указывать число привязок/связей с обнаруженными объектами, которые он будет поддерживать.

5.2.4.3 Режим связи

Объект должен указывать режим связи, используемый для передачи сообщений, который связан с процессом конфигурирования (режим многоадресной передачи, режим с адресацией любому устройству группы или режим одноадресной передачи).

5.2.4.4 Процесс конфигурирования

Объект должен указывать модель взаимодействия и протокол, которые он будет использовать для инициализации и/или реагирования на взаимодействия при конфигурировании. Объект также должен дополнительно указывать время ожидания на получение ответного сообщения; время на выдачу ответного сообщения; операцию, выполняемую после получения сообщений об ошибках/отказах и любые другие ограничения на усмотрение поставщика.

5.2.4.5 Безопасность и конфиденциальность

См. 5.2.7.

5.2.5 Требования к процессу эксплуатации

5.2.5.1 Эксплуатация приложения

Настоящий стандарт не содержит требований к эксплуатации приложения или его функциональности, однако объекты необходимо указывать со ссылкой на соответствующие спецификации, в частности — на рекомендации по функциональной совместимости, опубликованные в качестве Международных стандартов или профилей, и поддерживаемые промышленными ассоциациями, алгоритмами и функциональными возможностями, которые они реализуют.

5.2.5.2 Безопасность и конфиденциальность

См. 5.2.7.

5.2.6 Требования к процессу управления

5.2.6.1 Режим связи

Объект должен указывать режим связи, используемый для передачи сообщений, которые связаны с процессом управления (режим многоадресной передачи, режим с адресацией любому устройству группы или режим одноадресной передачи).

5.2.6.2 Процесс управления

Объект должен указывать модель взаимодействия и протокол, которые он будет использовать для инициализации и/или реагирования на взаимодействия при управлении. Он также должен указывать время ожидания на получение ответного сообщения; время на выдачу ответного сообщения; скорость формирования взаимодействий; ошибки, которые могут возникать, операцию, выполняемую после получения сообщений об ошибках/отказах и любые другие ограничения на усмотрение поставщика.

5.2.6.3 Безопасность и конфиденциальность

См. 5.2.7.

5.2.7 Требования к безопасности информации, ее защите, приоритету и доступу к информации объекта

5.2.7.1 Безопасность информации об объекте

Объект (или группа взаимодействующих объектов/приложений) должен указывать любые требования к безопасности информации, которые он может предъявлять к доступу/обмену данными между ним и другими объектами, включая методики и процессы.

5.2.7.2 Защита информации об объекте

Объект должен указывать (со ссылкой на международные стандарты, применимые к доменам приложений, в которых он участвует) принятые меры по защите информации и полученные сертификаты, которые подтверждают его соответствие этим стандартам.

5.2.7.3 Права доступа к информации объекта

Права доступа к информации любого объекта (группы взаимодействующих объектов/приложений) должны устанавливаться сущностью/приложением, которым они принадлежат, или владельцем объекта, в отношении своих представителей и третьих лиц, которым может потребоваться определенный контроль или получение информации от него. В тех случаях, когда предоставляемый объектом доступ одной стороне косвенно используется для доступа и другими сторонами, следует указывать приоритет и иерархию подобных взаимодействий и любые применяемые дополнительные методики.

5.2.7.4 Приоритет при контроле доступа к информации объекта

В тех случаях, когда к двум и более приложениям предъявляется требование по использованию или получению информации от объекта (или от группы взаимодействующих объектов/приложений), при доступе к информации объекта следует указывать способ определения приоритета.

Для получения более подробной информации об этом см. А.7

Приложение А
(справочное)

Этапы обнаружения, конфигурирования, эксплуатации и управления

А.1 Методология

А.1.1 Цели

Целью IFRS-спецификации является оказание помощи поставщикам, установщикам приложений, системным интеграторам и провайдерам услуг в идентификации оборудования и устройств, которые могут вводиться в эксплуатацию в производственных помещениях заказчика и использоваться в новых приложениях/сервисах независимо от базового коммуникационного протокола, внешних коммуникационных технологий или используемых внутридомовых HBES-устройств. Достижение этой цели подразумевает выполнение ряда требований, которым для обеспечения функциональной совместимости должны отвечать приложения/сервисы, заявившие соответствие настоящему стандарту.

А.1.2 Принятые допущения

Ниже перечислены допущения относительно существующих функциональных возможностей и практики применения настоящего стандарта:

- Существует множество действующих систем/протоколов, поддерживаемых в крупных организациях, требования к которым разрабатывались на протяжении многих лет и обеспечивали стабильный выпуск продукции. Некоторые из этих требований уже нашли свое отражение в национальных и международных стандартах, причем в настоящее время ведется большая работа по разработке новых стандартов, которые в долгосрочной перспективе будут постепенно сближаться. Другие требования не вошли в стандарты, однако получили твердую поддержку со стороны промышленных ассоциаций и пользователей, а некоторые из них уже нашли широкое применение. Организации, которые поддерживают и внедряют эти системы, уже определили правила, рекомендации и методики, обеспечивающие функциональную совместимость продуктов в системах;

- Прогнозируется разработка новых протоколов взаимодействия между различными устройствами, с использованием одной или нескольких систем/протоколов (в особенности тех, которые обеспечивают связь через один или несколько шлюзов внешних поставщиков с внутренней сетью или домашней локальной сетью). Спецификация на функциональную совместимость должна гарантировать, что представленные в ней требования будут совместимы с требованиями, относящимися к этим системам;

- Нарушения функциональной совместимости возможны во всех тех случаях, когда в спецификациях допускается возможность выбора или содержится неоднозначное толкование, причем возможности подобного выбора могут снижаться за счет принятия общей транспортной архитектуры и архитектуры межсетевого взаимодействия, функций, протоколов и методик эксплуатации, т. е. путем их сближения. Тем не менее, даже если функциональная совместимость реализована, выбор все же будет оставаться в отношении, например, абстрактных типов данных (которые реализуются в устройствах в конечных точках системы и которые, как правило, могут изменяться), взаимодействий с пользователем при монтаже и в процессе эксплуатации устройств (например, если они будут отличаться при вводе пароля), методик обеспечения безопасности информации (которые могут оказаться несовместимыми), измеряемых физических величин, а также реальных эффектов от изменений, вводимых исполнителями (которые могут использовать различные системы и алгоритмы);

- Взаимодействие между разнородными технологиями достигается с помощью функций шлюза. Несмотря на то, что разнородность технологий постоянно растет, всегда будут существовать шлюзы, обеспечивающие эти взаимодействия. Уровень, на котором шлюз реализует межсетевое взаимодействие, будет изменяться в зависимости от степени сближения различных функций передачи данных;

- Требования к функциональной совместимости применимы к любому объекту, в том числе и к устройству, оборудованию, датчику, исполнительному устройству, сети, протоколу, приложению и бизнес-сервису. Подобные объекты можно использовать в зданиях и жилых помещениях. Реализация принципов функциональной совместимости должна осуществляться многими разработчиками и организациями, действующими в конкретной среде.

А.2 Используемый подход

Метод, используемый для разработки IFRS-спецификации, относится к трем основным областям потенциальных нарушений функциональной совместимости, в которых проектировщики и разработчики могут делать свой выбор, т. е.:

- Техническая область — нарушения функциональной совместимости могут возникать в тех случаях, когда системы несовместимы на одном или нескольких уровнях системы связи, использующей в качестве основы эталонную модель взаимодействия открытых систем (OSI-RM). Эту несовместимость необходимо выявлять в испытательной лаборатории, а ответственность за ее выявление (с использованием таких межсетевых средств, как шлюзы или межплатформенное программное обеспечение) должна лежать в основном на инженерах и исполнителях. Тем не менее, существует несколько вариантов, при которых проблемы функциональной совместимости объектов будут сохраняться, например, при таких простых видах несовместимости, как несоответствие круглых

разъемов-вилок квадратным разъемам-гнездам. Европейский институт телекоммуникационных стандартов ETSI классифицирует техническую область по физической и синтаксической интероперабельности;

- Семантическая область — нарушения функциональной совместимости могут возникать в тех случаях, когда функции устройства или другого оконечного оборудования вне системы связи оказываются несовместимыми даже при возможности их установки и использования для «сквозной» передачи/приема сообщений. Семантические нарушения также могут возникать и в системе связи, например, при послойном сопоставлении SDU-полей в PDU-блоке. Эти нарушения необходимо рассматривать как технические, которые должны идентифицироваться инженерами в испытательной лаборатории, после чего все функции будут послойно функционально совместимы и взаимодействовать друг с другом. Вне системы связи пользователь будет иметь дело с объектами в устройствах, запрашиваемыми между ними операциями, взаимосвязью между измерениями (которые они проводят и результатами которых обмениваются) и реальными эффектами, которые они могут вызывать;

- Технологическая область — Нарушения могут возникать в тех случаях, когда ограничения, налагаемые используемой методикой, установщиком приложений, пользователем или алгоритмом, препятствуют выполнению каких-либо функций даже при доказанной семантической функциональной совместимости. Некоторые нарушения могут устраняться инженерами, а другие — с помощью нетехнических средств, например, с использованием руководства по эксплуатации, рекомендаций по применению передовых практических методов или формализованной систематической спецификации на прикладные задачи/операции. Может потребоваться соответствие целому ряду других стандартов, например, на функциональную безопасность или на подходящую для приложения модель данных. Эта область является наиболее проблемной, поскольку она затрагивает гораздо более широкий выбор вариантов, многие из которых являются произвольными или неожиданными для разработчиков системы.

В приложениях настоящего стандарта приведено информационное разбиение системы связи на различные уровни (в соответствии с эталонной моделью OSI для открытых систем) с целью обеспечения взаимодействия и функциональной совместимости систем, а также с целью взаимодействия и стимулирования использования средств, с помощью которых поставщики и исполнители могут заявлять о соответствии этих средств IFRS-спецификации.

Несмотря на наличие требований к технической/технологической функциональной совместимости, которые могли бы быть включены в настоящий стандарт, далее основное внимание будет уделяться семантической функциональной совместимости. Нарушение взаимодействия может проявляться в неспособности устройства выполнять свои функции, даже если устройства способны устанавливать взаимосвязь между собой. Эти нарушения могут влиять на последовательность выполняемых функциональных этапов (см. ниже).

А.3 Функциональные этапы

А.3.1 Общие положения

В данном разделе подробно описаны этапы обнаружения, конфигурирования, эксплуатации и управления, со ссылкой на уровни, принятые в эталонной модели взаимодействия открытых систем (OSI-RM).

А.3.2 Этап обнаружения

Этапом обнаружения называют процесс и способы, применяемые для поиска, локализации или размещения устройства/объекта с целью получения дескрипторов системных/прикладных объектов и реализации их функциональных возможностей у конечного пользователя (являющегося физическим лицом или какой-либо другой частью системы). Любая функциональная возможность системы может потребовать использования определенного элемента обнаружения. Устоявшейся практикой для данного этапа является указание (ссылка) в спецификациях на возможность самоорганизации.

Средства обнаружения — это совокупность методов и протоколов, которые позволяют объекту обнаруживать сервисы/функции, информировать об их наличии или отвечать на запросы, связанные с сервисом, путем предоставления информации касательно его местоположения (о логическом адресе или дескрипторе), характера предоставляемого сервиса (что он обеспечивает?), а также соответствия сервиса выданному запросу (насколько качественно выполнен запрос, т. е. касательно качества обслуживания (QoS)) в целом.

Поддержка процесса обнаружения является фундаментальным требованием, обеспечивающим функциональную совместимость в слабосвязанных системах (отвечающих настоящему стандарту), в которых устройства/сервисы будут допускаться к установке (профессионально или напрямую конечными пользователями), и в которых эти устройства/сервисы могут со временем изменяться.

Обнаружение устройства или объекта осуществляется по следующим двум сценариям: (i) для нового устройства/объекта, установленных в системе и намеренных предоставлять свои услуги по регистрации/оповещению; (ii) для нового устройства/объекта, установленных в системе и намеренных предоставлять услуги от какого-либо другого устройства (устройств)/объекта (объектов) (запрос на обнаружение). Таким образом, процесс обнаружения при взаимодействиях в системе является двусторонним.

Новое устройство, устанавливаемое в HBES-систему, перед его вводом в эксплуатацию, необходимо подсоединять к системе на нескольких уровнях. При этом предполагается, что устройство способно устанавливать физическую связь с имеющимся проводным/беспроводным средством связи; в случае использования кабельной системы устройство должно иметь совместимые разъемы, а в случае использования беспроводной — антенны, способные принимать и излучать энергию.

В таблице далее представлены подэтапы обнаружения, которые необходимо выполнять для ввода устройства в систему.

Таблица А.1

Уровень модели OSI	Обнаружение	Проблемы функциональной совместимости/взаимодействия/сосуществования	Опции
Средний, физический (PHY) уровень	Идентификация заданного канала (по частоте и временному интервалу), который используется другими устройствами, отвечающими той же спецификации	Наличие нескольких PHY-уровней для одного и того же средства связи, которые могут быть «прозрачными» для взаимодействия или требовать оперативного управления и диспетчеризации	Не требуется; предварительное конфигурирование, динамическое сканирование известного набора каналов или поиск сигнатур
	Синхронизация с другими устройствами, совместно использующими данный канал	Неизвестные сигнатуры и комбинации битов синхронизации	«Пакетный» режим работы асинхронной системы, осуществляемый путем согласования с контроллером функций по выделению временного интервала и частоты. Этот режим может изменяться динамически
	Регистрация для использования выбранного или назначенного канала и его службы	Подходящими могут оказаться несколько PHY-уровней. Требуется выбор нужного уровня (уровней)	Обязательны для некоторых систем, а в других системах — возможны
Уровень канала передачи данных (с функциями управления доступом к среде передачи или каналу связи (MAC))	Получение уникального локального адреса, согласование использования многоадресных адресов	Возможность существования нескольких MAC-каналов и сервисов по обработке данных на одном PHY-уровне, которые должны быть обнаружены	Предварительные или динамические, осуществляемые путем конфигурирования и опроса свободных адресов для собственного использования и обнаружения тех адресов, которые совместно используются другими группами при многоадресной передаче данных
	Регистрация используемых адресов и оповещение ассоциации	Сообщение о нескольких требуемых MAC-каналах/DLC-службах от служб, действующих на данном PHY-уровне	Обязательны в некоторых системах, в других системах — возможны
	Установление соединения безопасности (security association)	Ключи недоступны	Предварительно распределенные ключи или их обмен при регистрации. Не могут быть реализованы полностью
Сетевой уровень	Получение уникального сетевого адреса, согласование использования адресов при многоадресной адресации	Отсутствие доступных адресов и своевременного реагирования на процессы распределения	Предварительные или динамические, осуществляемые путем конфигурирования и опроса свободных адресов для собственного использования и обнаружения тех адресов, которые совместно используются другими группами в режиме многоадресной передачи данных
	Регистрация используемых адресов и оповещение ассоциации	Регистрация с использованием нескольких служб сети из тех, которые предлагаются в зарегистрированных MAC/DLC-службах	Обязательны в некоторых системах, а в других системах — возможны

Окончание таблицы А.1

Уровень модели OSI	Обнаружение	Проблемы функциональной совместимости/взаимодействия/сосуществования	Опции
Сетевой уровень	Выявление других устройств в системе и локальной сети с помощью функций шлюза	Шлюзы должны обеспечивать связь между устройствами одной подсети (посредством маршрутизации и пересылки базы данных) с устройствами в другой подсети	Предварительно сконфигурированные известные значения, присваиваемые общим соглашением или назначаемые динамически, и требующие дополнительного идентификатора для типа устройства
	Установление соединения безопасности (security association)	Ключи недоступны, процессы обмена данными не реагируют за указанное время	Предварительно определенные ключи или обмен данными при регистрации. Вообще не может быть реализовано
Транспортный уровень	Выявление активных портов и идентификаторов сеанса для устройств, обнаруженных в системе	Порты и сеансы, которые могут совместно использоваться приложениями. Шлюзы должны обеспечивать связь портов, используемых устройствами в одной подсети (посредством маршрутизации и пересылки базы данных) с портами, используемыми устройствами в другой подсети	Предварительно определенные, известные значения, которые идентифицируют приложение и протокол или динамически назначаются, требуя дополнительного идентификатора для типа устройства
	Установление соединения безопасности (security association)	Ключи недоступны, процессы обмена данными не реагируют за указанное время	Предварительно определенные ключи или обмен данными при регистрации. Вообще не может быть реализовано
Уровень приложения	Выявление объектов и служб, реализованных устройствами, которые обнаружены в системе	Предоставляемые объекты и службы, которые могут совместно использоваться приложениями. Шлюзы должны обеспечивать взаимодействие объектов, принадлежащих устройствам одной подсети (посредством маршрутизации и пересылки базы данных) с объектами, принадлежащими устройствам другой подсети	Предварительно определенные, известные значения, которые идентифицируют приложение и протокол; или динамически назначаются, требуя дополнительного идентификатора для типа устройства
	Установление соединения безопасности (security association)	Ключи недоступны, процессы обмена данными не реагируют за указанное время. Информация, предоставляемая пользователем или другим сервисным элементом, является неточной	Предварительно определенные ключи или обмен данными при регистрации. Вообще не может быть реализовано

В соответствии с настоящим стандартом допускается выполнение некоторых из указанных этапов, всех этапов, либо ни одного из этапов. Необходимые для выполнения этапы должны быть связаны с HBES-архитектурой. Некоторым системам может не потребоваться особый MAC/DLC- и сетевой уровни, другие системы могут использовать только многоадресную или групповую рассылку сетевого уровня (NWK-технология) и использовать только идентификаторы объектов.

Сложность процесса обнаружения может возрастать в зависимости от степени динамичности системы: в тех случаях, когда идентификаторы присваиваются статически и управляются глобальной схемой назначения имен, необходимость в их обнаружении отпадает, однако, как это часто бывает, идентификаторы присваивают по требованию.

Устройства и объекты, соответствующие настоящему стандарту, могут функционировать в децентрализованной инфраструктуре обнаружения. Последнее означает, что эти устройства/объекты не должны быть ни зависимыми, ни базирующимися на хранилище зарегистрированных активных/доступных сервисов, которые необходимо регистрировать с дескрипторами (или получать информацию о них) с целью завершения процессов обнаружения и конфигурирования.

Область работ по обнаружению может быть связана с топологическим (логическим или сетевым) диапазоном поиска сервиса. Устройства/объекты, отвечающие настоящему стандарту, должны иметь возможность конфигурировать и контролировать область обнаружения. Основными причинами предъявления этого требования является потенциальная конфиденциальность, соображения безопасности и продолжительность интервала обнаружения.

Если проблемы межсетевого взаимодействия и сосуществования решены неправильно, то маловероятно, что отображения в шлюзах будут содержать информацию, необходимую для правильной маршрутизации сообщений между различными пространствами имен: MAC-адресами, сетевыми адресами, портами на транспортном/сеансовом уровнях и идентификаторами объектов/сервисов. Устройства могут не обладать информацией относительно существования друг друга, содержания в них нужных объектов/сервисов, или же преобразование данных может оказаться неверным.

Опция установления соединения безопасности security association задается на каждом уровне выше физического уровня. Благодаря общей тенденции к объединению все большего числа устройств для развертывания сетей связи, возможность непредусмотренного обнаружения возрастает, что может приводить к несанкционированному проникновению, перехвату (прослушиванию) сообщений и прямой попытке нарушения защиты. Метод обеспечения безопасности, который призван защищать устройства и их взаимодействие и реализуется в одной или нескольких местах системы, является доминирующим.

А.3.3 Этап конфигурирования

После завершения процесса обнаружения объекты системы будут обладать отображениями объектов в тех местах, где они могут понадобиться для взаимодействия с целью реализации приложения.

Конфигурирование — это процесс, посредством которого устанавливаются взаимоотношения между объектами, которые их используют.

Примечание — Многие параметры, устанавливающие эти взаимоотношения, можно использовать для функционирования приложения, например, приложения для установки порога температуры в термостате.

Основная операция при конфигурировании — это формирование связи (или привязки) между объектами, необходимыми для взаимодействия. В некоторых системах эта привязка может осуществляться на последнем подэтапе обнаружения. Необходимость создания такой привязки зависит от типа HBES-системы: привязка может быть неявной (например, когда схема присвоения имен объектов реализуется статически, и активный объект всегда «узнает» другие объекты, с которыми он обменивается данными. Привязка может быть постоянной — на протяжении всего срока службы системы, или же постоянно обновляться или удаляться. Один объект может иметь несколько привязок с другими объектами, если функциональные возможности объекта многократно используются несколькими приложениями.

Привязку можно допускать или не допускать в зависимости от используемой методики или способа контроля доступа. Объект перед выполнением какой-либо операции (или при возврате информации об исполнении) может потребовать предъявления пароля от другого объекта, намеренного взаимодействовать с первым. Объект для привязки может инициализировать последовательность взаимодействий со своими владельцами и пользователями. Обмен ключами может выполняться в процессе привязки как части процедуры обеспечения безопасности системы.

Этап конфигурирования также может быть связан с одним из объектов, предоставляющим информацию другим объектам, которая позволяет этому объекту взаимодействовать с другими объектами. Например, в приложении для освещения, использующем средства электропередачи, переключатели и источники света, отсутствует естественная привязка: вполне вероятно, что любой переключатель может обнаруживать все источники света в установке, и наоборот. Объект-менеджер может взаимодействовать с жильцами дома для отображения связи между переключателями и источниками света. Сразу же после построения схемы соединений пары «переключатель/источник света» может появляться информация относительно существования этих пар и соответственно — выполняться привязки. Очевидно, что этот пример содержит много допущений относительно архитектуры, функций и протоколов для системы освещения, которые могут оказаться неприемлемыми в другом контексте.

Способность устройств взаимодействовать между собой с целью надлежащего конфигурирования своих взаимосвязей предполагает, что этап обнаружения также будет завершаться надлежащим образом. Одна из возможных проблем при этом может быть связана со временем, необходимым в процессе взаимодействия для формирования ответного сообщения.

А.3.4 Этап эксплуатации

После конфигурирования система и ее приложения переходят к этапу эксплуатации, на котором взаимодействия между объектами будут реализовывать функции приложения и способствовать достижению основной его цели.

В результате выполнения функций и реализующих их алгоритмов будут возникать общие последовательности из взаимодействий. Реальные изменения будут возникать в рабочей среде приложений, причем эти изменения будут инициализироваться показаниями датчиков, функционирование которых само может изменяться операциями, которые инициализируются исходным приложением. Стабильность таких процессов является проблемой функциональной совместимости и не рассматривается в настоящем стандарте.

Этап конфигурирования может приводить к образованию привязок объектов между собой типа «один к одному», «один ко многим», «многие к одному» (например, когда один светильник можно включать/выключать несколькими переключателями), или привязок типа «многие к одному», например, когда один переключатель может включать/выключать все источники света или «многие ко многим», т. е. когда несколько переключателей могут

включать/выключать различные группы светильников). В частном случае привязок типа «многие к одному» может возникать ситуация, при которой «многие» будут одновременно вызывать взаимодействия, изменяющие состояние данных объекта «один». При этом протокол взаимодействия должен предусматривать неизменность состояния объекта «один».

Распределенные алгоритмы и протоколы, обеспечивающие согласованность (иногда называемые «транзакционной прозрачностью»), хорошо известны в корпоративном секторе и реализуются с помощью распределенных протоколов обеспечения, поддерживающих обработку транзакций. Их свойства, на которые часто ссылаются при использовании аббревиатуры «ACID» (элементарность (атомарность), согласованность, изолированность, долговечность данных), в равной степени применимы и к устройствам в HBES-приложениях, которые совместно используются несколькими объектами, хотя фактически применяемые протоколы могут различаться в деталях.

А.3.5 Этап управления

Этап управления — это особый этап, который выполняется параллельно, но в количественном отношении отличается от стандартного режима работы системы. Наличие этого этапа позволяет выделенным объектам (процессам) управления получать привилегированную информацию относительно системы, ее компонентов и их состояния. Объекты управления могут имитировать поведение объекта, выполнять дистанционную диагностику, собирать данные из регистров (которые обычно недоступны для непривилегированных пользователей), выполнять установку локальных или глобальных систем в исходное состояние, перезапускать процессы обнаружения/конфигурирования и принудительно приводить систему в заданное состояние.

Уровень безопасности, необходимый для ввода этих объектов управления в систему и обеспечения их взаимодействия с системой, намного выше тех, которые требуются на других этапах.

А.4 Уровни функциональной совместимости

А.4.1 Уровень 0

Любая HBES-система на Уровне 0 является полностью автономной и способной работать в одной или нескольких прикладных областях, однако неспособной взаимодействовать с другими HBES-системами/технологиями. Эта система обладает структурой, которую определяет поставщик и которая не может изменяться без предварительного перепроектирования и новой установки.

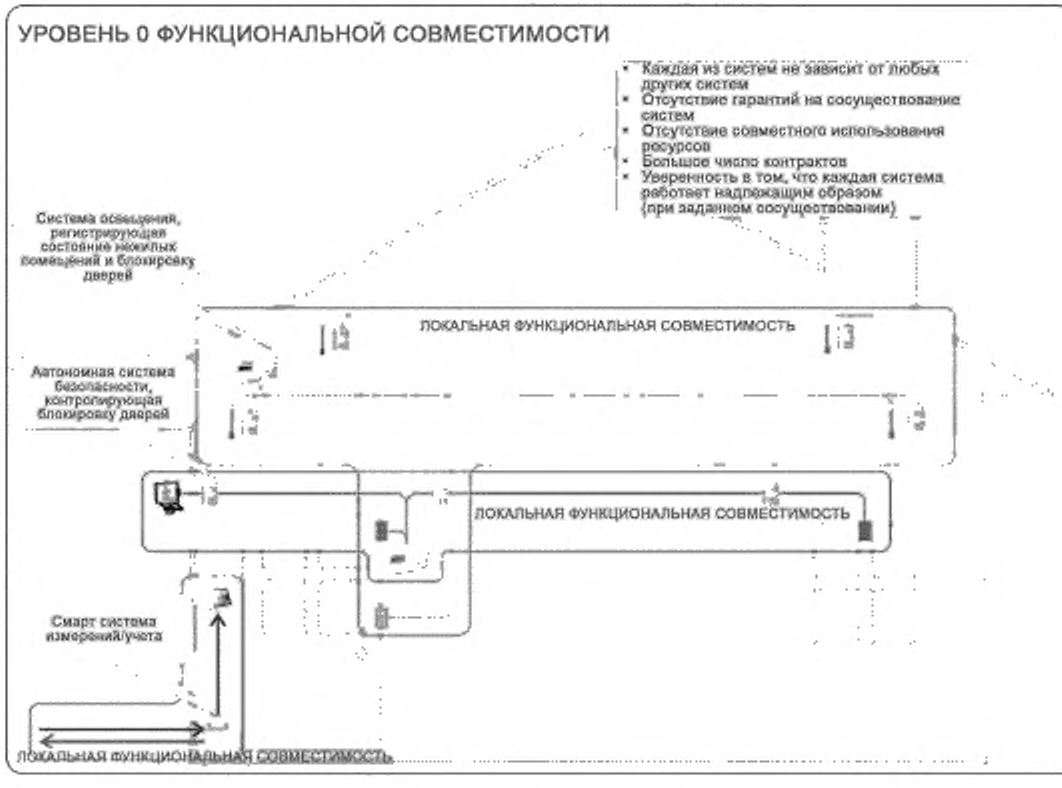

Рисунок А.1 — Комплекс систем Уровня 0 функциональной совместимости

При этом не утверждается, что данная система сможет сосуществовать с другими HBES-системами в одних и тех же помещениях (условиях). На рисунке А.1 показан комплекс систем Уровня 0, использующий сочетание спецификаций на системы связи, причем нельзя гарантировать, что они не будут создавать помехи друг для друга.

Любая функциональная совместимость, присущая системе Уровня 0, поддерживается только его HBES-спецификацией, а также проводимым разработчиками тестированием приложений, которые определены и используются в рамках конкретной системы.

Примеры —

- ***Система комфорт-контроля;***
- ***Система открывания/закрывания окон, жалюзи и занавесок;***
- ***Система для домашних развлечений и распределения аудио/видеоинформации.***

С учетом сказанного выше, ограничения на структуру системы Уровня 0 должны отсутствовать. Структура может содержать несколько взаимосвязанных средств связи (проводных или беспроводных), иметь компоненты шлюза/маршрутизатора, однако все эти компоненты должны соответствовать одной и той же HBES-спецификации.

Устройства/системы на Уровне 0 не претендуют на совместимость с любыми другими устройствами, даже с теми, которые принадлежат одному и тому же поставщику (или же другому поставщику, но реализующему ту же HBES-систему). При этом предполагается, что их функциональная совместимость тестируется торговой ассоциацией или разработчиками системы. Для систем Уровня 0, указанных в настоящем стандарте, требования к соответствию отсутствуют.

А.4.2 Уровень 1

Функциональная совместимость на Уровне 1 идентична функциональной совместимости на Уровне 0, за исключением того, что она обеспечивает сосуществование систем Уровня 1, т. е. систем, которые отвечают одной HBES-спецификации и полностью реализуются в соответствии с этой спецификацией.

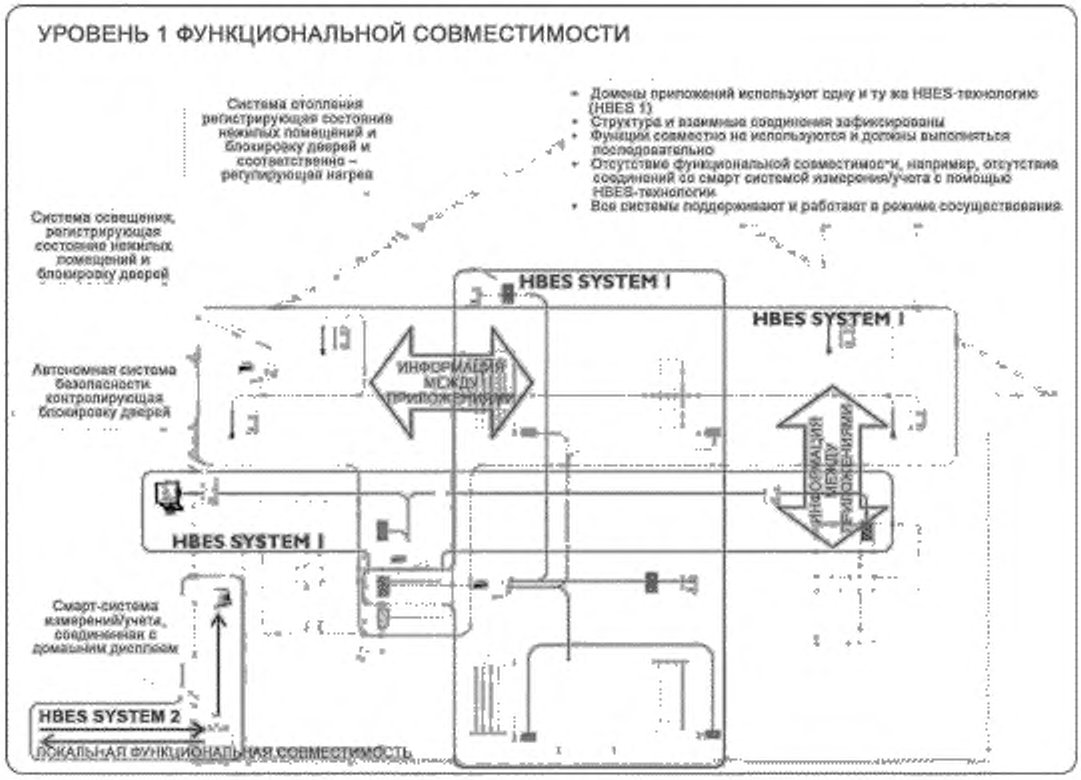

Рисунок А.2 — HBES-система Уровня 1 функциональной совместимости

Рисунок А.2 иллюстрирует жилое помещение, в котором в основном установлена система HBES 1. Поскольку одна и та же HBES-система способна функционировать во всех областях домена приложения, для передачи информации между ними никаких препятствий существовать не будет. Существует также ряд HBES-решений, которые устанавливают требования к обеспечению данного Уровня функциональной совместимости.

В тех случаях, когда с помощью приложения Smart Metering (Система смарт-учета) применяется система HBES 2, связь между доменами приложений будет отсутствовать.

Примеры —

- Комфорт-контроль, который позволяет объединять контроль отопления, освещения и вентиляции;

- Управление потреблением электроэнергии бытовыми приборами (холодильниками, стиральными машинами), взаимодействующее с комфорт-контролем.

С учетом сказанного выше, ограничения на структуру системы Уровня 1 будут отсутствовать. Эта структура может содержать несколько взаимосвязанных средств связи (проводных или беспроводных) и, следовательно, иметь компоненты шлюза/маршрутизатора, однако все эти компоненты должны соответствовать одной и той же HBES-спецификации.

Устройства, требующие функционального соответствия на Уровне 1, не претендуют на функциональную совместимость с любыми другими устройствами, даже с теми, которые имеют одного и того же поставщика (или же другого поставщика, но реализующего ту же HBES-систему). При этом предполагается, что функциональная совместимость устройств (в частности, структурная целостность операций, выполняемых этими устройствами и коллективно используемых двумя и более приложениями) тестируется торговой ассоциацией или разработчиками системы. В настоящем стандарте требования к подобному соответствию отсутствуют.

А.4.3 Уровень 2

Система Уровня 2 реализует требования, предъявляемые к двум и более HBES-спецификациям. В ней существует, по крайней мере, один шлюз или мост, способные связывать средства двух и более систем и обеспечивать взаимодействие между ними. Этот межсетевой интерфейс позволяет взаимодействовать устройствам, отвечающим любой из HBES-спецификаций. Последнее также обеспечивает взаимодействие между различными доменами приложений и обмен ресурсами, как и на Уровне 1.

Предполагается, что подобная функциональная совместимость тестируется и сертифицируется торговой ассоциацией или разработчиками системы, причем сертификация должна основываться на отраслевых стандартах, а не на стандартах на испытания на соответствие.

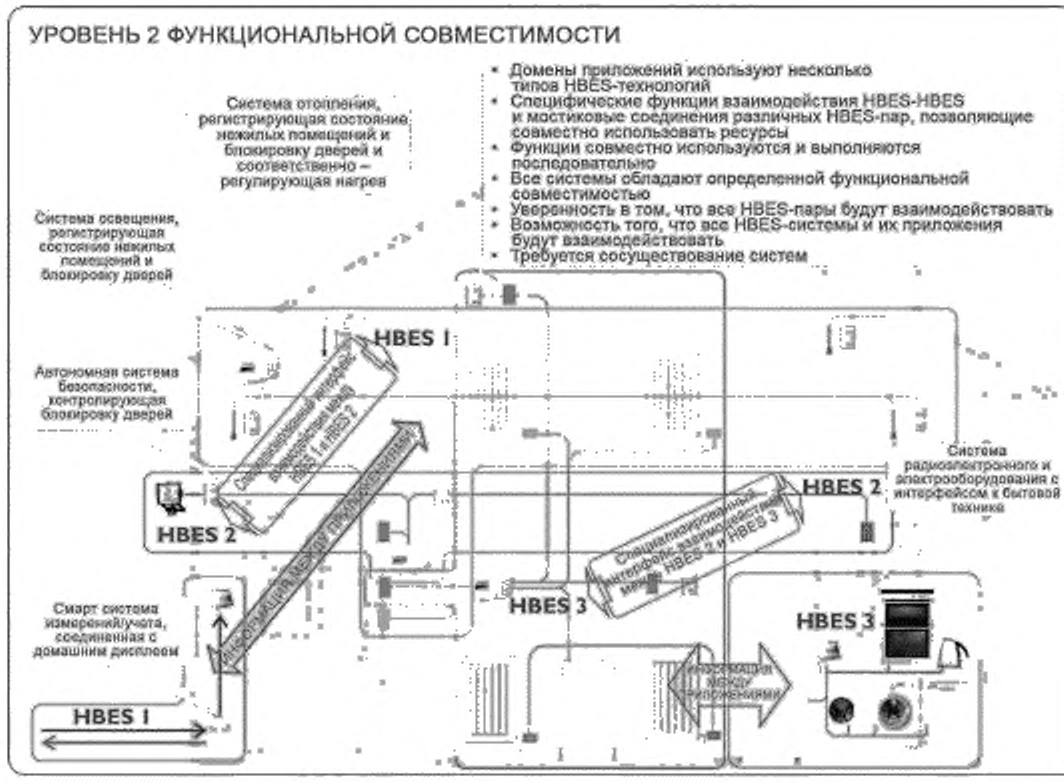

Рисунок А.3 — Несколько систем, взаимодействующих между собой на Уровне 2 функциональной совместимости

Рисунок А.3 иллюстрирует взаимосвязь между системой безопасности и смарт-системой измерений/учета с использованием специального интерфейса, обеспечивающего взаимодействие коммуникационных протоколов и позволяющего осуществлять взаимодействие между приложениями. Подобным интерфейсом может быть шлюз или мост между двумя HBES-системами, который согласован торговыми ассоциациями для каждой системы (или был специальным решением, предоставляемым установщиком приложений). После первоначальной установки интерфейса поставщик энергии может предоставить потребителю приложение для персонального компьютера (возможно, связанное с веб-сервисом), которое будет способно взаимодействовать с обоими приложениями.

Примеры —

- Система безопасности, позволяющая устанавливать связь с ее владельцем с помощью GSM SMS-сообщений для оповещений и контроля;

- Система управления потреблением электроэнергии, позволяющая взаимодействовать с розничными поставщиками электроэнергии с помощью веб-сервисов, встроенных в шлюз или в компьютерную систему;

- Смарт-система измерений/учета, позволяющая взаимодействовать с поставщиком энергии в частной сети с помощью собственных протоколов, с бытовыми приборами в доме с помощью каналов передачи данных и локальных беспроводных средств малого радиуса действия для управления энергопотреблением, а также с локальным дисплеем, использующим Zigbee-профиль и стандарт IEEE 802.15.4.

А.4.4 Уровень 3

Отличие систем Уровня 3 от системы Уровня 2 состоит в том, что их функциональная совместимость проверяется на соответствие Международным стандартам (что позволяет совместно использовать необходимые ресурсы) и обычно выполняется специальным установщиком приложений в рамках единого контракта на установку и техническое обслуживание системы.

Тем не менее, функциональная совместимость на Уровне 3 требует привлечения высококвалифицированных установщиков приложений/инженеров для создания системы, взаимодействующей с HBES-системами нескольких типов, причем каждая установка требует инженерного обеспечения, гарантирующего функционирование системы, а любые изменения в системе требуют привлечения высококвалифицированных инженеров.

Рисунок А.4 — Функциональная совместимость систем на Уровне 3

Система Уровня 3 имеет такие же характеристики, как для систем Уровня 1 (т. е. сосуществование нескольких приложений), так и систем Уровня 2 (т. е. взаимодействие нескольких систем связи).

Примеры —

- Домовая система безопасности, позволяющая устанавливать связь с владельцем дома с помощью GSM SMS-сообщений для его оповещений и контроля; при этом владелец дома с помощью SMS-сообщений может взаимодействовать и с системой комфорт-контроля дома;

- Смарт-система измерений/учета также позволяет использовать приложение для экстренного вызова медицинской помощи, наблюдения за поведением жильцов и использования частной сети поставщика электроэнергии (совместно с поставщиком медицинских услуг с целью выдачи предупреждений относительно возможных нарушений санитарно-гигиенических условий жизни жильцов в доме).

А.4.5 Уровень 4

Уровень 4 отличается от Уровней 0—3, поскольку в соответствии с требованиями IFRS-спецификации предусмотрен стандартный набор средств, позволяющий использовать устройства/приложения и взаимосвязи между ними, изменять и управлять ими в процессе функционирования системы. В других случаях Уровень 4 обладает всеми функциональными возможностями Уровня 3.

Устройства, обладающие определенной функциональностью и требующие соответствия на Уровне 4, могут взаимодействовать с другими устройствами с аналогичной функциональностью (или же с дополнительной функциональностью на этом же Уровне). Они могут быть взаимозаменяемыми при идентичности намеченных целей.

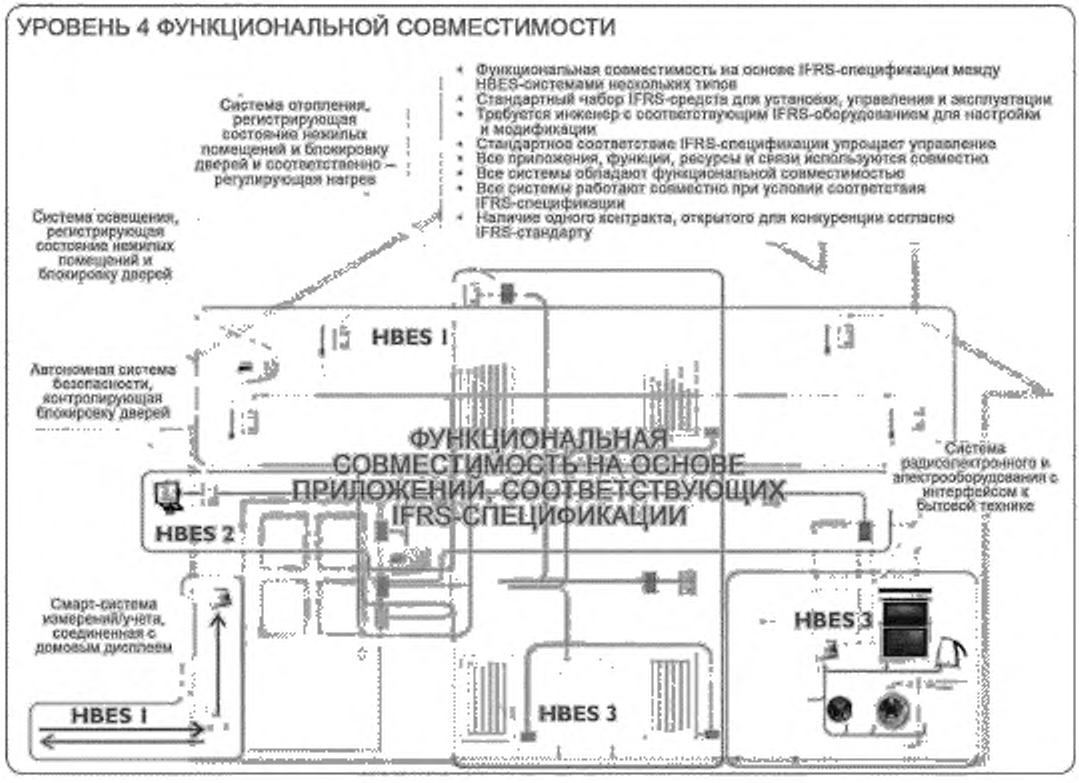

Рисунок А.5 — IFRS-функциональная совместимость на Уровне 4

Механизм верификации на Уровне 4 отличается от механизма верификации, используемого на Уровнях 0—3. Устройства, требующие функциональной совместимости на Уровне 4, должны отвечать требованиям соответствия, установленным в настоящем стандарте в отношении их возможностей по организации и установлению связи, по обнаружению и конфигурированию (вместе с соответствующими мерами безопасности). Поставщик приложений, предполагающий их использование, должен запрашивать дополнительную верификацию их пригодности для использования по назначению, с привлечением к тестированию специализирующейся на данном приложении организации.

Таблица А.2

Этап/Функция	Обнаружение	Конфигурирование	Эксплуатация	Управление системой
Процессы	Должны внутренне поддерживать этапы обнаружения и конфигурирования в процессе первоначальной настройки, сброса и модификации системы. Пользователь может вмешиваться в эти этапы для выборочного допуска и активации функциональных возможностей устройств		Приемлемы для функционирования системы. Устройства, совместно использующие несколько приложений, необходимо применять последовательно и безопасно	Недоступны для пользователя
Безопасность	Поскольку доступ к установке возможен извне помещений, то необходимо обеспечивать защиту от проникновения, прослушивания и отказа в обслуживании. Для разрешения установщику запрашивать удаление (сброс) дистанционных устройств и установку новых, следует предоставлять ему контроль доступа		Пользовательский интерфейс может обеспечивать контроль доступа, например, с помощью PIN-кода. Для приоритетной обработки событий и операций с более высоким приоритетом необходимо разрешать все конфликты	Поскольку доступ к установке возможен извне помещений, то необходимо обеспечивать защиту от проникновения, прослушивания и отказа в обслуживании
Средства реализации	Недоступны для пользователя			Доступны для установщика
Модель взаимодействия	Доступна и может применяться установщиком, но не пользователем			
	Операции можно активировать с помощью шлюзов между различными технологиями. Для создания интегрированной системы необходимо согласовывать меры по обеспечению взаимодействия и функциональной совместимости			
Поддержка перекрестных стандартов	Содержит один или несколько шлюзов, которые обладают информацией об устройствах и их возможностях на подсоединенных средствах			

Примеры:

- Приложение для экстренного вызова медицинской помощи, которое позволяет получать предупреждения от устройств, носимых пациентом, получающим медицинскую помощь на дому. Эти устройства устанавливают связь при помощи технологии Bluetooth и защищенного встроенного устройства управления eHealth в пользовательском шлюзе, который предоставляется поставщиками медицинских услуг и связи. Эти устройства также взаимодействуют с устройством управления энергоснабжением пациента и с системой комфорт-контроля с целью поддержания уровней энергопотребления, нагрева и освещения.

В рамках указанных выше ограничений, характерные ограничения на структуру системы Уровня 4 или на ее функциональные возможности по внутреннему/внешнему подсоединению в помещениях будут отсутствовать.

Устройства, обладающие определенной функциональностью и требующие соответствия на Уровне 4, будут обеспечивать взаимодействие с другими устройствами с аналогичной или дополнительной функциональностью на этом же Уровне. Они могут быть взаимозаменяемыми при наличии у них одной и той же конкретной цели. Эта функциональность относится и к соответствующим устройствам независимо от средств, используемых для связи, например:

- На Уровне 4 датчик падения в мобильном телефоне с помощью встроенных в него акселерометров обеспечивает связь (обмен данными) с использованием протокола IEEE 11073 для объектов-приложений, переносимого в простой протокол доступа к объектам SOAP с помощью системы пакетной радиосвязи общего пользования GPRS. Этот датчик пришел на смену морально устаревшему датчику падения, использовавшего технологию Bluetooth. Пожилой человек может использовать либо любой из этих датчиков, либо оба датчика одновременно. Помощник, осуществляющий уход за этим пожилым человеком, может устанавливать эти датчики самостоятельно. Ответственность за сертификацию датчиков на реальное падение несут органы здравоохранения, которые должны быть уверены в возможности взаимодействия устройств и сосуществования с другими приложениями;

- Термостат, использующий Zigbee- и 802.15.4-протоколы, установлен в гостиной жилого дома, жильцы которого жалуются, что в остальной части дома слишком холодно; по этой причине они ре-

шили установить второй термостат, который будет использоваться для регулирования температуры в верхних помещениях. Жильцы обращаются к своему приоритетному онлайн-поставщику и по ошибке приобретают термостат, предназначенный для устройств Уровня 2. После того, как он был доставлен, жильцы установили его в нужное место в верхнем помещении и включили: поскольку у термостата отсутствовали средства для его обнаружения системой Уровня 4, то он не заработал. Возвратив термостат поставщику и выбрав термостат, предназначенный для Уровня 4, они снова предприняли попытку использовать его, однако вновь ничего не получалось до тех пор, пока жильцы не догадались нажать большую красную кнопку сброса, которую они заметили на термостате. Система комфорт-контроля обнаружила термостат, и поскольку монитор был включен, на нем появилось сообщение-запрос на подтверждение допуска этого термостата к эксплуатации.

Функциональная совместимость на Уровне 4 также может требоваться для программных компонентов, например, для приложений Java, которые загружаются в телефон или шлюз, или же активируются для выполнения операций в удаленной среде («облаке») вне помещений.

А.4.6 Уровень 5

Устройства, требующие функциональной совместимости на Уровне 5, способны автоматически адаптироваться к изменениям, которые могут происходить по инициативе потребителя-владельца системы. Последнее не означает, что взаимодействие с владельцем, пользователем или жильцами помещений полностью исключается, поскольку весьма вероятно, что это взаимодействие потребует либо само устройство, либо приложение на этапе завершения процедуры конфигурирования.

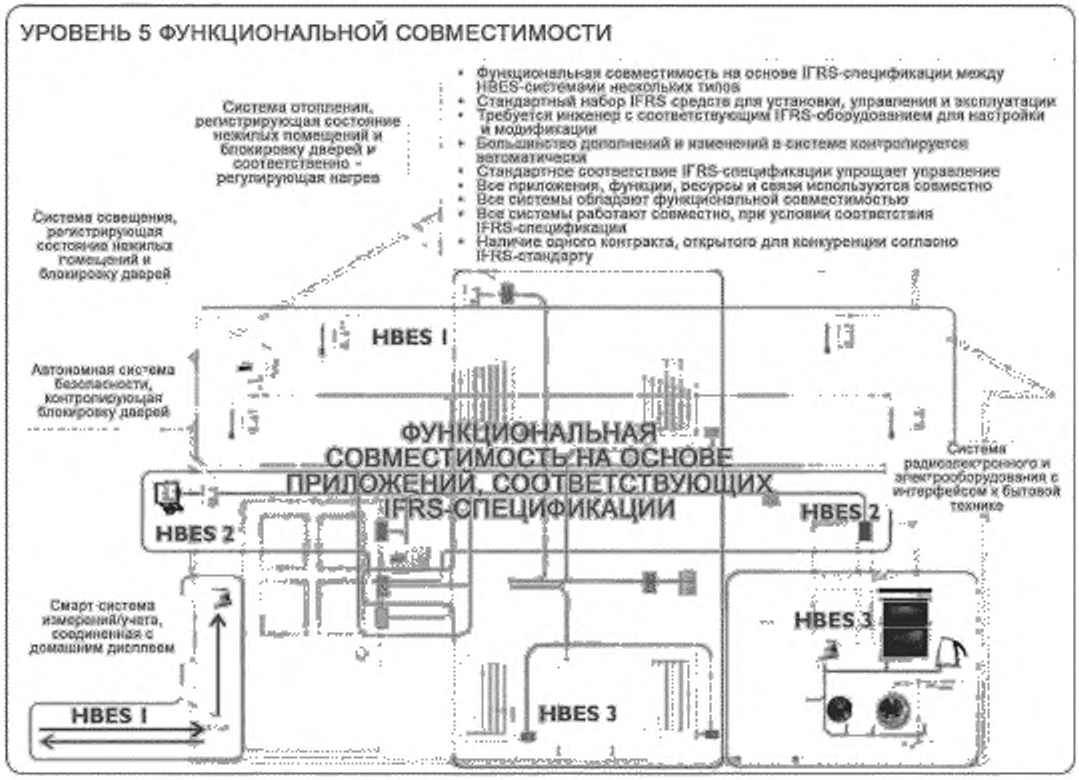

Рисунок А.6 — IFRS-функциональная совместимость на Уровне 5

Например, детектор движения на Уровне 5 не требует взаимодействия со своей локальной инфраструктурой связи для обнаружения шлюза, получения его сетевого адреса и объявления идентификатора объекта/функций для частичного завершения процесса конфигурирования. Для получения допуска к приложению установщик приложений или владелец, вероятно, должны будут обозначить приложение, к которому относится сам детектор, для чего потребуется взаимодействие с системой (функцией) управления.

Таблица А.3

Этап/Функция	Обнаружение	Конфигурирование	Эксплуатация	Управление системой
Процессы	Должны внутренне поддерживать этапы обнаружения и конфигурирования в процессе первоначальной настройки, сброса и модификации системы. Пользователь может вмешиваться в эти этапы для выборочного допуска и активации функциональных возможностей устройств		Приемлемы для функционирования системы. Устройства, совместно использующие несколько приложений, необходимо применять последовательно и безопасно	Недоступны для пользователя
Безопасность	Поскольку доступ к установке возможен извне помещений, то необходимо обеспечивать защиту от проникновения, прослушивания и отказа в обслуживании. Для разрешения установщику запрашивать удаление (сброс) дистанционных устройств и установку новых, следует предоставлять ему контроль доступа		Пользовательский интерфейс может обеспечивать контроль доступа, например, с помощью PIN-кода. Для приоритетной обработки событий и операций с более высоким приоритетом необходимо разрешать все конфликты	Поскольку доступ к установке возможен извне помещений, то необходимо обеспечивать защиту от проникновения, прослушивания и отказа в обслуживании
Средства реализации	Доступны пользователю, включая доступ к внешним программным интерфейсам и протоколам			Доступны только для установщика
Модель взаимодействия	Доступна и может задействоваться установщиком и пользователем			
	Операции можно активизировать с помощью шлюзов между различными технологиями			
Поддержка перекрестных стандартов	Содержит один или несколько шлюзов, которые обладают информацией об устройствах и их возможностях на подсоединенных средствах			

А.4.7 Уровень 6

Уровень 6 расширяет функциональные возможности на Уровне 5 и открывает дополнительный доступ к устройствам для активации выполнения функций управления, которые могут потребоваться для диагностических целей, обновления прошивки или сбора статистических данных.

В отличие от Уровней 1—5, Уровень 6 требует более строгой защиты и контроля доступа для защиты от несанкционированного доступа. Поскольку операции управления могут потребовать согласия владельца, должны быть созданы условия для верификации операций и предотвращения их отказа любыми участниками связи.

Рисунок А.7 — IFRS-функциональная совместимость на Уровне 6

В отличие от Уровней 1—5, для обеспечения защиты от несанкционированного доступа Уровень 6 требует принятия более жестких мер безопасности и контроля доступа. Поскольку операции управления могут потребовать согласия владельца устройства, необходимо создать условия для верификации операций и обеспечить их отказоустойчивость. В остальном Уровни 5 и 6 не отличаются.

Таблица А.4

Этап/Функция	Обнаружение	Конфигурирование	Эксплуатация	Управление системой
Процессы	Должны внутренне поддерживать этапы обнаружения и конфигурирования в процессе первоначальной настройки, сброса и модификации системы. Пользователь может вмешиваться в эти этапы для выборочного допуска и активации функциональных возможностей устройств		Приемлемы для функционирования системы. Устройства, совместно использующие несколько приложений, необходимо применять последовательно и безопасно	Доступны для пользователя
Безопасность	Поскольку доступ к установке возможен извне помещений, то необходимо обеспечивать защиту от проникновения, прослушивания и отказа в обслуживании. Для разрешения установщику запрашивать удаление (сброс) дистанционных устройств и установку новых, следует предоставлять ему контроль доступа		Пользовательский интерфейс может обеспечивать контроль доступа, например, с помощью PIN-кода. Для приоритетной обработки событий и операций с более высоким приоритетом необходимо разрешать все конфликты	Поскольку доступ к установке возможен извне помещений, то необходимо обеспечивать защиту от проникновения, прослушивания и отказа в обслуживании

Окончание таблицы А.4

Этап/Функция	Обнаружение	Конфигурирование	Эксплуатация	Управление системой
Средства реализации	Доступны для пользователя, включая доступ к внешним программным интерфейсам и протоколам			
Модель взаимодействия	Доступна и может задействоваться установщиком и пользователем			
	Операции можно активизировать с помощью шлюзов между различными технологиями. Для создания интегрированной системы необходимо согласовывать меры по обеспечению взаимодействия и функциональной совместимости			
Поддержка перекрестных стандартов	Содержит один или несколько шлюзов, которые обладают информацией об устройствах и их возможностях на подсоединенных средствах			

А.4.8 Сочетание различных уровней функциональной совместимости в рамках одной и той же установки

Поскольку разнообразие HBES-технологий/приложений и их взаимосвязь постоянно растет, а некоторые элементы системы со временем могут изменяться сами по себе, то, скорее всего, устройства и приложения, соответствующие различным IFRS-уровням, будут размещаться в одних и тех же помещениях.

В таблице далее приведены прогнозы относительно функциональной совместимости продуктов, относящихся к различным уровням функциональной совместимости. Таблицу следует интерпретировать следующим образом: прогноз относительно функциональной совместимости продуктов на Уровне [*строка*] при их вводе в систему для продуктов на Уровне [*столбец*].

Для полноты анализа в эту таблицу также включены и продукты Уровней 2 и 3, поскольку на этих Уровнях имеется возможность взаимодействия (в том числе и на самих Уровнях), что может обеспечивать доступ к продуктам более высокого Уровня.

Таблица А.5

Уровень	2,3	4	5	6
2,3		Продукты Уровней 2—3 должны иметь возможность взаимодействовать с любыми другими продуктами на Уровнях 4, 5 и 6 (в рамках функциональных возможностей Уровней 2—3), однако интеграция устройств Уровней 4, 5 и 6 требует квалифицированной установки и конфигурирования		
4	Для продуктов, квалифицированно установленных на Уровнях 4, 5 и 6, существует возможность их применения в системах на Уровнях 2 и 3 и взаимодействия с продуктами на Уровнях 2 и 3 (но только при конфигурировании в ручном режиме)		Продукты на Уровне 4 должны взаимодействовать с продуктами на Уровне 5 (при вмешательстве оператора) и не смогут адаптироваться к изменениям в конфигурации продукта на Уровне 5 (без вмешательства оператора)	Продукты на Уровне 4 могут взаимодействовать с продуктами на Уровне 6 (при вмешательстве оператора) и не смогут адаптироваться к изменениям в продуктах на Уровне 6 (без вмешательства оператора) и не будут поддерживать функции управления на Уровне 6 (используемые локально или дистанционно)
5		Продукты на Уровне 5 должны взаимодействовать с продуктами на Уровне 4 и иметь возможность автоматически обнаруживать/конфигурировать их		Продукты на Уровне 5 должны быть совместимы с продуктами на Уровне 6 и иметь возможность автоматически обнаруживать/конфигурировать их
6		Продукты на Уровне 6 должны взаимодействовать с продуктами на Уровнях 4 и 5 и иметь возможность автоматически обнаруживать/конфигурировать их (локально и дистанционно). Они также не могут выполнять функции управления продуктами на Уровне 4 или 5		

А.5 Прецеденты использования

А.5.1 Методология

А.5.1.1 Общие положения

Прецеденты, приведенные в данном разделе, использовались в качестве основы при разработке настоящего стандарта; они также могут служить тест-примерами для валидации проекта и призваны проиллюстрировать общие проблемы, не исчерпывая все возможные варианты.

В настоящем стандарте используются следующие возможные прецеденты, которые могут происходить при функционировании системы:

- например, кто-то/что-то
(делает.....)
(необходимо знать ....) и
необходимо (получить следующую информацию.....)
(выполнить следующее.....)
и необходимо использовать следующие ресурсы
(Объект 1, Объект 2, ..., Объект n — 1, Объект n)
следующим образом (набор методов .....)

А.5.1.2 Описание прецедентов использования

Прецеденты использования — это способ фиксации требуемых взаимоотношений (характера поведения) системы и требований, предъявляемых заинтересованными сторонами, которые равным образом применимы ко всем их видам (взаимоотношений и требований). Прецеденты использования — это также основа для описания различных аспектов системных требований. При этом необходимо выделять требования к функциональной совместимости, в то время как основные части описания какого-либо стандартного прецедента дают только контекст и фон для их понимания. Для этого, а также для выявления проблем функциональной совместимости и исключения второстепенных деталей приняты пять концепций «W» (Who, What, Where, When и Why) [кто, что, где, когда и почему] и одна концепция «H» (how) [как].

Если в прецедентах приводятся требования к функциональной совместимости какой-то части системы, то в рассматриваемых примерах необходимо акцентировать (в табличной форме) внимание на взаимосвязь между IFRS-спецификацией и другими компонентами системы. Пять W-концепций должны формулироваться установщиком приложений или пользователем, которым следует устанавливать требования, а одна концепция (H) — должна определять элементы применяемой IFRS-спецификации.

Таблица А.6

Who (Кто?)	Указание основной заинтересованной стороны (объекта), которая(ый) инициирует взаимодействие с системой (в особенности — с IFI-средой). Этой стороной могут быть компоненты системы (например, датчик, исполнительный механизм) или пользователи системы (например, конечный пользователь, установщики приложений и инженер-специалист по техническому обслуживанию). Заключение основной заинтересованной стороны подразумевает его намерения и перспективы
What (Что?)	Предоставление деталей пошагового взаимодействия для выявления любых требований (как и при стандартном описании прецедента использования). Вместо регистрации подробных сведений о процессе функционирования системы обеспечивается получение контекста операции взаимодействия и определяется сопричастность к взаимодействию
Why (Почему?)	Поддержка и обоснование проблем взаимодействия, приведенных в конкретном прецеденте (по возможности установление их необходимости и важности)
Where (Где?)	Описание места, где происходят взаимодействия
When (Когда?)	Определение фазы жизненного цикла системы, т. е. фазы установки, ввода в эксплуатацию, эксплуатации, технического обслуживания или модернизации
How (Как?)	Определение способа принятия концептуальных решений, обеспечиваемых IFI-средой
Приоритет	Связь с уровнем функциональной совместимости будет давать приоритет в рамках разработки и развития IFI-среды

Следующая таблица содержит пример, иллюстрирующий способ документирования прецедентов использования; в данном случае — это использование датчика обнаружения движения для включения/выключения освещения. Когда этот датчик обнаруживает людей в помещении, свет загорается; при их выходе — свет выключается.

Таблица А.7

Who (Кто?)	Датчик обнаружения движения (системная интеграция)
What (Что?)	1. Датчик обнаруживает движение 2. Датчик выдает сигнал на переключатель освещения 3. Переключатель освещения включает осветитель
Why (Почему?)	1. Датчик обнаружения движения и переключатель освещения выполнены по различным домашним сетевым технологиям 2. Датчик обнаружения движения находится в сети с высокой степенью защиты, а переключатель освещения — в сети с низкой степенью защиты
Where (Где?)	Информация о движении передается от датчика к переключателю освещения
When (Когда?)	На этапе эксплуатации
How (Как?)	1. Преобразование сетевого формата датчика в сетевой формат переключателя освещения 2. Согласование уровней безопасности датчика и переключателя освещения
Приоритет	Уровень 2 и 3 функциональной совместимости, высокий приоритет

А.6 IFRS-методология

А.6.1 Общие положения

Концепция функциональной совместимости и (межсетевого) взаимодействия производит впечатление общепринятой, однако определения терминов в различных контекстах могут существенно различаться.

Для иллюстрации причин и степени их различий интерпретация определений, приведенных в 3.3 настоящего стандарта, может быть разбита на несколько уровней.

А.6.2 Физический уровень, трассы и средства связи (PHY-уровень)

Элементами, которые должны обеспечивать взаимодействия, могут, например, быть проводные/беспроводные устройства передачи данных, вилки/гнезда разъемов и т. п., несовместимость которых является обычным явлением, а типичным примером могут служить штепсельные сетевые и телефонные розетки. В этих случаях устройства, использующие, например, переменное напряжение 220 В 50 Гц, в основном являются совместимыми, но могут не взаимодействовать из-за наличия региональных различий, хотя применение шлюза в виде адаптера или, возможно, кабеля, позволяет восстанавливать взаимодействие между различными устройствами. Если устройство рассчитано на напряжение сетевого питания 110 В 60 Гц, то невозможно его взаимодействие с устройством, которое питается только напряжением 220 В, однако благодаря наличию в источнике питания внутреннего шлюза, определяющего тип питающего напряжения, это нарушение функциональной совместимости практически исчезает.

Средство связи используется несколькими сервисами, что может приводить к возникновению проблем их сосуществования, на что существует две основные причины:

- сервисы используют различные протоколы (для параметров времени, форматов сообщений и сигнализации, включая выдачу сообщений о ширине спектра, кодировании и модуляции, называемые в своей совокупности «PHY-уровнем»), которые способны создавать помехи друг другу. Последнее скорее относится к проблеме сосуществования, поскольку эти средства могут работать параллельно, например, в различных диапазонах спектра (хотя часто это не делается). Например, устройства на линии электропередачи, в которых реализован стандарт ITU-T G.9960 (IEEE 1990), снабжаются протоколом G.cx, который позволяет им поддерживать несколько сервисов. Во-первых, эти устройства должны периодически сообщать о своем присутствии и своем типе, передавая сигнатуру, которая должна однозначно идентифицировать их и устройства других типов; во-вторых, эти устройства должны использовать протокол мультиплексирования, который обеспечивает их разделение по времени доступа к средствам связи. В этом случае остается неясным, каким образом будет осуществляться поддержка устройств устаревших типов, которые установлены и работали до развертывания устройств, отвечающих рекомендациям G.9960, но неспособны сосуществовать из-за невозможности реализации протокола G.cx. Еще один пример — это полоса частот ISM 2,4 ГГц, чрезмерно используемая устройствами с различными протоколами, которые могут создавать взаимные помехи или конфликтовать друг с другом самыми непредсказуемым и нежелательным образом. Для функциональной совместимости необходимо достижение удовлетворительного разделения работы устройств во времени и пространстве;

- сервисы используют один и тот же протокол доступа, однако это все же не позволяет им должным образом совместно работать из-за ошибочности реализации какого-либо устройства или неоднозначности в интерпретации стандарта на другие активные устройства. Последнее частично создает проблему при утверждении типа устройства и тестирования на PHY-уровне, однако с большей вероятностью эта проблема будет решаться на более высоком уровне.

А.6.3 Управление каналом передачи данных (DLC)

На DLC-уровне обеспечивается управление доступом к каналу передачи данных (MAC), хотя MAC-управление обычно может обладать такими аспектами, которые также будут зависеть от PHY-спецификации (например, синхронизация или выбор канала связи), граница между которыми не всегда очевидна. Эталонная модель взаимодействия открытых систем (OSI-RM) позволяет идентифицировать функциональные обязанности DLC-управления в конкретном контексте взаимодействия между устройствами, однако многие современные спецификации способны обеспечивать DLC-уровень для локального/удаленного мостового соединения, релейного управления, маршрутизации и создания виртуальных подсетей (например, VLAN IEEE 802.1q, или ITU-T G.9960). В некоторых системах маршрутизация может выполняться только на DLC-уровне. OSI-RM-модель предусматривает возможность выполнения этого на сетевом уровне, подробное пояснение приведено ниже.

При условии обеспечения сосуществования на PHY-уровне (см. выше), различные виды DLC-управления будут взаимно «прозрачными» и сосуществующими, поэтому проблемы функциональной совместимости могут быть связаны с конкретными вариантами реализации и DLC-функционированием в рамках отдельных спецификаций, а также со связью (взаимодействием) между различными видами DLC-управления (или между различными экземплярами одного и того же вида DLC-управления на шлюзах), которые выполняют функции мостового соединения, релейного управления и маршрутизации.

Реализация и варианты функционирования DLC-управления, как правило, описаны в рекомендациях, изложенных в соответствующих спецификациях, которые предназначены для подсоединения совместимых устройств к средствам связи и обмена пакетами данных с другими совместимыми устройствами, требуя при этом использования устройствами MAC-протоколов, адресов и режимов адресации (в режимах одноадресной, групповой и многоадресной передачи данных, см. ниже), а также постоянного использования управляющих данных. Функции DLC-шлюза действуют везде, где различные средства связи/PHY-уровни взаимосвязаны. Примером может служить аналоговый модем коммутируемой линии передачи данных ITU-T V-серии. Этот тип DLC-шлюза является «прозрачным» мостом или реле, функции которых аналогичны таковым, реализованным во внутренних широкополосных DSL-шлюзах на DLC-уровне; вызов выполняется по ISP-технологии по назначенной VP/VC-паре с использованием такого протокола управления, как, например, Q.931 или X.21; пользовательские данные кодируются с использованием PPPoATM-протокола или любого другого аналогичного протокола кадровой синхронизации. Проблемы функциональной совместимости, связанные с протоколом Q.931, часто обусловлены выбором несовместимой нумерации схем. Существуют соглашения относительно использования VP- и VC-номеров, однако они выбираются разработчиками и могут конфликтовать между собой.

Пример — Аналоговый модем коммутируемой линии передачи данных реализует RS232-интерфейс (согласно EIA-спецификации) по одному каналу, обращенному к последовательному порту компьютера, а также один или несколько протоколов серии ITU-T V по второму каналу, обращенному через телефонную коммутируемую сеть общего пользования (PSTN) к другому модему, подсоединенному к устройству, которое предоставляет сервис коммутируемого доступа; этот модем взаимодействует между двумя каналами, переводя битовые потоки пользовательских символов в сигнализацию V-серии. Существует также требование контроля, налагаемое PSTN-сетью, а именно — необходимость выдачи сообщения на модем относительно номера для набора, что представляется с помощью отдельного протокола, широко используемого для набора команд Hayes AT. Если номер представляется в стандартном формате ITU-T X.121, то вызов должен устанавливаться в любом месте, причем модем также должен воспринимать сигналы готовности к приему набора номера, сигналы «занято» и сигналы «недоступно», которые до сих пор различаются во всем мире. В прошлом наблюдались частые нарушения функциональной совместимости модемов, которые неправильно выполняли свои функции, или же из-за несоответствия PSTN-сети (или же из-за нарушений взаимодействия, когда функции реализовались правильно, однако чрезмерная задержка, ложные сигналы и помехи на линии превышали время «полезного» функционирования сети).

Пример — DLC-шлюз может связывать различные устройства в помещениях, например, компьютерную приставку к телевизору (STB) с HDMI-портом, с реле к другим телевизорам, использующим рекомендации G.9960 для линии электропитания. STB-приставка должна использовать надлежащее время (выделенный интервал) и пространство при мультиплексировании линии электропитания для поддерживаемых протоколов. Эта приставка может содержать порт, соответствующий протоколу IEEE 802 (.3 — Ethernet; .11 — WiFi), через который приставка может получать контент телевизионной программы (помимо контента, получаемого через антенный ввод), и, возможно, Zigbee- или ИК-порт для локального программирования или связи с устройствами системы экстренного вызова медицинской помощи пожилым людям и инвалидам. Данный тип DLC-шлюза находится на DLC-уровне, но несмотря на то, что у него имеются явные функции более высокого уровня (например, перекодирование контента в формате 802.2 в HDMI- или G.9960-потоке), информация не интерпретируется им для целей маршрутизации.

Пример — Перспективные «умные» системы измерений (учета) также могут выполнять аналогичную роль — подключаться к внешнему сервису, возможно, к DSL-сервису широкополосного до-

ступа, системе пакетной радиосвязи общего пользования (GPRS) или программируемому логическому контроллеру (PLC). Эти системы также способны подключать одно или несколько средств связи, внутренних по отношению к помещениям, в том числе к линии электропитания, или к беспроводной линии связи малого радиуса действия, которая соединяется с неэлектрическими счетчиками расхода (например, газа).

DLC-шлюзы, которые обеспечивают маршрутизацию с целью поддержки виртуальных сетей, являются стандартными для ICT-приложений устройствами, но до сих пор не так широко используемыми в домашних и строительных системах (за исключением систем для больших помещений), однако в будущем они могут стать стандартными, хотя их технология в настоящее время уже хорошо освоена и является совместимой и взаимодействующей.

Процессы маршрутизации описаны ниже, в А.6.4.

А.6.4 Сетевой уровень и маршрутизация (NWK)

Эталонная модель взаимодействия открытых систем (OSI-RM) определяет функциональные возможности маршрутизации на сетевом уровне.

Сеть характеризуется набором идентификаторов, пространством имен под единым управлением (с семантикой адресов, задающих их местоположение в сети). Назначение идентификаторов состоит в определении направления пересылки информации (маршрутизации) на основе заданных критериев или изучения с использованием вмешательства пользователя или протокола управления.

Устройство, которое поддерживает два или более экземпляров сетевого уровня, является маршрутизатором между пространствами имен, имеющим соединения с несколькими средствами связи, поэтому оно на DLC-уровне, как было указано выше, выполняет функции шлюза, а также, возможно, некоторые (или все) DLC-функции. Тем не менее, их функционирование может изменяться в соответствии с требованиями, предъявляемыми к данному уровню.

Согласно принятому определению функциональной совместимости, устройства должны обладать способностью обмениваться между собой информацией. Любое устройство должно иметь возможность идентифицировать любое другое устройство, чтобы выполнять передачу информации от ее источника (через один или несколько маршрутизаторов) в пункт назначения. По этой причине при маршрутизации необходима возможность совместного использования устройством своих идентификаторов (с общим пониманием их смысла). Эти идентификаторы должны присваиваться таким образом, чтобы сообщение могло бы непрерывно передаваться с помощью маршрутизаторов между источниками информации и ее получателями. Сеть Internet имеет единые схемы назначения имен и адресов, обеспечивающие доставку той информации, которая будет использоваться всеми устройствами, обладающими функциональной совместимостью; должны также существовать полномочия, позволяющие присваивать идентификаторы на систематической основе. В HBES-системах используются различные схемы назначения имен и адресов с различной семантикой. Существуют отраслевые организации, которые контролируют присвоение имен/адресов или дают рекомендации по использованию отдельных систем.

Задача функций межсетевого взаимодействия маршрутизатора состоит в обеспечении надлежащей маршрутизации информации и контроле нарушений пространства HBES-имен. Эта задача должна быть сете-ориентированной и управляться межсегментными (hop-by-hop) маршрутизаторами; или же устройство-ориентированной, например, при использовании маршрутизации с явным перечислением адресов последовательно проходимых узлов (маршрутизацией по источнику). В любом случае необходимая информация для преобразования идентификаторов и выбора надлежащих последующих связей будет занимать память для хранения правил маршрутизации и баз данных для пересылки информации на следующий сегмент.

Обмен информацией не обязательно происходит по схеме «один к одному». Большинство современных систем имеют несколько режимов адресации, включая одноадресную схему («от одного к одному»), групповую схему адресации («от одного к n»), альтернативную адресацию («от одного к n») или многоадресную схему («от одного ко всем»). На маршрутизаторы возлагаются конкретные обязательства по пересылке данных в групповом и многоадресном режиме:

- адреса в режиме групповой передачи данных поступают из определенного подпространства имен и могут назначаться с определенным значением, т. е. с адресацией к «осветительным устройствам» с одним значением, и с другой адресацией к «нагревательным устройствам» — с другим значением. Адреса могут изыматься из общей памяти адресов по требованию, для чего требуется дополнительная поддержка протокола с целью общего выбора устройств (которые намерены использовать эти адреса) и установление путей маршрутизации. Сообщение, отправленное в режиме групповой адресации данных, будет приниматься всеми устройствами, намеренными получать сообщения по данному адресу. Групповая рассылка может реализовываться путем поступательной многоадресной передачи, однако это может создавать избыточный трафик и приводить к дублированию сообщений (при наличии в соединениях между средствами связи замкнутых контуров);

- широковещательное сообщение идентифицируется с помощью назначенного удаленного адреса, которое каждое из устройств должно быть готовым принять. Во избежание перегрузок и распространения дублирующих сообщений маршрутизаторы должны ограничивать распространение этих сообщений лишь на определенное число сегментов, число которых в интернет-сетях обычно равно 0, т. е. многоадресная пересылка сообщений будет приостанавливаться на любом маршрутизаторе, который будет принимать отдельное решение о необходимости дальнейшей пересылки сообщений.

Наконец, поскольку связь между конечными пунктами стала «сквозной», возникают проблемы функциональной совместимости протоколов при адресации. Эти проблемы не следует рассматривать на DLC-уровне и ниже, поскольку все взаимодействия не «видны» вне DLC-уровня (даже при наличии взаимосвязей нескольких DLC-экземпляров, реализованных по одной и той же технологии), однако на сетевом уровне, возможно, придется иметь дело со следующими проблемами:

- несовместимость длины сообщений — сообщение, передаваемое от одного устройства одной и той же сети, может оказаться слишком длинным для его отправки в виде цельного сообщения на следующем сегменте. Если это сообщение невозможно фрагментировать, то две сети не смогут взаимодействовать, и соответственно не смогут взаимодействовать друг с другом и сетевые устройства;
- необходимость организации многоэкранного интерфейса, подтверждение приема сообщений и управление потоками данных — соответствующие протоколы могут быть принципиально несовместимыми, например, исходная система требует подтверждение, которое получатель никогда не будет формировать; или приемник может формировать подтверждение на нижнем уровне (например, на DLC- или на более высоком уровне, например, на транспортном уровне, см. ниже), чтобы шлюз затем переводил это подтверждение на сетевой уровень;
- наличие другой управляющей информации, например, относительно порядковых номеров, которые можно непосредственно заменять;
- различия между маршрутизацией по источнику и межсегментной маршрутизацией;
- привязка по времени, с указанием времени на формирование ответного сообщения или времени на его ожидание/подтверждение.

А.6.5 Транспортный и сеансовый уровни (TRS)

На этих уровнях необходимо устанавливать привязки между объектами в устройствах, в которых используется «сквозное» соединение на нижних уровнях для доставки сообщений от источника в пункт назначения. Они также могут устанавливать право собственности на устройства и функции для их совместного использования в различных приложениях.

В большинстве HBES-систем элементами, которые «видны» на этих уровнях, являются дескрипторы, идентифицирующие объекты прикладного уровня. Многие из указанных проблем функциональной совместимости и взаимодействия между различными схемами назначения имен объектов/ссылок аналогичны тем, которые используются для адресов на сетевых уровнях. Способы сопоставления различных систем аналогичны, т. е. требуется база данных, которая обеспечивает преобразование между пространствами имен.

Проблемы функциональной совместимости протоколов также аналогичны тем, которые были рассмотрены для сетевого уровня.

А.6.6 Прикладной и представительский уровни (APP)

В определенной степени проблемы функциональной совместимости и взаимодействия, рассмотренные для сетевого, транспортного и сеансового уровней, применимы и для данного уровня, т. е. необходимо устранить нарушения целостности имен и протоколов, чтобы связь между конечными пунктами могла стать сквозной. Функции шлюза должны обеспечивать согласование несовместимых протоколов, например, сформированное подтверждение как конкретное ответное сообщение на прикладном уровне получателя отправителю, ожидающему подтверждения на транспортном уровне.

Говоря более конкретно относительно этих двух уровней, формат сообщений, как и модель взаимодействия, будут различаться в разных системах. В некоторых системах используется модель типа «считывание-запись» информации или модель типа «установка/получение», в которой дескриптор объекта, получающего сообщение, и содержимое других полей сообщений определяют операции, которые должен выполнять получатель сообщения. При этом будет возвращаться стандартный ответ на операцию считывания/записи информации. В других системах допускается использовать более качественную модель (например, на основе стандарта ASN.1 или IDL-языка), в которой операции, их коды и информационные поля будут различаться в различных приложениях. При этом информационные поля могут кодироваться несколькими способами, например, с фиксированным или переменным форматом (например, TLV-методом, который также используют в базовых правилах кодирования на представительском уровне OSI-модели). Расположение этих полей может иметь значение.

А.6.7 Основные проблемы, связанные с IFRS-спецификацией

Настоящий стандарт не устанавливает однозначный способ решения рассмотренных ранее проблем или не определяет функциональные возможности отдельных элементов. Его роль состоит в определении возможностей по предоставлению необходимой и достаточной информации для обеспечения функциональной совместимости между устройствами связи. Очевидно, что при этом межплатформенное программное обеспечение и шлюзы играют важную роль. Кроме того, в настоящем стандарте не рассматриваются вопросы функционирования этих объектов из-за наличия нескольких спецификаций на архитектуру, функциональные требования и протоколы (некоторые из которых уже превратились в стандарты), разработанные различными рабочими группами.

На основании вышесказанного необходимо обобщить информацию, которую периферийное устройство, требующее функциональной совместимости на Уровнях 4 и выше, должно выдавать на уровнях, на которых функционирует система связи, а именно на:

- PHY-уровне: информация о соответствии требованиям базового PHY-стандарта и используемых дополнительных функциях в соответствии с возможностями уровня в части функциональной совместимости по обнаружению, конфигурированию, управлению и безопасности (если они были реализованы);

- DLC-уровне: информация о соответствии требованиям базового DLC-стандарта и используемых дополнительных функциях в соответствии с возможностями уровня в части функциональной совместимости по обнаружению, конфигурированию, управлению и безопасности (если они были реализованы), индикации функций PHY-уровня, которые используются для поддержки имеющихся функциональных возможностей, а также идентификации диапазонов адресов и отображений;

- NWK-уровне: информация о соответствии требованиям базового NWK-стандарта и используемых дополнительных функциях, а также диапазоне адресов и алгоритме обнаружения; информация об утвержденном диапазоне параметров данных, используемых информационных полях и алгоритме использования; информация об утвержденных параметрах синхронизации: минимальные/ стандартные/ максимальные задержки при получении ответного сообщения, минимальные/ стандартные/ максимальные значения времени ожидания ответного сообщения; информация об используемых дополнительных функциях в части функциональной совместимости по обнаружению, конфигурированию, управлению и безопасности (если они были реализованы); информация о функциональных возможностях DLC- и/или PHY-уровней;

- TRS-уровнях: информация о соответствии требованиям базового TRS-стандарта и используемых дополнительных функциях; утвержденный диапазон ссылок на объекты и алгоритм для их получения; утвержденный диапазон значений данных сообщений, информация об используемых полях управления и алгоритмах их формирования; утвержденные параметры синхронизации: минимальные/ стандартные/ максимальные задержки при получении ответного сообщения, минимальные/ стандартные/ максимальные значения времени ожидания ответного сообщения; информация об используемых дополнительных функциях в соответствии с возможностями уровня в части функциональной совместимости по обнаружению, конфигурированию, управлению и безопасности (если они были реализованы), информация о функциональных возможностях NWK-, DLC- и/или PHY-уровней;

- APP-уровнях: информация о соответствии требованиям базового APP-стандарта и используемых дополнительных функциях; утвержденный диапазон ссылок на объекты и информация об алгоритмах их формирования; утвержденные диапазоны и значения других используемых идентификаторов и алгоритмах их формирования; утвержденный диапазон значений используемых сообщений, информация об используемых полях управления и алгоритмах их формирования; утвержденные параметры синхронизации: минимальные/ стандартные/ максимальные задержки при получении ответного сообщения, минимальные/ стандартные/ максимальные значения времени ожидания ответного сообщения; информация об используемых дополнительных функциях в соответствии с возможностями уровня в части функциональной совместимости по обнаружению, конфигурированию, управлению и безопасности (если они были реализованы); информация о функциональных возможностях TRS-, NWK-, DLC- и/или PHY-уровней.

Указанное выше является основой для технической и семантической функциональной совместимости устройств, подсоединенных к одной и той же подсети, а также устройств и шлюзов, подсоединенных к этой подсети. При этом предполагается, что большая часть требуемой информации может предоставляться путем ссылки на существующие стандарты.

Функции, заложенные в устройство, в котором реализованы возможности шлюза, дополнительно должны обеспечивать функциональную совместимость. Во-первых, указанную выше информацию необходимо предоставлять каждому поддерживаемому средству связи/технологии подсети, а во-вторых, каждой подсети, к которой подсоединен шлюз, необходимо предоставить следующую дополнительную информацию (со ссылкой на входные (In-трассы) и выходные трассы (Out-трассы)):

- для PHY-уровня: информацию о преобразовании In-трассы PHY-уровня в Out-трассу (любого уровня) на этапах обнаружения, конфигурирования, управления и обеспечения безопасности (если они были реализованы) в соответствии с уровнем функциональной совместимости;

- для DLC-уровня: информацию о преобразовании In-трассы DLC-уровня в Out-трассу (любого уровня) при использовании возможностей обнаружения, конфигурирования и управления. При использовании любой из этих возможностей следует указывать диапазоны адресов/идентификаторов и преобразование In-трассы в Out-трассу. Также требуется указание преобразования управляющей информации;

- для NWK-уровня: информацию о преобразовании In-трассы NWK-уровня в Out-трассу (любого уровня) при использовании возможностей обнаружения, конфигурирования и управления. При использовании любой из этих возможностей следует указывать диапазоны адресов и преобразования. Также требуется указание преобразования управляющей информации;

- для TRS-уровней: информацию о преобразовании In-трассы TRS-уровней в Out-трассу (любого уровня) при использовании возможностей обнаружения, конфигурирования и управления. При использовании любой из этих возможностей следует указывать диапазоны адресов и преобразования. Также требуется указание преобразования управляющей информации;

- для APP-уровней: информацию о преобразовании In-трассы APP-уровней в Out-трассу (любого уровня) при использовании возможностей обнаружения, конфигурирования и управления. При использовании любой из этих возможностей следует указывать диапазоны адресов и преобразования. Также требуется указание преобразования управляющей информации.

Требования к наличию информации, указанные выше, являются основой для технической и семантической функциональной совместимости устройств, подсоединенных к подсетям, а также для передачи информации через шлюзы, соединяющие эти подсети. При этом предполагается, что большая часть требуемой информации может предоставляться путем ссылки на существующие стандарты.

А.6.8 Рабочие допущения

Процесс сбора и классификации информации, которая призвана поддерживать заключение о соответствии и позволяет тестировать ее при соответствующей настройке, предусмотрен в рамках процедуры стандартизации, например, с помощью моделей-проформ PICS и PIXIT, которые должны использовать:

- Модель данных, которая получает спецификации на объекты, но не является приоритетной на этапе разработки IFRS-спецификации в процессе стандартизации. В перспективе данная модель все же может потребоваться, и для ее реализации необходимо выбрать язык; при этом желательно, чтобы он был совместим с языком и методологией, с помощью которых будут формироваться сценарии и варианты использования модели данных;
- PICS- и PIXIT-проформы, которые могут потребоваться при возникновении проблем с функциональной совместимостью. После углубленного изучения этих проблем некоторые из них могут рассматриваться как требования к межсетевому взаимодействию (см. выше);
- Тематику, которая должна охватывать PICS- и PIXIT-информацию и включать в себя: физический уровень (трасса, вилка/гнездо разъема, средство связи); канальный уровень (MAC-, DLC-уровни, включая переадресацию Уровня 2); сетевой уровень (адресация подсетей и устройств, режим распределения); транспортный уровень («сквозная» доставка сообщений и «сквозная» адресация); сеансовый уровень (обнаружение, конфигурирование и платформенно-зависимые протоколы); уровень представления (абстрактный и конкретный синтаксис структуры сообщений); уровень приложения (спецификация на объект и протоколы взаимодействия). Установлено, что используемые термины могут оказаться несовместимыми с терминами, используемыми при других подходах к спецификациям;
- Конкретные технологические HBES-платформы, которые уже могут обладать эквивалентными проформами соответствия для всех, некоторых или ни одного из указанных уровней (например, в тех случаях, когда дается ссылка на существующие стандартизованные спецификации соответствия);
- Кроме того, несколько технологических платформ с рекомендациями по функциональной совместимости, которые хорошо известны и стандартизованы CENELEC, CEN и ETSI и определяют основу для создания проформ, которые необходимо включать в IFRS-соглашение;
- Безопасность, которая в таких межплатформенных системах с различным местоположением является ключевой проблемой и источником многих нарушений функциональной совместимости и уязвимости. Некоторая часть терминологии может потребовать дальнейшего изучения. Основное внимание должно быть уделено требованиям к соответствию, а не к конкретным решениям.

А.6.9 Обоснование выбора функциональных этапов и связанных с ними процессов

А.6.9.1 Общие положения

Таблица А.8

Этап/Функция	Обнаружение	Конфигурирование	Эксплуатация	Управление системой
Процессы	Описание методов, связанных с обнаружением объекта в конкретной системе	Описание методов, используемых для конфигурирования объекта или объекта-приложения в конкретной системе	Описание операции, с помощью которой приложения создаются и функционируют в конкретной системе	Описание способа управления объектом (объектами) в конкретной системе
	Обнаружение			
Безопасность	Уровень безопасности, предоставляемый конкретной системой по результатам обнаружения	Уровень безопасности, предоставляемый конкретной системой по результатам конфигурирования	Уровень безопасности, предоставляемый любым приложением в рамках конкретной системы	Уровень безопасности, предоставляемый конкретной системой по результатам управления системой
		Доступ к объекту и требования безопасности		
Средства реализации	Методы, используемые конкретной системой для выполнения операции обнаружения	Методы, используемые конкретной системой для выполнения операции конфигурирования	Методы, используемые конкретной системой для определения и создания приложений/моделей приложений	Методы, используемые конкретной системой для выполнения операций управления системой
	Описание идентификатора объекта	Конфигурирование объекта		Управление объектом

Окончание таблицы А.8

Этап/Функция	Обнаружение	Конфигурирование	Эксплуатация	Управление системой
Модель взаимодействий	Методы, используемые конкретной системой для обеспечения взаимодействия между объектами в процессе их обнаружения	Методы, используемые конкретной системой для обеспечения взаимодействия между объектами в процессе конфигурирования		Методы, используемые конкретной системой для обеспечения взаимодействия между объектами в процессе управления системой
			Взаимодействие объектов	
			Модель	
Поддержка перекрестных стандартов	Регистрация стандарта, системы, подсистемы или протокола, которые были идентифицированы как обладающие конкретным интерфейсом с другим протоколом; подобные преобразования или прикладные программные интерфейсы (API) часто создают с помощью специального протокола и потоков данных по направлениям от него или к нему.			

В каждом столбце рассмотренной выше таблицы продукт может соответствовать IFRS-спецификации на любом Уровне — от 0 до 6.

А.6.9.2 Проблемы архитектуры

Функции, обеспечивающие сопряжение между системами, средствами связи и протоколами для продуктов и гарантирующие функциональную совместимость на Уровне 3 и выше, должны существовать в разных формах, начиная с Уровня 0 и выше:

- Устройство, поддерживающее 2 интерфейса для разделения средств связи, реализующих единственную HBES-спецификацию. Данное устройство должно реализовывать взаимодействие на канальном уровне, получая сообщения по одному каналу и ретранслируя их по-другому, без изменения содержимого сообщений. Проблемы функциональной совместимости сохраняются между функциями, реализованными во взаимодействующих устройствах, подсоединенных к средствам связи;
- Устройство, поддерживающее 3 или более интерфейсов для разделения средств, реализующих единственную HBES-спецификацию. Данное устройство является маршрутизатором и должно использовать протокол маршрутизации согласно установленной спецификации. Существуют также и другие аспекты функциональной совместимости (см. выше);
- Устройство, реализующее один интерфейс к средству связи, отвечающему единственной HBES-спецификации, а также второй интерфейс — к другой системе. Данная ситуация возникает с устройствами, которые подсоединяются к сети Internet через домашний шлюз, используя Internet-протокол в качестве протокола преобразования данных.

А.7 Аспекты информационной безопасности и защиты информации

А.7.1 Общие положения

Функциональная совместимость подразумевает взаимодействие и совместную работу нескольких устройств, систем и сетей, но как только уровень функциональной совместимости превысит Уровень 3 (и, возможно, дойдет до Уровня 6), могут возникать новые требования к функционированию объекта, а именно требования, касающиеся того, что может или не может делать объект, или кто или какая система может давать разрешение на управление данным объектом. Кроме того, необходимо учитывать различные аспекты безопасности конкретных объектов в системах и приложениях. Очевидно, что то, что может быть безопасным и защищенным в закрытой системе, может оказаться небезопасным или незащищенным в случаях ее открытия за счет функциональной совместимости для нескольких других систем.

Что касается аспектов информационной безопасности, то любая информационная система может подвергаться прослушиванию, и даже при шифровании сообщений устройство прослушивания может получать ценную информацию об операциях объекта. На любом уровне функциональной совместимости потоки сообщений между одинаковыми и/или различными, но взаимодействующими системами должны защищаться от лиц, не имеющих санкционированного доступа к этим системам, способных изменять сообщения, а также от несанкционированного доступа из Интернета или от попыток нарушения защиты системы и ее целостности, обусловленных отказом от обслуживания. Сообщения должны проходить аутентификацию, валидацию и верификацию на уровнях, на которых системы функционируют в дистанционном режиме.

Что касается аспектов защиты информации, то любое приложение или подсоединенное устройство будет подвергаться соответствующим рискам, если управление ими будет удаленным от основного устройства (если устройство дистанционного управления непосредственно не спарено с самим устройством). Чем дальше средство

управления находится от приложения/устройства и чем больше удаленных пользователей, желающих контролировать это приложение/устройство, тем выше будут риски. В случае приложений, которые являются абсолютно дистанционными и автоматически инициализируемыми, структура приложения/процесса должна обеспечивать (a) возможность информирования ими любого устройства относительно своего существования и проблем, которые могут возникать в связи с защитой информации при ее контроле третьей стороной, и (b) возможность оценки информации, поступающей от сторонних приложений/устройств с тем, чтобы функционирование конкретного приложения/процесса не препятствовало функционированию стороннего приложения/ устройства (например, выдаче приложением команды на управление энергопотреблением системы жизнеобеспечения дома, и получению информации об отключении подачи электроэнергии от источника электроснабжения (в случае смарт-системы учета/измерений).

В части установления приоритетов, во всех случаях, касающихся критически важных для защиты информации аспектах, приложения/устройства должны обладать более высоким приоритетом по отношению к другим, хотя использование этого приложения/устройства другими устройствами/приложениями может быть связано с более низким приоритетом и правом доступа к некоторым функциям.

В общем случае, поскольку уровень функциональной совместимости повышает ответственность разработчика приложения и его установщика (по умолчанию ответственность закрепляется за разработчиком приложения). При этом требуется разработка стратегии для определения риска и его устранения в случае использования автоматического и дистанционного режимов функционирования приложения. Кроме того, чем выше удаленность устройств управления и число передаваемых сообщений, позволяющих осуществлять надлежащее управление, тем выше риски информационной безопасности.

Процесс прохождения потока данных от отправителя к получателю (получателям) перед их отправкой или исполнением должен подвергаться определенному тестированию, однако в определенной области применения проверки могут не понадобиться (например, в случае, когда система полностью автономна и не может обмениваться информацией с внешними устройствами).

Последнее утверждение можно проиллюстрировать следующей таблицей:

Таблица А.9 — Безопасность/защита информации, доступ к ней и приоритет, обеспечиваемые на различных уровнях функциональной совместимости

Уровень функциональной совместимости	Безопасность информации	Защита информации	Приоритет	Права доступа к информации
0	Может потребоваться защита информации для предотвращения прослушивания	Компоненты всегда должны функционировать безопасно, если ими управляют удаленно [a)]	Неприменимо	Неприменимо
1	Может потребоваться защита средств связи для предотвращения прослушивания	Компоненты всегда должны функционировать безопасно, если ими управляют удаленно [a)]	В любом защитном устройстве или жизненно важном обеспечивающем устройстве, компоненте или приложении одно приложение должно обладать приоритетом управления	Кроме приложения с наивысшим приоритетом, приложения с более низким приоритетом могут обладать ограниченной функциональностью для определенного устройства/объекта
2	Необходимо обеспечить защиту от несанкционированного доступа к системе, отказа от обслуживания и перехвата информации	В тех случаях, когда компоненты контролируются двумя и более приложениями (возможно, из различных систем), должна обеспечиваться безопасность любой результирующей операции [a)]	В любом защитном устройстве или жизненно важном обеспечивающем устройстве, компоненте или приложении одно приложение должно обладать приоритетом управления	Кроме приложения с наивысшим приоритетом, приложения с более низким приоритетом могут обладать ограниченной функциональностью для определенного устройства/объекта

Продолжение таблицы А.9

Уровень функциональной совместимости	Безопасность информации	Защита информации	Приоритет	Права доступа к информации
3	Необходимо обеспечить защиту от несанкционированного доступа к системе, отказа от обслуживания и перехвата информации	В тех случаях, когда компоненты контролируются двумя и более приложениями (возможно, из различных систем), должна обеспечиваться безопасность любой результирующей операции [a]	В любом защитном устройстве или жизненно важном обеспечивающем устройстве, компоненте или приложении одно приложение должно обладать приоритетом управления	Кроме приложения с наивысшим приоритетом, приложения с более низким приоритетом могут обладать ограниченной функциональностью для определенного устройства/объекта
4	Необходимо обеспечить защиту от несанкционированного доступа к системе, отказа от обслуживания и перехвата информации [b]	В тех случаях, когда компоненты контролируются двумя и более приложениями (возможно, из различных систем), должна обеспечиваться безопасность любой результирующей операции [a] [c]	В любом защитном устройстве или жизненно важном обеспечивающем устройстве, компоненте или приложении одно приложение должно обладать приоритетом управления. Ответственность за обеспечение безопасности возлагается на установщика приложений [c]	Кроме приложения с наивысшим приоритетом, приложения с более низким приоритетом могут обладать ограниченной функциональностью для определенного устройства/объекта. Ответственность за определение прав доступа лежит на установщике приложений.
5	Необходимо обеспечить защиту от несанкционированного доступа к системе, отказа от обслуживания и перехвата информации [b] [d].	В тех случаях, когда компоненты контролируются двумя и более приложениями (возможно, из различных систем), должна обеспечиваться безопасность любой результирующей операции [a] [c] [e]	В любом защитном устройстве или жизненно важном обеспечивающем устройстве, компоненте или приложении одно приложение должно обладать	Кроме приложения с наивысшим приоритетом, приложения с более низким приоритетом могут обладать ограниченной функциональностью для определенного
	Имеет большое значение аутентичность приложений, автоматически управляемая и контролируемая		приоритетом управления. Ответственность за обеспечение безопасности возлагается на установщика [c] [e]	устройства/объекта. Ответственность за определение прав и уровней доступа лежит на установщике приложений [e]
6	Необходимо обеспечить защиту от несанкционированного доступа к системе, отказа от обслуживания и перехвата информации. Имеет большое значение аутентичность приложений, автоматически управляемая и контролируемая [f]	В тех случаях, когда компоненты контролируются двумя и более приложениями (возможно, из различных систем), должна обеспечиваться безопасность любой результирующей операции и валидация инструкций для дистанционного управления [a] [c] [e] [g]	В любом защитном устройстве или жизненно важном обеспечивающем устройстве, компоненте или приложении одно приложение должно обладать приоритетом управления. Ответственность за обеспечение безопасности возлагается на установщика [c] [e] [g]	Кроме приложения с наивысшим приоритетом, приложения с более низким приоритетом могут обладать ограниченной функциональностью для определенного устройства/объекта. Ответственность за определение прав и уровней доступа лежит на установщике приложений [e] [g]

Продолжение таблицы А.9

[a] Необходимо помнить, что работа устройств в автоматическом режиме может приводить к возникновению опасных ситуаций, например, при регулировке органов управления на плите (духовке), на стиральной машине или котле центрального отопления — их ручные настройки будут более безопасными; снижение риска может достигаться при условии того, что автоматическое дистанционное управление не будет задавать такие параметры, которые пользователь не будет устанавливать вручную. Тем не менее, в тех случаях, когда установка параметров выполняется полностью дистанционно, важно обеспечивать безопасность условий функционирования устройств при выполнении ими операций, а также их неизменность, поскольку эти параметры задавались в ручном режиме, а затем устанавливались для работы в автоматическом режиме. Подобным образом можно настраивать и плиту для дистанционного управления (с возможностью выдачи определенного запроса на приготовление того или иного блюда). Тем не менее, если в промежутке между настройкой и работой плиты будет открыта ее дверца, то режим автоматической работы должен быть отменен еще до выполнения этого запроса.

Если работа системы в удаленном режиме является необходимой для поддержания жизнеобеспечения (например, в устройствах телемедицины), то необходимо предотвращать выполнение с помощью приложений таких работ (отличающихся от работ, непосредственно связанных с данным устройством и используемых в других областях применения), которые могут поставить под угрозу жизнь человека. Например, система управления энергопотреблением должна обладать информацией относительно наиболее важной системы дома и ее минимальной потребности в энергопотреблении.

На Уровнях 0—3 разработчики приложений, устройств и бытового радиоэлектронного/электрического оборудования несут ответственность за обеспечение безопасности информации, определяемыми правами доступа к ней. Выше Уровня 3 также применимы требования, указанные в сноске c).

[b] Установщик приложений несет ответственность за то, что рабочая конфигурация и локальное управление будут надлежащими и защищены средствами обеспечения безопасности. Последнее может означать необходимость использования локальной защиты информации паролем или с помощью шифрования информационных потоков.

[c] На Уровнях 3 и выше функциональной совместимости любое устройство/объект могут управляться несколькими приложениями. Ответственность за предоставление им конкретных прав доступа к конкретным приложениям лежит на установщике приложений.

[d] Например, объект или устройство способно выполнять жизненно важные операции, и одновременно — быть частью приложения, которое важно для другого сервиса. При этом необходимо существование иерархии доступа, приоритетов и контроля, которая способна устанавливать более высокие приоритеты для жизненно важных обеспечивающих операций по отношению к другим операциям, выполняемым другими достаточно важными приложениями. Следует также понимать, что обстоятельства могут изменяться и, соответственно — изменяться и приоритеты прав доступа; при этом установщик приложений должен учитывать это и иметь возможность изменять права доступа при установке нового оборудования, устройств или объектов (или при их модификации новыми пользователями).

[e] При автоматическом конфигурировании системы, установке новых устройств, оборудования/объектов, или же при реализации новых приложений с помощью нового оборудования/систем, конфигурация системы, при необходимости, должна надлежащим образом защищаться с помощью соответствующих средств защиты.

[f] Как и в c), отмечается, что существует ответственность за обеспечение защиты информации, реализуемая за счет контроля доступа и интерпретации приоритета конкретного оборудования/устройств. Принимая во внимание последнее, ответственность за это должен нести установщик приложений, поскольку оборудование/устройства устанавливаются автоматически и сами определяют свой приоритет для получения права доступа и управления тем или иным оборудованием, объектами или устройствами. Например, приложение для управления энергопотреблением для наиболее эффективного использования энергии может контролировать температуру в помещении, однако это приложение будет блокироваться системой жизнеобеспечения, задачей которой является поддержание на определенном уровне комфортных условий для пациента.

Последнее означает, что все приложения, используемые на Уровне 5, необходимо аутентифицировать; они должны разрабатываться для оценки работы других приложений/устройств, совместно функционирующих с ними, и в тех случаях, когда обнаруживается, что некоторые выполняемые приложениями операции могут создавать проблемы безопасности (или при возникновении проблем в других устройствах/приложениях), подобные операции должны блокироваться или согласовываться с операциями других приложений.

[g] Как и в e), отмечается, что при определенных обстоятельствах может возникать необходимость в защите конкретных операций. При этом для управления домом и выполнения удаленных операций вся цепочка передачи данных должна обладать уровнем безопасности, приемлемым для контролируемого приложения. Любое приложение (его данные) может искажаться при использовании небезопасного канала связи, поэтому на Уровне 6 функциональной совместимости при управлении домом необходимо обеспечивать надежность и безопасность всех сообщений и жизненно важных приложений.

Окончание таблицы А.9

Как и в е), отмечается, что безопасность информации и контроль доступа к ней и приоритет весьма важны, однако помимо подконтрольного приложения это управление может распространяться и на дистанционные системы, в которых могут использоваться интеллектуальные средства определения приоритета, а также устанавливаться новые приложения. При этом необходимо, чтобы дистанционная система имела возможность опрашивать приложения/устройства с целью определения их свойств, атрибутов и параметров, а также с целью поддержания максимального уровня безопасности и повторного задания иерархии прав доступа и приоритетов. Важно обеспечить полный анализ и продуманность любой модификации существующей системы (в особенности — при проектировании автономных систем).

А.7.2 Ссылки и стандарты

Существует множество стандартов и спецификаций, относящихся к информационной безопасности и методам шифрования сообщений, разработанным многими организациями по стандартизации. Роль настоящего стандарта состоит не в предоставлении перечня соответствующих документов (хотя на некоторые из них также существуют ссылки). Основной целью настоящего стандарта в отношении информационной безопасности и защиты информации, прав доступа и приоритетов при управлении объектами, системами/устройствами является предоставление разработчику рекомендаций в части оценки существующих рисков и возможностей нарушения безопасности информации, возможных проблем с ее защитой и способов решения этих проблем путем задания надлежащих уровней доступа к информации и приоритетов, при которых два или более объектов будут иметь доступ к объекту или возможность управления им.

Приложение Б
(справочное)

Пример декларации о соответствии требованиям функциональной совместимости

Б.1 Область применения

В настоящем стандарте, в качестве примера, приводится проформа декларации о соответствии реализации функциональной совместимости (IICS) требованиям IFRS-спецификации, а также подробно описываются вспомогательные функции, в дополнение к функциям, которые являются обязательными для реализации.

Б.2 Ссылки

В нижеперечисленных документах содержатся положения, которые при наличии ссылок в тексте настоящего стандарта становятся его неотъемлемой частью:

1) Стандарты комплекса ГОСТ Р ИСО/МЭК 9646 «Информационная технология. Взаимосвязь открытых систем. Методология и основы аттестационного тестирования» (все части).

Б.3 Требования соответствия IICS-спецификации

Б.3.1 Общие положения

Настоящая IICS-спецификация применима к системам/устройствам, требующим функциональной совместимости на Уровнях 4, 5 и 6. В ней представлены следующие общие требования к соответствию на этих уровнях, за исключением случаев, указанных ниже:

Б.3.2 Требования к описанию идентификатора объекта

Требования настоящего стандарта на Уровнях 4, 5 и 6 заключаются в однозначной идентификации любого объекта (устройства, оборудования, системы, приложения или сервиса) в пространстве (пространствах) имен системы в целом и ее подсистем:

Объекты, соответствующие данному подпункту, должны предоставлять:

- Уникальное имя для возможности использования объекта внешними объектами посредством существующих интерфейсов; средства для получения этого имени не регламентируются или не требуют определения в настоящем стандарте;
- Тип данных, с указанием идентификатора; данные о средствах получения типа данных и его семантики (например, кода продукта или имени абстрактной спецификации на тип данных);
- Местоположение в системе, с указанием одного или нескольких сетевых адресов; форматы адресов, которые могут поддерживаться; режимы связи (с одноадресной/многоадресной адресацией или с прямой адресацией любому устройству группы); средства, с помощью которых они были получены, а также основополагающие HBES-спецификации, из которых они были получены;
- Дескриптор или другие средства обращения к нему в течение всего срока их применения в действующей системе; информация о средствах, с помощью которых сформирован дескриптор;
- Другие постоянные идентификаторы (например, серийный номер).

Б.3.3 Требования к функциональному описанию объекта

Б.3.3.1 Общие положения

Требования к функциональному описанию объекта, отвечающие настоящему стандарту, могут выполняться лишь при наличии достаточного объема информации об объектах. За исключением тех случаев, когда иное четко не оговорено, к Уровням 4, 5 и 6 применимы следующие частные требования:

Б.3.3.2 Классификация объектов

Объект должен предоставлять информацию, достаточную для возможности его использования другими объектами, включая аспекты безопасности, защиты и доступности информации. Минимально предоставляемая информация должна включать в себя предполагаемую область применения объекта, целевой домен приложения и текстовое описание, а также описание средств связи, показатели/гарантии качества и другую дополнительную информацию (по усмотрению производителя). Описание должно предоставляться в виде удобочитаемого текста.

В следующих частных случаях для описания поддерживаемых интерфейсов следует использовать один из FDL-языков описания типа данных, операций и атрибутов. Операции должны определяться их функциональной сигнатурой, включая входные, выходные и входные/выходные параметры и возвращаемый результат их выполнения, а также содержать принятые входные значения и сформированные выходные значения. Атрибуты могут включать в себя время на прием запрашиваемых операций и реагирования на них; скорость, с которой могут запрашиваться операции; ограничения на доступ к считыванию/записи данных; идентификаторы, используемые в PDU-модуле для выделения полей, из которых они были составлены, а также другую информацию, которую можно считать достаточной для обеспечения функциональной совместимости.

Допустимыми FDL-языками являются ASN.1, XML (при этом должны указываться стандартные OMG-схемы), Corba IDL, ISO RPC IDL или другие, определенные фактическим стандартом или методом. Если какой-либо из

языков не позволяет включать обязательную информацию, в описании необходимо указывать синтаксис, используемый для описания этой информации, а также предоставлять необходимые данные в виде комментариев в тексте.

Б.3.3.3 Интерфейс для обнаружения объекта

Объект должен предоставлять описание с использованием одного из FDL-языков описания его типов данных, операций и атрибутов, поддерживающих процесс обнаружения объекта.

Б.3.3.4 Интерфейс для конфигурирования объекта

Объект должен предоставлять описание с использованием одного из FDL-языков описания его типов данных, операций и атрибутов, поддерживающих процесс конфигурирования объекта.

Соответствие этому требованию является необязательным на Уровне 4 и обязательным — для Уровней 5 и 6.

Б.3.3.5 Интерфейс для управления объектом

Объект должен предоставлять описание с использованием одного из FDL-языков описания его типов данных, операций и атрибутов, поддерживающих процесс управления объектом.

Соответствие этому требованию является необязательным на Уровне 4 и обязательным — для Уровней 5 и 6.

Б.3.3.6 Интерфейс для эксплуатации объекта

Объект должен предоставлять описание с использованием одного из FDL-языков описания его типов данных, операций и атрибутов. Конкретные аспекты

Б.3.4 Требования к процессу обнаружения

Б.3.4.1 Общие положения

Необходимо указывать средства, с помощью которых описывающая объект информация извлекается из функционального интерфейса объекта и предоставляется в качестве входных/выходных параметров интерфейса для обнаружения (включая синтаксис и семантику информации, закодированной в операциях обнаружения). Синтаксис и семантику необходимо заимствовать из одного из указанных выше FDL-языков.

Б.3.4.2 Самоописание объекта

Объект, участвующий в процессе обнаружения, должен предоставлять о самом себе информацию объектам, намеревающимся его обнаружить. При этом объект должен указывать число связей с запрашивающими объектами, которые он будет поддерживать.

Б.3.4.3 Режим связи

Объект должен указывать режим связи, используемый для передачи сообщений, связанных с процессом обнаружения, включая режим одноадресной рассылки, групповой рассылки или рассылки любому устройству группы.

Б.3.4.4 Процесс обнаружения

Объект должен указывать модель взаимодействия/обмена сообщениями, которые он использует для инициализации и/или реагирования на взаимодействия в операциях обнаружения, которые он реализует. Объект также должен дополнительно указывать для каждой такой операции область, где это применимо: семантику выполнения, ответ (ответы) и ошибку (ошибки), которые он будет воспринимать и предпринимать соответствующие меры; время, в течение которого объект будет ожидать ответных сообщений; время, необходимое для формирования ответного сообщения; скорость, с которой объект осуществляет взаимодействие; ошибки, которые объект может выдавать; операции, выполняемые после получения сообщений об ошибках/нарушениях, а также любые другие ограничения, реализуемые по усмотрению поставщика.

Объект может предоставлять каталог продуктов (конечных устройств, шлюзов, программного обеспечения, веб-сервисов) и их объекты, с которыми объект был протестирован на функциональную совместимость в части операций обнаружения.

Б.3.4.5 Область обнаружения

Объект, ограничивающий область обнаружения, должен указывать степень подобного ограничения по времени, пространству и логическим аспектам. Объект, находящийся в шлюзе и участвующий в процессах обнаружения, должен указывать ограничения, применимые к области обнаружения и любым другим дополнительным ограничениям.

Б.3.4.6 Безопасность и конфиденциальность

Объект, участвующий в процессе обнаружения, должен указывать условия, необходимые для авторизации и аутентификации выданных им запросов.

Объект, участвующий в процессе обнаружения, должен указывать обстоятельства, при которых он будет принимать/отклонять выданные ему запросы, а также ответные сообщения, которые он будет выдавать.

Б.3.5 Требования к процессу конфигурирования

В тех случаях, когда не оговорено иное, следующие частные требования считаются применимыми к Уровням 4, 5 и 6.

Б.3.5.1 Привязки

Объект, участвующий в процессе конфигурирования, должен указывать количество привязок с запрашивающими объектами, которые он будет поддерживать.

Объект, участвующий в процессе настройки, должен указать количество привязок с обнаруженными объектами, которые он будет поддерживать.

Б.3.5.2 Режимы связи

Объект должен указывать режимы связи, используемые для передачи сообщений, связанных с конфигурированием, включая режим одноадресной рассылки, групповой рассылки или рассылки любому устройству группы.

Б.3.5.3 Процесс конфигурирования

Объект должен указывать используемую модель взаимодействия и обмена сообщениями для инициализации и/или реагирования на операции конфигурирования, которые он реализует. Объект также должен указывать для каждой операции (где это применимо) семантику выполнения; ответное сообщение (сообщения) и ошибку (ошибки), которые он может воспринимать, а также возможные ответные меры; время, в течение которого объект будет ждать ответного сообщения; время, необходимое для формирования ответного сообщения; скорость, с которой объект осуществляет взаимодействие; ошибки, которые объект может допускать; операцию, выполняемую после получения сообщений об ошибках или нарушениях, а также и любые другие ограничения, накладываемые по усмотрению поставщика.

Объект может предоставлять каталог своих продуктов (оконечных устройств, шлюзов, программного обеспечения, веб-сервисов) и связанных с ними объектов, с которыми они были протестированы на функциональную совместимость операций конфигурирования.

Б.3.5.4 Безопасность и конфиденциальность

Объект, участвующий в процессе конфигурирования, должен указывать условия, необходимые для авторизации и аутентификации запросов к нему.

Объект, участвующий в процессе конфигурирования, должен указывать обстоятельства, при которых он будет принимать/отклонять запросы к нему, а также формировать ответное сообщение (сообщения).

Б.3.6 Требования к эксплуатации

Б.3.6.1 Эксплуатация приложения

Объекты должны содержать (со ссылкой на удобочитаемый текст) соответствующие спецификации на алгоритмы и функциональные возможности, которые они реализуют.

Объект должен указывать на используемые модели взаимодействия и обмена сообщениями, которые он использует для инициализации и/или реагирования на реализуемую операцию эксплуатации объекта. Объект также должен указывать семантику выполнения для каждой операции (где это применимо); ответное сообщение (сообщения) и ошибку (ошибки), которую он может воспринимать, а также принятые меры; время, в течение которого объект будет ждать ответного сообщения; время, необходимое для формирования ответного сообщения; скорость, с которой объект осуществляет взаимодействие; ошибки, которые объект может допускать; операцию, выполняемую после получения сообщений об ошибках или нарушениях, а также любые другие ограничения, накладываемые по усмотрению поставщика.

Объект может представлять собой каталог продуктов (оконечных устройств, шлюзов, программного обеспечения, веб-сервисов) и их объектов, с которыми они были протестированы на функциональную совместимость для операций эксплуатации объекта.

Б.3.6.2 Безопасность и конфиденциальность

Объект, участвующий в процессе эксплуатации, должен указывать условия, необходимые для авторизации и аутентификации запросов к этому объекту.

Объект, участвующий в процессе эксплуатации, должен указывать обстоятельства, при которых он будет принимать/отклонять запросы к нему, а также формировать ответное сообщение (сообщения).

Б.3.7 Требования к управлению

За исключением случаев, когда иное не оговорено, следующие частные требования применимы к Уровням 4, 5 и 6.

Б.3.7.1 Режим связи

Объект должен указывать режимы связи, используемые для передачи сообщений (которые связаны с управлением), включая режим одноадресной рассылки, групповой рассылки или рассылки любому устройству группы.

Б.3.7.2 Процесс управления

Объект должен указывать модель взаимодействия и обмена сообщениями, которые он использует для инициализации и/или реагирования на реализуемую операцию управления объектом. Объект также должен указывать для каждой подобной операции (где это применимо) семантику выполнения; ответное сообщение (сообщения) и ошибку (ошибки), которую он может воспринимать, а также принятые меры; время, в течение которого объект будет ждать ответного сообщения; время, необходимое для формирования ответного сообщения; скорость, с которой объект осуществляет взаимодействие; ошибки, которые объект может допускать; операции, выполняемые после получения сообщений об ошибках или нарушениях, а также любые другие ограничения, накладываемые по усмотрению поставщика.

Б.3.7.3 Безопасность и конфиденциальность

Объект, участвующий в процессе управления, должен указывать условия, необходимые для авторизации и аутентификации запросов к этому объекту.

Объект, участвующий в процессе управления, должен указывать обстоятельства, при которых он будет принимать/отклонять запросы к нему, а также формировать ответное сообщение (сообщения).

Объект, участвующий в процессе управления объектом и одновременно запрашиваемый несколькими управляющими приложениями, должен указывать условия, необходимые для выполнения ACID-требований к операциям, запрашиваемым этими приложениями.

Б.4 Инструкции по выполнению требований IICS-спецификации

Б.4.1 Общие положения

В IICS-спецификации используется табличный подход с дополнительным текстовым описанием. Подробные инструкции и рекомендации приведены в соответствующих разделах.

В тех случаях, когда это возможно, требования соответствия должны предъявляться с учетом базовых стандартов.

Дополнительная информация может предоставляться в соответствующих полях. Иногда это требуется, однако информация также может предоставляться по усмотрению поставщика.

Б.4.2 Пояснения к условным обозначениям в таблице

—	Информация, которая не требуется или не предоставляется
M	Необходимая информация.
O	Информация, которая может предоставляться по усмотрению разработчика. Если не указано иное, то никакие требования не могут предъявляться в отношении функциональной совместимости, и никакое заключение не может быть сделано.
C	Если информация поддерживается, то это необходимая информация (M); в противном случае — это информация, которая не требуется или не предоставляется («—»).

Предоставляемая информация может принимать следующие формы:

1. Конкретной ссылки на стандарт, который применяется к конкретной записи с указанием применимых положений (форма предпочтительного утвердительного ответа);
2. Ответа «Да», означающего верифицированную функциональную возможность;
3. Ответа «Нет», означающего, что функциональная возможность отсутствует (или была протестирована и признана негодной). В этом случае существует вероятность того, что продукт не полностью удовлетворяет требованиям соответствия IFRS-спецификации, однако если эта возможность поддерживается другими способами, то следует указывать это отдельно.
4. Символа «—», означающего отсутствие предоставленной информации.

Б.5 Общие положения заключения о соответствии требованиям функциональной совместимости

См. заполненную таблицу ниже:

Условия соответствия		Уровень 4	Уровень 5	Уровень 6
Обнаружение	Процесс	M	M	M
	Безопасность	M	M	M
	Средства реализации	M	M	M
	Модель взаимодействия	M	M	M
Конфигурирование	Процесс	M	M	M
	Безопасность	M	M	M
	Средства реализации	M	M	M
	Модель взаимодействия	M	M	M
Эксплуатация	Процесс	M	M	M
	Безопасность	M	M	M
	Средства реализации	M	M	M
	Модель взаимодействия	M	M	M
Управление	Процесс	—	—	M
	Безопасность	—	—	M
	Средства реализации	—	—	M
	Модель взаимодействия	—	—	M

Б.6 Частные положения заключения о соответствии требованиям функциональной совместимости

Б.6.1 Общие положения

Нижеуказанная информация должна предоставляться при частичном выполнении требований (см. Б.3.2 и Б.3.3).

Идентификатор устройства	<Идентификатор, используемый организацией для обозначения устройства >
Внедренный стандарт (стандарты)	<Перечень внедренных стандартов>
Соответствие требованиям функциональной совместимости	<Перечень соответствий со стандартными спецификациями на функциональную совместимость>
FDL-язык, используемый в каталогах	ASN.1 C XML C IDL C и другие C
Описание устройства	<Описательная информация, характеризующая устройство>
Взаимодействующие устройства[a]	<Перечень продуктов, которые были протестированы на функциональную совместимость в соответствии с требованиями IICS-спецификации>
[a] Предполагается, что связь между устройством и совместимыми устройствами не зависит от топологии промежуточных шлюзов.	

Б.6.2 Каталог объектов

Информация, указываемая в каталоге объектов, поддерживает частичное соблюдение положений, указанных в Б.3.2 и Б.3.3 настоящего стандарта.

Каждому объекту, поддерживаемому устройством, должна предоставляться следующая информация.

Идентификатор объекта	Цель	Можно запрашивать	Будет принят
<Идентификатор объекта>[a]	<Что объект делает>	<Идентификатор операции>[b]	< Идентификатор операции >[b]
		... при необходимости	... при необходимости
		< Идентификатор операции >[b]	< Идентификатор операции >[b]
Классификация объектов	< Описательная информация об объекте, указанная в классификаторе объектов, см. Б.3.3 >		
Контроль доступа	< Обзор ограничений при запросе/принятии операций >		
Условия безопасности	< Обзор способов обеспечения безопасности >		
[a] <Идентификатор объекта> должен легко отслеживаться в исходных базовых стандартах или описании продукта (устройства). [b] <Идентификатор операции> должен легко отслеживаться в исходных базовых стандартах и должен быть аналогичным таковому, используемому в Б.6.3 ниже.			

Б.6.3 Каталог операций

Информация, представляемая в каталоге объектов, поддерживает частичное соблюдение условий, указанных в Б.3.2 и Б.3.3 настоящего стандарта.

Для каждой операции, поддерживаемой объектами в устройстве, необходимо предоставлять следующую информацию:

Идентификатор операции	Цель	Описание	Кодирование сообщений
< Идентификатор операции >[a]	<Что делает операция>	<FDL-условия>[b]	<Кодирование>[b]
		... при необходимости	... при необходимости
		<FDL-условия>[b]	< Кодирование >[b]
Описание интерфейса для функционирования [c]	<Описательная информация относительно операции, описанной в Б.3.3, включая условия управления доступом и безопасностью>		

Окончание таблицы

Описание интерфейса для обнаружения[c]	<Описательная информация относительно операции, описанной в Б.3.3, включая условия управления доступом и безопасности>					
Описание интерфейса для конфигурирования[c]	<Описательная информация относительно операции, описанной в Б.3.3, включая условия управления доступом и безопасности>					
Описание интерфейса для управления[c]	<Описательная информация относительно операции, описанной в Б.3.3, включая условия управления доступом и безопасности>					
Семантики исполнения	Не более одного	Ровно один раз	Не реже одного раза	Параллельно	<Число одновременно действующих экземпляров >	
Хронирование, временная синхронизация	Ожидание		<Максимальное время на ожидание>	Отклик	< Максимальное время на отклик>	
Скорость передачи данных	Формирование		<Максимальная скорость>	Прием	< Минимальная скорость >	
			<Средняя скорость>		< Средняя скорость >	
			<Пиковая скорость>		<Пиковая скорость>	
Отклики	<Принято>[d]			<Отклонено>[d]		
Ошибки	<Принято>[d]			<Отклонено>[d]		
Примечания	<Дополнительная информация>					

[a] <Идентификатор операции> должен легко отслеживаться в базовом стандарте.

[b] В тех случаях, когда это возможно, данное описание должно составляться на FDL-языке, указанном в Б.6.1, и содержать число строк, необходимых для этапов связи и выполнения операции. В этом описании необходимо указывать имя операции; ее входные/выходные и изменяемые параметры; и результат (результаты) выполнения этой операции или ошибку (ошибки). Для более уместного и понятного представления информация может заноситься в поле «Примечания».

[c] Информация относительно конкретной операции должна указываться в соответствующей строке. В общем случае ожидается, что из четырех строк будет выбираться одна строка, однако можно выбирать несколько строк.

[d] Информация должна содержать описание полученных результатов или кодов, а также выполненные операции. Можно вводить нужное число записей.

Б.6.4 Каталог совместимости объектов и операций

Если конечные взаимодействующие продукты перечислены в таблице Б.6.1, то для каждого однорангового продукта может предоставляться следующая информация (которая будет определять идентификаторы взаимодействующих объектов, операций и сервисов).

Одноранговый продукт	<Идентификатор продукта>	Код продукта	<Код>	Редакция	<Версия>
Описание	<Текст описания>				
Шлюзы[a]					
<Идентификатор шлюза$_1$>	<Идентификатор продукта>	Код продукта	<Код>	Редакция	<Версия>
	Вход	<Стандарт, соответствующий…>	Выход	<Стандарт, соответствующий…>	
	Примечания	<Текст описания>			

Окончание таблицы

<Идентификатор шлюза$_2$>	<Идентификатор продукта>	Код продукта	<Код>	Редакция	<Версия>
	Вход	<Стандарт, соответствующий…>	Выход	<Стандарт, соответствующий…>	
	Примечания	<Текст описания>			
.....					
<Идентификатор шлюза$_1$>	<Идентификатор продукта>	Код продукта	<Код>	Редакция	<Версия>
	Вход	<Стандарт, соответствующий…>	Выход	<Стандарт, соответствующий…>	
	Примечания	<Текст описания>			

Объект		Операции		Дополнительная операция, предупреждения
<Мой идентификатор объекта>	<Идентификатор одноранговой объекта$_1$>	<Моя операция$_{11}$>	<Одноранговая операция$_{11}$>	<Необходимо указывать уровень функциональной совместимости, утвержденный для данного сочетания>
		< Моя операция $_{12}$>	<Одноранговая операция$_{12}$>	
		…	…	
		< Моя операция$_{1n}$>	<Одноранговая операция$_{1n}$>	
<Мой объект> <Идентификатор одноранговой объекта$_2$> < Идентификатор$_2$>		< Моя операция$_{21}$>	<Одноранговая операция$_{21}$>	
		< Моя операция$_{22}$>	<Одноранговая операция$_{22}$>	
		…	…	
		< Моя операция$_{2n}$>	<Одноранговая операция$_{2n}$>	

[a] Могут предоставляться описания продуктов-шлюзов.

Б.6.5 Заявка о соответствии реализации протоколу на верхних уровнях (APP)

Б.6.5.1 Общие положения

Устройства, которые в случае «сквозных» взаимодействий претендуют на функциональную совместимость на определенном уровне (т. е. на функциональность на уровнях приложения, представления и на сеансовом/транспортном уровнях (APP)) должны предоставлять информацию (см. таблицу ниже) для каждого подключения к поддерживаемым средствам связи (одного — для оконечного устройства, нескольких — для устройства, обладающего возможностями шлюза), которые управляют протоколом уровня приложений.

Уровень	Обнаружение	Конфигурирование	Управление	Безопасность
4	O	O	O	C[b]
5	M[a]	M[a]	M[a]	C[b]
6	M[a]	M[a]	M[a]	C[b]

Окончание таблицы

[a] Если эти функции поддерживаются на APP-уровнях, то соответствующий стандарт и его часть (если они применимы) должны указываться путем ссылки на стандарты, перечисленные в Б.6.1.

[b] Если на APP-уровнях предусмотрены либо средства безопасности, либо отдельные функциональные возможности, то следует ссылаться на соответствующий стандарт. Если не задействованы никакие из этих средств безопасности, то в это поле следует ввести пометку «—».

Б.6.5.2 Дополнительные требования к шлюзам на APP-уровнях

Для устройств, реализующих возможности шлюза, в нижеприведенной таблице следует указывать как можно больше экземпляров для каждой пары интерфейсов и в каждом направлении передачи. Предполагаемый поток информации поступает на вход APP-уровней (принимаемый в шлюз) и передается на выход APP-уровней (передаваемый через шлюз); при этом в каждую строку можно вводить несколько записей, например, пометку «—», если поток или отображение не поддерживаются.

APP-идентификатор	Выход APP-уровней						
Вход APP-уровней	Режим распределения NWK/DLC (M[a])			Обнаружение	Конфигурирование	Управление	Безопасность
	Одноадресный	Групповой	Многоадресный				
Обнаружение	M[b]	M[b]	M[b]	M[c]	M[c]	M[c]	M[c]
Конфигурирование	M[b]	M[b]	M[b]	M[c]	M[c]	M[c]	M[c]
Управление	M[b]	M[b]	M[b]	M[c]	M[c]	M[c]	M[c]
Безопасность	M[b]	M[b]	M[b]	M[c]	M[c]	M[c]	M[c]
Примечания							

[a] Необходимо указывать используемый сервис нижнего уровня. При использовании нескольких сервисов следует подробно указать их в отдельном примечании.

[b] Необходимо указывать способ сопоставления протоколов с соответствующими режимами распределения.

[c] Необходимо указывать протокол, который используется на входе и аттестуется на применяемом уровне связи; если функция не реализована с помощью функциональных возможностей APP-уровней, то следует ввести пометку «—» (или же эта функция должна указываться в отдельном примечании).

	Выход APP-уровней		
Вход APP-уровней	Подтверждение	Управление потоками данных	Хронирование
Подтверждение	—	M[a]	M[b]
Управление потоками данных	M[a]	M[a]	M[b]
Данные	M[a]	M[a]	M[b]
Управление [c]	M[a]	M[a]	M[b]

[a] Необходимо указывать применяемые сочетания (с конкретными протоколами). При этом предполагается, что подтверждения не будут самоподтверждаться.

[b] Необходимо указывать время отклика на выходе на сообщения, поступающие на входе (минимальное/стандартное/максимальное).

[c] Функции управления могут включать в себя организацию сеансов для отдельных приложений на APP-уровнях.

	Выход TRS-уровней		
Вход TRS-уровней	Подтверждение	Управление потоками данных	Хронирование
Подтверждение	—	M[a]	M[b]
Управление потоками данных	M[a]	M[a]	M[b]
Данные	M[a]	M[a]	M[b]
Управление [c]	M[a]	M[a]	M[b]

[a] Необходимо указывать применяемые сочетания (с конкретными протоколами). При этом предполагается, что подтверждения не будут самоподтверждаться.

[b] Необходимо указывать время отклика на выходе на сообщения, поступающие на входе (минимальное/стандартное/максимальное).

[c] Функции управления могут включать в себя организацию сеансов для отдельных приложений на APP-уровнях.

Б.6.6 Заявка о соответствии реализации протоколу на сетевом уровне и уровне маршрутизации (NWK)

Б.6.6.1 Общие положения

Устройства, претендующие на функциональную совместимость на определенном уровне, должны предоставлять информацию (см. таблицу ниже) для каждого подключения к поддерживаемым средствам связи, которые управляют протоколом сетевого уровня.

Уровень	Маршрутизация	Обнаружение	Конфигурирование	Управление	Безопасность
4	C[a]	O	O	O	C[c]
5	C[a]	M[b]	M[b]	M[b]	C[c]
6	C[a]	M[b]	M[b]	M[b]	C[c]

[a] Если устройство не обладает возможностями маршрутизации, то необходимо вводить пометку «—». Если устройство само является маршрутизатором, то необходимо вставлять запись «Да» и указывать протокол маршрутизации.

[b] Если эти функции поддерживаются на NWK-уровне, то следует ссылаться на соответствующий стандарт.

[c] Если на NWK-уровне предусмотрены либо средства безопасности, либо отдельные функциональные возможности, то следует ссылаться на соответствующий стандарт.

Б.6.6.2 Дополнительные требования к шлюзам на NWK-уровне

Если установленная отметка в поле «Маршрутизация» — не равна «—», то для каждой функции в соответствии с нижеприведенной таблицей требуется соответствующая информация. Предполагаемый поток данных проходит от входа NWK-уровня до выхода NWK-уровня; при этом в каждую строку может быть введено несколько записей, в т. ч. допускается указание «—»; в другом случае поток данных или отображение не поддерживаются.

	Выход NWK-уровня						
Вход NWK-уровня	Одноадресный режим	Групповой режим	Многоадресный режим	Обнаружение	Конфигурирование	Управление	Безопасность
Одноадресный режим	M[a]	M[a]	M[a]	—	—	—	—
Групповой режим	M[a]	M[a]	M[a]	—	—	—	—
Многоадресный режим	M[a]	M[a]	M[a]	—	—	—	—
Обнаружение	M[b]	M[b]	M[b]	M[c]	M[c]	M[c]	M[c]
Конфигурирование	M[b]	M[b]	M[b]	M[c]	M[c]	M[c]	M[c]
Управление	M[b]	M[b]	M[b]	M[c]	M[c]	M[c]	M[c]
Безопасность	M[b]	M[b]	M[b]	M[c]	M[c]	M[c]	M[c]
Диапазон адресов	M[d]	M[d]	M[d]	M[d]	M[d]	M[d]	M[d]

Окончание таблицы

[a] Эти пометки указывают на преобразование соответствующих типов сообщений с входа на выход, например, при преобразовании одноадресного сообщения, полученного на входе, в многоадресное сообщение на выходе; эти пометки также необходимо вводить при наличии любых различий в типах данных.

[b] Необходимо указывать способ преобразования протоколов в соответствующие режимы распространения, например, каким образом обнаружение может выполняться посредством многоадресной передачи.

[c] Необходимо указывать протокол, который используется на входе и аттестуется на том уровне связи, на котором он применяется; если функция не была реализована с помощью функциональных возможностей NWK-уровня, то следует вводить пометку «—».

Пример — Запрос на обнаружение на входе, поступивший по внешней DSL-линии, которая подсоединена к сети Internet и закодирована с помощью HTTPS-протокола, преобразуется в запрос на обнаружение на DLC-уровне на выходе (это является конкретной HBES-технологией). Запись может считываться как «Y, In: HTTPS (APP) -> <NWK function>». Эта информация может представляться в виде отдельного примечания;

[d] Необходимо указывать преобразование между диапазонами адресов на входе и на выходе для соответствующих функций. Если отображение не выполняется, то необходимо вводить пометку «—».

	Выход NWK-уровня				
Вход NWK-уровня	Фрагментация	Подтверждение	Управление потоками данных	Источник/ межсегментная маршрутизация «hop-by-hop[e]»	Хронирование
Фрагментация	M[a]	M[a], [b]	M[a]	—	C[b]
Подтверждение	—	—	M[a]	—	M[d]
Управление потоками данных	—	M[a]	M[a]	—	M[d]
Источник/ межсегментная маршрутизация «hop-by-hop[e]»	—	—	—	M[c]	M[d]
Данные	M[a]	M[a]	M[a]	—	M[d]
Управление	M[a]	M[a]	M[a]	—	M[d]

[a] Необходимо указывать применяемые сочетания (с конкретными протоколами). При этом предполагается, что подтверждения и управление потоками данных на входе не будут фрагментироваться, и что подтверждения не будут самоподтверждаться.

[b] Если фрагменты на входе подтверждаются индивидуально, то время на ответ (минимальное/стандартное/максимальное) должно указываться на выходе.

[c] Индикация сочетания источника данных с межсегментной маршрутизацией (hop-by-hop routing) на входе и выходе.

[d] Необходимо указывать время отклика на выходе на соответствующие сообщения, поступающие со входа (минимальное/стандартное/максимальное).

[e] Маршрут, созданный так, что каждый коммутатор в пути использует свою собственную таблицу маршрутизации для определения следующего промежутка (хопа), предполагая, что все коммутаторы будут выбирать непротиворечивые хопы для того, чтобы информация была доставлена по назначению.

Б.6.7 Заявка о соответствии реализации протоколу передачи данных и управления доступом к среде передачи и каналу связи (DLC/MAC)

Б.6.7.1 Общие положения

Устройства, претендующие на функциональную совместимость определенного уровня, должны предоставлять информацию, указанную в нижеприведенной таблице для каждого подключения к поддерживаемым средствам связи и использующим DLC-протокол.

Уровень	DLC			Обнаружение	Конфигурирование	Управление	Безопасность
	Управление	Данные	Шлюз				
4	M[a]	M[a]	C[b]	O	O	O	C[d]
5	M[a]	M[a]	C[b]	C[c]	C[c]	C[c]	C[d]
6	M[a]	M[a]	C[b]	C[c]	C[c]	C[c]	C[d]

[a] Необходимо указывать поддерживаемые стандарты или спецификации.

[b] Если устройство не обладает возможностями по маршрутизации, то необходимо вводить пометку «—». Если устройство само является маршрутизатором, то необходимо вводить запись «Да», с последующим уточнением типа функции — моста, реле или маршрутизатора (в последнем случае следует указывать протокол маршрутизации, например, в соответствии со стандартом IEEE 802.1q).

[c] Если эти функции поддерживаются на DLC-уровне, то необходимо давать ссылку на соответствующий стандарт; в противном случае — вводить пометку «—»; дополнительная информация приведена в нижеприведенной таблице для шлюза.

[d] Если средства безопасности предоставляются либо с помощью DLC-протокола, либо с помощью отдельной функциональной возможности, то необходимо дать ссылку на соответствующий стандарт.

Б.6.7.2 Дополнительные требования к шлюзам на DLC/MAC уровне

Если отметкой под DLC-шлюзом является «Y», то для каждой функции DLC-шлюза необходимо предоставлять информацию в соответствии с нижеприведенной таблицей. Предполагаемый поток информации проходит от входа DLC-уровня до выхода DLC-уровня, и каждую строку можно заполнять несколькими отметками: либо «—», если поток или преобразование не поддерживается, например, если конкретная функция на входе DLC-уровня реализуется иным образом на выходе DLC-уровня.

	Выход DLC-уровня							
Вход DLC-уровня	Одноадресный режим	Групповой режим	Многоадресный режим	Шлюз	Обнаружение	Конфигурирование	Управление	Безопасность
Одноадресная передача (адресация)	M[a]	M[a]	M[a]	—	—	—	—	—
Групповая передача (адресация)	M[a]	M[a]	M[a]	—	—	—	—	—
Многоадресная передача (адресация)				—				
Шлюз	—	—	—	M[b, d]	M[d]	M[d]	M[d]	M[d]
Обнаружение	M[c]	M[c]	M[c]	M[d]	M[d]	M[d]	M[d]	M[d]
Конфигурирование	M[c]	M[c]	M[c]	M[d]	M[d]	M[d]	M[d]	M[d]
Управление	M[c]	M[c]	M[c]	M[d]	M[d]	M[d]	M[d]	M[d]
Безопасность	M[c]	M[c]	M[c]	M[d]	M[d]	M[d]	M[d]	M[d]
Диапазоны адресов	—	—	—	M[e]	M[e]	M[e]	M[e]	M[e]

[a] Эти записи указывают на преобразование соответствующих типов сообщений со входа на выход в соответствии с режимом распределения, например, при преобразовании одноадресного сообщения, полученного на входе, в многоадресное сообщение на выходе; эти записи также необходимо вводить при наличии любых различий в типах данных.

[b] Необходимо установить тип функции шлюза: мост, реле или маршрутизатор, вместе с применимыми стандартами.

[c] Указание того, каким образом протоколы соотносятся с управляющими или информационными сообщениями, например, обнаружение может быть реализовано посредством сообщения, которое обозначается как управляющее сообщение.

Окончание таблицы

[d] Необходимо указывать протокол, используемый на входе и аттестованный на применяемом уровне связи. Если функция не реализуется с использованием функциональных возможностей DSL-канала связи, то необходимо вводить пометку «—». Например, запрос на входе от внешнего DSL-канала связи, подсоединенного к Internet-устройству и закодированного с помощью HTTPS-протокола, преобразуется в запрос на обнаружение на DLC-уровне на выходе (это является конкретной HBES-технологией). Запись может считываться как «Y, In: HTTPS (APP) -> < DLC function>». Эта информация может представляться в виде отдельного примечания.

[e] Необходимо указывать преобразование между диапазонами адресов на входе и выходе соответствующих функций. При отсутствии преобразований необходимо вводить пометку «—».

Б.6.8 Заявка о соответствии реализации протоколу на физическом уровне (PHY)

Устройства, претендующие на свою функциональную совместимость на определенном уровне, должны предоставлять информацию, указанную в нижеприведенной таблице для каждого подключения к поддерживаемым средствам связи.

Уровень	Коннектор	Средство связи	PHY	Обнаружение	Конфигурирование	Управление	Безопасность
4	M[a]	M[a]	M[a]	O	O	O	C[c]
5	M[a]	M[a]	M[a]	C[b]	C[b]	O	C[c]
6	M[a]	M[a]	M[a]	C[b]	C[b]	C[b]	C[c]

[a] Необходимо указывать поддерживаемые стандарты, например. RJ45 (разъем), Cat 5 UTP (средство связи), стандарт IEEE 802.3 (PHY).

[b] Если эти функции поддерживаются на PHY-уровне, например, сканирование согласно стандарту IEEE 802.11 AP/STA, то необходимо ссылаться на соответствующий стандарт, а при его отсутствии — ставить отметку «—».

[c] Если средства обеспечения безопасности информации действуют либо через коннектор, средство связи или с помощью PHY-функции (либо с помощью какой-либо другой функции), то следует ссылаться на соответствующий стандарт.

УДК 658.52.011.56:006.354 ОКС 35.240.99, 97.120

Ключевые слова: системы промышленной автоматизации и интеграция, интероперабельность, уровни интероперабельности, принципы интероперабельности

БЗ 10—2019/108

Редактор *Г.Н. Симонова*
Технический редактор *И.Е. Черепкова*
Корректор *О.В. Лазарева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 23.09.2019. Подписано в печать 07.10.2019. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 6,98. Уч.-изд. л. 6,30.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,

117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru