ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71576— 2024

СИСТЕМЫ КИБЕРФИЗИЧЕСКИЕ

Общие положения

Издание официальное

Москва
Российский институт стандартизации
2024

Предисловие

1 РАЗРАБОТАН Некоммерческим партнерством «Русское биометрическое общество содействия развитию биометрических технологий, систем и коммуникаций» (Некоммерческое партнерство «Русское биометрическое общество») и Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 194 «Киберфизические системы»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 августа 2024 г. № 1131-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ДЕЙСТВУЕТ ВЗАМЕН ПНСТ 416—2020

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.rst.gov.ru)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ КИБЕРФИЗИЧЕСКИЕ

Общие положения

Cyberphysical systems. General principles

Дата введения — 2025—01—01

1 Область применения

Настоящий стандарт устанавливает общие положения (принципы) в области киберфизических систем (КФС).

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:
ГОСТ Р 71531 Системы киберфизические. Термины и определения

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 и определения

В настоящем стандарте применены термины и определения по ГОСТ Р 71531, а также следующий термин с соответствующим определением:

3.1 **оркестровка:** Автоматическое размещение, координация и управление сложными компьютерными системами и службами.

4 Общие положения

Сфера применения КФС очень широка по своей природе. Существует большое количество и разнообразие доменов, сервисов, приложений, а также устройств.

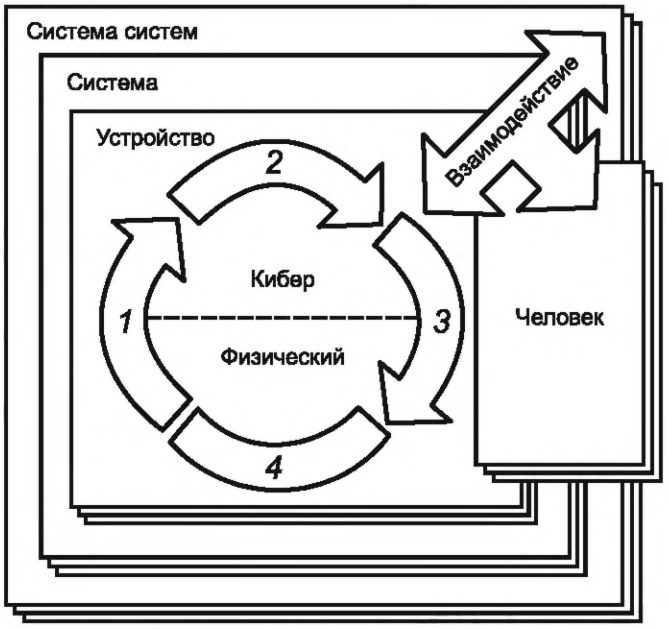
КФС могут коллаборироваться (сотрудничать) друг с другом для получения большего эффекта. КФС может быть оркестрирована другая КФС, которая логически взаимодействует с ней.

4.1 Концептуальная модель

Концептуальная модель КФС представлена на рисунке 1. Там выделены потенциальные взаимодействия устройств и система систем (SoS) (например, инфраструктура КФС). КФС может быть как

Издание официальное

отдельным киберфизическим устройством, так и состоять из одного или нескольких киберфизических устройств, которые образуют КФС или могут быть КФС, состоящей из нескольких КФС, которые состоят из нескольких киберфизических устройств.



1 — информация; *2* — решение; *3* — действие; *4* — физическое состояние

Рисунок 1 — Концептуальная модель КФС

Данный пример является рекурсивным и зависит от перспективы (т. е. киберфизическое устройство с одной точки зрения может быть только устройством, а с другой — может быть КФС).

4.2 Требования к методологии разработки

Методология разработки определяет следующие аспекты:

а) спецификация, моделирование и анализ.

Киберфизические системы по своей сути параллельны. Как минимум, кибер- и физическая подсистемы сосуществуют во времени, но даже внутри этих подсистем параллельные процессы являются общими. Модели параллелизма в физическом мире (сосуществующая физическая динамика во временном континууме) сильно отличаются от моделей параллелизма в программном обеспечении (произвольное чередование последовательностей атомарных действий) и от моделей параллелизма в сетях (асинхронные, частично упорядоченные дискретные действия или временные интервалы, управляемые часами). Согласование этих расходящихся моделей параллелизма и обеспечение совместимости и связи между компонентами, имеющими разные модели параллелизма, являются центральной проблемой КФС.

При разработке КФС должна быть обеспечена функциональная совместимость технологий и инструментов, используемых при проектировании КФС.

Киберфизические системы обычно включают в себя несколько вычислительных платформ, взаимодействующих через сети связи, которые являются открытыми или закрытыми и могут зависеть от предметной области. Задачи, которые необходимо решить при проектировании КФС:

- методы контроля доступа к среде передачи и их влияние на динамику системы;
- промежуточное программное обеспечение, программное обеспечение и API, обеспечивающие координацию в сетях;
- контроль времени проведения сетевых транзакций;
- отказоустойчивость.

При проектировании КФС должна быть обеспечена синхронизация часов, которая необходима для реализации:

- раннего обнаружения удаленных сбоев;
- организованного использования общих ресурсов, таких как пропускная способность сети;

- временной метки данных датчиков с помощью глобально значимых меток времени;

- координированного спящего режима во взаимодействующих беспроводных устройствах для экономии заряда батареи.

Технологии синхронизации часов включают в себя: IEEE 1588 Протокол точного времени (PTP) для IP в Ethernet, шины с синхронизацией по времени (TTA, ARINC, FlexRay, Ethernet с синхронизацией по времени) и протоколы беспроводной синхронизации времени;

б) управление масштабируемостью и сложностью.

Киберфизические системы по своей сути гетерогенны. Физическая область КФС может быть мультифизической, сочетая, например, механическое управление движением, химические процессы, биологические процессы и операторов-людей. Кибердомен КФС может сочетать в себе сетевые технологии, языки программирования, модели программных компонентов и механизмы параллелизма. Таким образом, методологии разработки и инструменты, которые поддерживают эти методологии, должны масштабироваться до крупных проектов, облегчать анализ и способствовать пониманию сложных систем.

Для управления масштабируемостью и сложностью КФС должны быть учтены следующие факторы:

- модульность и компонуемость. Многие КФС представляют собой системы систем, композиции различных подсистем, обычно разрабатываемые разными командами, часто из разных организаций. Модульность — это проблема проектирования подсистем (модулей) с четко определенными интерфейсами, которые можно использовать в различных контекстах. Компонуемость — это возможность комбинировать модули. Связанной с этим проблемой является композиционность, которая относится к способности понять сложную систему путем понимания ее компонентов и того, как они комбинируются;

- синтез. Алгоритмические методы синтеза могут показывать реализации более высокого качества по сравнению с методами, разработанными вручную;

- устаревшие системы. Интеграция ранее существовавших проектов (устаревших систем) в новые проекты является практической необходимостью для многих приложений КФС. Такая интеграция становится особенно сложной, когда методологии и инструменты проектирования меняются;

в) валидация и верификация.

Валидация — это процесс определения того, соответствует ли конструкция потребностям пользователя. Верификация — это процесс определения того, соответствует ли конструкция набору требований, спецификаций и правил. Если требования, спецификации и правила изложены на формальном языке, верификация может быть автоматизирована — такой процесс называется формальной верификацией. Верификация может быть частью процесса валидации, но, как правило, валидацию нельзя формализовать, поскольку она связывает проект системы с намерениями. Для задач валидации и верификации могут быть использованы инструменты моделирования, при этом необходимо обеспечить адекватный охват условий эксплуатации, сценариев и входных данных системы.

4.3 Требования к безопасности и кибербезопасности

КФС должна быть безопасной, т. е. необходимо обеспечить гарантию, что работа системы не инициирует переход системы в опасные состояния и, следовательно, не приведет к потерям в целом и авариям в частности.

Для обеспечения безопасности при проектировании КФС должны быть учтены следующие критерии:

а) анализ рисков.

Необходимо проанализировать условия и определить, что система может перейти в состояние, приводящее к потерям. Необходимо идентифицировать:

- небезопасные управляющие действия — действия, которые в определенном контексте и в наихудшем случае приведут к опасности. Небезопасные управляющие действия включают:

  необеспечение управляющего действия,

  обеспечение управляющего действия,

  обеспечение потенциально безопасного управляющего действия слишком рано, слишком поздно или в неправильном порядке,

  слишком долгое управляющее действие или преждевременное прерывание управляющего действия (для непрерывных управляющих действий);

б) ограничения безопасности.

Ограничения безопасности определяют перечень условий или действий, которые система должна сохранять, чтобы не перейти в опасное состояние;

в) потери.

Потери определяют, что считается неприемлемыми результатами работы системы.

Для обеспечения кибербезопасности КФС должна удовлетворять следующим требованиям:

а) устойчивость.

В контексте КФС устойчивость — это способность системы продолжать удовлетворительно работать в условиях непредвиденных воздействий, сбоев подсистем или в условиях окружающей среды или воздействий, выходящих за пределы указанного рабочего диапазона. Факторами, повышающими устойчивость, являются отказоустойчивость, обнаружение ошибок и адаптация;

б) конфиденциальность.

В контексте CPS конфиденциальность — это проблема защиты информации о людях от несанкционированного доступа со стороны других людей или машин;

в) устойчивость к злонамеренным атакам.

Все сетевые вычислительные системы сталкиваются с риском злонамеренных атак. Поскольку сети КФС становятся более открытыми, они тоже становятся уязвимыми. К особым проблемам относятся «черные ходы», атаки типа «отказ в обслуживании», трояны и вирусы;

г) обнаружение вторжений.

Необходимо учитывать как физические, так и кибервторжения. Технологии, которые можно использовать для обнаружения вторжений, включают:

- встраиваемые технологии компьютерного зрения: обнаружение и отслеживание движения, обнаружение людей, распознавание лиц;
- модели синхронизации: позволяют обнаруживать временные аномалии, которые могут выявить вторжение.

5 Отличительные особенности киберфизических систем

К отличительным особенностям КФС относятся:

- ориентация на сервисы. Сервисы КФС реализуются на основе сервисно-ориентированной эталонной архитектуры;
- интеллектуальная самоорганизация. КФС обеспечивает способность принимать решения самостоятельно;
- способность людей и КФС объединяться для решения общих проблем и общаться друг с другом;
- виртуализация мира производства на разных уровнях детализации, от датчиков и до исполнительных механизмов для всей КФС;
- формирование базы знаний на основе технологической и технической информации;
- обеспечение междисциплинарной модульности, гибкой адаптации к изменяющимся требованиям путем замены или расширения отдельных модулей;
- возможности в реальном времени. Алгоритмы и технологии больших данных, предоставляемые в режиме реального времени;
- оптимизация производственного процесса с использованием алгоритмов и больших данных для повышения общей эффективности оборудования;
- интеграция данных по дисциплинам и по жизненному циклу;
- доступ к данным, надежно хранящимся в облаке или интрасети.

6 5-уровневая архитектура киберфизических систем

5-уровневая архитектура КФС представлена на рисунке 2.

5-уровневая архитектура КФС состоит из следующих уровней:

- уровень 1 «Коммуникационная среда» («Подключи и работай», свободное соединение, сенсорная сеть);
- уровень 2 «Конверсия» (интеллектуальная аналитика для работоспособности компонентов и многомерной корреляции дат, прогноз деградации и производительности);
- уровень 3 «Киберуровень» (модель двойника для компонентов и машин, машина времени для идентификации вариаций и памяти, кластеризация для подобия в сборе данных);
- уровень 4 «Самопознание» (комплексное моделирование и синтез, удаленная визуализация для человека, совместная диагностика и принятие решений);

Рисунок 2 — 5-уровневая архитектура КФС

- уровень 5 «Самоконфигурация» (самонастройка для устойчивости, саморегулирование на отклонение, самооптимизация на возмущение).

КФС включает следующие модули и компоненты:

- сенсорный модуль — осуществляет сбор данных из физического мира через датчики;
- модуль управления данными — состоит из вычислительных устройств и различных носителей информации;
- сервисно-ориентированные модули: полученные данные распознаются и отправляются в доступные службы;
- прикладной модуль;
- Интернет следующего поколения: разрешение приложениям выбирать путь или пути, по которым их пакеты проходят между источником и пунктом назначения;
- датчики и исполнительные механизмы: исполнительный механизм получает команды от прикладного модуля и выполняет их.

УДК 004.738:006.354 ОКС 35.110

Ключевые слова: киберфизическая система, общие положения, архитектура киберфизических систем

Редактор *З.А. Лиманская*
Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 02.09.2024. Подписано в печать 04.09.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 0,93. Уч.-изд. л. 0,74.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru