

Криптографические протоколы для защиты данных, передаваемых в системах Интернета вещей и АСУ ТП

Ольга Шемякина

Менеджер по сертификации



Содержание

Индустрия 4.0

02

Особенности взаимодействия в
индустриальных системах

06

Аспекты безопасности
взаимодействия
в M2M и IoT

17

Протокол CRISP

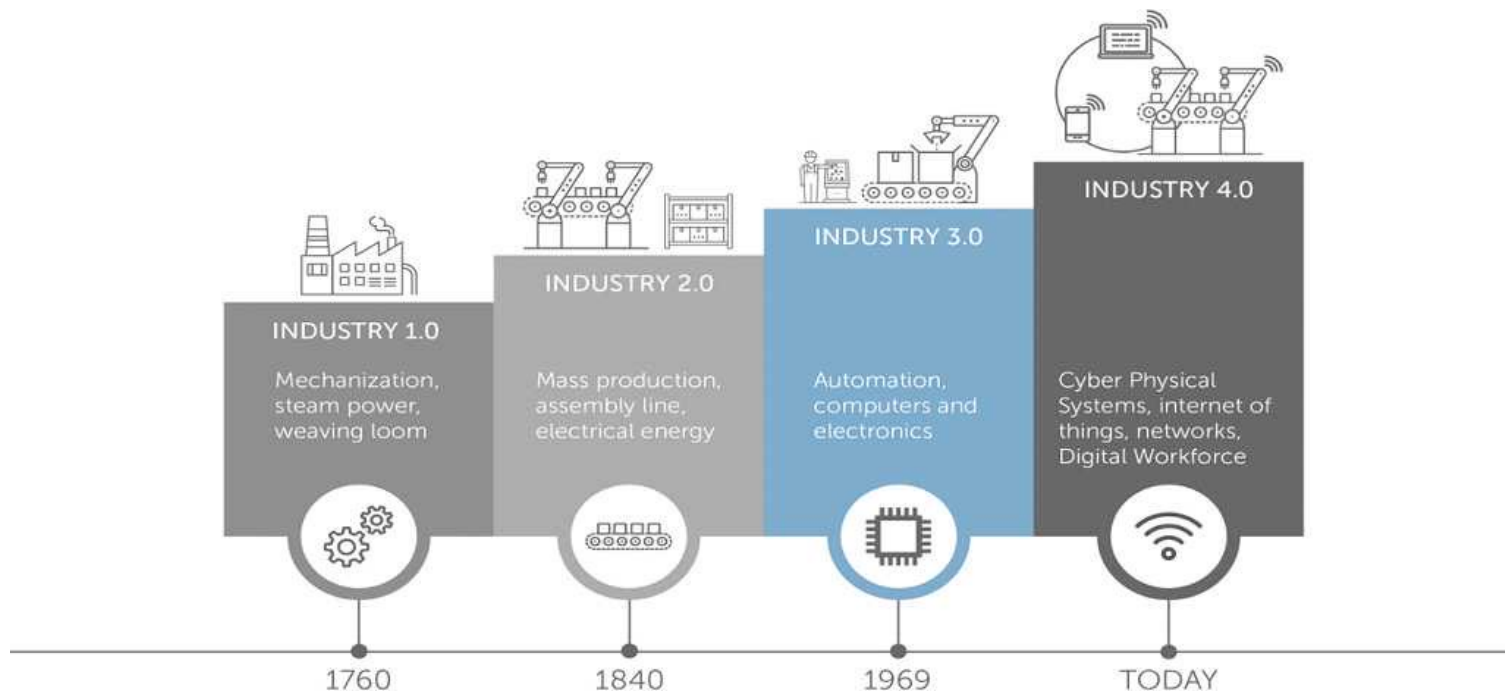
23

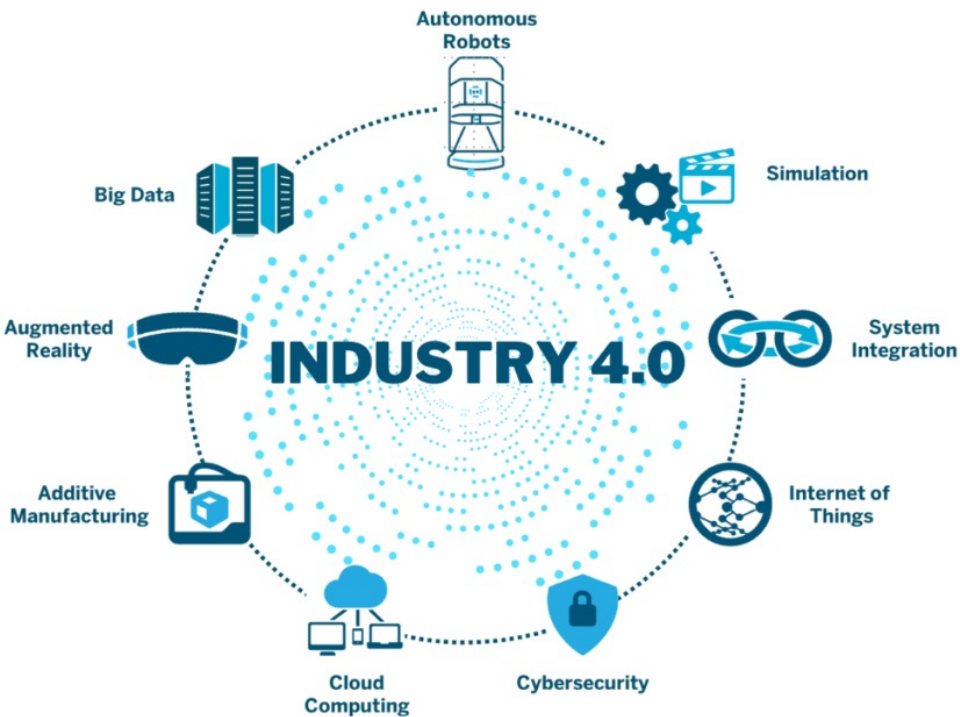
Порассуждаем?

35

Индустрия 4.0

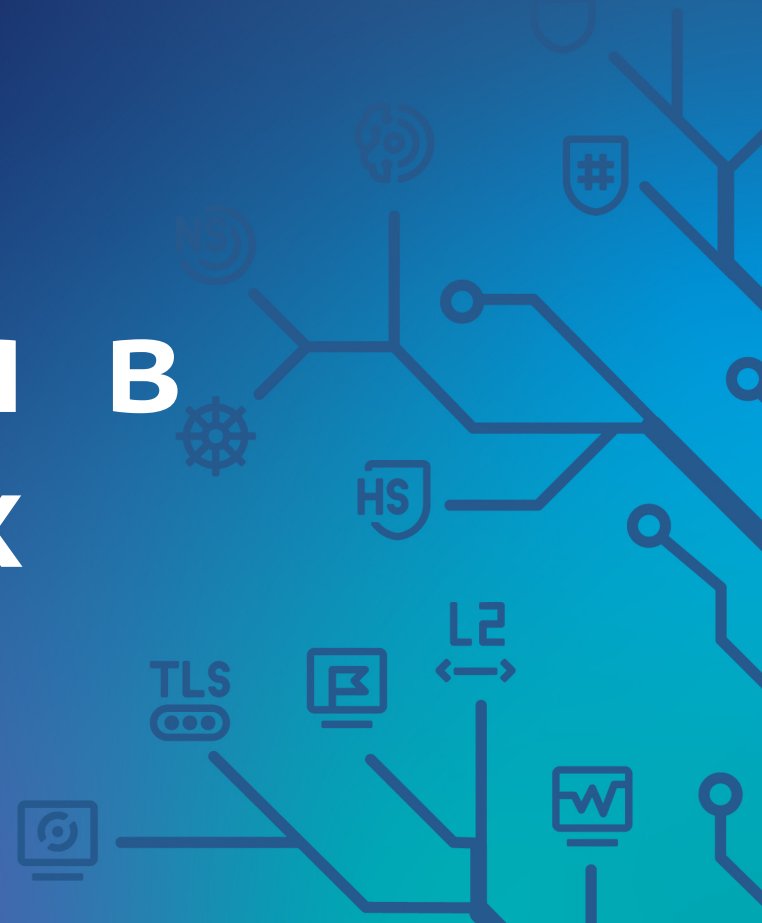
Индустриальные революции



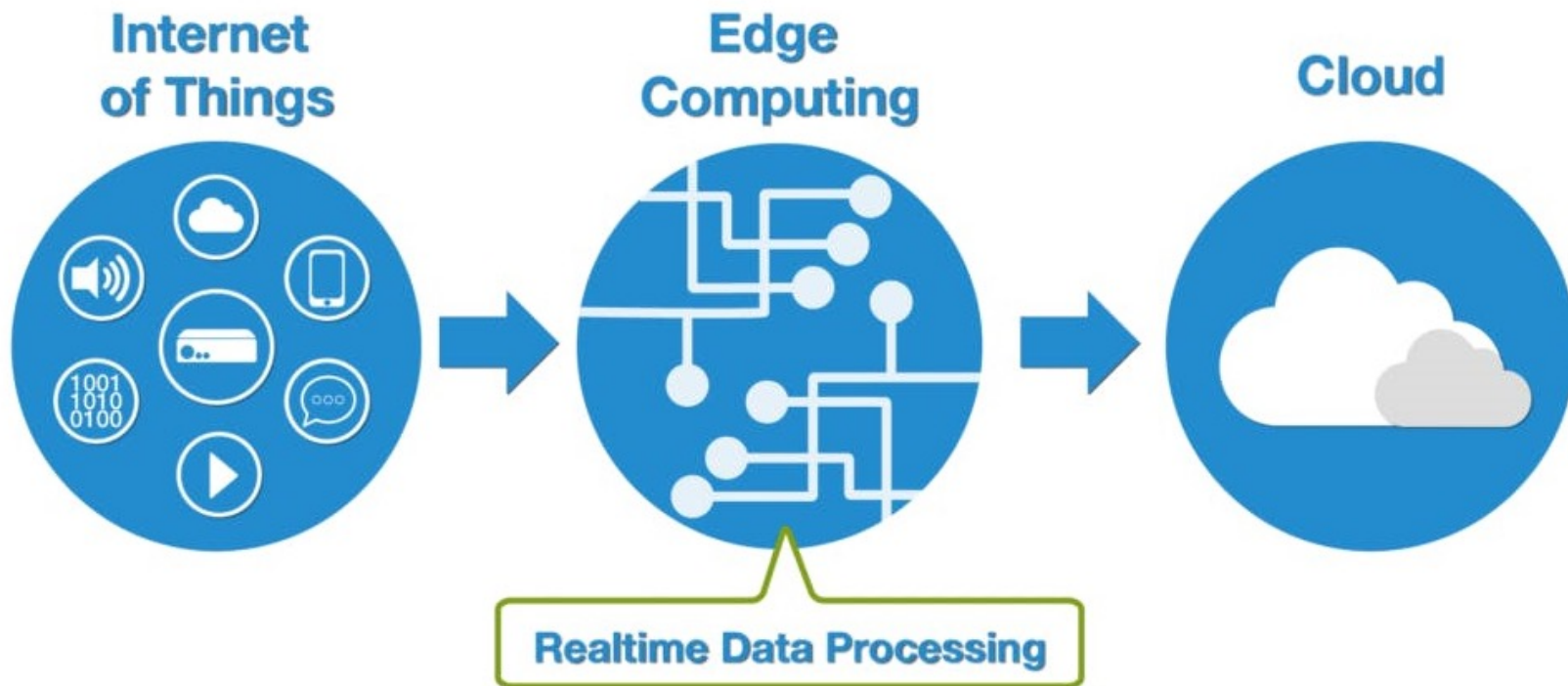


- Кибер-физические системы
- Интернет вещей
- Автономные роботы
- Облачные вычисления
- Аналитика больших данных
- Искусственный интеллект

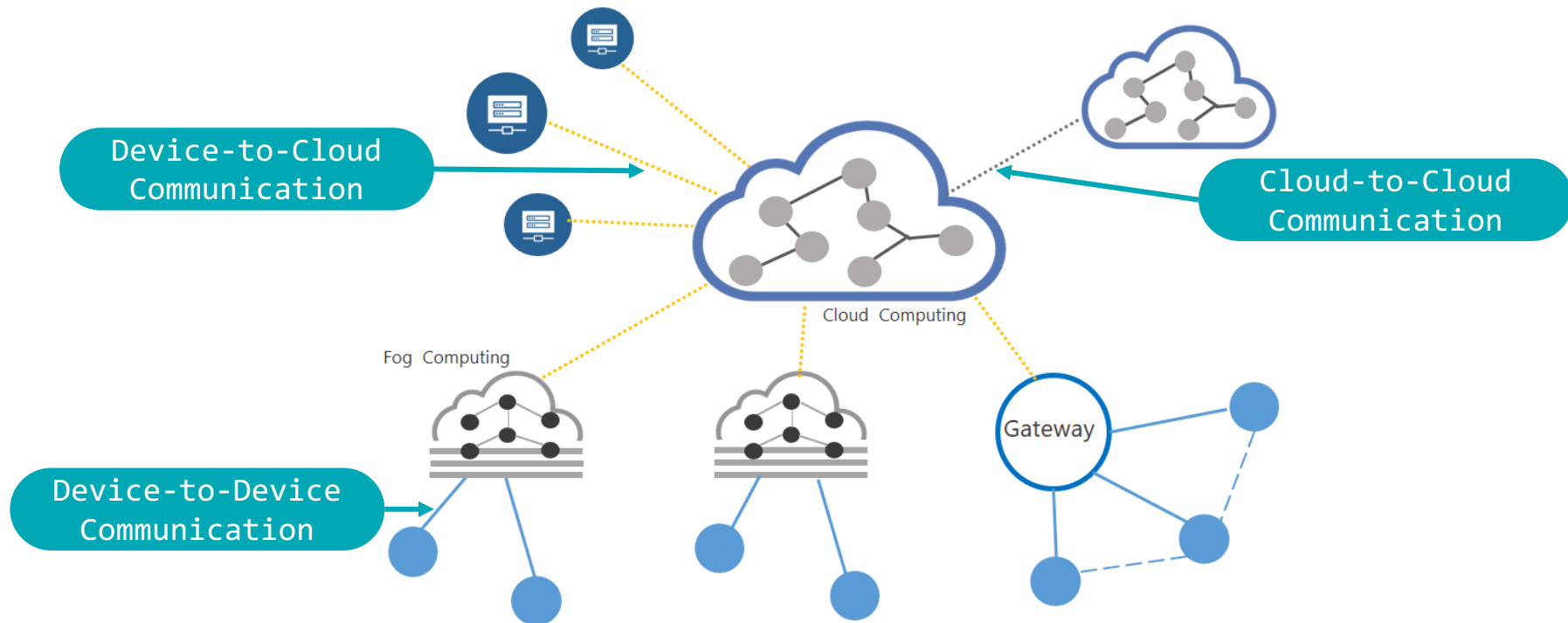
Особенности взаимодействия в индустриальных системах



Вычисления в IoT

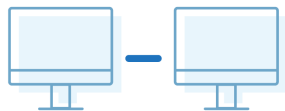


Виды взаимодействия в M2M и IoT

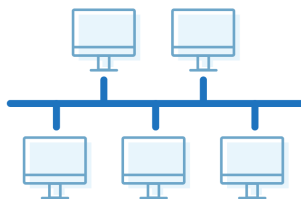


Топология связей М2М

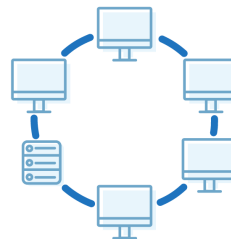
1 Point to point



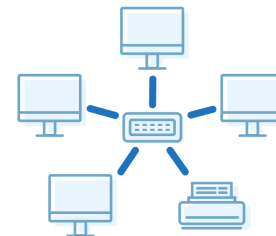
2 Bus



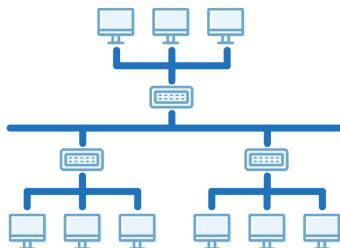
3 Ring



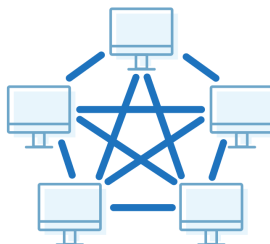
4 Star



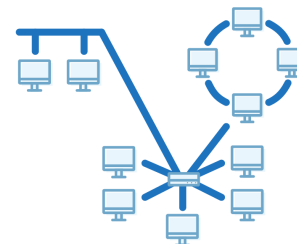
5 Tree



6 Mesh



7 Hybrid



Модели взаимодействия в М2М и IoT



Запрос-
Ответ



Push-Pull



Издатель-
Подписчик

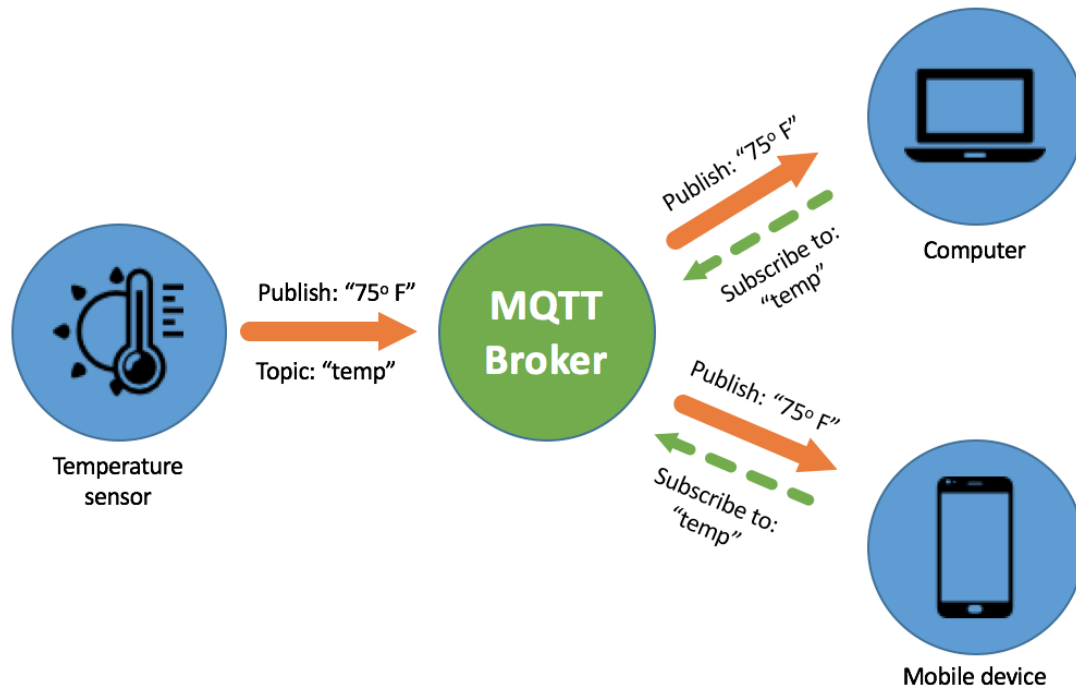


Точка-
Точка

Не обязательно интерактивное

Не обязательно «точка-точка»

MQTT: пример модели «Издатель-подписчик»



Промышленные технологии

ASCII



ASHRAE BACnet™

CANopen



Low Power WAN (LPWAN)
Technologies



CC-Link™



DLR
Device Level Ring



RPMA



DeviceNet™



EtherCAT®

EtherNet/IP™



IEC 61131-3

IEEE 1588



LLDP
Link Layer Discovery Protocol

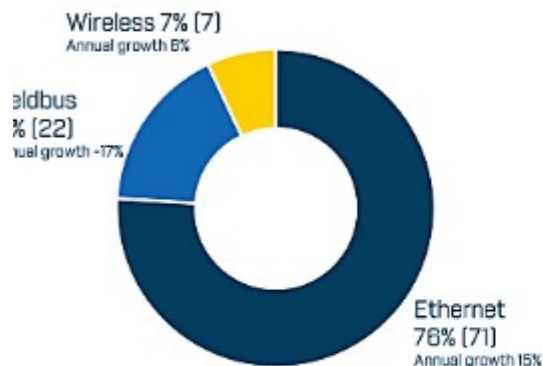


MTCONNECT



Рынок промышленных систем 2025

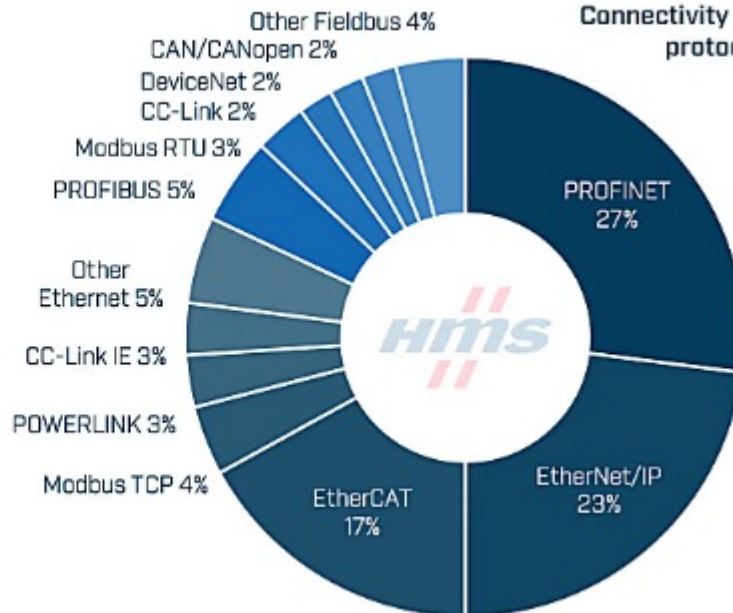
Connectivity by type



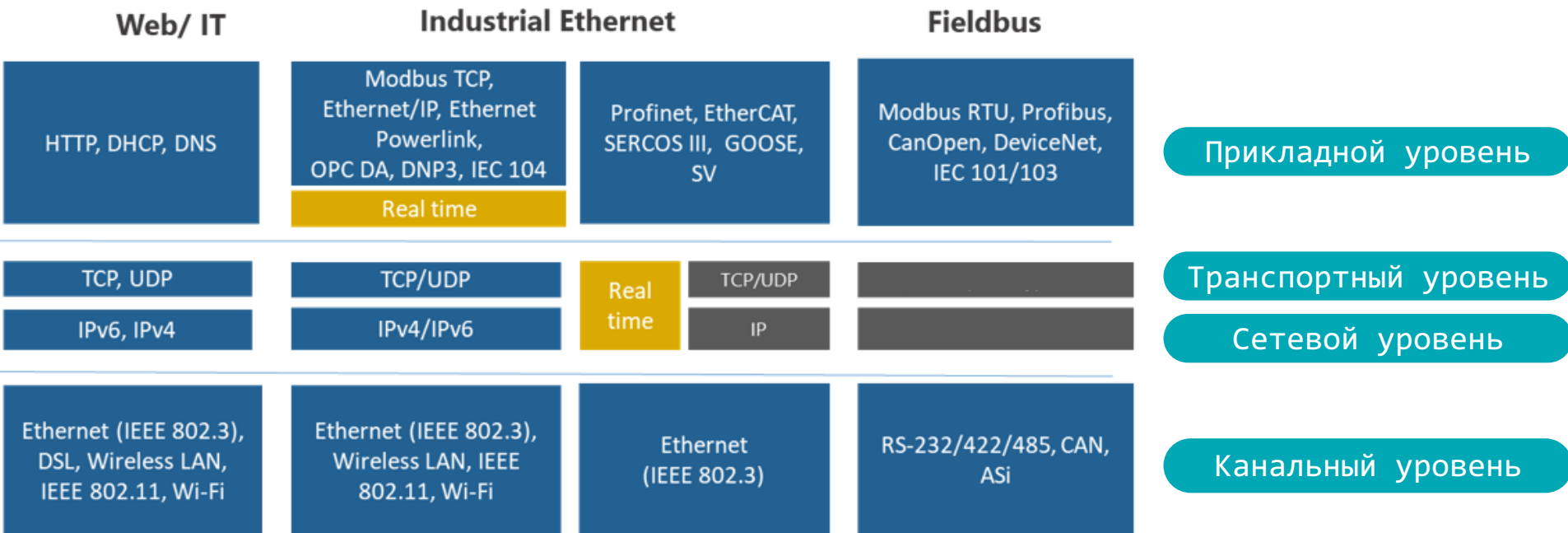
Overall growth in number of new nodes is expected to be +7,7% in next 5 years 2025-30.

HMS Networks' estimation for 2025 based on number of new installed nodes within Factory Automation, consolidated view based upon several market studies and our own statistics.

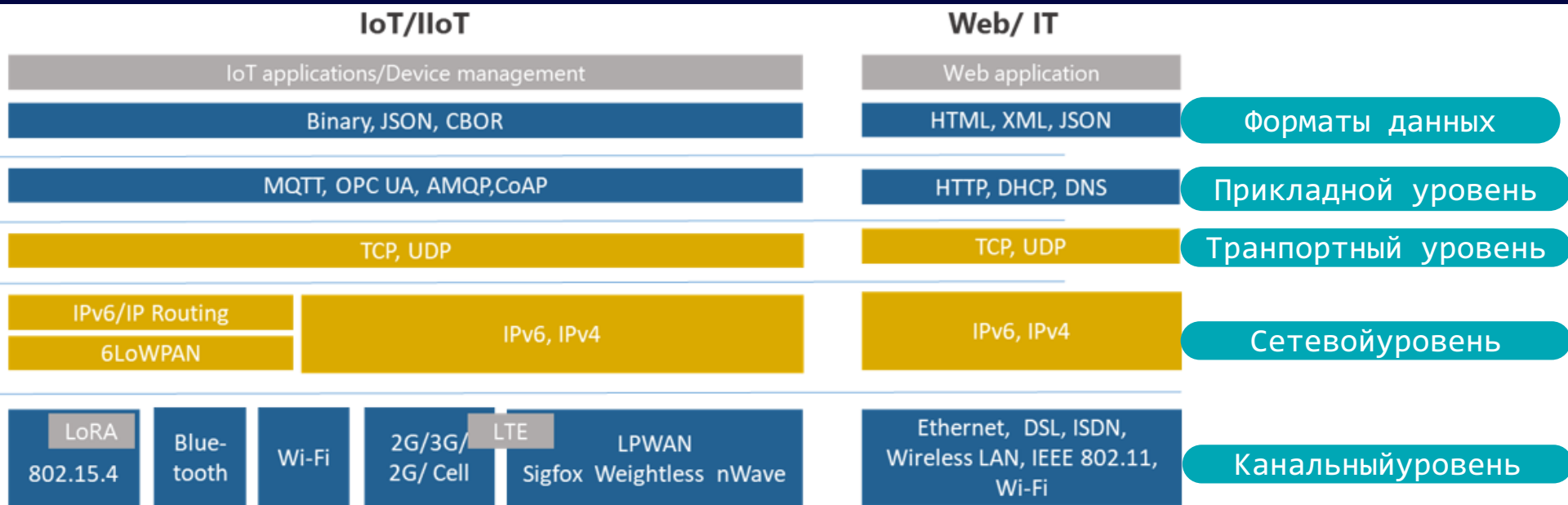
Connectivity by protocol



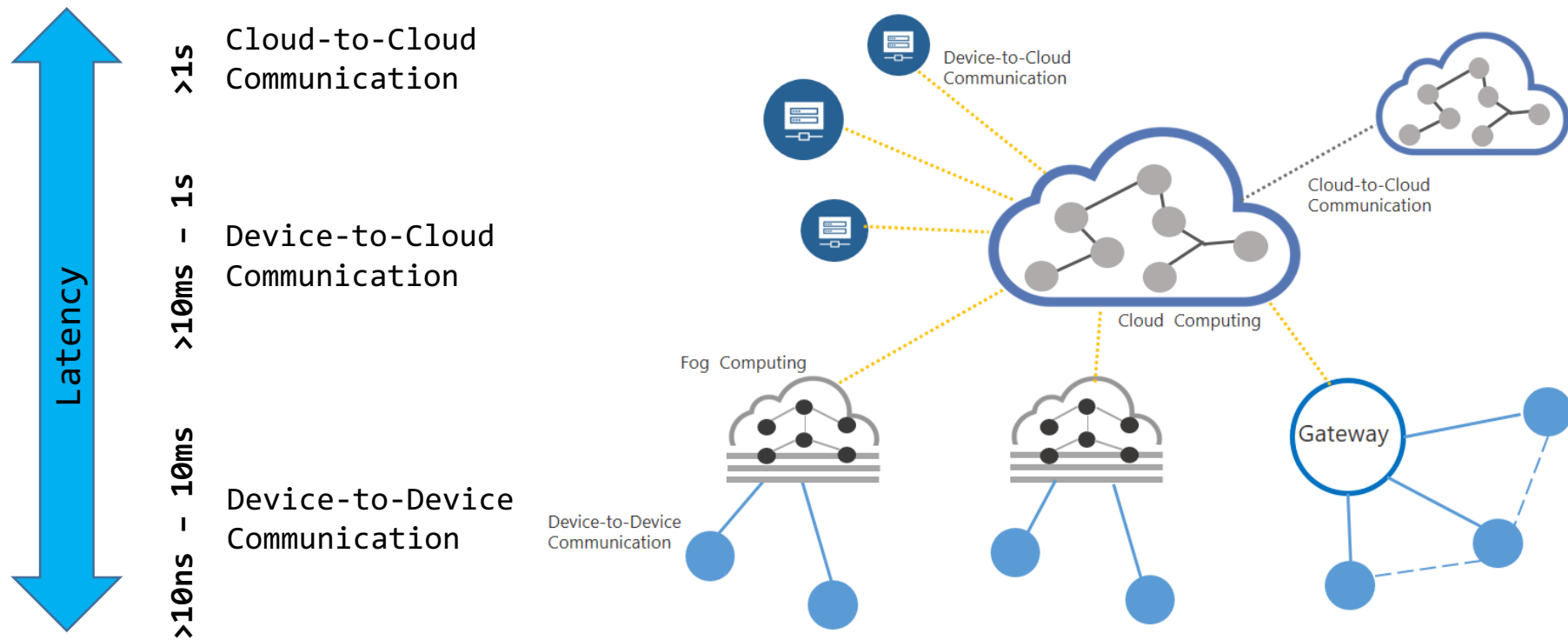
Стеки протоколов M2M и Web/IT



Стеки протоколов IoT и Web/IT



Требования по задержкам в M2M и IoT



Аспекты безопасности взаимодействия в M2M и IoT



Основные угрозы

- Изменение сообщений
- Навязывание ложных сообщений
- Навязывание обработанных ранее сообщений
- Подмена устройств

Приоритет функций безопасности

Web/IT

- Конфиденциальность
- Целостность
- Доступность

M2M и IoT

- Доступность
- Целостность
- Конфиденциальность

Защита промышленных протоколов

Международный опыт



MMS

IEC 62351-4 Security
Profiles for IEC 61850
MMS Messages



GOOSE, SV

IEC 62351-6 Security
Profiles for IEC 61850
GOOSE & SV Messages



Modbus

Modbus/TCP security



OPC UA

Защищенное поколение
протоколов OPC



IEC 60870-5

IEC 62351-5 Security profiles
для всех протоколов IEC 60870-5

Особенности

- Большое количество протоколов
- Протоколы реального времени, требования по задержкам
- Низкая пропускная способность
- Небольшой размер сообщений
- Неинтерактивные протоколы
- Групповое взаимодействие
- Нет встроенных механизмов защиты
- Низкоресурсные устройства
- Требования к энергопотреблению
- Целостность и аутентичность

Требования

- Независимость от протоколов прикладного и транспортного уровня
- Небольшой размер добавляемых данных
- Неинтерактивность
- Поддержка группового взаимодействия
- Симметричная криптография
- Небольшое число алгоритмов
- Целостность и аутентичность
- Защита от атак повтора

Защищенные протоколы IT

Стандартизованные и разрабатываемые в РФ



TLS, DTLS

Стек TCP/IP

Установление
сессии

Асимметричные
алгоритмы

Нет группового
взаимодействия



IPSec, IPsec

Защита IP

Нет группового
взаимодействия



CMS

Большой размер
сообщений



SRTP

Защита потоков
данных

Специализированные протоколы

Стандартизованные в РФ



МР 26.4.003-2019 «Информационная технология. Криптографическая защита информации. Использование российских криптографических механизмов для реализации обмена данными по протоколу d1ms»



МР 26.4.003-2018 «Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств»

Протокол CRISP



Cryptographic Industrial Security Protocol

ГОСТ Р 71252-2024



Основные идеи

Ненадежные и «слабые» каналы

- Неинтерактивный
- Не специфицируется установление ключей
- Сообщение содержит всю информацию, необходимую для его обработки

Требования к задержкам

- Симметричные алгоритмы
- Несколько сообщений обрабатываются на одном ключе

Небольшой размер

- Неявная адресация
- Детали определяются криптонабором
- Некоторые поля выполняют несколько функций

Структура CRISP-сообщения



Структура CRISP-сообщения

KeyId может быть использовано для

- Явной адресации
- Поддержки группового взаимодействия
- Выбора конкретного ключа из множества
- ...

Структура CRISP-сообщения

SeqNum используется для

- Защиты от атак повтора
- Защиты от навязывания устаревших сообщений
- Обработки сообщений не по порядку
- Генерации синхропосылки
- Вычисления производного ключа

Механизм
скользящего
окна

- Отправители и получатель(и) имеют общий базовый ключ
- У каждого отправителя уникальный SourceId
- Получатель может определить базовый ключ на основе полей ExternalKeyIdFlag, KeyId и, возможно, внешней информации
- Не регламентируется способ задания начального номера сообщения
- Максимальный размер CRISP сообщения составляет 2048

Криптонаборы

CS = 1 (MAGMA-CTR-CMAC)

Имитовставка

- «Магма» в режиме CMAC

Шифрование

- «Магма» в режиме гаммирования

Вычисление производного ключа

- «Магма» в режиме CMAC
- SeqNum, SourceId

Длина MAC

- 4 байта

CS = 2 (MAGMA-NUL-CCMAC)

Имитовставка

- «Магма» в режиме CMAC

Шифрование

- NULL

Вычисление производного ключа

- «Магма» в режиме CMAC
- SeqNum, SourceId

Длина MAC

- 4 байта

Криптонаборы

CS = 3 (MAGMA-CTR-CMAC8)

Имитовставка

- «Магма» в режиме CMAC

Шифрование

- «Магма» в режиме гаммирования

Вычисление производного ключа

- «Магма» в режиме CMAC
- SeqNum, SourceId

Длина MAC

- 8 байт

CS = 4 (MAGMA-NUL-CCMAC8)

Имитовставка

- «Магма» в режиме CMAC

Шифрование

- NULL

Вычисление производного ключа

- «Магма» в режиме CMAC
- SeqNum, SourceId

Длина MAC

- 8 байт

Криптонаборы

CS = 5 (KUZNECHIK-CTR-CMAC8)

Имитовставка

- «Кузнечик» в режиме CMAC

Шифрование

- «Кузнечик» в режиме гаммирования

Вычисление производного ключа

- «Кузнечик» в режиме CMAC
- SeqNum, SourceId

Длина MAC

- 8 байт

CS = 6 (KUZNECHIK-NULL-CMAC8)

Имитовставка

- «Кузнечик» в режиме CMAC

Шифрование

- NULL

Вычисление производного ключа

- «Кузнечик» в режиме CMAC
- SeqNum, SourceId

Длина MAC

- 8 байт

Свойства безопасности



ЦЕЛОСТНОСТЬ



АУТЕНТИФИКАЦИЯ ДАННЫХ



ЗАЩИТА ОТ АТАК ПОВТОРА



КОНФИДЕНЦИАЛЬНОСТЬ

Опционально

Обоснование стойкости



On security aspects of CRISP

<https://eprint.iacr.org/2023/1303.pdf>



On security aspects of CRISP

<https://ctcrypt.ru/files/files/2023/07/08.pdf>



On the tightness of CRISP security bounds

https://www.researchgate.net/publication/393919544_On_the_tightness_of_CRISP_security_bounds

Порассуждаем?



Вопросы

1

Набор протоколов на
«все случаи жизни»
Все быстро меняется

2

Спецификация ключевой
системы
Требуется
вариативность

3

«Облегченная» PKI
Проблемы управления
доверием

4

Вариативность
реализаций
ПО под разные платформы
Различные аппаратные
реализации

5

Проходной
шифратор
Обратная сторона
универсальности –
сложность
встраивания

Подписывайтесь
на наши соцсети,
там много интересного




инфотекс

Olga.Shemyakina@infotecs.ru





Спасибо за внимание!

