Некоторые подходы к криптографической защите коммуникаций в IoT и M2M

Марина Сорокина,
руководитель направления продуктового развития

История вопроса

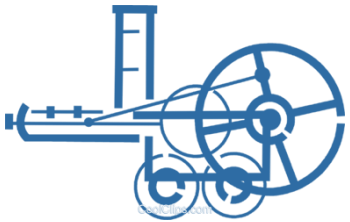
infotecs

Сегодня

- 100+ реализованных проектов по защите каналов для M2M систем, в т.м числе для РЖД, Электоэнергетики и т.д
- 20+ технологических партнерств по защите M2M коммуникаций и IIoT
- Пилотные проекты по защите M2M и IoT коммуникаций в сфере нефтянной, газовой промышленности
- 60+ человек заняты разработкой продуктов для защиты инфорации в промышленных системах

M2M + IoT = Industry 4.0

Индустрия 4.0



«Индустрия 1.0»

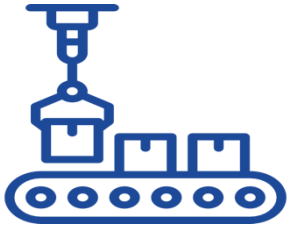
Механизация:
замена физической силы на энергию пара

1784 г.

«Индустрия 2.0»

Электрофикация:
Внедрение конвеерного производства

1870 г.



«Индустрия 3.0»

Автоматизация:
Внедрение роботизированных систем с ЧПУ

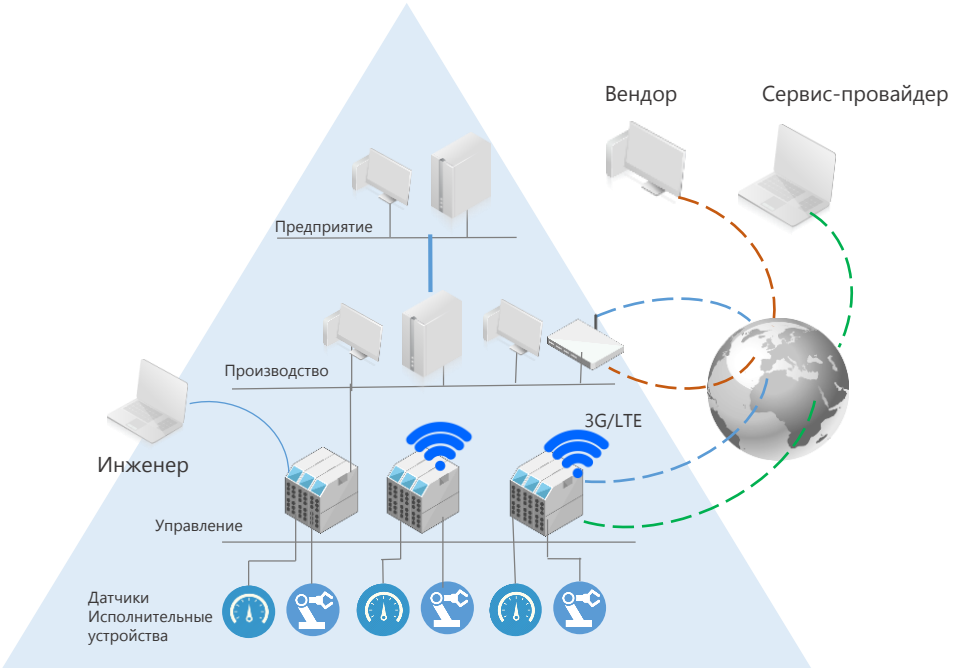
1969 г.

«Индустрия 4.0»

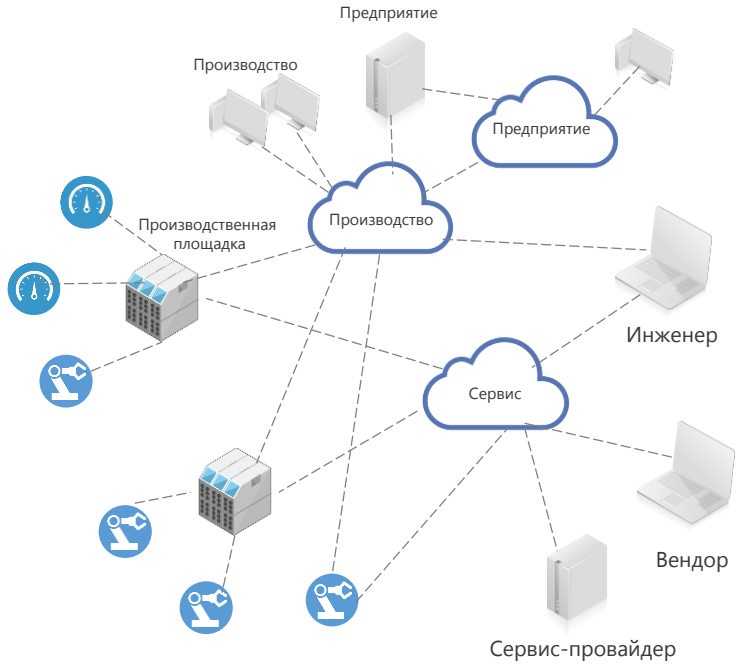
Цифровизация:
Умное производство и киберфизические системы

сегодня

Industry 4.0

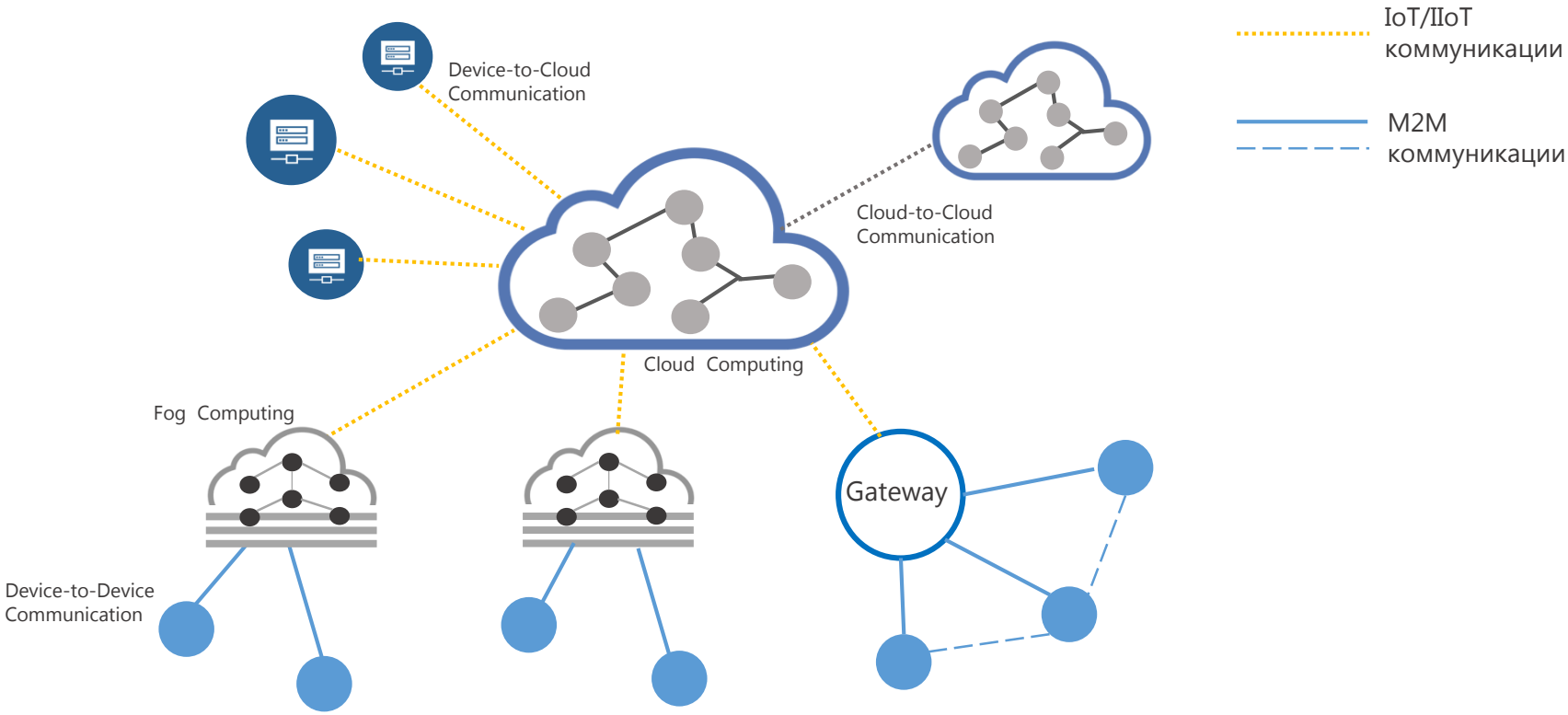


Современная АСУ ТП

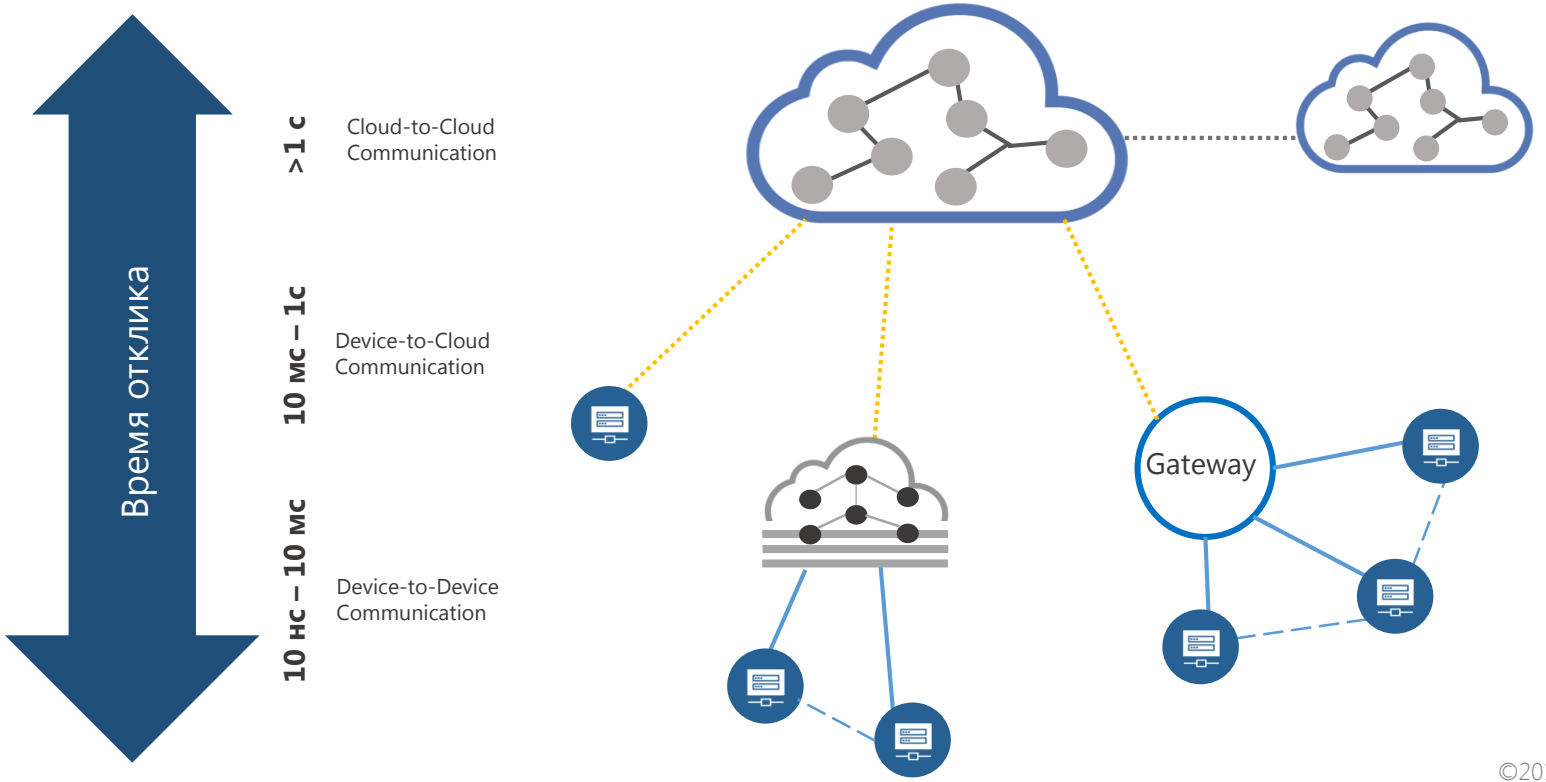


IIoT

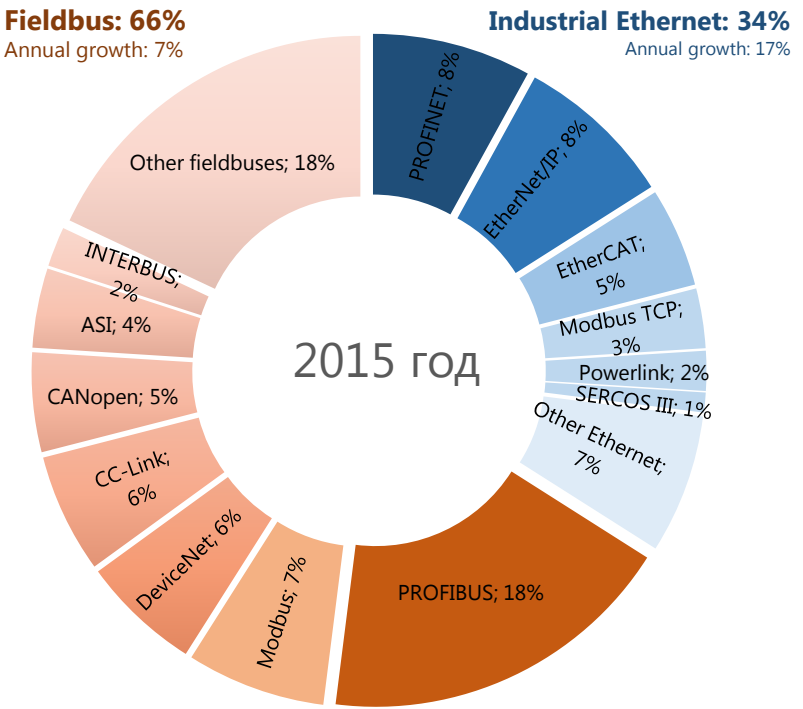
M2M и IoT коммуникации

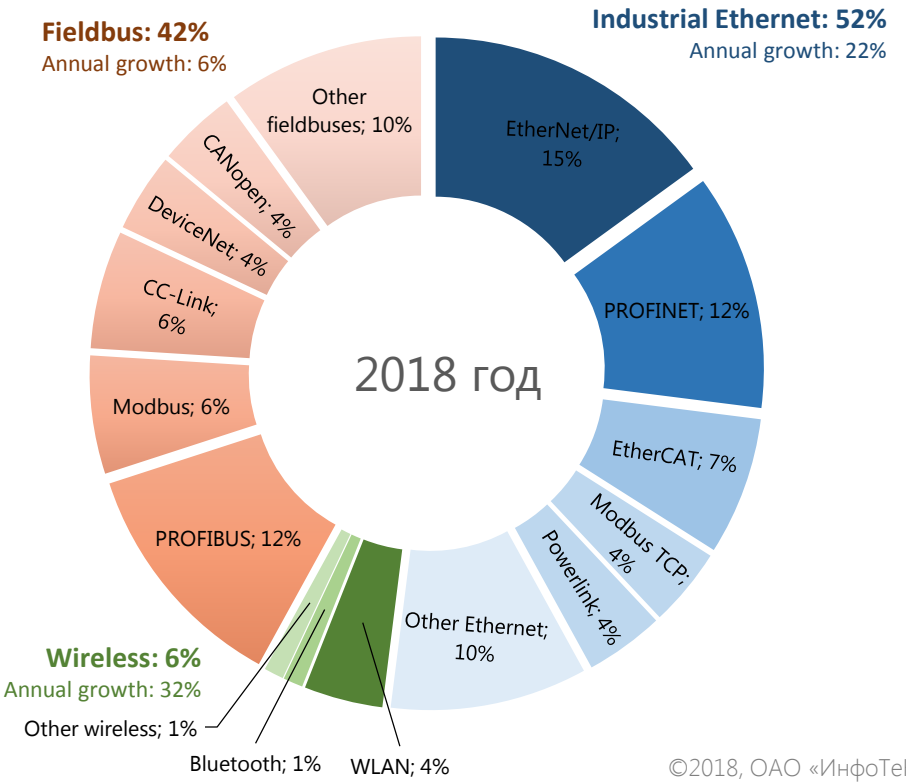


Латентность для IoT и M2M коммуникаций



Промышленные M2M протоколы



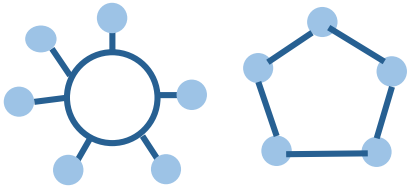


Source: HMS Industrial Networks

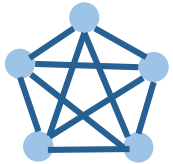
Топология M2M протоколов

Общая шина

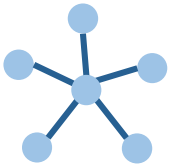
Кольцо



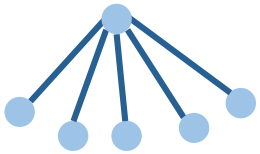
Полносвязная



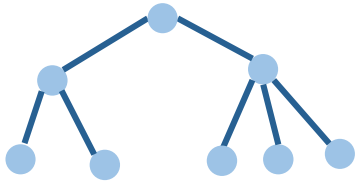
Звезда



Звезда-Иерархия



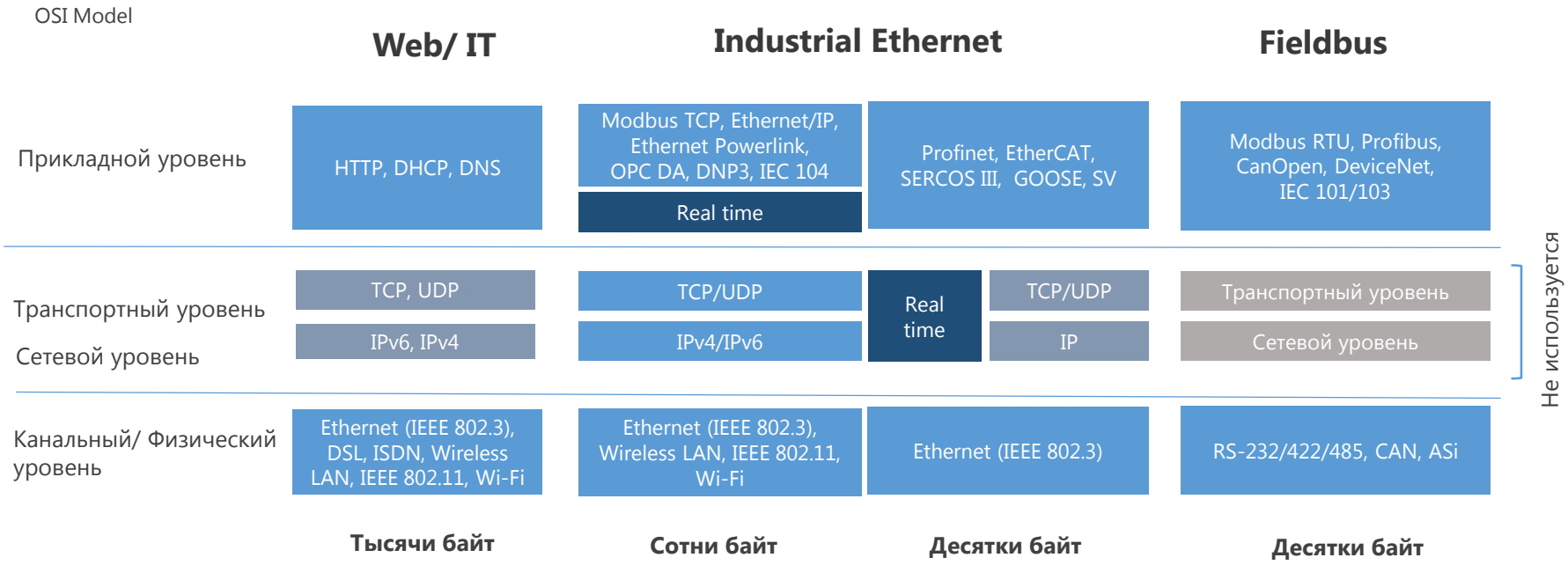
Дерево



Модель взаимодействия

- Точка-точка
- Broadcast
- Multicast
- Подписочная модель
- Request/Response

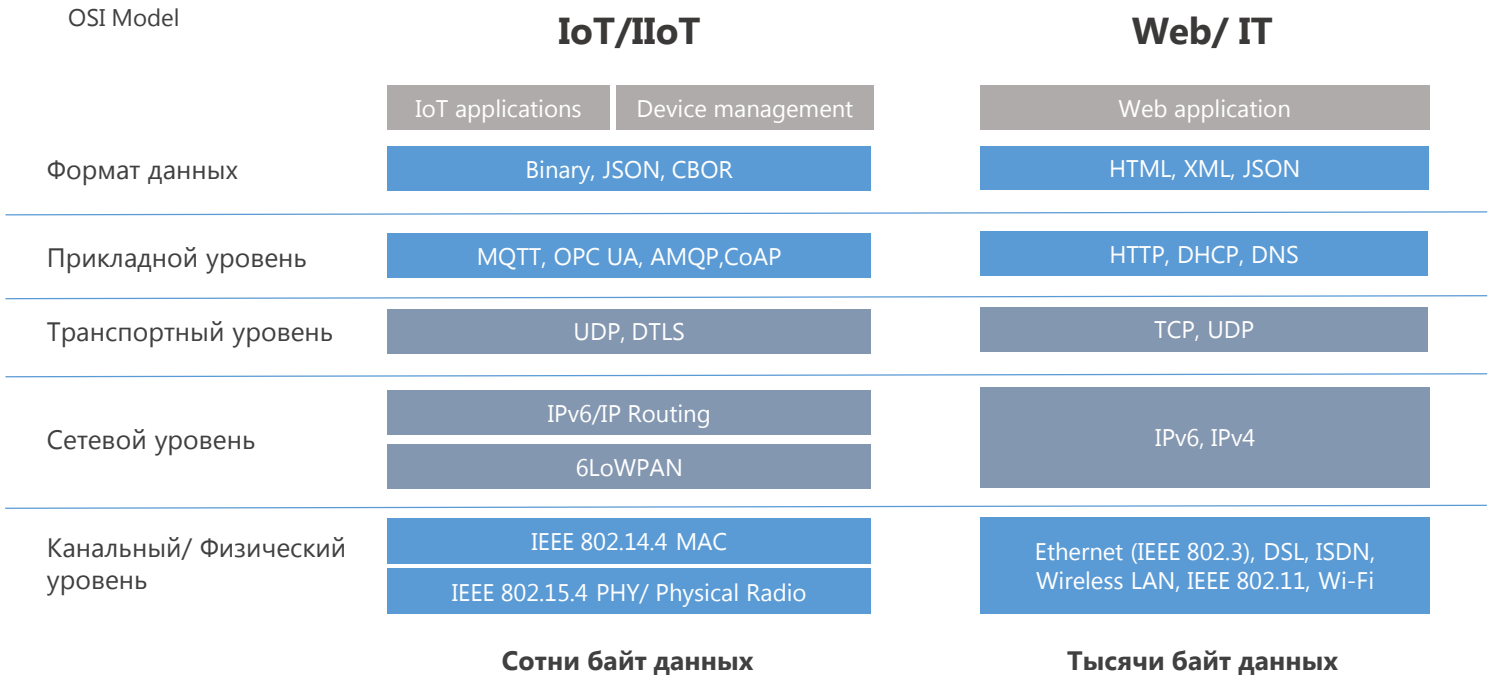
Стек M2M протоколов



Основные IoT/IIoT протоколы

- OPC UA
- MQTT
- AMQP
- CoAP
- REST/HTTP
- LoRaWAN
- LoWPAN
- И многие другие …

Сравнение IoT протоколов с Web



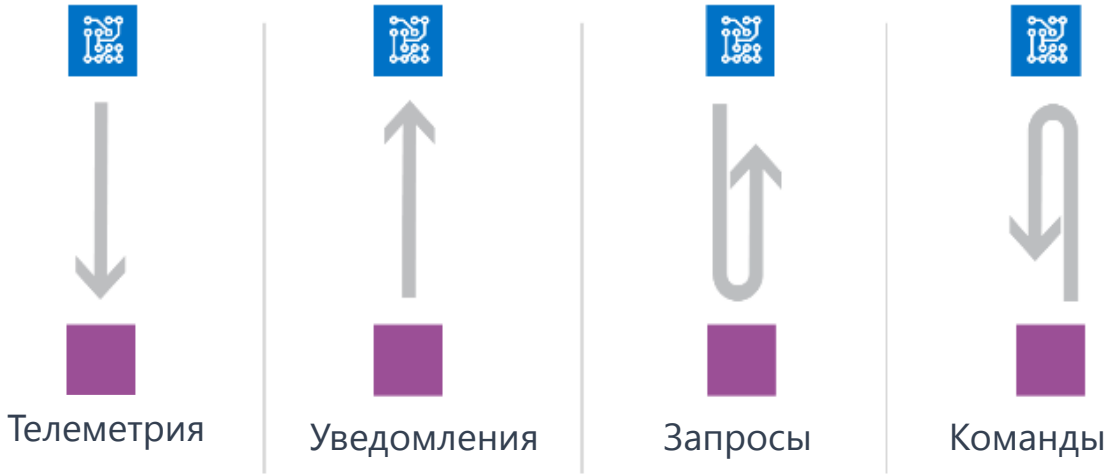
Сравнение IoT/IIoT протоколов

	MQTT	OPC UA	AMQP	REST	CoAP	LoRaWAN LoWPAN
Транспорт	TCP/IP	TCP/IP	TCP/IP	TCP/IP	UDP/IP	TCP/IP
Взаимодействие	Publish-Subscr.	Request-Respon	Point-to-point	Request-Respon	Request-Respon	Point-to-point
Применение	Device-to-Cloud Cloud-to-Cloud	Device-to-Cloud Cloud-to-Cloud Device-to-Device	Device-to-Cloud Cloud-to-Cloud Device-to-Device	Device-to-Cloud Cloud-to-Cloud	Device-to-Cloud Cloud-to-Cloud	Device-to-Cloud Cloud-to-Cloud
Латентность	низкая	низкая	низкая	высокая	высокая	низкая
Real-time	условно	Real-time	условно	нет	нет	нет
ИБ	TLS	профиль	TLS	HTTPS	DTLS	TLS/ DTLS На уровне чипа

Особенности ИБ для M2M и IoT

Основные угрозы

Назначение M2M и IoT/IIoT коммуникаций



Модель угроз

- Изменения команд/ данных (нарушение целостности)
- Подмена команд
- Навязывание ложных данных
- Изменение конфигурации
- Навязывание старых данных
- Подмена устройства

Приоритеты

Web/IT

- Конфиденциальность
- Целостность
- Доступность

M2M
IoT/IIoT

- Доступность
- Целостность
- Аутентичность
- Конфиденциальность

Основные аспекты защиты M2M и IoT/IIoT коммуникаций

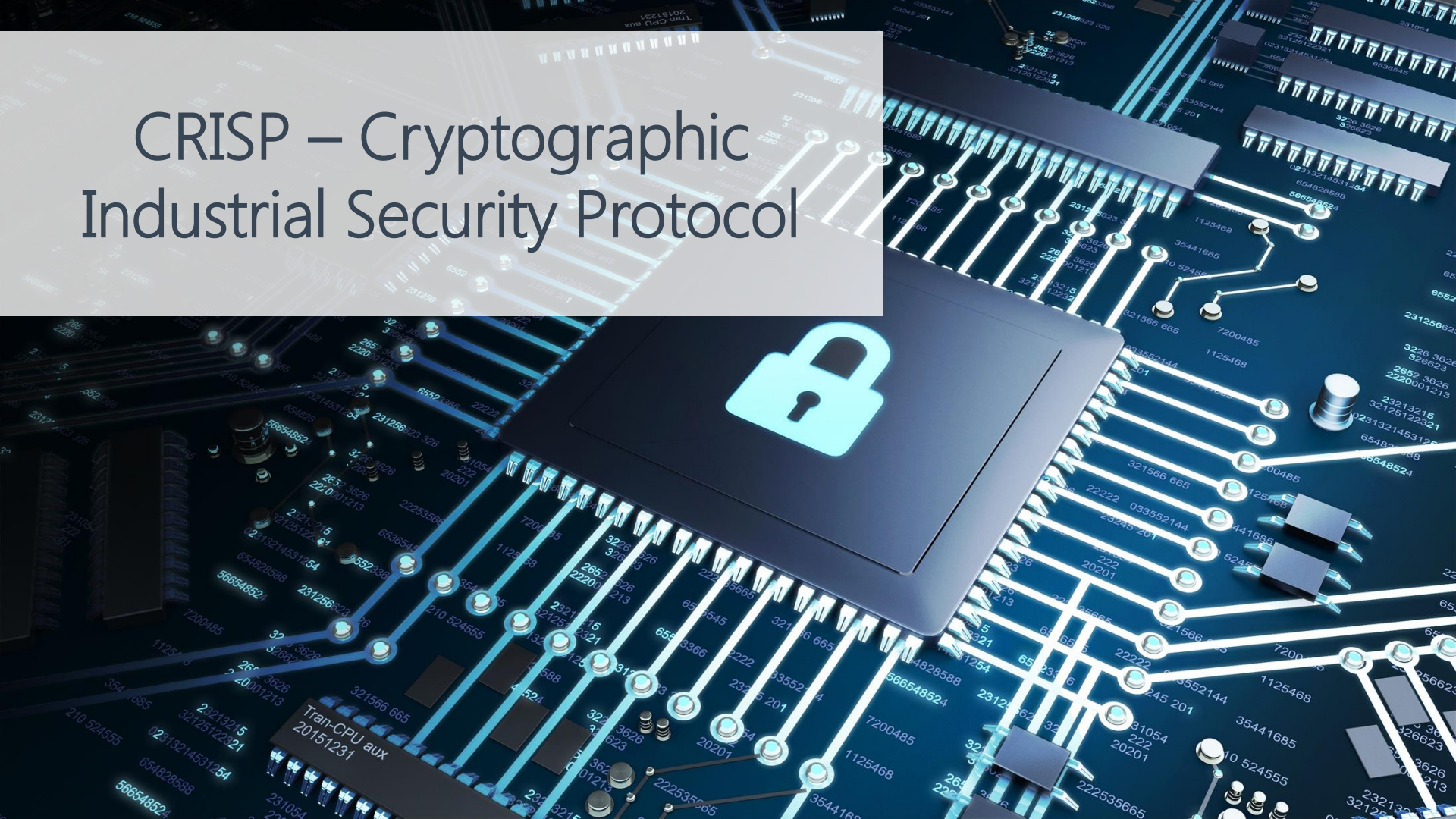
- Очень большое разнообразие протоколов
- Использование разных каналов / Использование слабых каналов
- Распространенность мультикаста и подписочной модели
- Многие протоколы являются real-time и критичны к задержкам
- Передача данных объемом в десятки-сотни байт/ критичность к оверхеду
- Большая часть M2M протоколов не являются TCP/IP base
- M2M протоколы в большинстве не подразумевают механизмов защиты коммуникаций
- Беспроводные IoT протоколы имеют встроенную в чипы защиту коммуникаций на западных алгоритмах
- Аутентичность и целостность важнее конфиденциальности

infotecs

Резюме

- IPSec VPN – требует установления сессии и плохо работает на слабых каналах, большой оверхед, TPC/IP based
- ViPNet VPN - большой оверхед, TPC/IP based
- TLS - требует установления сессии, большой оверхед
- CMS - большой оверхед, задержки
- Рекомендованные в РФ криптографические протоколы не решают поставленной задачи

CRISP – Cryptographic Industrial Security Protocol



Криптографический протокол для M2M и IoT

Cryptographic Industrial Security Protocol

CRISP

Не всегда надежные каналы/ ограниченная пропускная способность
- без установления сессии -> предварительно распределенные ключи
- каждое сообщение несет всю необходимую информацию для обработки

Целостность и аутентичность важнее конфиденциальности
- обязательная имитозащита/опциональное шифрование
- защита от «чтения назад» не обязательна

Минимальный overhead
- адресация абонентов неявная, через протоколы целевой системы
- все криптографические детали определяются номером криптографического набора

Минимальные задержки обработки
- только симметричные механизмы
- минимальный набор механизмов

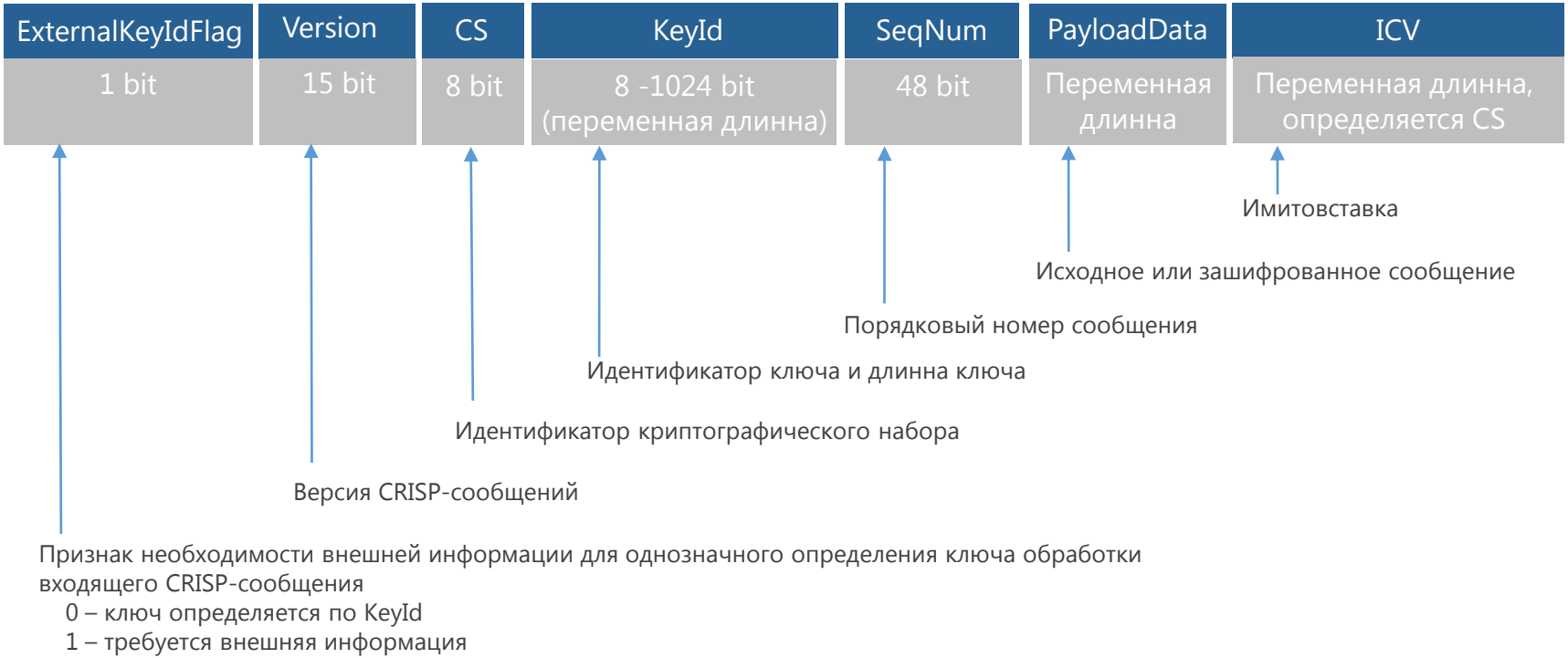
Криптографический протокол CRISP

CRISP (Cryptographic Industrial Security Protocol) - бессессионный протокол защищенной передачи данных для индустриальных систем, M2M и IoT/IIoT коммуникаций

- Обеспечение целостности,
- Обеспечение конфиденциальности
- Аутентификация источника сообщений
- Защита от навязывания повторных сообщений

- У абонентов общий секретный ключ
- Защита данных – блочный шифр, имитовставка
- Малый размер вспомогательных данных – 12 байт + имитовставка
- Поддержка адресных (один к одному) сообщений
- Поддержка многоадресных (один ко многим) сообщений

Структура CRISP-сообщений



CRISP: Механизмы защиты

Криптонабор CS=1

Целостность и аутентичность
- блочный шифр «Магма» в режиме выработки имитовставки по ГОСТ 34.13-2015

Конфиденциальность
- блочный шифр «Магма» в режиме гаммирования по ГОСТ 34.13-2015

Диверсификация ключей
- блочный шифр «Магма» в режиме выработки имитовставки
- контроль нагрузки на ключ/данные для диверсификации – *SequenceNumber*

Защита от навязывания повторных сообщений
- счетчик сообщений *SequenceNumber* + движущееся окно принятых сообщений
- уникальность значений счетчика в сроки действия одного *KeyIdentifier*

Криптонабор CS=2

Целостность и аутентичность
- блочный шифр «Магма» в режиме выработки имитовставки по ГОСТ 34.13-2015

Диверсификация ключей
- блочный шифр «Магма» в режиме выработки имитовставки
- контроль нагрузки на ключ/данные для диверсификации – *SequenceNumber*

Защита от навязывания повторных сообщений
- счетчик сообщений *SequenceNumber* + движущееся окно принятых сообщений
- уникальность значений счетчика в сроки действия одного *KeyIdentifier*

Решение SIES с протоколом CRISP

- Встраиваемое пассивное решение
- Базовые криптографические функции в простом API
- Централизованное управление ключевой информацией
- Возможность гибкой похода в реализации сценариев защиты информации

- Индустриальное исполнение
- Поддержка промышленный интерфейсов и протоколов
- Резервируемость и масштабируемость

Уровень автоматизированного управления и полевой уровень:

ViPNet SIES Core

Операторский уровень:

ViPNet SIES Server
ViPNet SIES Client

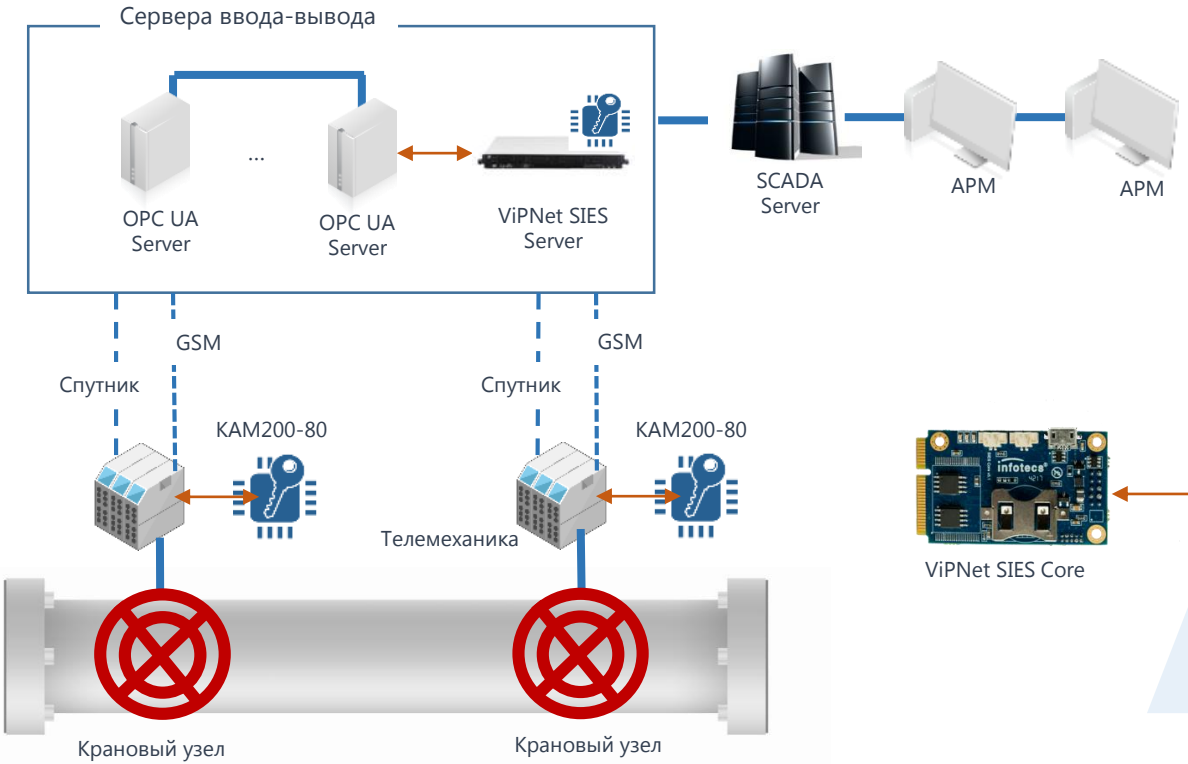
Управление :

ViPNet SIES MC
ViPNet SIES WorkStation

Планы по CRISP

- Пилотирование решение ViPNet SIES в составе продуктов партнеров на индустриальных объектах
- Разработка рекомендаций по использованию CRISP в протоколах M2M и IoT: Modbus TCP, Modbus RTU, OPC UA, GOOSE, МЭК-69780-104, МЭК-69780-101
- Обсуждение протокола как рекомендации в рамках рабочей группы №4 «Криптографические механизмы для M2M и индустриальных сетей» ТК26

Пример защиты системы управления задвижками газопровода




infotecs
Спасибо за внимание!