A person in a dark suit and tie is holding a large, metallic gear. The gear is semi-transparent, revealing a circuit board underneath. The background is a blurred office setting with a computer monitor and keyboard. The overall color palette is cool, with blues and greys.

Некоторые подходы к криптографической защите коммуникаций в IoT и M2M

Марина Сорокина,
руководитель направления продуктового развития

История вопроса



Сегодня

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



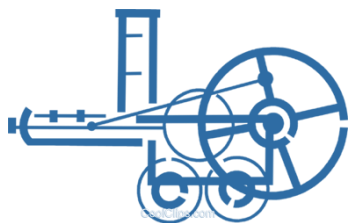
M2M + IoT = Industry 4.0

DATA

IOT



Индустрия 4.0



«Индустрия 1.0»

Механизация:
замена физической силы
на энергию пара

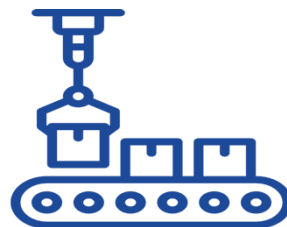
1784 г.



«Индустрия 2.0»

Электрoфикация:
Внедрение конвейерного
производства

1870 г.



«Индустрия 3.0»

Автоматизация:
Внедрение
роботизированных
систем с ЧПУ

1969 г.

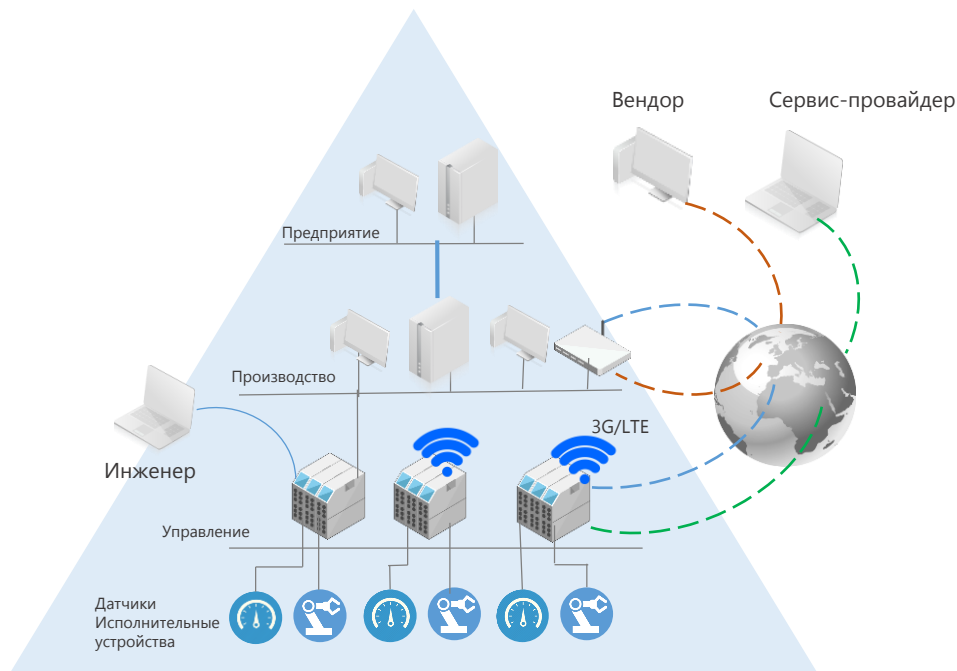


«Индустрия 4.0»

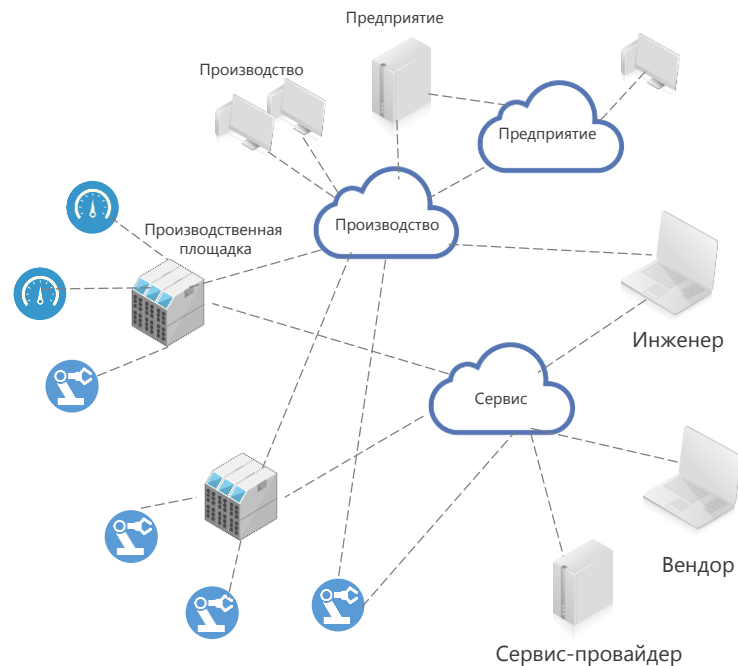
Цифровизация:
Умное производство и
киберфизические
системы

сегодня

Industry 4.0

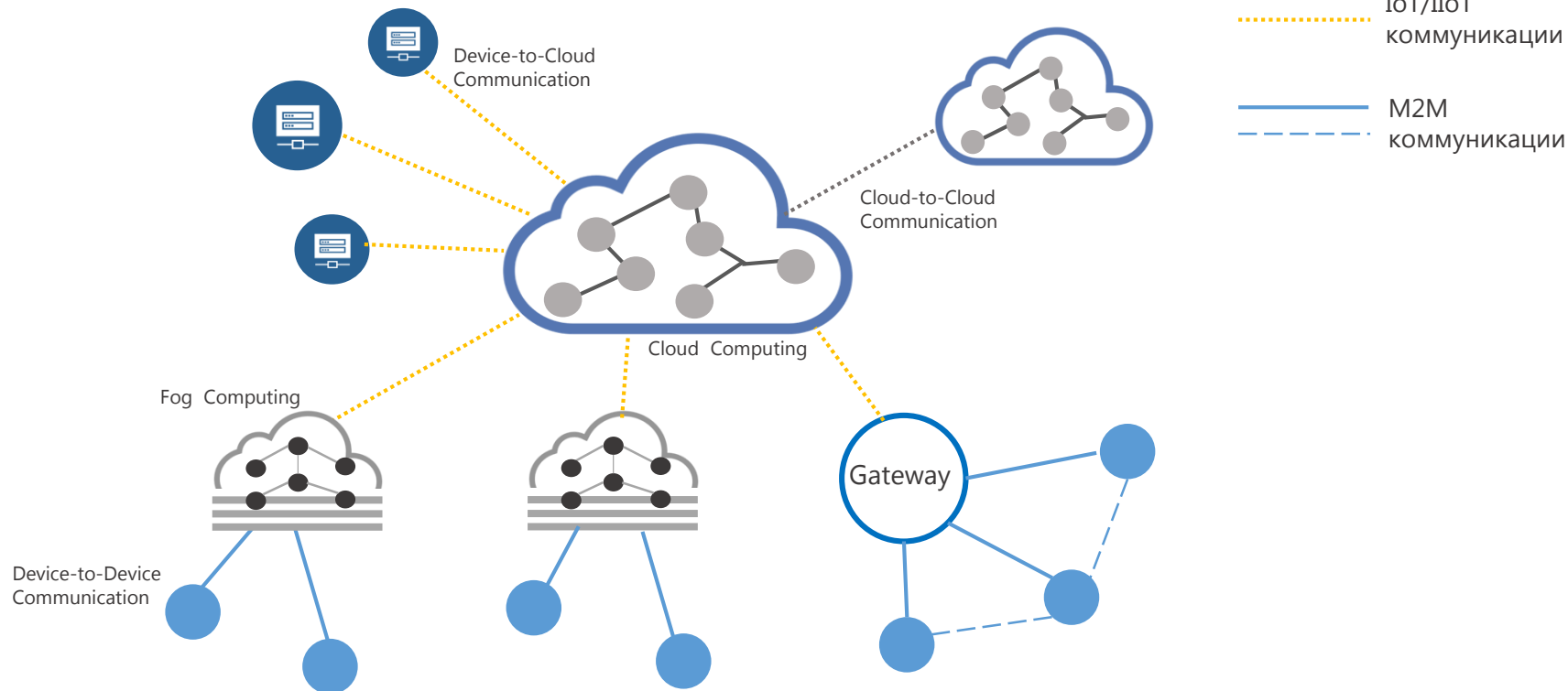


Современная АСУ ТП

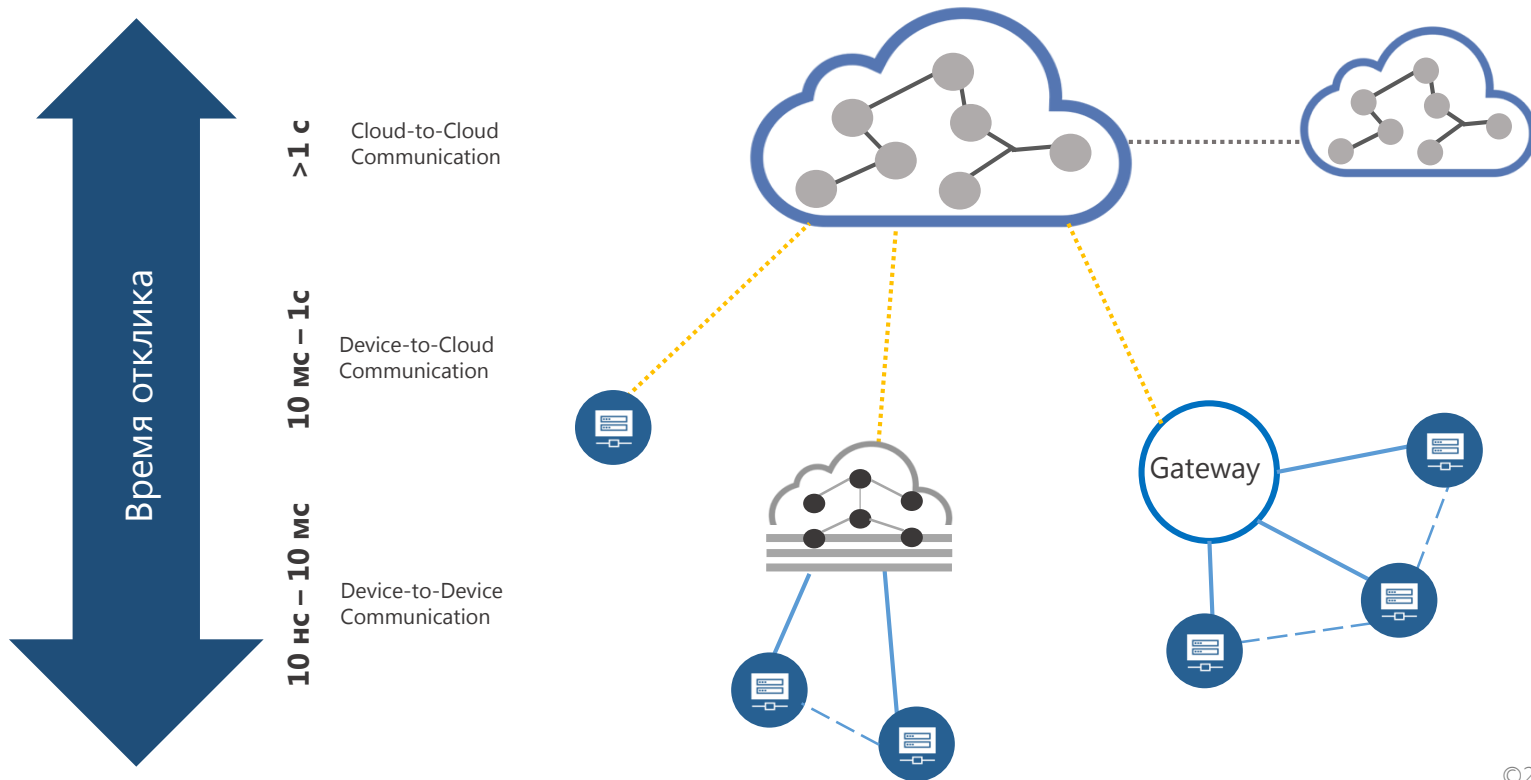


IIoT

M2M и IoT коммуникации



Латентность для IoT и M2M коммуникаций



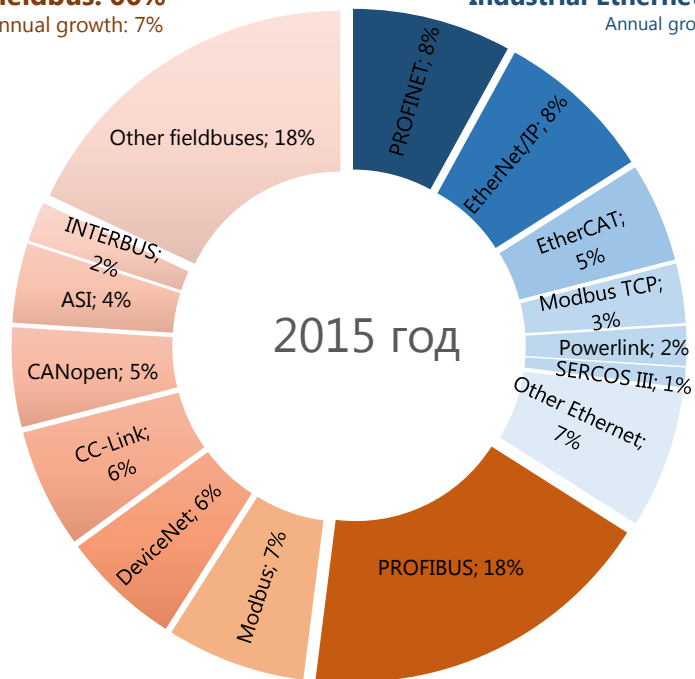
Промышленные M2M протоколы

Fieldbus: 66%

Annual growth: 7%

Industrial Ethernet: 34%

Annual growth: 17%



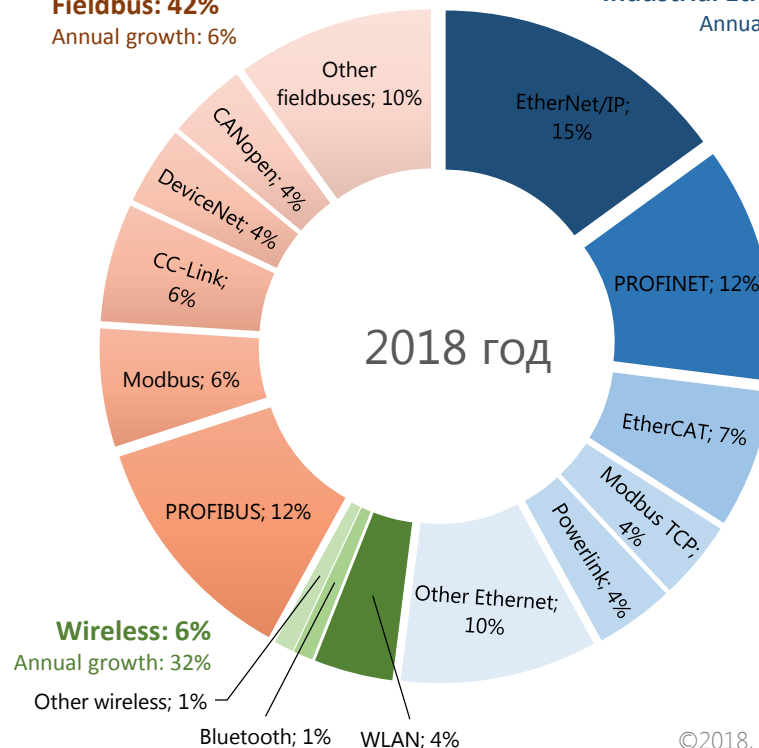
Source: HMS Industrial Networks

Fieldbus: 42%

Annual growth: 6%

Industrial Ethernet: 52%

Annual growth: 22%



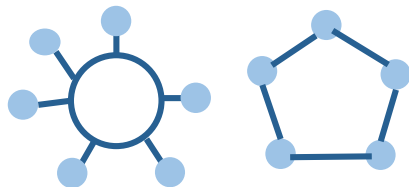
©2018, ОАО «ИнфоТеКс».

Топология M2M протоколов

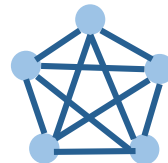
Общая шина



Кольцо



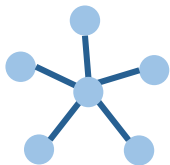
Полносвязная



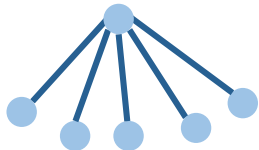
Модель взаимодействия

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

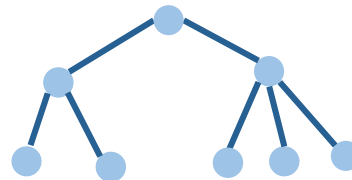
Звезда



Звезда-Иерархия



Дерево



Стек M2M протоколов

OSI Model

Web/ IT

Industrial Ethernet

Fieldbus

Прикладной уровень

HTTP, DHCP, DNS

Modbus TCP, Ethernet/IP,
Ethernet Powerlink,
OPC DA, DNP3, IEC 104

Real time

Profinet, EtherCAT,
SERCOS III, GOOSE, SV

Modbus RTU, Profibus,
CanOpen, DeviceNet,
IEC 101/103

Транспортный уровень

TCP, UDP

TCP/UDP

Real
time

TCP/UDP

Транспортный уровень

Сетевой уровень

IPv6, IPv4

IPv4/IPv6

IP

Сетевой уровень

Канальный/ Физический
уровень

Ethernet (IEEE 802.3),
DSL, ISDN, Wireless
LAN, IEEE 802.11, Wi-Fi

Ethernet (IEEE 802.3),
Wireless LAN, IEEE 802.11,
Wi-Fi

Ethernet (IEEE 802.3)

RS-232/422/485, CAN, ASi

Тысячи байт

Сотни байт

Десятки байт

Десятки байт

Не используется

Сравнение IoT протоколов с Web

OSI Model	IoT/IIoT	Web/ IT
	IoT applications Device management	Web application
Формат данных	Binary, JSON, CBOR	HTML, XML, JSON
Прикладной уровень	MQTT, OPC UA, AMQP, CoAP	HTTP, DHCP, DNS
Транспортный уровень	UDP, DTLS	TCP, UDP
Сетевой уровень	IPv6/IP Routing 6LoWPAN	IPv6, IPv4
Канальный/ Физический уровень	IEEE 802.14.4 MAC IEEE 802.15.4 PHY/ Physical Radio	Ethernet (IEEE 802.3), DSL, ISDN, Wireless LAN, IEEE 802.11, Wi-Fi
	Сотни байт данных	Тысячи байт данных

Сравнение IoT/IIoT протоколов

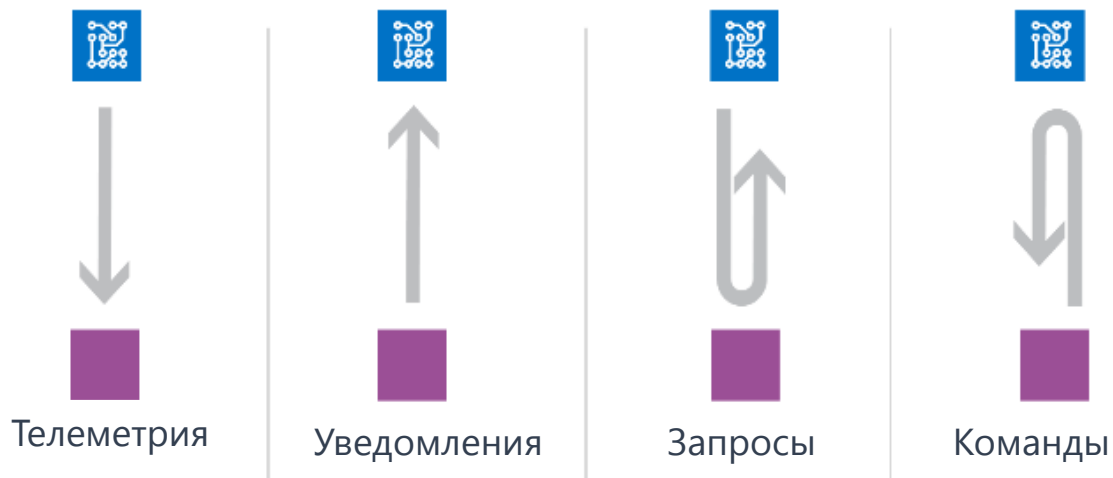
	MQTT	OPC UA	AMQP	REST	CoAP	LoRaWAN LoWPAN
Транспорт	TCP/IP	TCP/IP	TCP/IP	TCP/IP	UDP/IP	TCP/IP
Взаимодействие	Publish-Subscr.	Request-Respon	Point-to-point	Request-Respon	Request-Respon	Point-to-point
Применение	Device-to-Cloud Cloud-to-Cloud	Device-to-Cloud Cloud-to-Cloud Device-to-Device	Device-to-Cloud 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

- IPSec VPN – требует установления сессии и плохо работает на слабых каналах, большой оверхед, TCP/IP based
- ViPNet VPN - большой оверхед, TCP/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

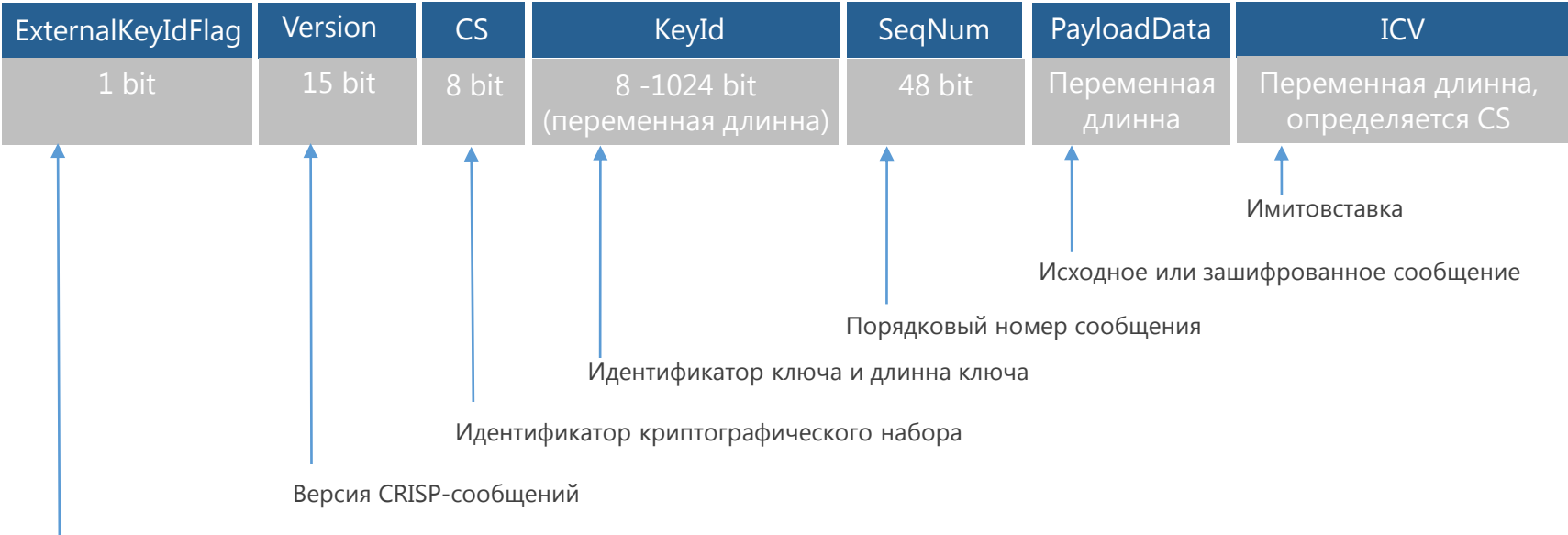
- только симметричные механизмы
- минимальный набор механизмов

Криптографический протокол CRISP

CRISP (Cryptographic Industrial Security Protocol) - бессессионный протокол защищенной передачи данных для промышленных 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



Признак необходимости внешней информации для однозначного определения ключа обработки входящего CRISP-сообщения
 0 – ключ определяется по KeyId
 1 – требуется внешняя информация

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 :

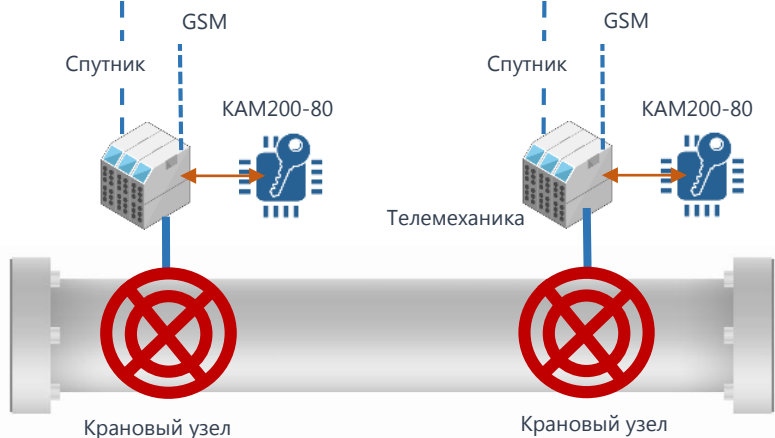
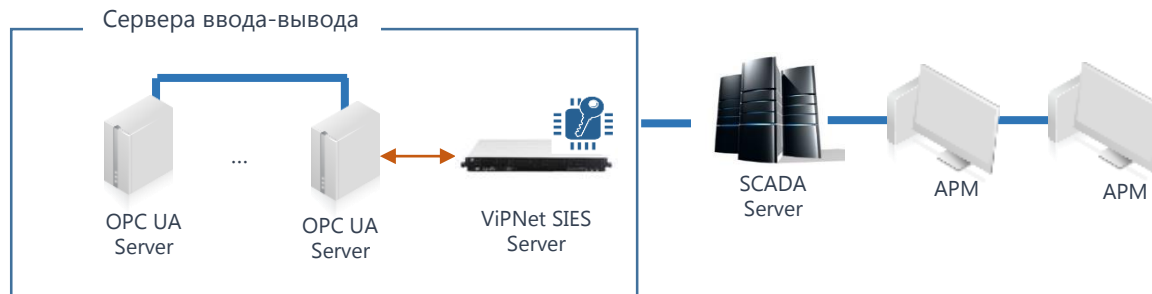
ViPNet SIES MC
ViPNet SIES WorkStation

Планы по CRISP

- Пилотирование решение ViPNet SIES в составе продуктов партнеров на промышленных 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 промышленных сетей» ТК26



Пример защиты системы управления задвижками газопровода



The background of the slide is a photograph of a landscape at sunset. In the foreground, several wind turbines are silhouetted against the bright orange and yellow sky. In the middle ground, several high-voltage power line towers are visible, stretching across the horizon. The sun is low on the horizon, creating a strong glow and casting long shadows. The overall scene is a mix of renewable energy (wind) and traditional infrastructure (power lines).

Спасибо за внимание!