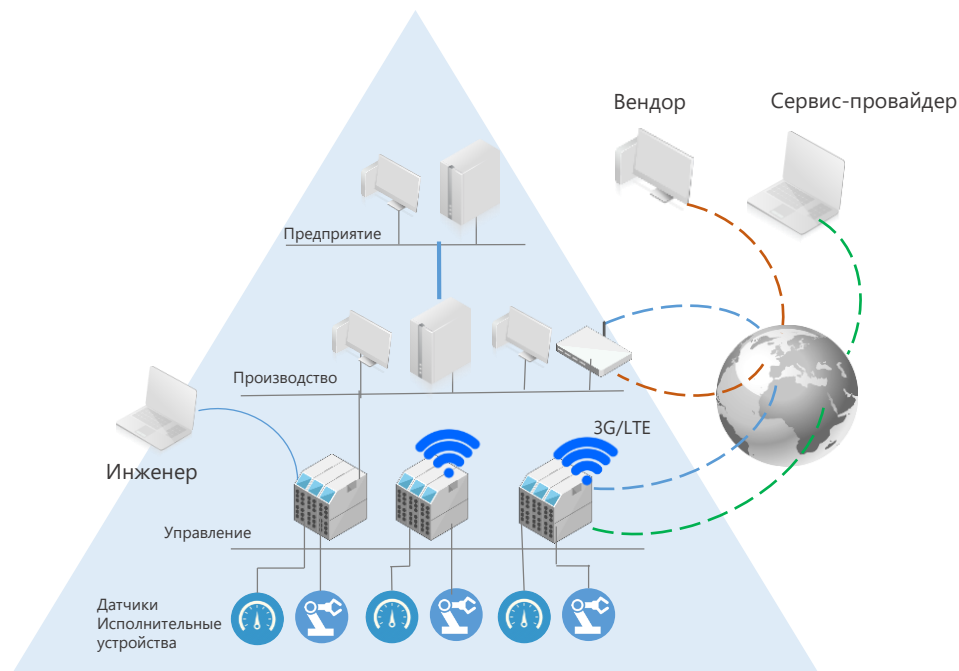
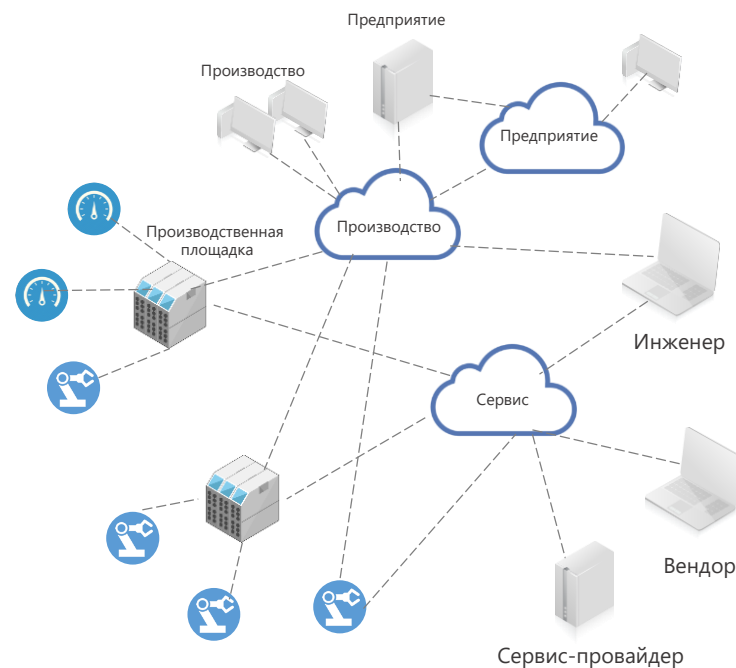


Дмитрий Гусев
ОАО «ИнфоТеКС»

Индустрия 4.0 :: объекты защиты

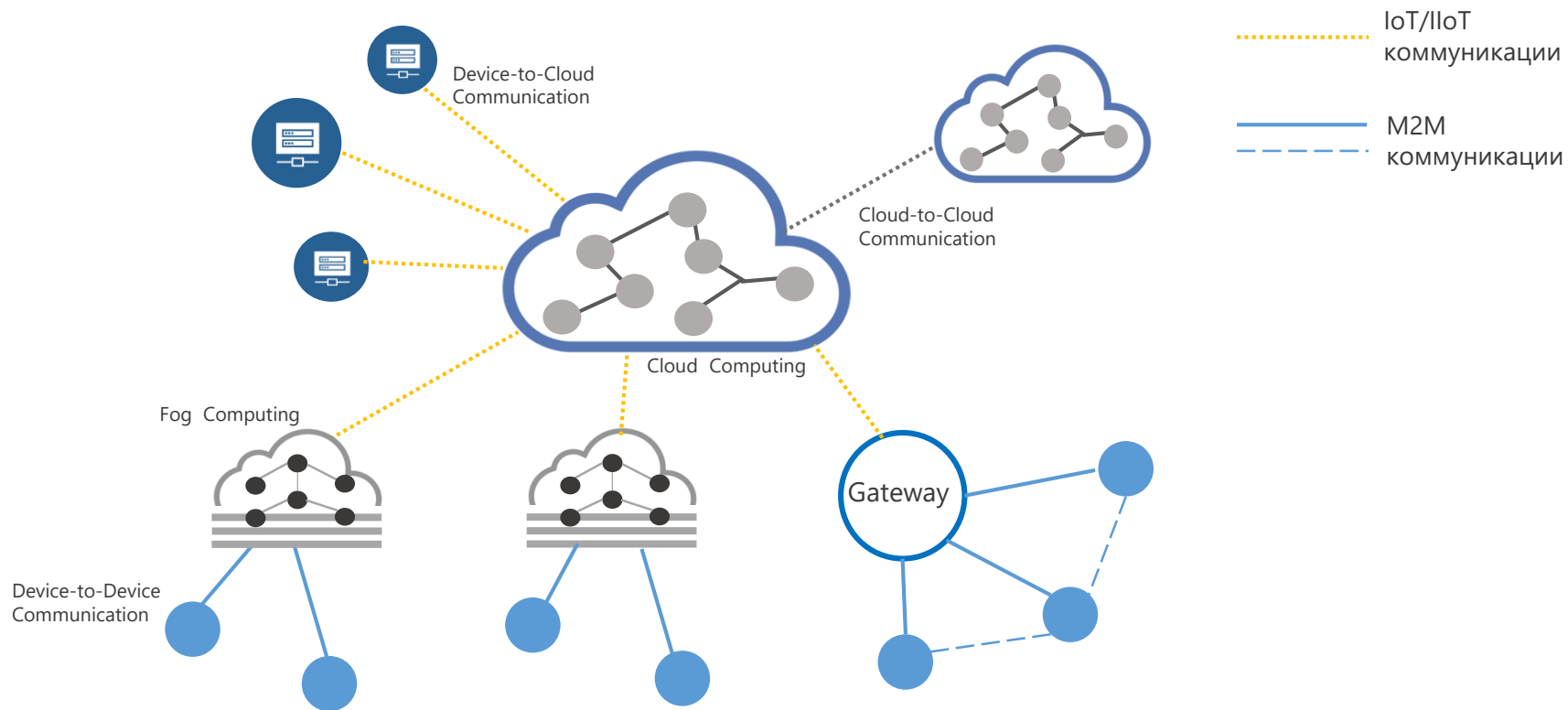


Современная АСУ ТП

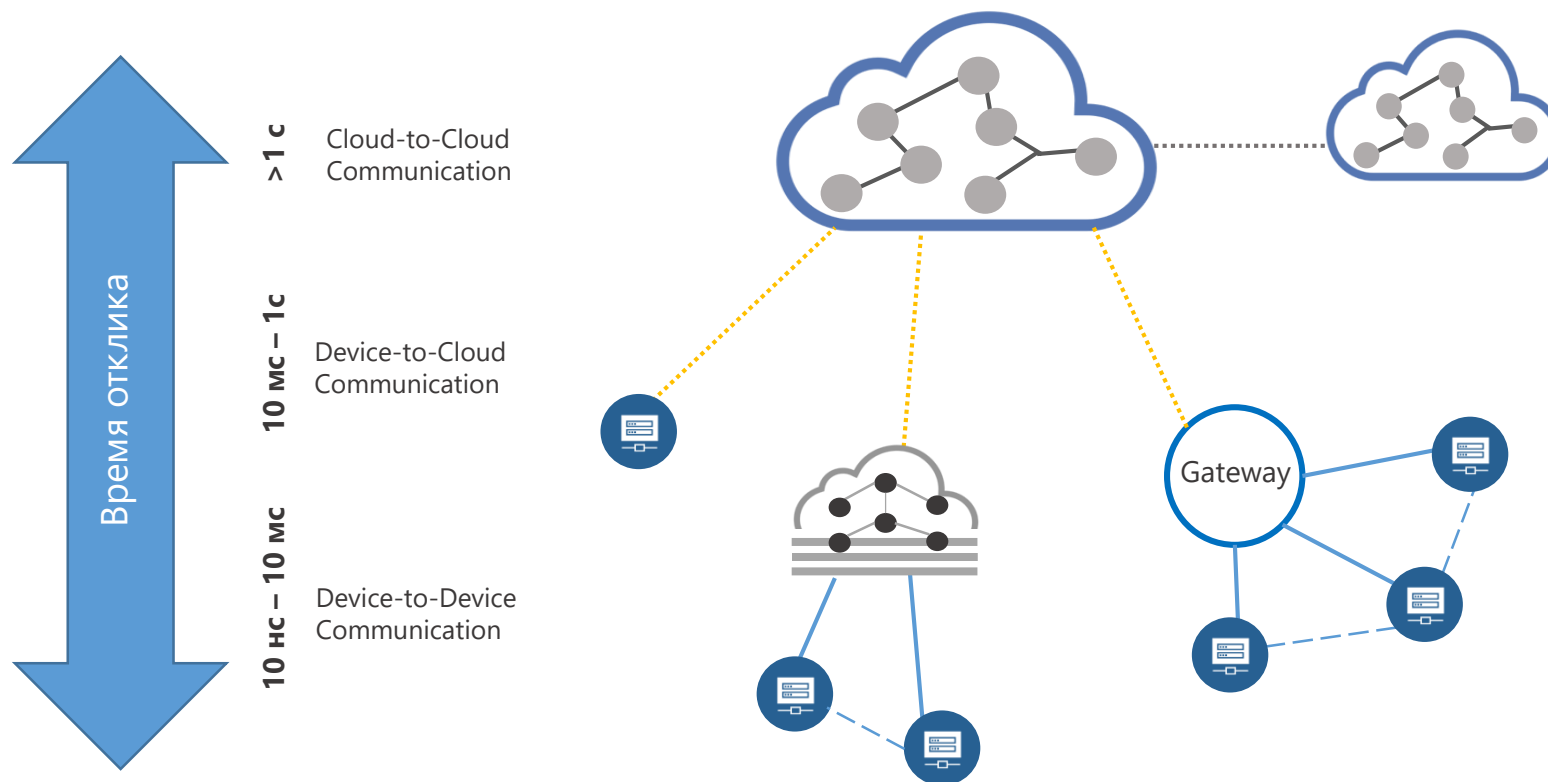


IIoT

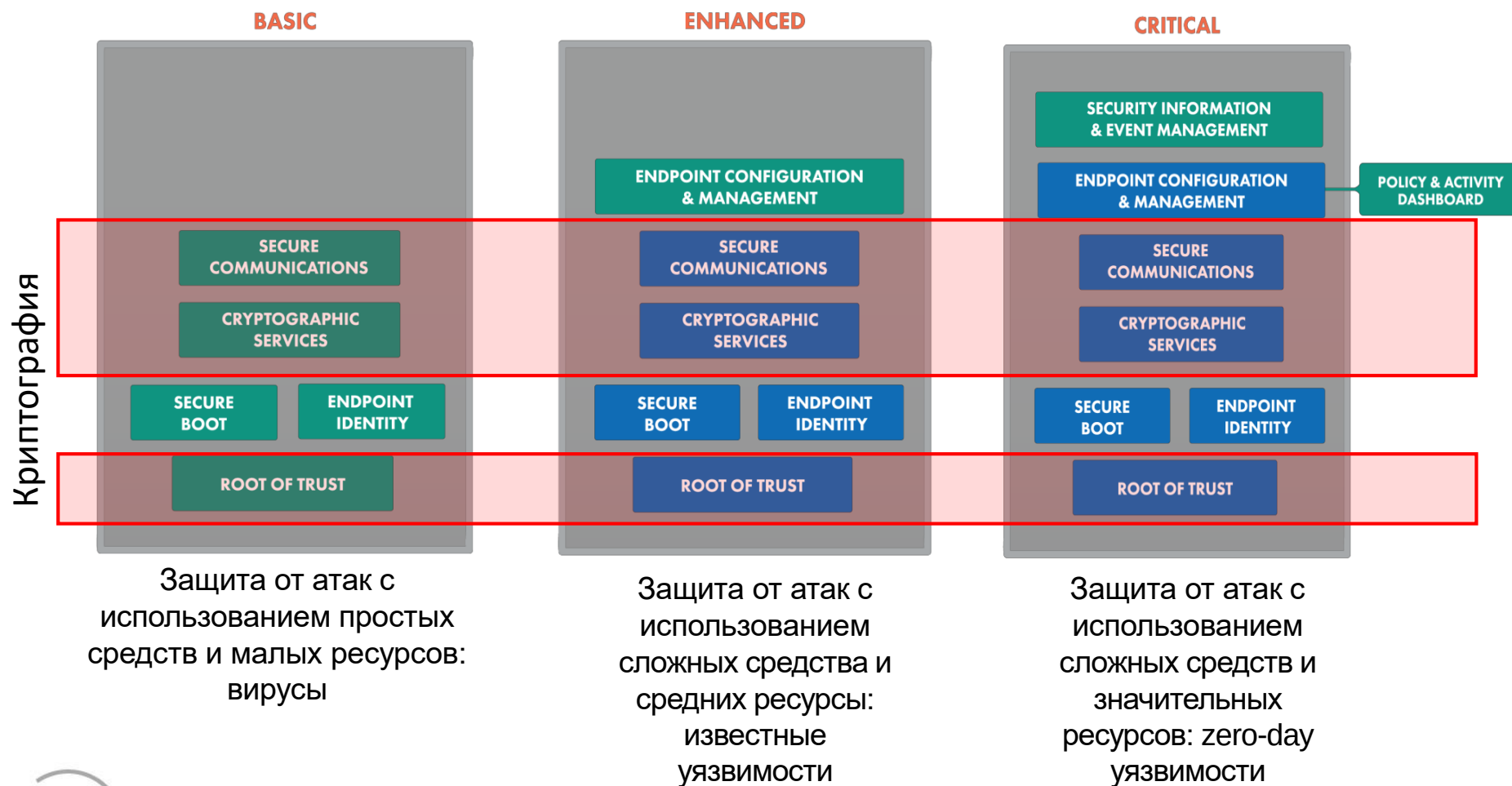
Индустрия 4.0 :: коммуникации



Латентность в сетях IIoT



Международная практика :: 3 уровня безопасности



Основные аспекты защиты M2M/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
- M2M протоколы в большинстве не подразумевают механизмов защиты коммуникаций
- Некоторые беспроводные IIoT протоколы имеют встроенную в защиту коммуникаций на западных криптоалгоритмах
- Аутентичность и целостность важнее конфиденциальности

Проблемы разработки элементов IIoT



- Разработчики систем IoT считают безопасность проблемой №1
- Разработчики не разбираются в безопасности
- Разработчики всегда оставляют безопасность «на потом»
- Разработчикам необходим простой инструмент для обеспечения безопасности

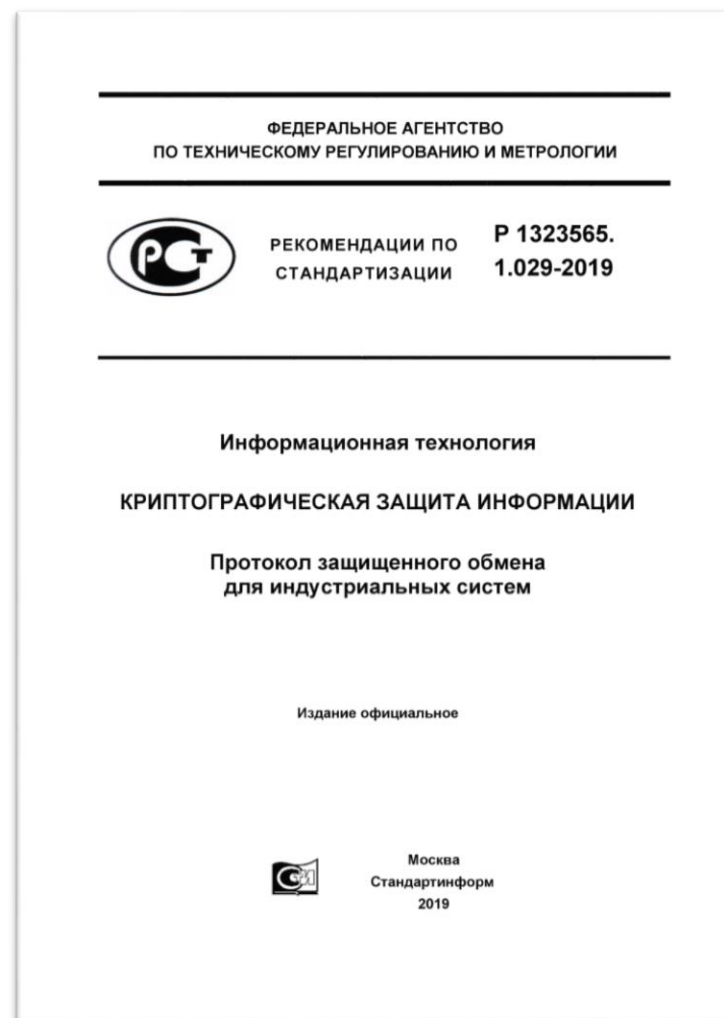
Работы в области стандартизации

CRISP

(Cryptographic Industrial Security Protocol)

протокол защищенной передачи данных
для M2M/IIoT- коммуникаций

- Обеспечение целостности
- Обеспечение конфиденциальности (опционально)
- Защита от навязывания повторных сообщений
- Защита данных – блочный шифр, имитовставка по ГОСТ
- Поддержка адресных (один-к-одному) сообщений
- Поддержка многоадресных (один ко многим, подписочная модель) сообщений
- Явная и неявная адресация абонентов
- Минимальный оверхед (12 байт + имитовставка)



Решение ViPNet SIES

(Security for Industrial & Embedded Solutions)



- СКЗИ классов КС1/КС3, не требуют проведения встраивания
- Возможность использования криптографии на разных по вычислительной мощности устройствах
- Нет зависимости от ОС и архитектуры устройств

- Поддержка протоколов **CRISP**, CMS
- Криптография по ГОСТ Р 34.12-2015, Р 34.11-2012, Р 34.10-2012
- Комплект разработчика ViPNet SIES Core SDK для Windows/Linux
- ViPNet SIES Core в вариантах аппаратного модуля или ПО для встраивания в PLC/RTU

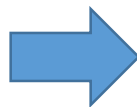


Планы развития ViPNet SIES как криптографической инфраструктуры Платформы Доверия

- Переход на отечественную элементную базу для ПАК ViPNet SIES Core (процессор Элвис IoT-01) – 2021-2022 гг.
- Реализация ViPNet SIES Core в составе ядра доверия на процессорах Элвис – 2021 г.
- Новая версия протокола CRISP
- Реализация облачной криптографической платформы для IIoT на базе решения ViPNet SIES и облачной платформы УЦ Инфотекс Интернет Траст – 2020 г.



Снижение порога вхождения в индустриальную криптографию для разработчиков средств АСУ до уровня сложности/стоимости конечного устройства!



Решение задачи импортозамещения таких зарубежных платформ как ARM Mbed/Crypto, Mocana и пр.

A photograph of a landscape at sunset or sunrise. In the foreground, several wind turbines are silhouetted against the bright, orange sky. In the background, a series of high-voltage power lines stretch across the horizon. The sun is low on the right side, creating a strong glow and casting long shadows.

Спасибо!