



# Криптография в IoT

## Обзор состояния в контексте противостояния

Алексей Лукацкий

Бизнес-консультант по безопасности

23.03.16

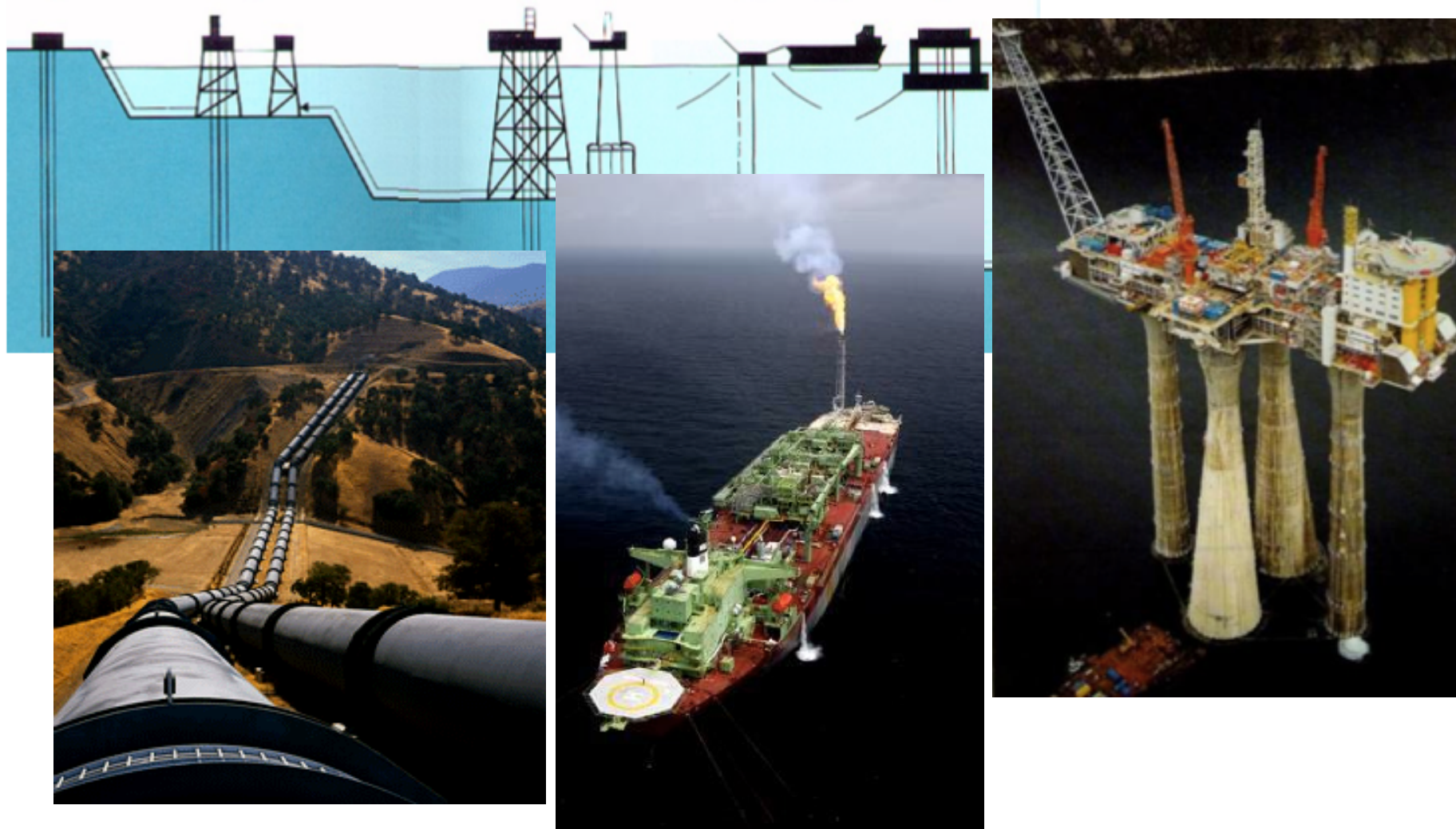
# Интернет вещей бывает не только таким



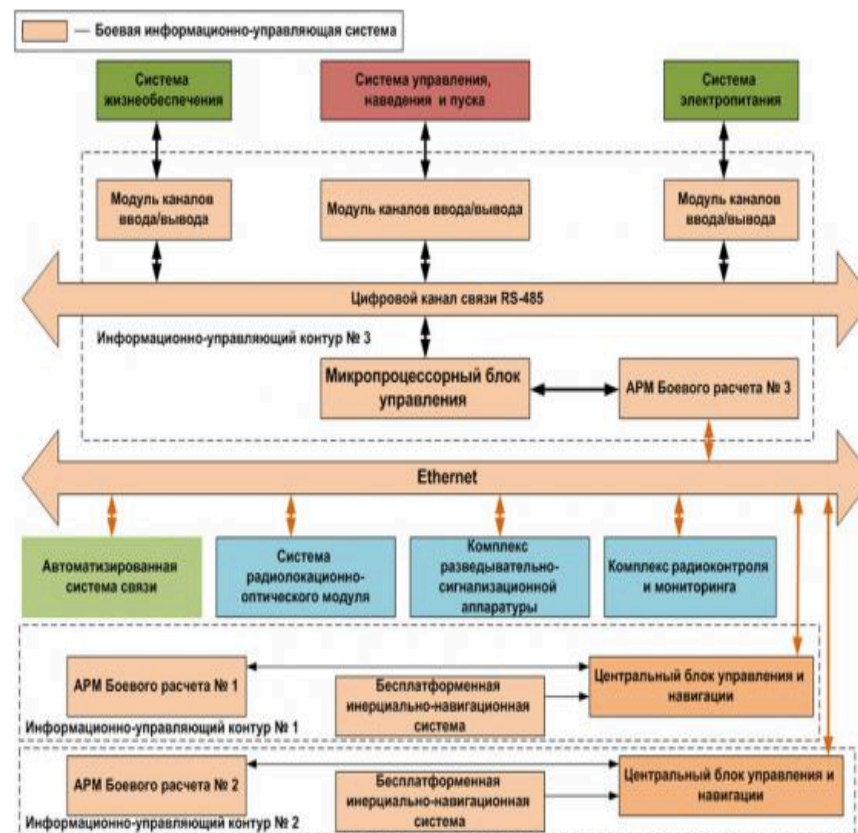
# Пищевой Интернет вещей



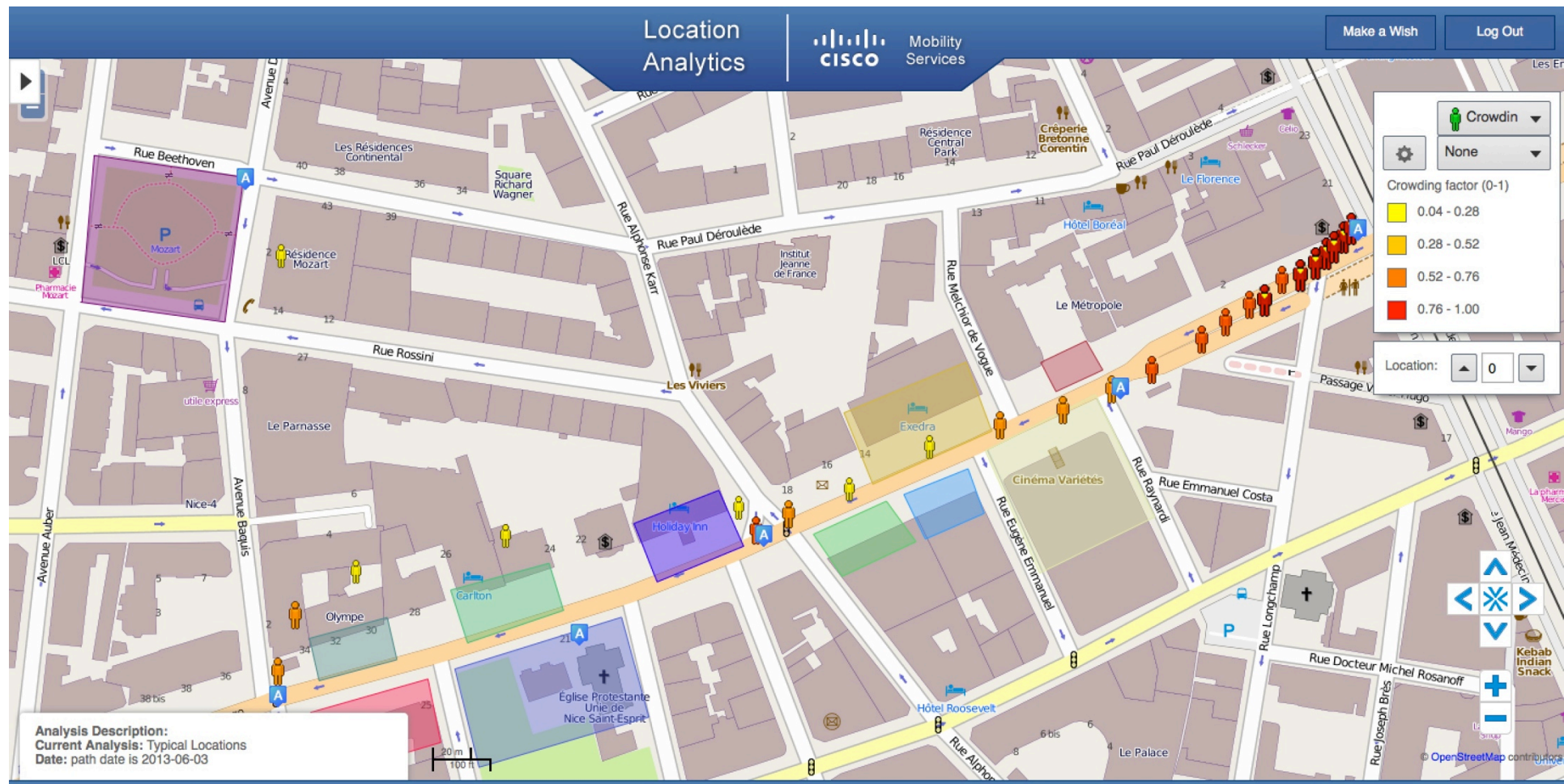
# Промышленный Интернет вещей



# Военный Интернет вещей



# Муниципальный Интернет вещей



# Детский Интернет вещей



# Сантехнический Интернет вещей

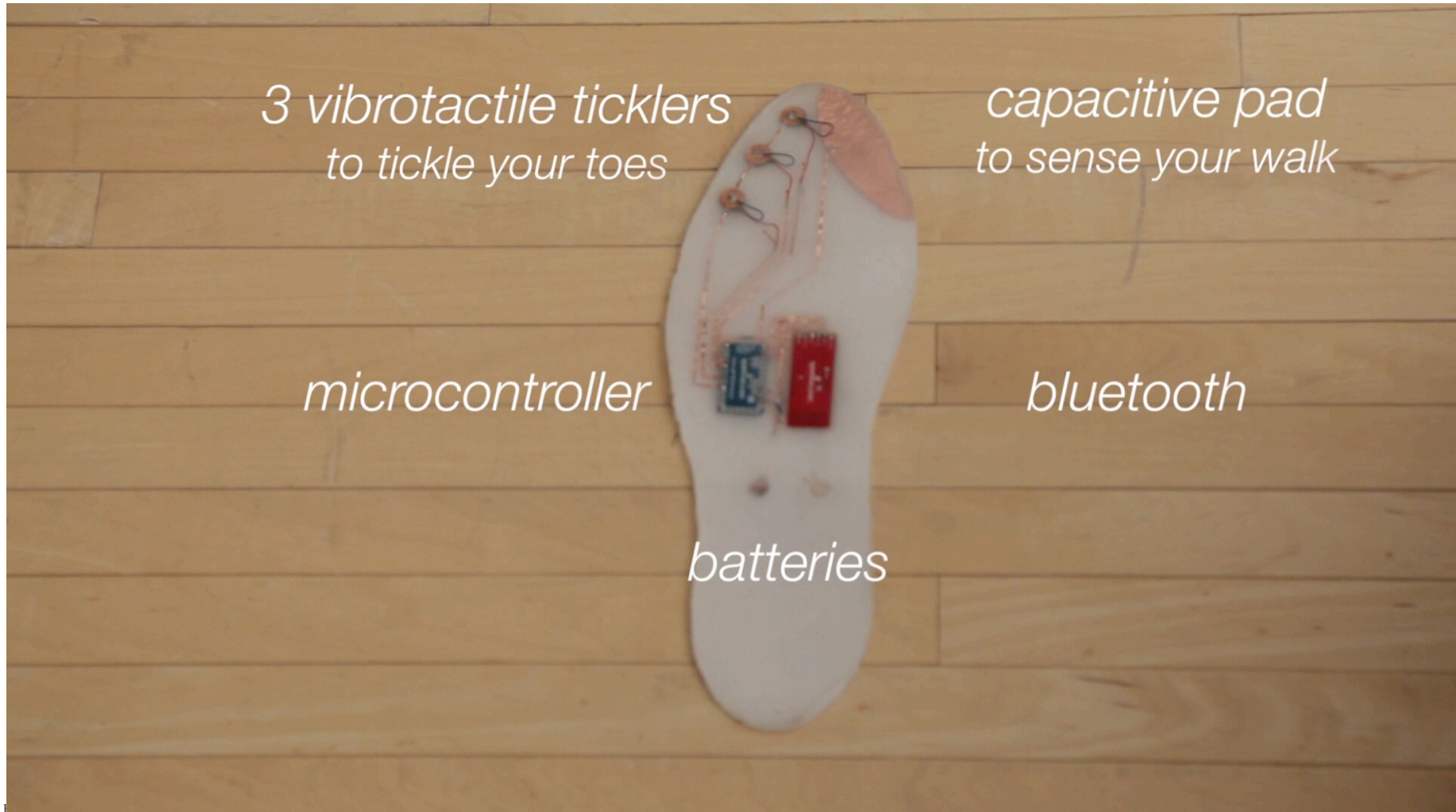




# Медицинский Интернет вещей



# Обувной Интернет вещей



# Сексуальный Интернет вещей



Нужна ли криптография в IoT?



# Какие проблемы ИБ есть в IoT сегодня?

- Аутентификация датчиков/сенсоров/контроллеров/шлюзов
- Аутентификация запросов для доступа к датчикам/сенсорам/контроллерам/шлюзам
- и их конфигурации
- Конфиденциальность передаваемых данных
- Обеспечение целостности данных и команд
- Анонимность и приватность (в контексте консьюмерского IoT)

**Криптография — это решение?**

# Чем определяется применение криптографии?

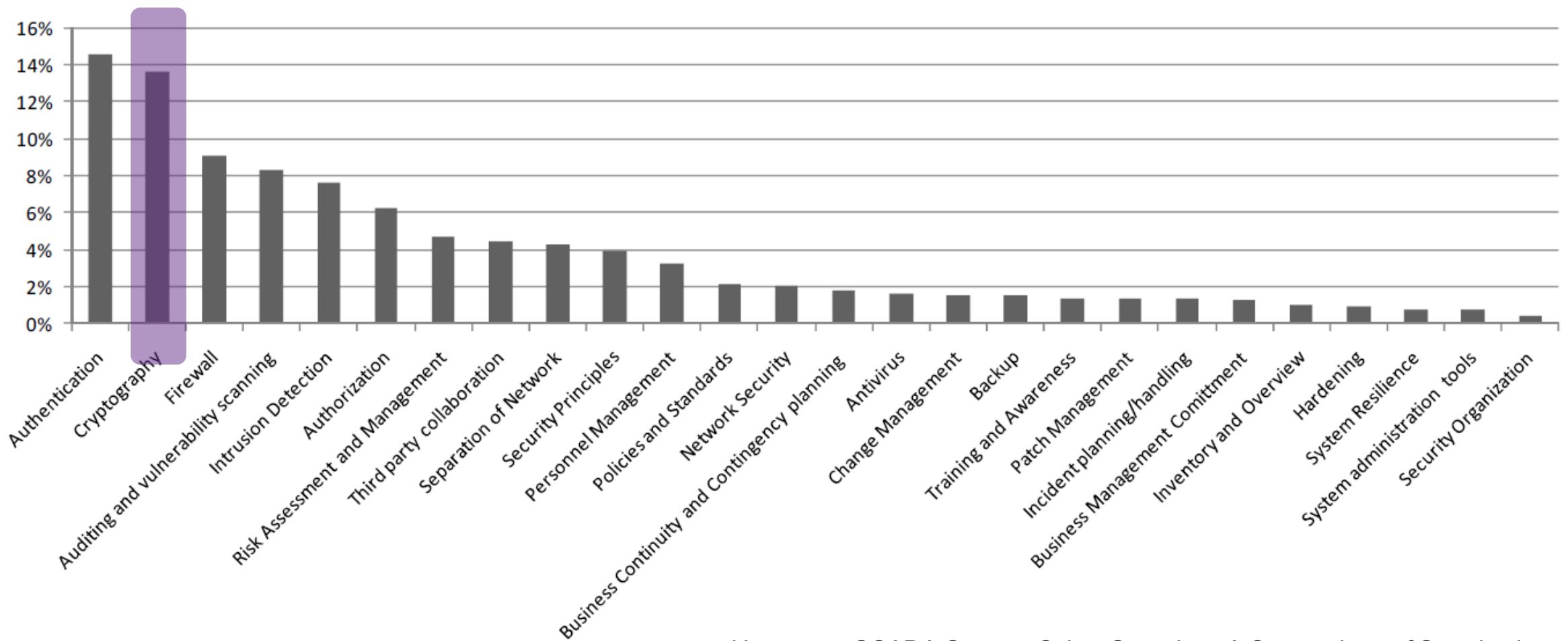
## Необходимость

- Критичность информации для бизнеса, государства и(или) гражданина
- Критичность информации для управления IoT

## Требование

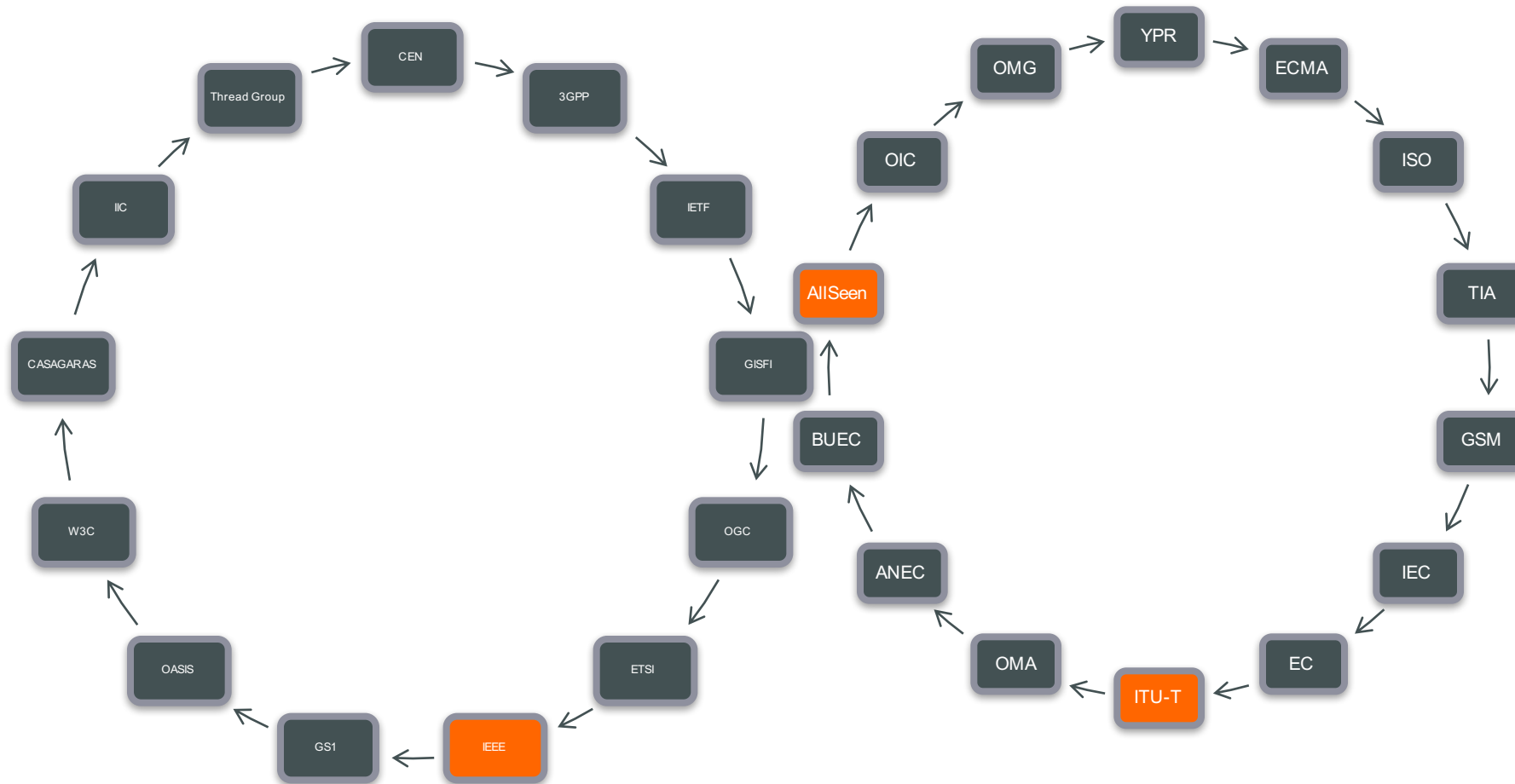
- Корпоративный стандарт
- Отраслевые требования
- Приказ регулятора
- Федеральное законодательство

# Что говорят международные стандарты по ICS?



Источник: SCADA System Cyber Security – A Comparison of Standards

# Множество участников в стандартизации консьюмерского IoT



А еще есть Apple HomeKit и HealthKit!



# Фрагментированные усилия по стандартизации ☹️



# Множество проектов по стандартизации IoT

- Joint Coordination Activity on Internet of Things (JCA-IoT) при ITU-T

Создана в феврале 2011-го года

Преемница JCA-NID (с 2006 года)

- Опубликован консолидированный отчет почти по всем мировым инициативам по стандартизации Интернета вещей

122 (!) страницы

250+ (!) стандартов, рекомендаций и их проектов, касающихся Интернета вещей

Всего 5 (!) относится к защите информации

<http://www.itu.int/en/ITU-T/jca/iot/Pages/default.aspx>

INTERNATIONAL TELECOMMUNICATION UNION  
TELECOMMUNICATION  
STANDARDIZATION SECTOR  
STUDY PERIOD 2013-2016

JOINT COORDINATION ACTIVITY  
ON INTERNET OF THINGS  
**JCA-IoT-D-2 Rev.9**  
English only  
Original: English  
Geneva, 19 November 2014

**Deliverable**  
Source: Editor of IoT Standards Roadmap  
Title: IoT Standards Roadmap

This document represents the second deliverable of JCA-IoT. It was updated by the roadmap editor after the 11th JCA-IoT meeting (Geneva, 19 November 2014), as agreed by the meeting.

This document contains a collection of Standards/ITU-T Recommendations that fit into the scope of JCA-IoT. It includes Standards/ITU-T Recommendations related to Internet of Things (IoT), network aspects of identification systems, including RFID (NID) and ubiquitous sensor networks (USN).

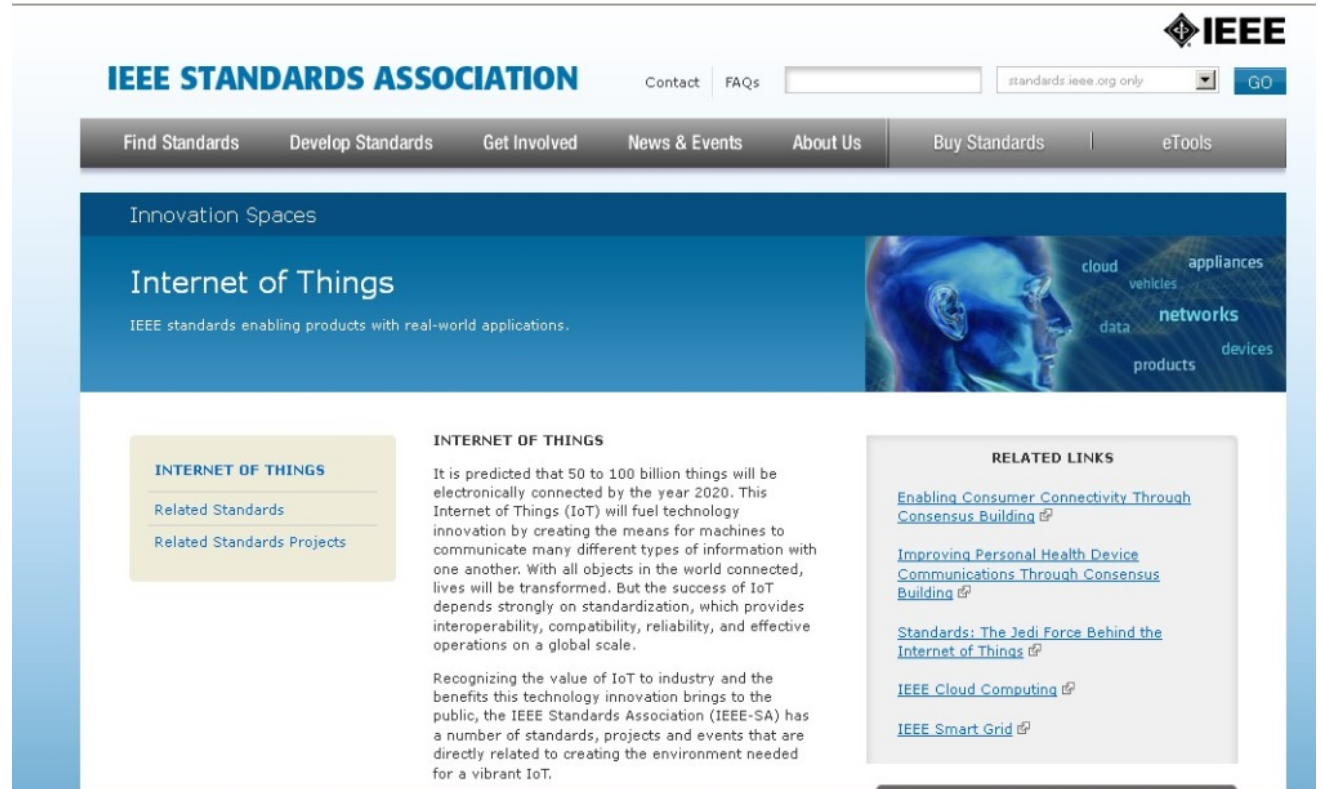
JCA-IoT participants are invited to review it and provide updated information to the editor of this document, Mr Jun Seob Lee ([juns@etri.re.kr](mailto:juns@etri.re.kr)) or to the JCA-IoT secretariat ([tblcaiot@itu.int](mailto:tblcaiot@itu.int)).

Contact: Jun Seob LEE Tel: +82 42 860 3859  
ETRI Fax: +82 42 861 5404  
Korea (Republic of) Email: [juns@etri.re.kr](mailto:juns@etri.re.kr)

Attention: This is not a publication made available to the public, but an Internal ITU-T Document intended only for use by the Member States of ITU, by ITU-T Sector Members and Associates, and their respective staff and collaborators in their ITU related work. It shall not be made available to, and used by, any other persons or entities without the prior written consent of ITU-T.

# Кто все-таки задает тон в стандартизации – ITU или IEEE?

- IEEE P2413 – Standard for an Architectural Framework for the Internet of Things
- Опирается на 140 существующих IEEE стандартов, имеющих отношение к IoT
- Ориентирован на различные вертикали IoT (транспорт, медицина и т.п.)
- Включает также и раздел по безопасности (security, safety, privacy)
- Будет стремиться взаимодействовать с другими органами по стандартизации



The screenshot displays the IEEE Standards Association website. At the top, the IEEE logo is visible on the right, and the text "IEEE STANDARDS ASSOCIATION" is centered. Below this, there are navigation links: "Find Standards", "Develop Standards", "Get Involved", "News & Events", "About Us", "Buy Standards", and "eTools". A search bar is also present with the text "standards.ieee.org only" and a "GO" button. The main content area features a blue header with the text "Innovation Spaces" and "Internet of Things". Below this, there is a sub-header "IEEE standards enabling products with real-world applications." and a graphic of a human head profile with various IoT-related terms like "cloud", "vehicles", "appliances", "data", "networks", "products", and "devices" floating around it. The main content area is divided into three columns: "INTERNET OF THINGS" with links for "Related Standards" and "Related Standards Projects"; "INTERNET OF THINGS" with a paragraph of text and a sub-section "Recognizing the value of IoT to industry and the benefits this technology innovation brings to the public, the IEEE Standards Association (IEEE-SA) has a number of standards, projects and events that are directly related to creating the environment needed for a vibrant IoT."; and "RELATED LINKS" with several hyperlinks such as "Enabling Consumer Connectivity Through Consensus Building", "Improving Personal Health Device Communications Through Consensus Building", "Standards: The Jedi Force Behind the Internet of Things", "IEEE Cloud Computing", and "IEEE Smart Grid".

# Пока лучше не становится...

## КАК МНОЖАТСЯ СТАНДАРТЫ:

(СМ.: ЗАРЯДНЫЕ УСТРОЙСТВА, КОДИРОВКИ, МГНОВЕННЫЕ СООБЩЕНИЯ И Т.Д.)



# Безопасность IoT – мы только в начале пути

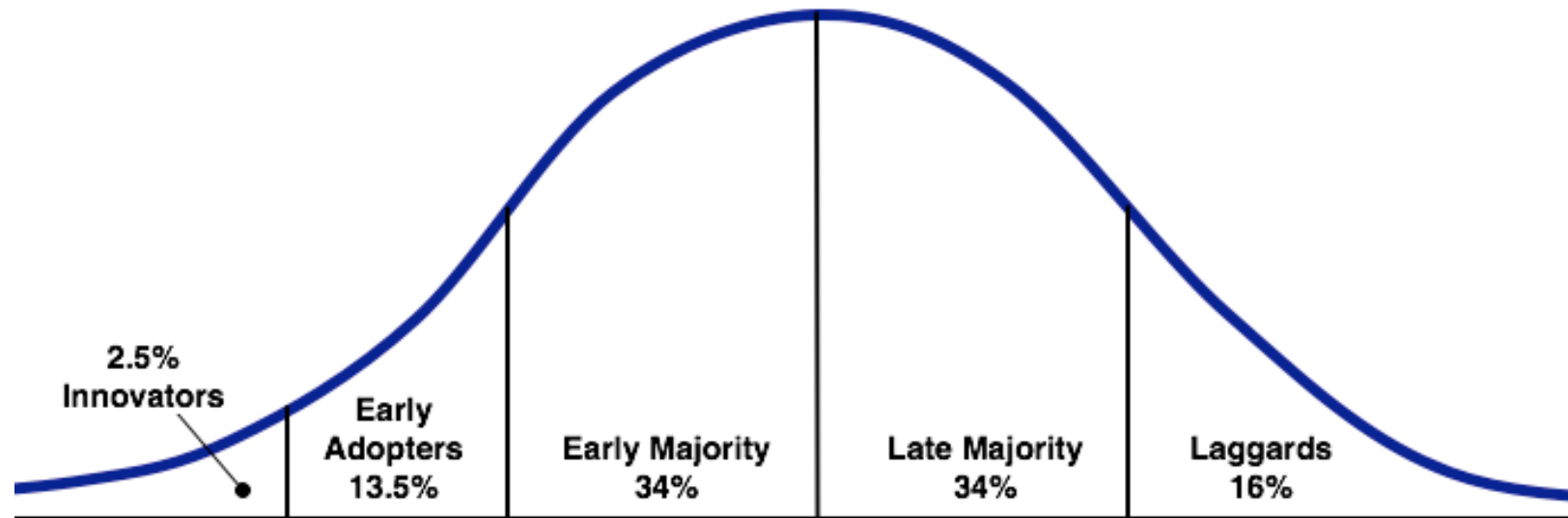
- Консьюмерский Интернет вещей сегодня практически никак не защищен

Отсутствие серьезного ущерба

Отсутствие стандартов не только защиты, но и взаимодействия

Безопасность может быть реализована только на уровне производителя, который пока не понимает (не заинтересован) в решении данного вопроса

Со временем ситуация должна измениться



Source: Everett Rogers, Diffusion of Innovations model

Где в IoT нужна криптография?



# 4 основных элемента IoT

Система мониторинга  
и управления



Консолидированная  
информация о процессе и  
управление процессом

\*\*\*

RTU / PLC / шлюз



Аккумулируют данных от  
большого количества датчиков  
и получают команды

\*\*

Коммуникации



Различные типы  
промышленных и  
персональных сетей, а также  
соединение с внешним миром

\*\*

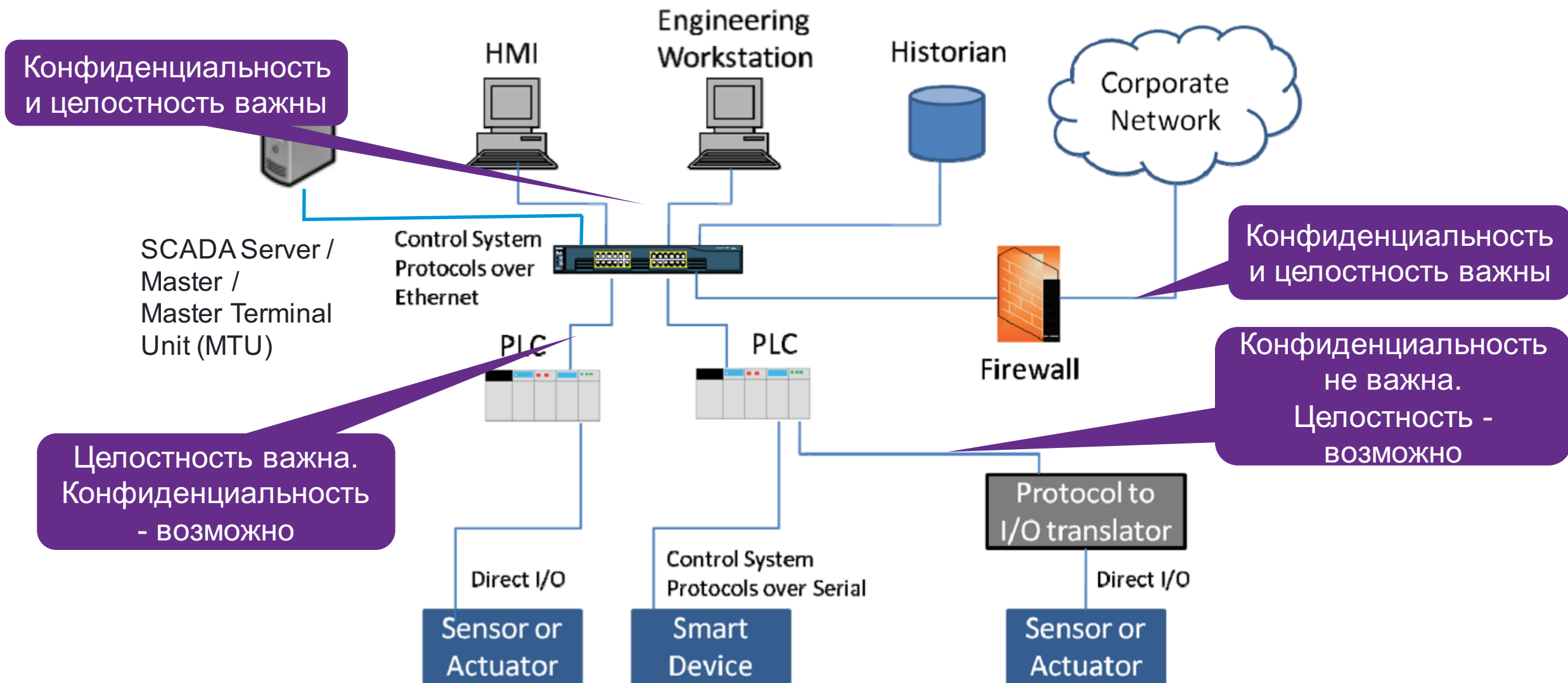
«Полевые» устройства  
(сенсоры/датчики)



Аналоговые и  
неинтеллектуальные, а также  
«умные» устройства

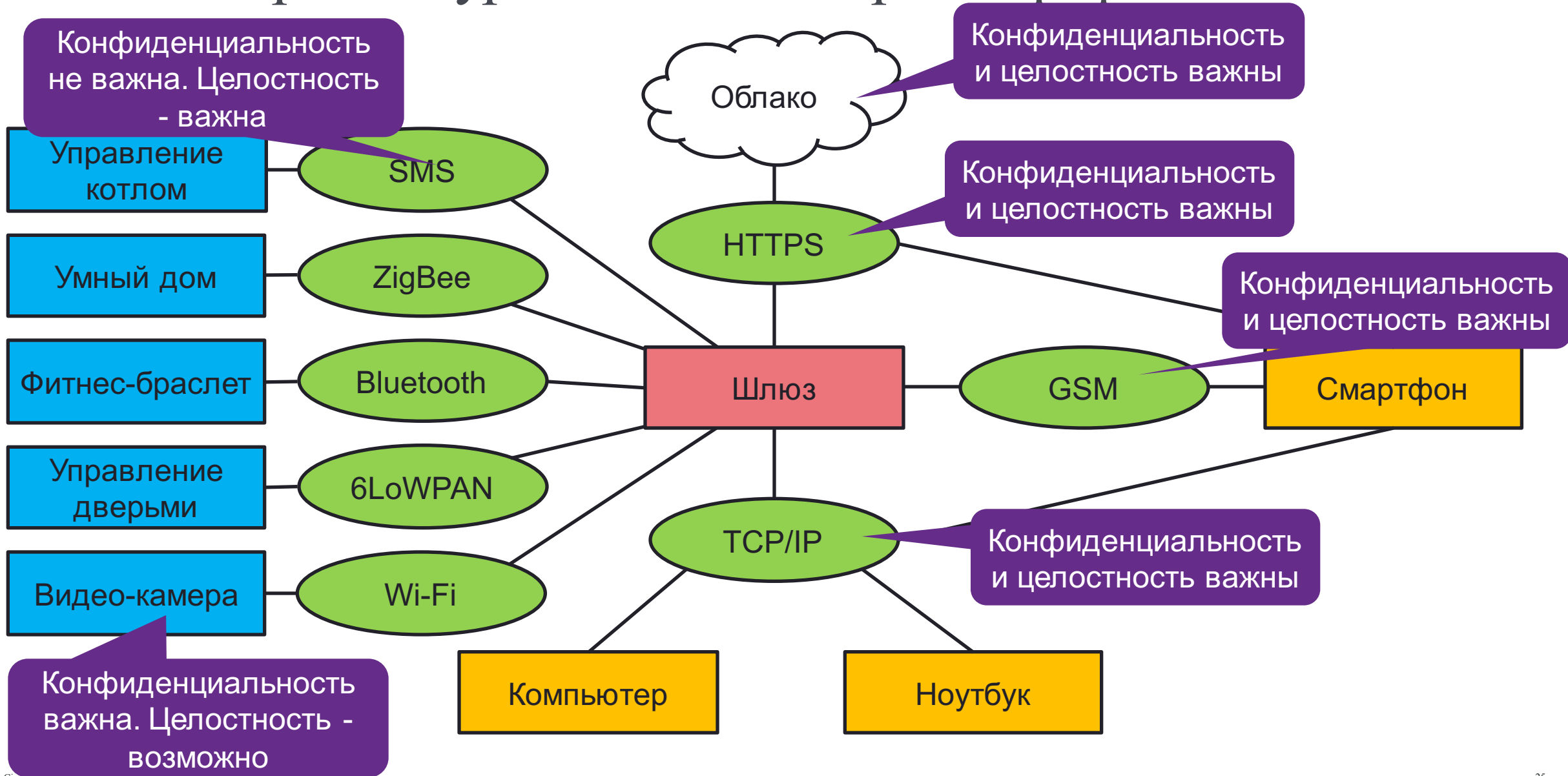
\*

# Типичная архитектура АСУ ТП и место криптографии





# Типичная архитектура IoT и место криптографии



# А что говорят ФСТЭК и ФСБ?

- Федеральное законодательство пока не требует обеспечения конфиденциальности данных в IoT

## АСУ ТП от ФСТЭК

- Конфиденциальность при необходимости, определяемой оператором/заказчиком АСУ ТП
- СКЗИ (если необходимы) могут быть любыми

## КСИИ от ФСТЭК

- Требования к защите коммуникаций (для КСИИ II типа – для управления КВО)
- Применение только сертифицированных СКЗИ

## КИИ от ФСБ

- Требований пока не установлено

## IoT от...

- Регуляторы вообще не замечают

Почему корпоративная криптография не подходит?



# Особенности IoT

- От недоверенной среды до контролируемой зоны
- От мобильности до стационарности
- Низкое энергопотребление
- Автономность работы
- Однонаправленное взаимодействие
- «Отсутствие» пользователя

# Не любая криптография и не каждому процессу

- Контролирующие процессы (включен/выключен, открыто/закрыто, высокая/низкая опасность, начал тренировку/закончил, принять лекарство...)

Конфиденциальность **может быть** актуальной, но не с помощью «тяжелого» ГОСТ 28147-89

Возможно применение облегченной (легковесной) криптографии (в России принятые стандарты легковесной криптографии отсутствуют)

- Управляющие процессы (перекрыть вентиль, включить мотор, принять лекарство, включить дефибриллятор...)

Конфиденциальность вторична

Целостность на первом месте

- Криптостойкость для IoT-процессов может быть гораздо ниже, чем для долгосрочного хранения данных в офисной сети или для защиты гостайны



# Почему не любая криптография подходит?

- Передача данных в IoT оценивается не только и не столько скоростью передачи, которая для СКЗИ обычно измеряется на больших пакетах (400+ байт)
- В IoT гораздо большее значение имеет размер защищаемой информации и требование по задержкам

Зачастую защитить надо всего несколько бит информации

В отдельных стандартах электроэнергетики требуется обеспечивать передачу данных с задержкой не более  $10^{-6}$

Размер ключа шифрования для ГОСТ 28147-89 составляет 256 бит, что в десятки раз превосходит размер шифруемого блока

Многие СКЗИ добавляют к каждому шифруемому пакету еще около 80 байт (зависит от СКЗИ)

+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:	ETHERNET – заголовок VIPNet - пакета
+ IP: ID = 0xC0C3; Proto = UDP; Len: 196	IP-заголовок VIPNet – пакета
+ UDP: Src Port: (55777); Dst Port: (55777); Length = 176 (0xB0)	UDP-заголовок VIPNet – пакета (8 байт) Присутствует, если инкапсуляция производится в UDP-формат.
Data: Number of data bytes remaining = 350 (0x015E)	Зашифрованное тело исходного пакета
IPLIR: IPLIR (<IL41>, UDP encapsulation)	Служебный заголовок VIPNet – пакета
Open info = Open info(37 bytes)	Открытая часть VIPNet – пакета (37 байт)
Dst ID = 65836 (0x1012C)	Идентификатор получателя (4 байта)
Additional Flags = 7 (0x7)	Служебные флаги (1 байт)
Key number = 4294967295	Номер ключа, на котором зашифрован пакет (4 байта)
Encr. method: GOST	Метод шифрования (1 байт)
Key size = 32 (0x20)	Размер ключа(1 байт)
Salt = 0x337B491AAEF1F488	Синхропосылка (8 байт)
Imito = 0x5AFD4A6FD12FE7C8	Имитозащитная вставка (8 байт)
Src ID = 65951 (0x1019F)	Идентификатор источника (4 байта)
Broadcast: No	Тип пакета и другие флаги (1 байт)
Version = 11 (0xB)	Версия инкапсуляции (1 байт)
IL41	Сигнатура VIPNet-пакета (4 байта) – используется для предварительного опознавания VIPNet пакета

# Риторические вопросы

- Может ли быть применен ГОСТ 28147-89 для шифрования и электронной подписи данных на цифровой подстанции, соединенной с ЦДУ каналов в 56 Кбит/сек?
- Может ли какая-либо СКЗИ обрабатывать короткие пакеты от нескольких десятков тысяч одновременно передающих информацию устройств?  
А как управлять криптографическими ключами для такого количества устройств?
- Может ли корпоративный VPN-шлюз работать на улице в температурном диапазоне от -40 до +60?

# И наконец еще одна проблема

## Samsung Galaxy S5

- 4-ядерный процессор
- 2,5 ГГц
- 2 Гб RAM
- 128 Гб SD Card
- Энергия батареи 30 кДж
- Ежедневная зарядка

## Asset Tracking Tag

- 16-тибитный процессор
- 6-12 МГц
- 512 байт (!) RAM
- 16 Кб flash-памяти
- Длительность работы без перезарядки – десятки тысяч часов

За чей счет будут реализовываться миллионы инструкций криптографической поддержки?



The image shows the dark silhouettes of an offshore oil rig against a bright, golden sunset sky. The rig's complex structure, including cranes and platforms, is visible against the horizon. The water in the foreground is dark and textured. The overall scene is industrial and atmospheric.

Какая криптография нужна в IoT?

# Варианты реализации криптографии

## Часть протокола взаимодействия

- ZigBee
- Secure DNP3
- DNPsec
- Secure Modbus
- OPC
- 6LoWPAN

Повлиять нельзя

## Встроенная в оборудование

- Неприменима для «старого» оборудования
- Не все устройства из-за нехватки системных ресурсов и требований к автономной работе поддерживают «лишний» функционал
- Некоторые производители контроллеров стали оснащать свои решения встроенной криптографией

Повлиять можно только при выборе оборудования

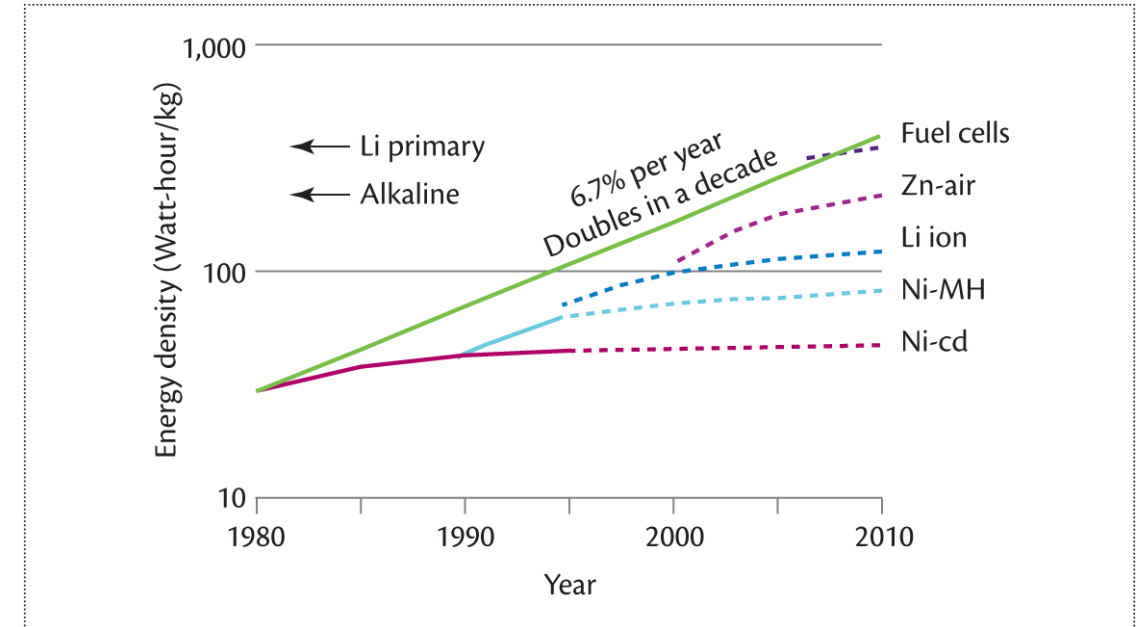
## Наложенная

- Самый популярный вариант
- Подходит для «старых» устройств и зарубежных АСУ ТП, в которых необходимо обеспечить дополнительные гарантии
- Идеальна для удаленного доступа

Максимально управляемая ситуация

# Как решить проблемы с большим энергопотреблением?

- Не реализовывать механизмы защиты вообще
- Рост мощности современных батарей (закон Мура)
- Брать энергию окружающей среды (harvest energy)
- Новая «математика»  
    Может быть клеточные автоматы?
- Использовать «физику» устройств и коммуникаций для обеспечения целостности и конфиденциальности



# Резюме: от чего зависит применение криптографии в IoT?

- Необходимость или законодательные требования
- Местонахождение объекта IoT (доступность для нарушителя)
- Сегмент IoT (передача данных по открытым каналам связи)
- Технологический процесс
- Используемые типы коммуникаций в IoT
- Используемые протоколы IoT
- Число объектов IoT
- Требования по задержкам в IoT
- Физическая среда функционирования СКЗИ
- Необходимость сертификации и отношение регулятора

ID	Constraint/Feature
C1	Resource Constrained RTU
C2	High Resiliency
C3	Low Bandwidth and Low Latency Communications
C4	Long Node Life
C5	Real Time
C6	Structured Network
C7	Phased Delivery
C8	RTUs Physically Insecure
C9	RTU Clocks Initially Unsynchronised
C10	RTU Clocks Synchronised After Initialisation

# Где вы можете узнать больше?



Пишите на [security-request@cisco.com](mailto:security-request@cisco.com)



Быть в курсе всех последних новостей вам помогут:



<http://www.facebook.com/CiscoRu>



<http://twitter.com/CiscoRussia>



<http://www.youtube.com/CiscoRussiaMedia>



<http://www.flickr.com/photos/CiscoRussia>



<http://vkontakte.ru/Cisco>



<http://blogs.cisco.ru/>



<http://habrahabr.ru/company/cisco>



<http://linkedin.com/groups/Cisco-Russia-3798428>



<http://slideshare.net/CiscoRu>



<https://plus.google.com/106603907471961036146/posts>



<http://www.cisco.ru/>



Благодарю  
за внимание

