Интернет вещей

Тенденции и проблемы

Mr. Yakov Dolmatsky
Head of ICS Cyber Security Department
Israel Ministry of Environmental Protection

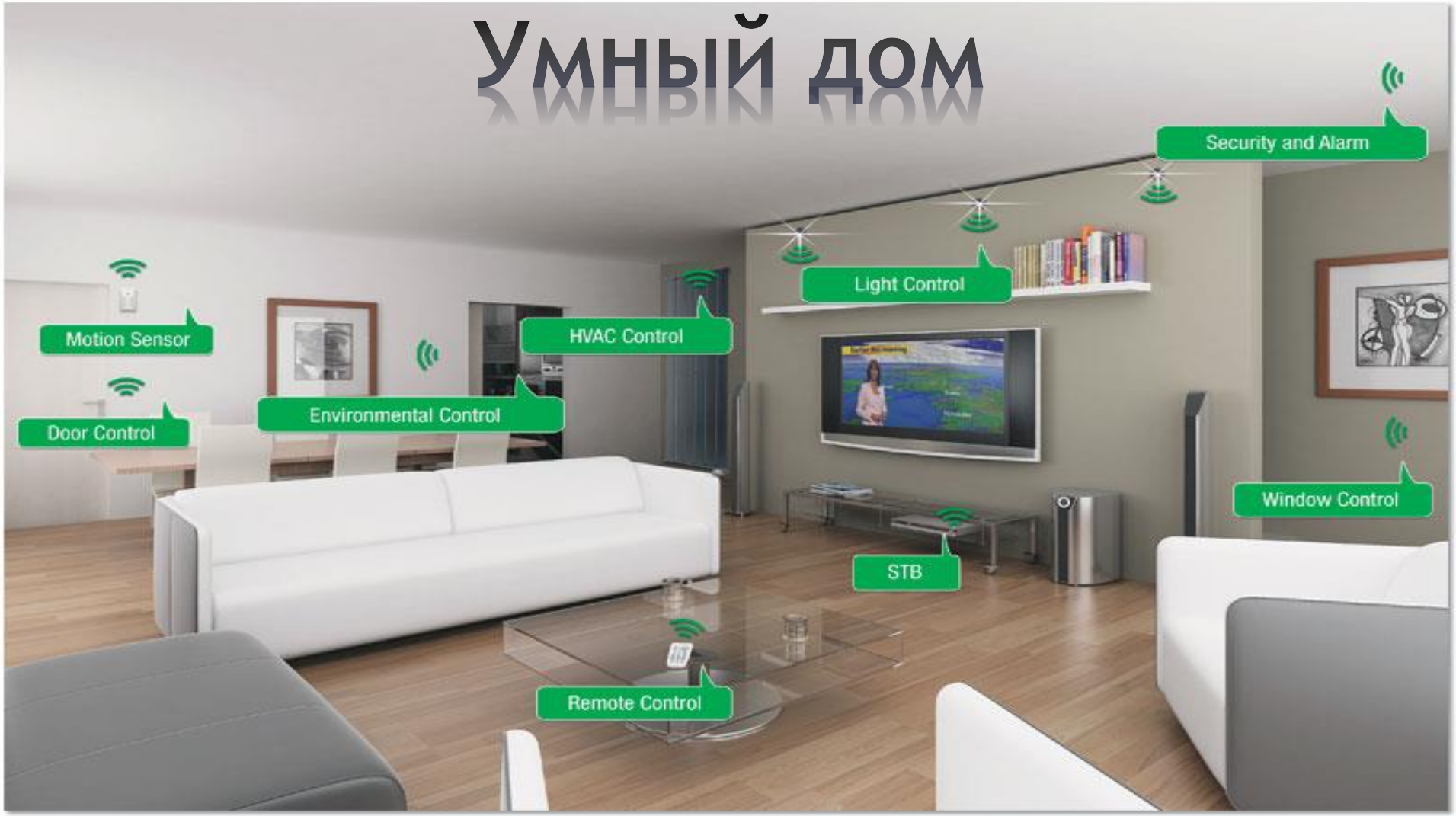
Интернет вещей*

Интернет вещей (ИВ; англ. Internet of Things, IoT) – *
это способы взаимодействия физических объектов, устройств и систем между собой и с окружающим миром с применением различных технологий связи и стандартов соединения.

https://iot.ru/wiki/internet-veshchey

Anything
Any Device
Anyone
Anybody
Any Service
Any Business
Any Path
Any Network
Any Place
Anywhere
Anytime
Any Context
The
INTERNET
of THINGS
is everywhere!

Умный дом


Security and Alarm
Light Control
Motion Sensor
HVAC Control
Door Control
Environmental Control
Window Control
STB
Remote Control

Умная кухня

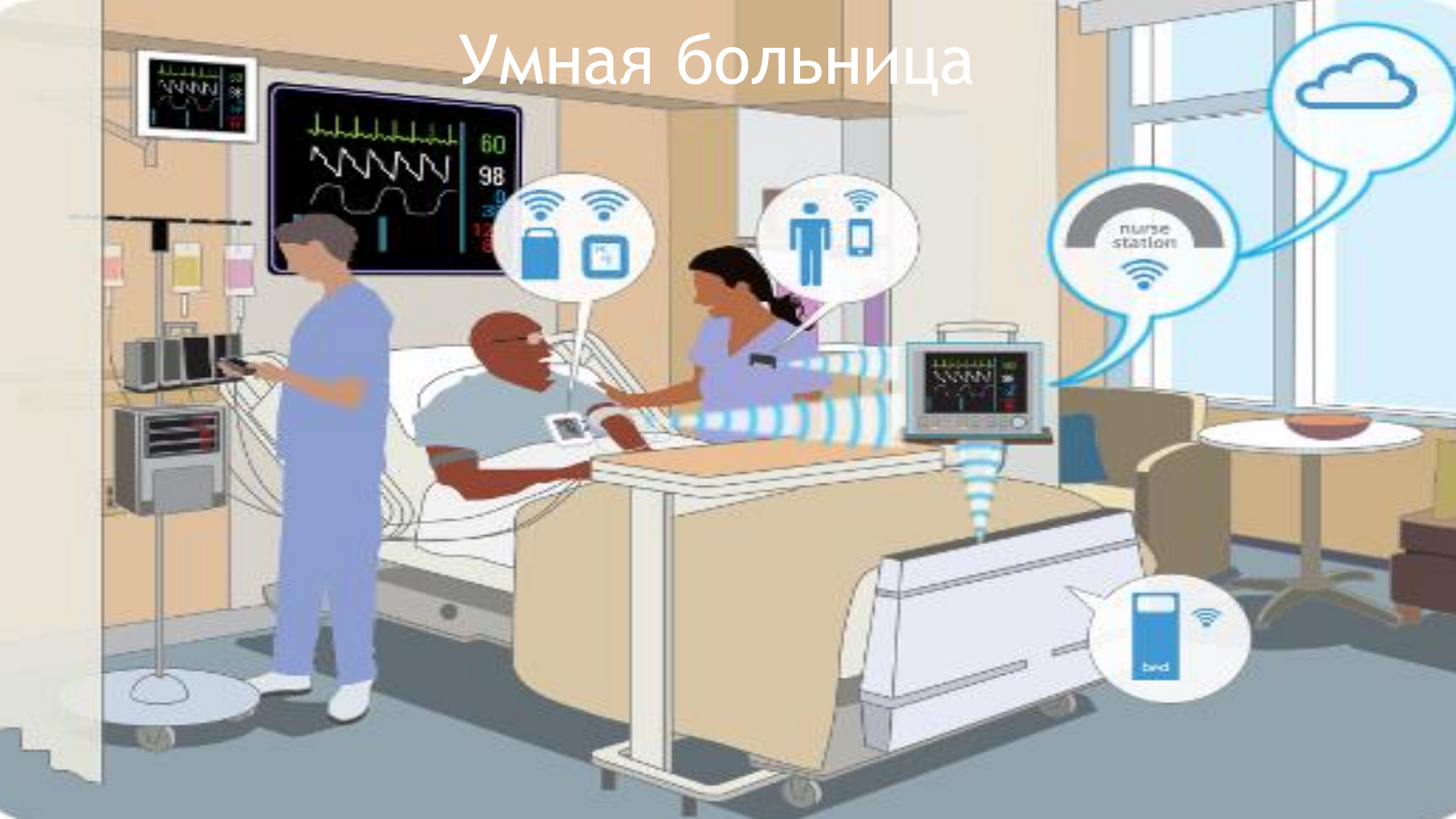
05.06.40
PERSONAL NUTRITION
SUGGESTED MEA
ANALYSIS
FOOD LOG
3:33 PM
24°

Умный санузел

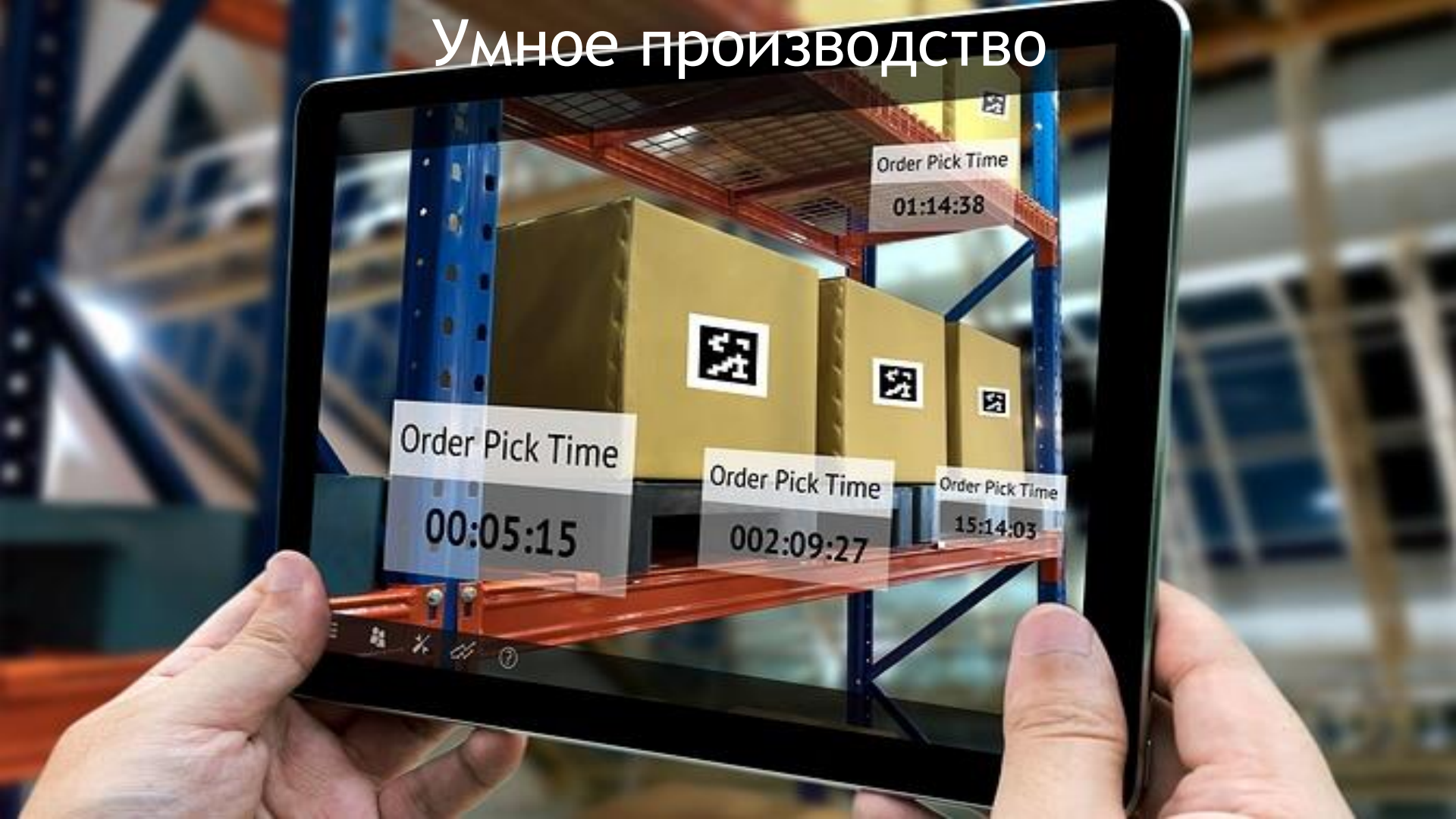
Умная машина

Умный транспорт

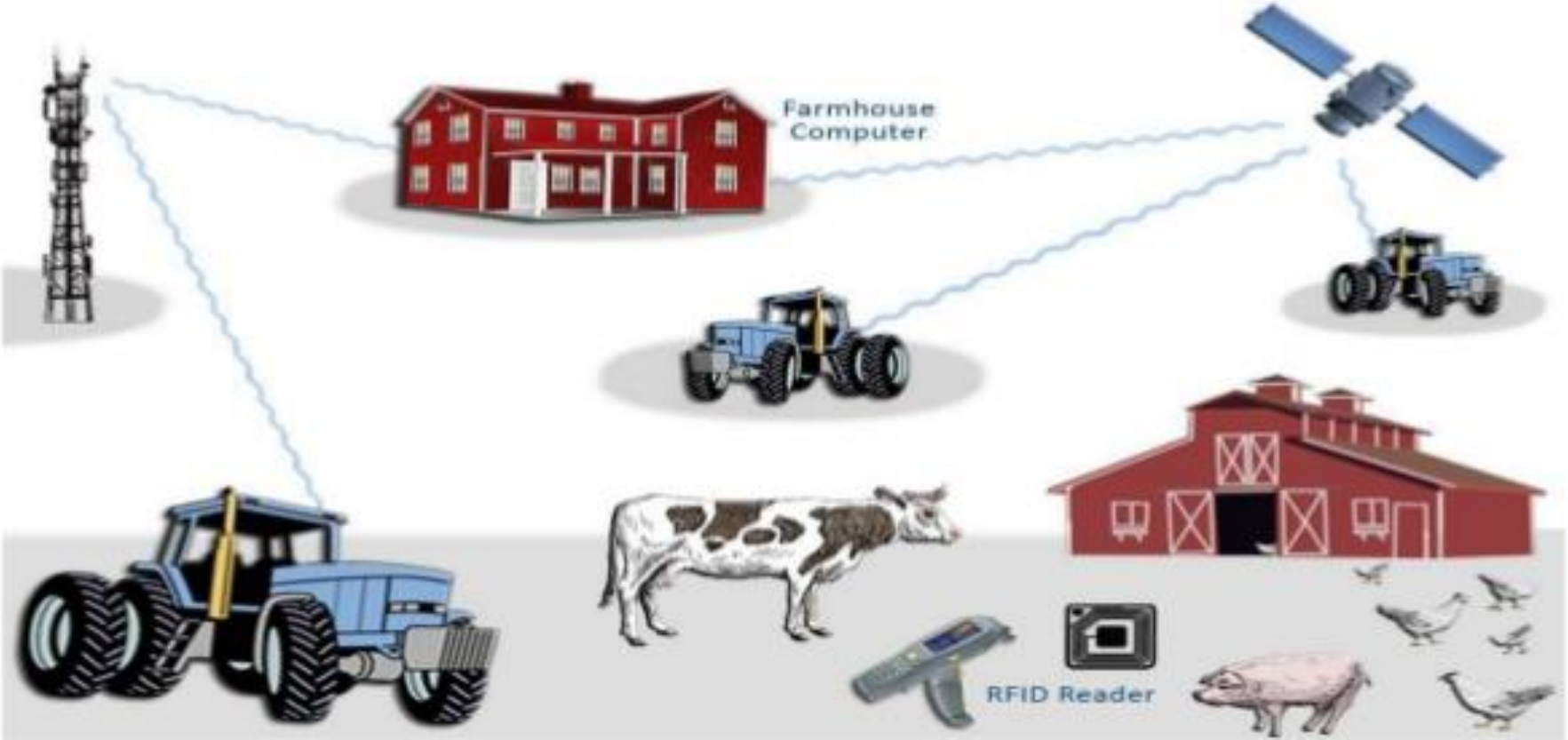
Умная больница



Умное производство

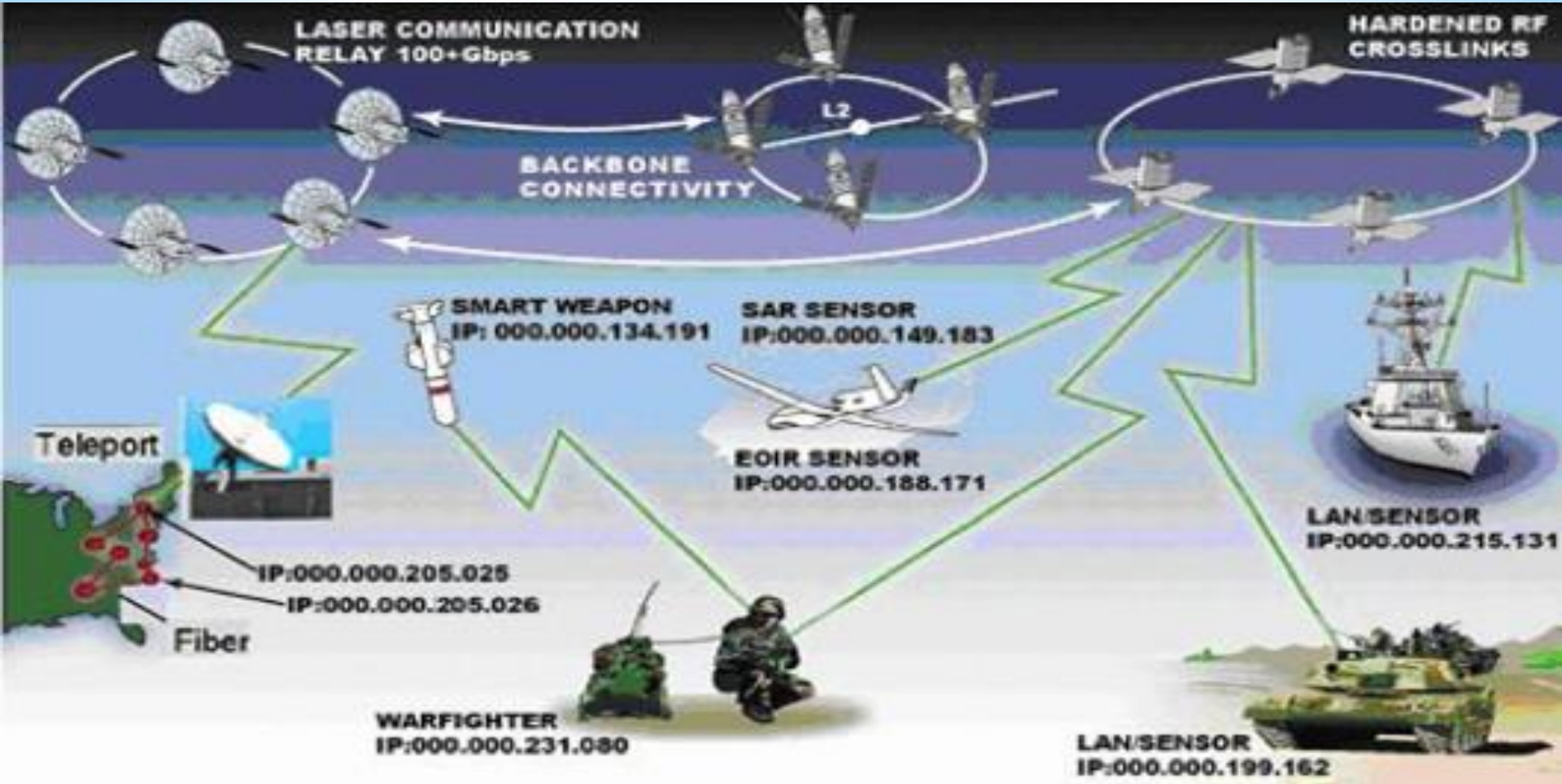


Умная ферма



Умный город

Умная армия

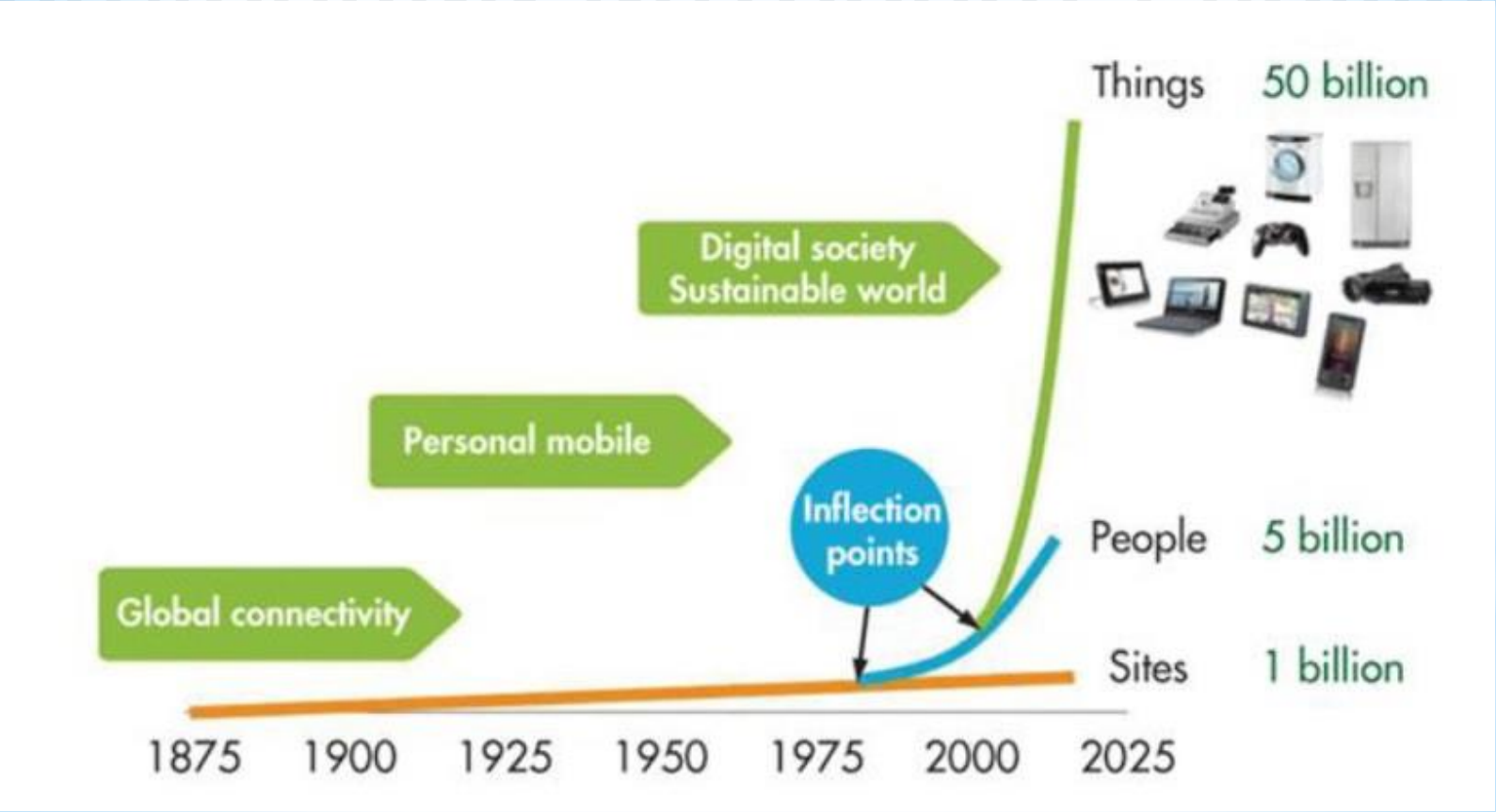

LASER COMMUNICATION
RELAY 100+Gbps
HARDENED RF
CROSSLINKS
L2
BACKBONE
CONNECTIVITY
SMART WEAPON
IP: 000.000.134.191
SAR SENSOR
IP:000.000.149.183
Teleport
EOIR SENSOR
IP:000.000.188.171
LAN/SENSOR
IP:000.000.215.131
IP:000.000.205.025
IP:000.000.205.026
Fiber
WARFIGHTER
IP:000.000.231.080
LAN/SENSOR
IP:000.000.199.162

Умная планета

http://www.beechamresearch.com/article.aspx?id=4

Всё это управляется с помощью

Тенденции интернета вещей



Проблемы и вопросы

Вопрос №1*

В случае аварии с участием автомобиля, управляемого IoT, кто несёт юридическую ответственность?

Необходимо законодательство в мире IoT

Вопрос №2*

IoT – Как защититься от вмешательства в личную жизнь?

Минимизировать сбор личной информации от потребителей

Обеспечить надлежащую защиту всех собранных личных данных с ограничением доступа к собранной личной информации

Обеспечить деидентификацию или анонимизацию данных

http://www.express.co.uk/news/world/602646/baby-monitor-internet-hack-security-Phillips-research-Rapid7-alert

Вопрос №3

Почему интернет вещей может быть опасным?

Мы должны сказать: Нет IoT без SoT!

Различия в решениях безопасности IoT

Практическое использование инструментов IoT:

* потребительский сектор
* муниципальный сектор
* промышленный сектор
* военный сектор

В каждом секторе необходим свой подход к решению вопросов информационной безопасности, основанный на управлении рисками

Безопасность интернета вещей

- Производители не видят существующих рисков при имплементации решений безопасности IoT .
- Отсутствуют регуляторные требования по вопросам безопасности IoT .
- Фрагментированные усилия по стандартизации . Около 30 различных организаций пытаются стандартизировать интернет вещей .
- Стандартные решения информационной безопасности не всегда подходят для интернета вещей. Требуется адаптация или поиск новых решений.

IoT – слабые места

* Стандартные учетные записи от производителя, слабая аутентификация

IoT – слабые места

* Отсутствие поддержки со стороны производителей для устранения уязвимостей
* Трудно или невозможно обновить программное обеспечение и ОС

IoT – слабые места

* Использование текстовых протоколов и ненужных открытых портов

IoT – слабые места

* Используя слабость одного гаджета, хакеру очень легко попасть во всю сеть (использование слабого звеня цепи)

IoT – слабые места

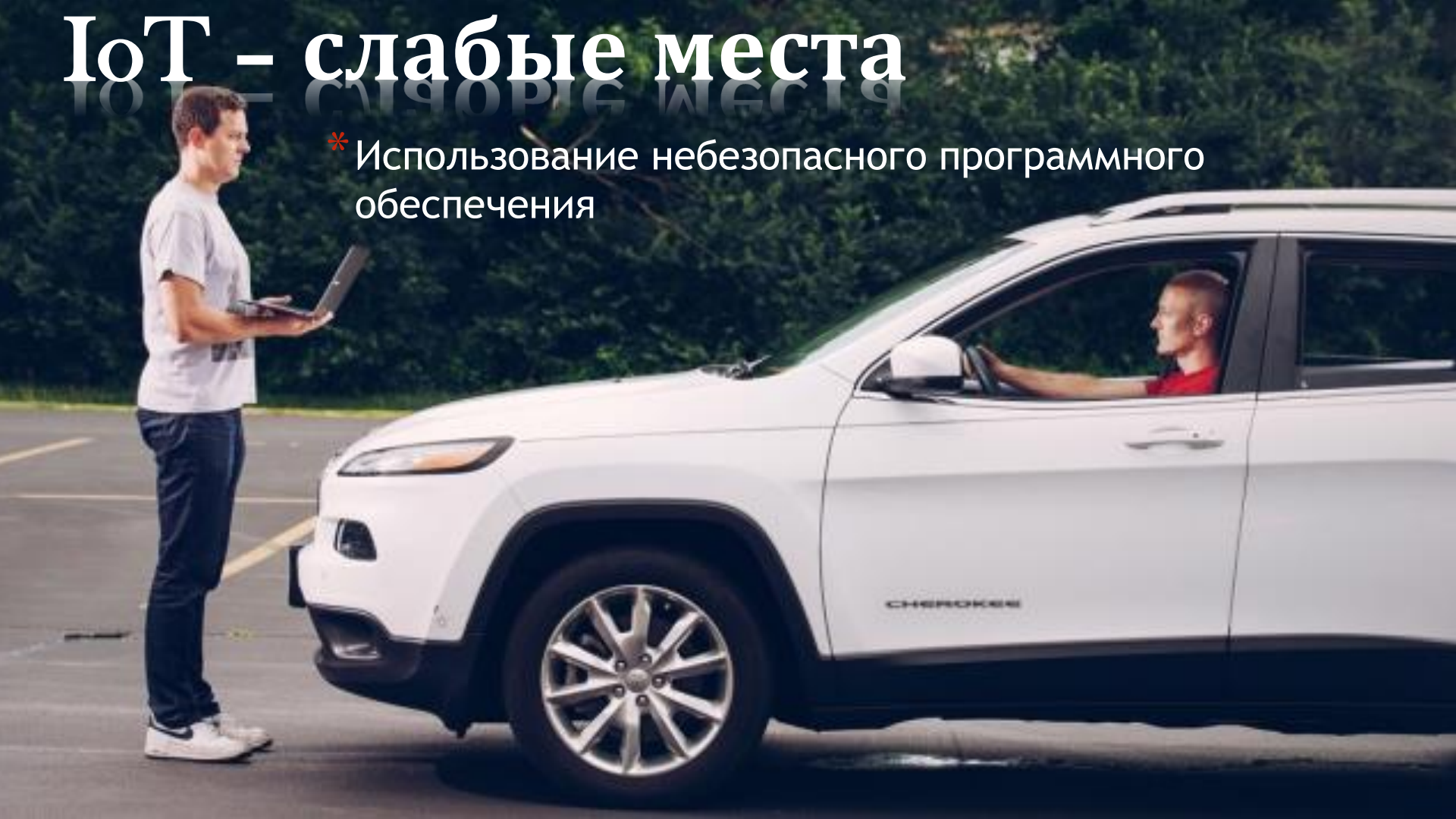
* Использование незащищённых мобильных технологий

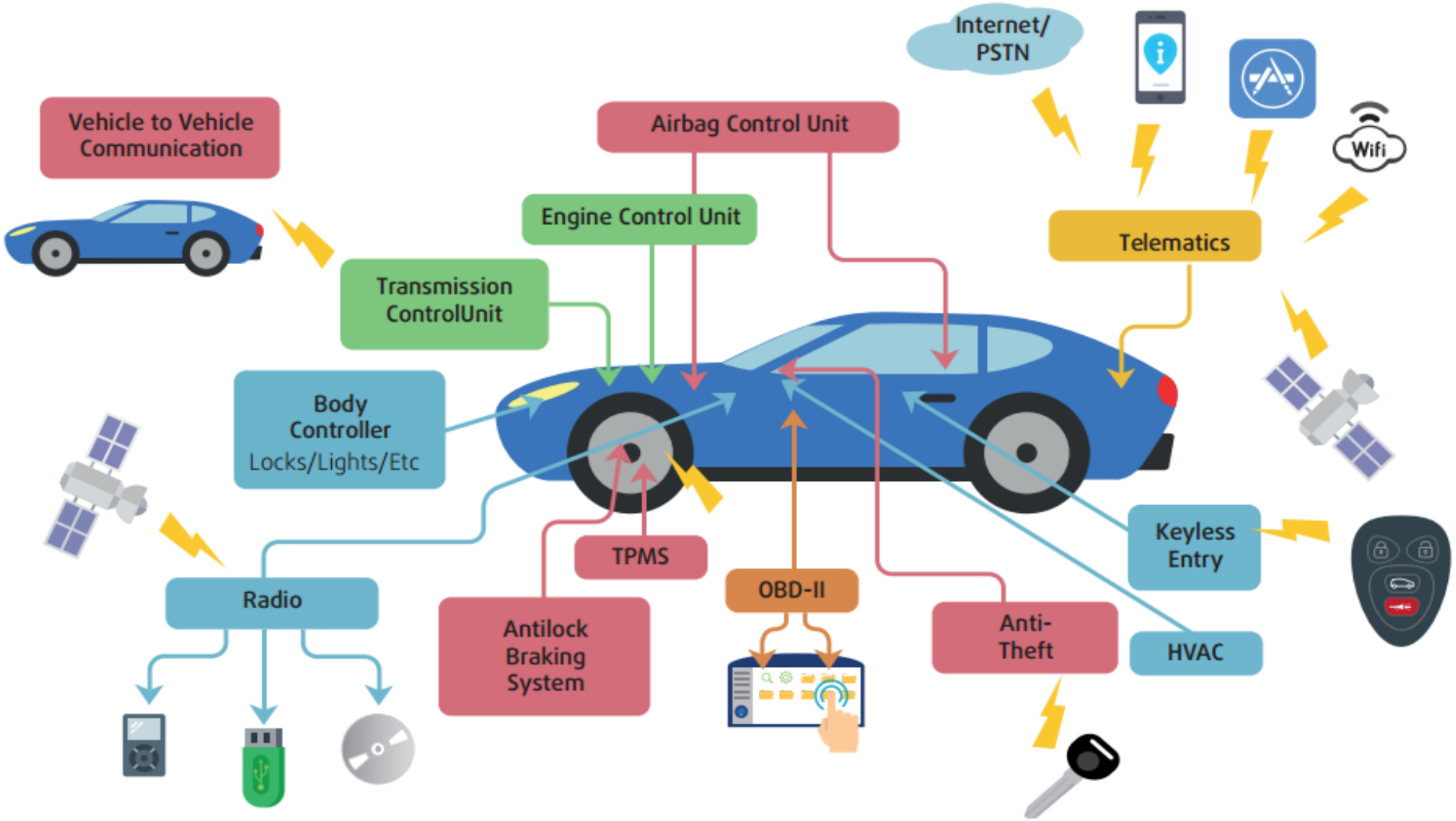
IoT – слабые места

* Использование незащищённой облачной инфраструктуры

IoT – слабые места

* Использование небезопасного программного обеспечения




Internet/
PSTN
Vehicle to Vehicle
Communication
Airbag Control Unit
Wifi
Engine Control Unit
Telematics
Transmission
ControlUnit
Body
Controller
Locks/Lights/Etc
Keyless
Entry
TPMS
OBD-II
Radio
Antilock
Braking
System
Anti-
Theft
HVAC

IoT – слабые места

* Использование уязвимостей оборудования IoT для кибер атак третьей стороны (DoS / DDoS)

Заключение

* Цифровой мир и интернет вещей все плотнее вплетается в нашу жизнь.
* Необходимо уже сегодня искать и находить решения проблем интернета вещей, иначе завтра может быть уже поздно.

Вопросы и ответы*

Ссылки:

* http://www.beechamresearch.com/article.aspx?id=4
* https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9
* http://www.express.co.uk/news/world/602646/baby-monitor-internet-hack-security-Phillips-research-Rapid7-alert
* http://www.utsystem.edu/offices/board-regents/uts165-standards
* https://republic.ru/posts/54335
* http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/internet-of-things-risk-and-value-considerations.aspx
* https://www.owasp.org/index.php/IoT_Security_Guidance
* https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf
* https://www.owasp.org/images/3/36/IoTTestingMethodology.pdf
* http://www.rs-online.com/designspark/electronics/knowledge-item/eleven-internet-of-things-iot-protocols-you-need-to-know-about
* http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/
* http://www.calcalist.co.il/articles/0,7340,L-3702614,00.html
* https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201605_he.pdf
* https://iot.ru/bezopasnost/tendentsii-informatsionnoy-bezopasnosti-v-internete-veshchey
* https://iotconf.ru/ru/news/internet-veshchey-neset-ugasayushchie-potentsialnie-ugrozi-bezopasnosti