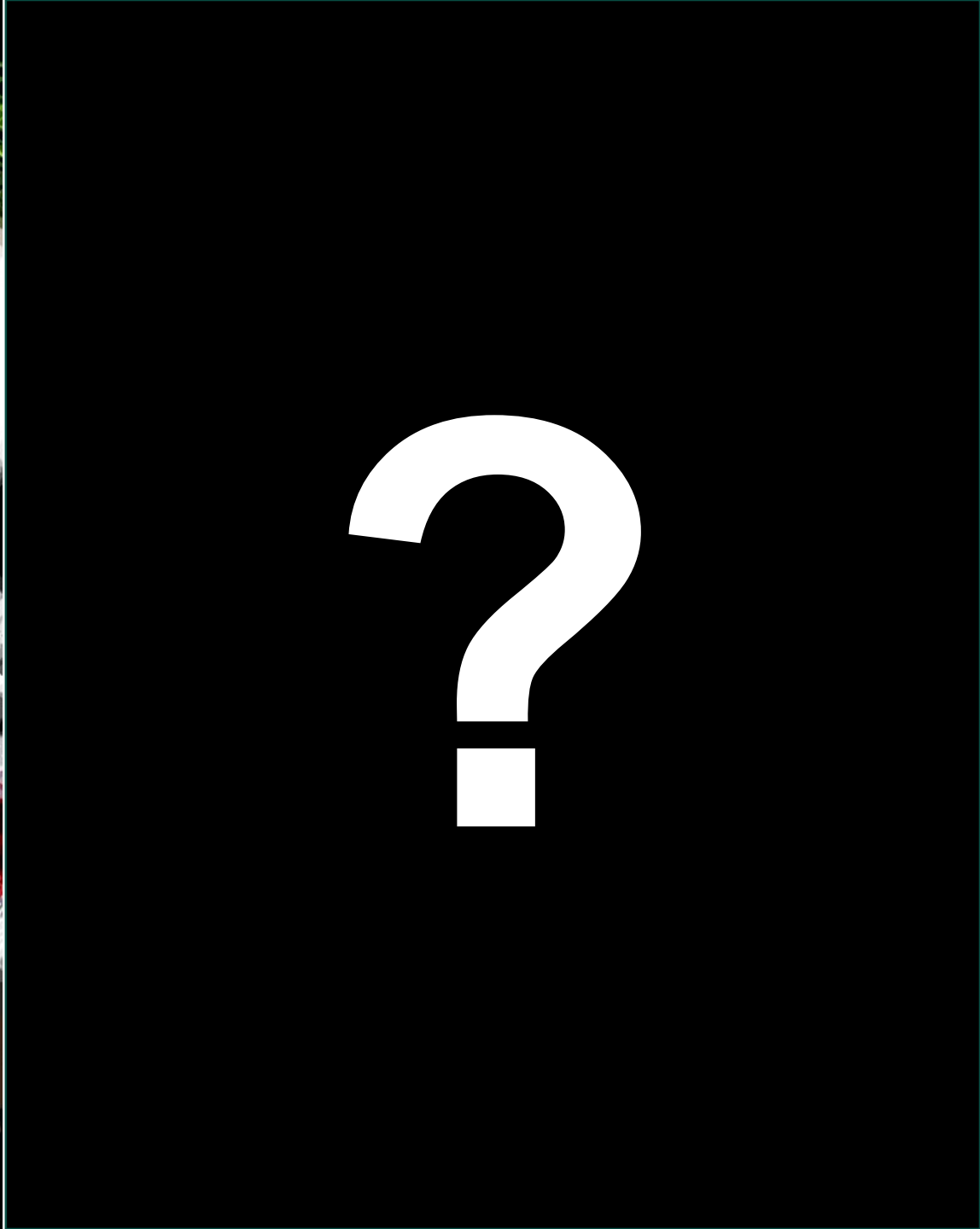


WHY SO
SERIOUS?





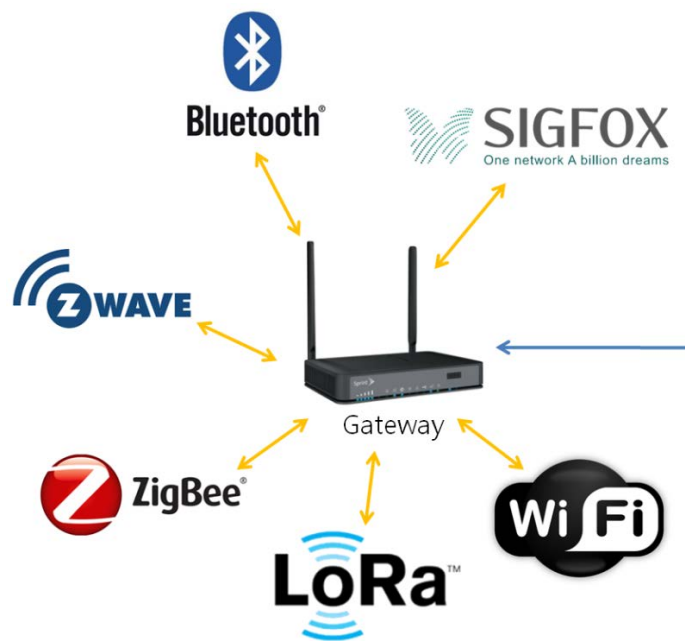




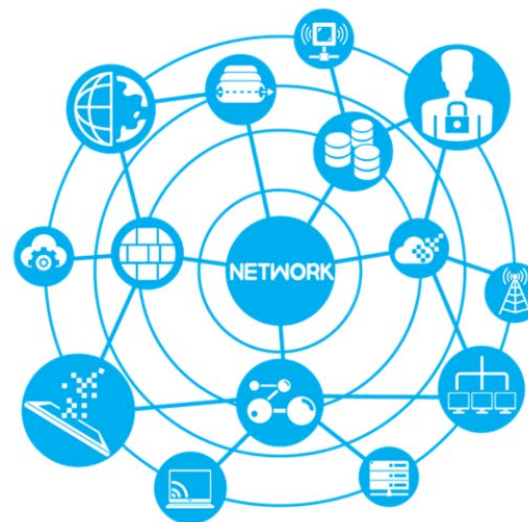
Умные Вещи



Шлюзы



Сеть



Облако



Пользовательский доступ и контроль



Бизнес аналитика



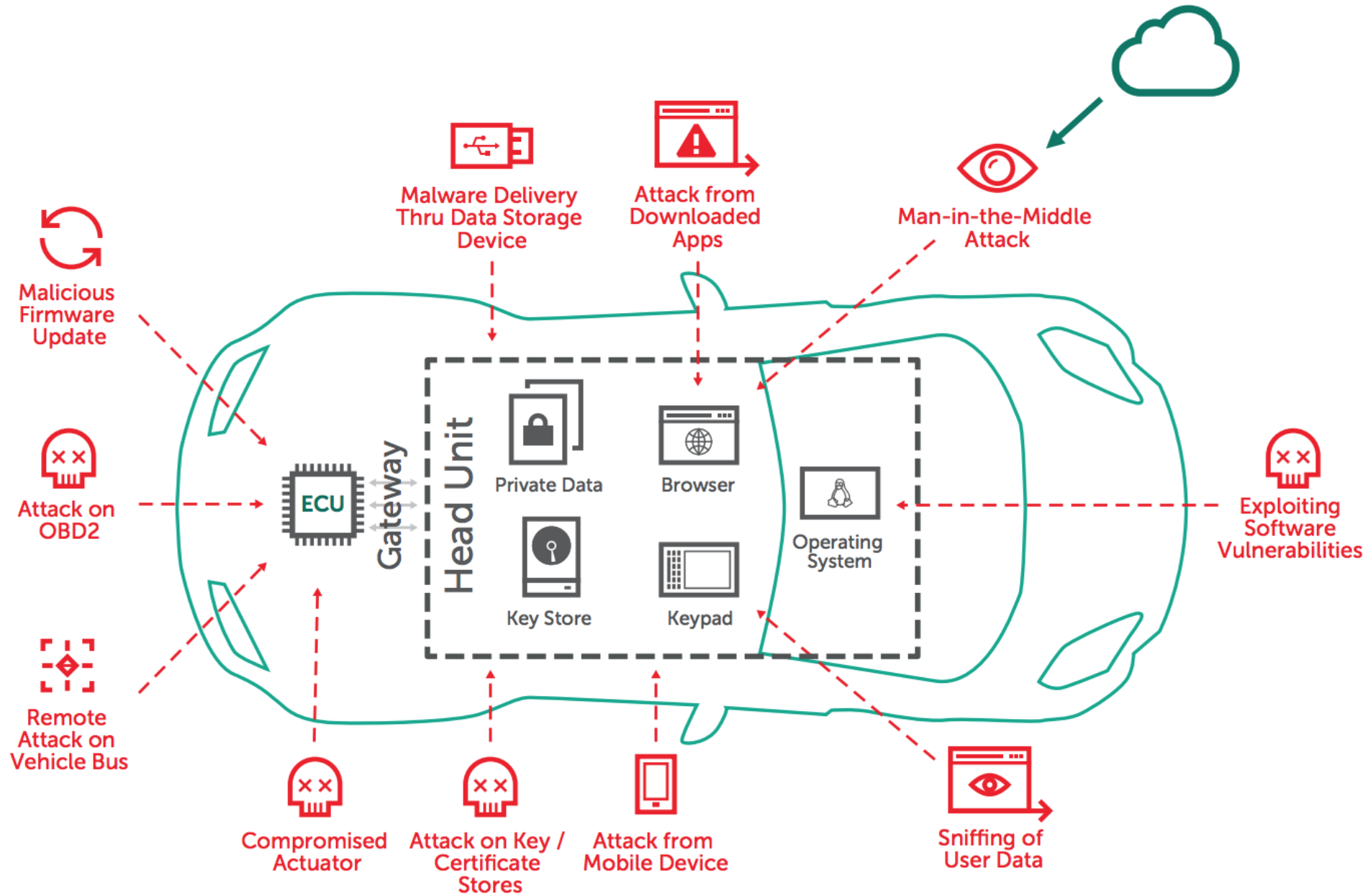
Сервера и СХД

- Каждый элемент инфраструктуры Интернета Вещей – это сложная киберсистема со своими уязвимостями.





Connected car threats







АТАКИ НА ИНТЕРНЕТ ВЕЩЕЙ

- *BotNet (roBot Network) – сети устройств, зараженных вредоносным ПО и использующих ресурсы их для несанкционированной деятельности*

MIRAI

Mirai был обнаружен в августе 2016 и наименование пошло от имени одного из моделей, который назывался “mirai.()”. Mirai это исполняемый модуль Linux и его основная цель это камеры наблюдения DVRs, роутеры, Linux сервера и другие устройства, которые используют Busybox, распространённую библиотеку для IoT устройств.

BASHLITE

Заражает Linux системы и использует их для организации DDoS атак. В 2014 BASHLITE использовал для распространения уязвимость Shellshock для заражения устройств с BusyBox. В 2016 было около 1 миллиона устройств, зараженных BASHLITE.

- **Свободное ПО является наиболее популярным среди разработчиков IoT, но при этом очень уязвимо. Необходимо найти баланс между удобством и защищенностью**



Примеры атак и проблем с Safety у IoT устройств



Производитель «умных» замков Lockstate умудрился заблокировать входные двери сотням своих клиентов, выпустив неудачное обновление прошивки. После установки проблемного апдейта перестала работать встроенная в замок клавиатура, поэтому открыть дверь оказалось невозможно.



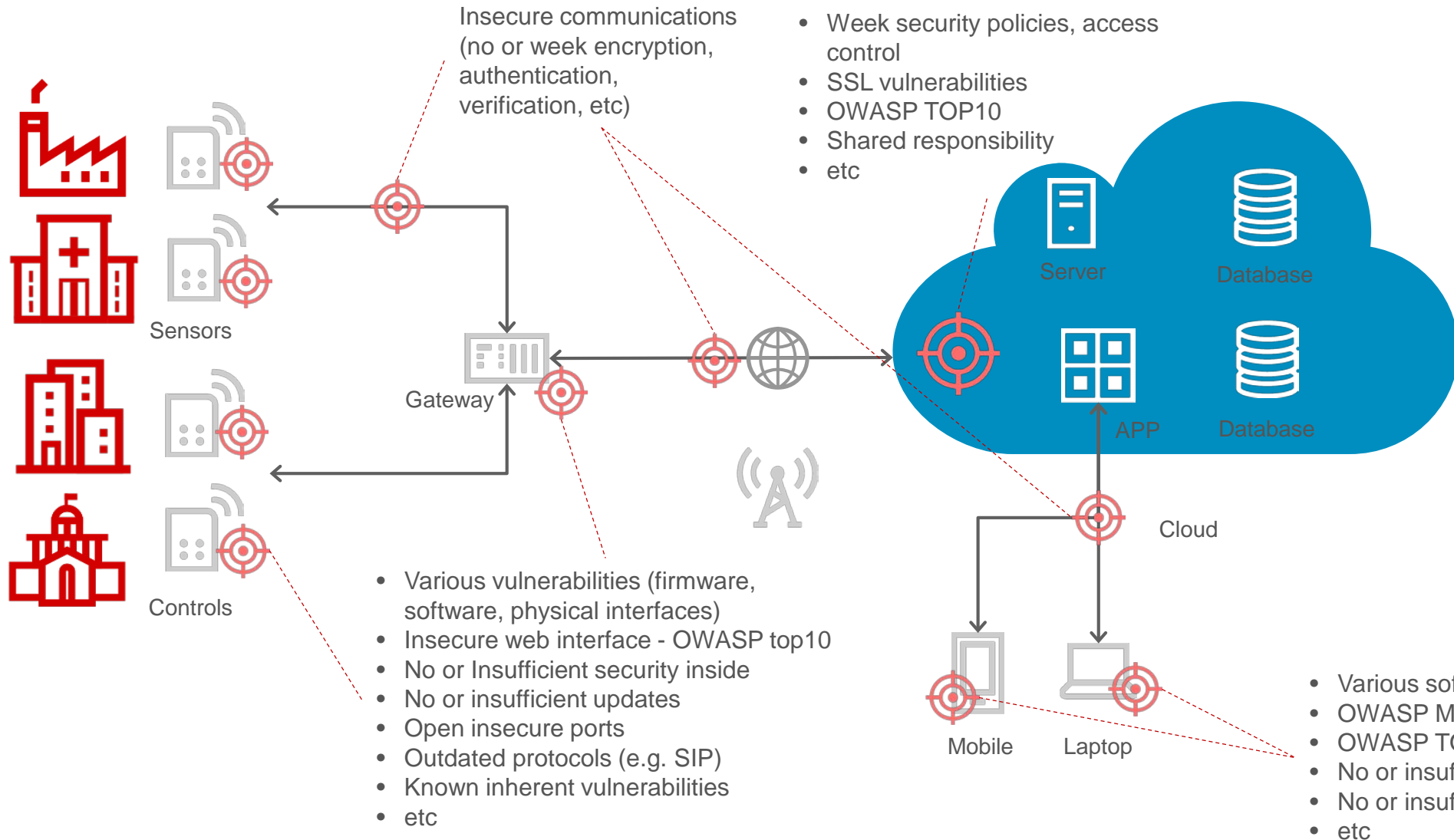
Уязвимости в «умной» системе безопасности производства iSmartAlarm. Обнаружены проблемы с проверкой подлинности SSL-сертификатов и управлением доступа, ошибки аутентификации, а также уязвимость, позволяющую вызвать отказ в обслуживании. Злоумышленники могут проэксплуатировать уязвимости с целью вывести из строя сигнализацию и, к примеру, ограбить дом.



Food and Drug Administration объявило об отзыве некоторых моделей кардиостимуляторов производства компании Abbott.

Причиной отзыва послужили обнаруженные в устройствах уязвимости, позволяющие злоумышленникам получить контроль над. В частности хакер может снизить заряд аккумулятора устройства или ускорить сердцебиение.

УЯЗВИМОСТИ ЮТ И УМНЫХ ГОРОДОВ/ЗДАНИЙ



What these weaknesses can be used for:

- Device to bot-nets
- Altering device's behavior: for spying, sabotage
- Sensitive data theft: spying
- Extracting private credentials
- Device as a backdoor to the user or corporate network
- Cause irreversible damage
- Invade user privacy
- etc





Безопасная ОС для интернета вещей

РЕАЛИЗОВАННЫЕ ПРОЕКТЫ



Карта

Изм. параметры | Объект | События | Параметры управления | Дашборды

Поиск: Шум. Подъезд | Текущее знач... | Единица изм... | Дата значения | Пороги

| Изм. параметр... | Текущее знач... | Единица изм... | Дата значения | Пороги |
|---------------------------------------|-----------------|----------------|---------------------|--------|
| Шум. Подъезд | 42.444 | дБ | 2018-10-15 15:06:09 | ✓ |
| CO2. Подъезд | 417 | ppm | 2018-10-15 15:05:34 | ✓ |
| Кол-во обращений. ОБРАЩЕНИЕ ГРАЖДАН.1 | 1 | | 2018-08-20 11:59:45 | ✓ |
| Напряжение, фаза 1. моск.SN:312078313 | 225.19 | В | 2018-10-15 15:03:55 | ✓ |
| Напряжение, фаза 2. моск.SN:312078313 | 225.69 | В | 2018-10-15 15:03:55 | ✓ |
| Напряжение, фаза 3. моск.SN:312078313 | 226.36 | В | 2018-10-15 15:03:55 | ✓ |
| Напряжение, фаза 1. моск.SN:303084128 | 233.13 | В | 2018-10-15 15:03:55 | ✓ |
| Напряжение, фаза 2. моск.SN:303084117 | 232.32 | В | 2018-10-15 15:03:55 | ✓ |

ОБЩАЯ ИНФОРМАЦИЯ. ЭЛЕКТРОЭНЕРГИЯ - МОСКВ. В(800):700-40-70

Общая информация | Щитовая №1 | ПАРАМЕТРЫ ПРИБОРОВ УЧЕТА ЭЛЕКТРОЭНЕРГИИ | НОРМАТИВНЫЕ ЗНАЧЕНИЯ НАПРЯЖЕНИЯ И ЧАСТОТЫ

Сила тока: 212.01^А

Активная мощность: 46877.37^{Вт}

| Напряжение Фаза | Напряжение Фаза | Напряжение Фаза | Частота тока |
|-----------------|-----------------|-----------------|--------------|
| А | В | С | 50 Гц |
| 226.81 в | 226.98 в | 227.71 в | 49.99 Гц |
| 221.64 в | 222.16 в | 221.99 в | 50 Гц |

ВОДОСНАБЖЕНИЕ - Москва/канал 8(499)-763-34-34. ЦЕНТРАЛЬНОЕ ОТОПЛЕНИЕ - Диспетчер 8(495) 539-53-53

Общее потребление ГВС/ХВС | ПАРАМЕТРЫ ГВС/ХВС | ПАРАМЕТРЫ ТЕПЛОСНАБЖЕНИЯ | НОРМАТИВНЫЕ ЗНАЧЕНИЯ ГВС/ХВС

Потребление ГВС (НОРМА...): 88,286 м³/сут

Потребление ХВС (НОРМА...): 52,581 м³/сут

| Температура в подстанции | Температура в обратном трубопроводе | Давление в подстанции | Давление в обратном трубопроводе | Потребление |
|--------------------------|-------------------------------------|-----------------------|----------------------------------|-------------|
| ГВС1: 58.94 °C | 53.86 °C | 9.10 атм | 0 атм | 363.32 м³ |
| ГВС2: 8 атм | 54.02 °C | 8 атм | 4.50 атм | 279.18 м³ |
| ХВС1: 167.94 м³ | | | | |
| ХВС2: 304.10 м³ | | | | |

ТЕМП НА ВХОДЕ В ЗДАНИЕ: 71.03 °C | ТЕМПЕРАТУРА ПОДАЧИ ПОТРЕБИТЕЛЮ: 51.86 °C | ТЕМП ПОСЛЕ ПОТРЕБИТЕЛЯ: 39.79 °C | ТЕМП НА ВЫХОДЕ ИЗ ЗДАНИЯ: 39.79 °C | ТЕПЛОВАЯ ЭНЕРГИЯ С НАЧАЛА МЕС: 361.03 ккал

ЧТО МЫ БУДЕМ ЗАЩИЩАТЬ ЗАВТРА?

ИНДУСТРИАЛЬНЫЕ ОБЪЕКТЫ



ТРАНСПОРТ И ТРАНСПОРТНЫЕ СИСТЕМЫ



МЕДИЦИНСКОЕ ОБОРУДОВАНИЕ



KasperskyOS

ВСТРАИВАЕМЫЕ УСТРОЙСТВА



БЫТОВАЯ ТЕХНИКА



ИНТЕЛЛЕКТУАЛЬНЫЕ ЗДАНИЯ





WHY
SO
SERIOUS?