Специфика АСУ — сплошные сложности или преимущество?

Каракулин Сергей

Множество проблем защиты IT-инфраструктуры на предприятии

Проприетарные протоколы

Слабые машины

Администратор – источник проблем

Страх потери гарантии

Обновление раз в 2 года

Нельзя использовать облачные сервисы

Старые операционные системы

Узкие каналы передачи данных

Случайные блокировки

Нет ресурсов

Персонал не понимает в IT

Ложные срабатывания

Нет экспертизы

KASPERSKY lab

Основным назначением АСУ ТП является обеспечение непрерывности ОТ-процессов

Не все атаки направлены на IT-инфраструктуру АСУ ТП

Некоторые атаки на цифровую среду могут иметь своей целью ОТ-инфраструктуру

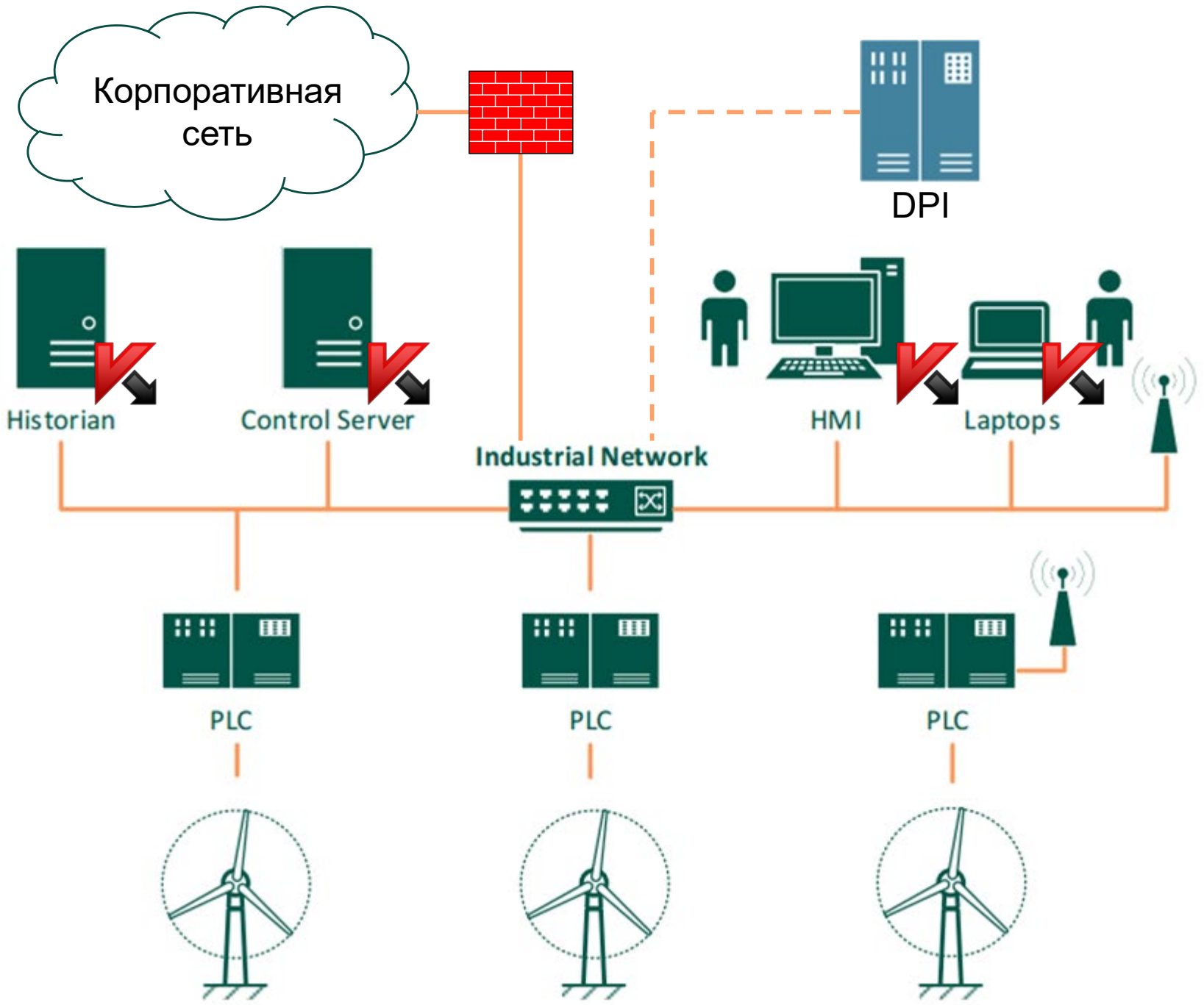
Некоторые атаки на ОТ могут быть чисто физическими (перекрытый клапан, оторванный датчик, присоединенный ложный датчик)

Особенности АСУ ТП…

… - это их преимущества!

- Работают непрерывно
- Критичны к задержкам
- Управляют повторяющимся тех. процессом

KASPERSKY lab



- Перечень коммуникаций
- Перечень используемых приложений
- Использование переносных запоминающих устройств
- Перечень сетевых взаимодействий
- Контроль команд
- Контроль целостности тех. процесса

KASPERSKY lab

1

Индустриальные данные сенсоров и команд управления тесно связаны физикой процессов и логикой управления

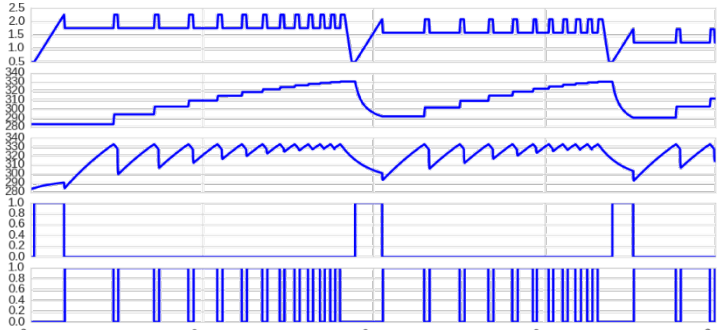
2

Любое (преднамеренное или нет) изменение в одном сигнале влечет изменение в связанных с ним сигналах

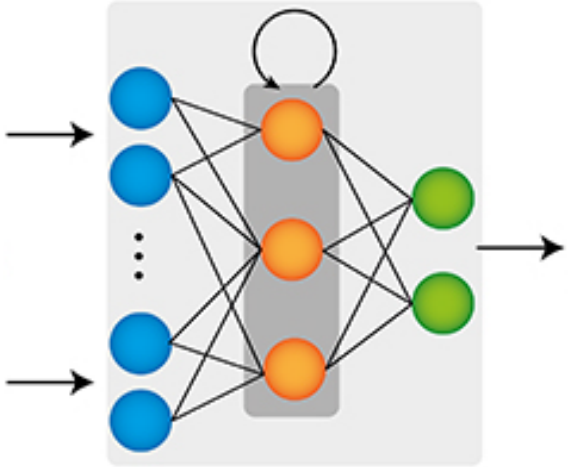
KASPERSKY lab

Корреляции в сигналах могут быть выучены, а изменения обнаружены методами машинного обучения

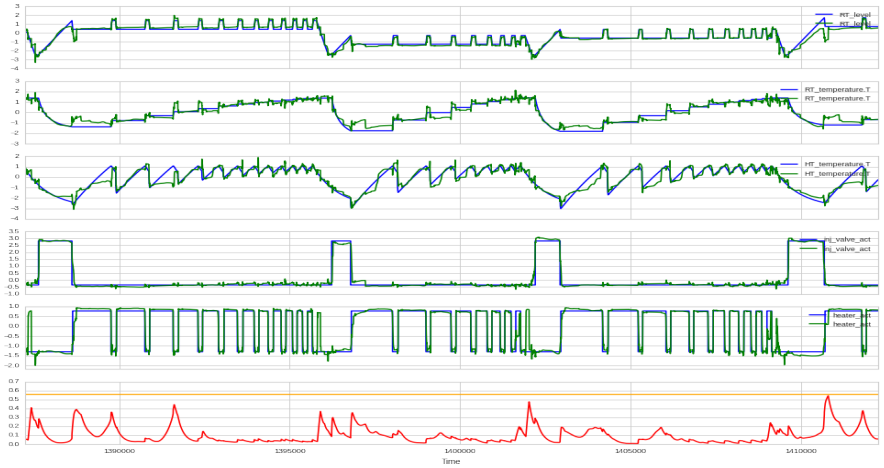
Вход: Многомерный сигнал



Нейронная сеть



Предсказание, Наблюдение, Ошибка

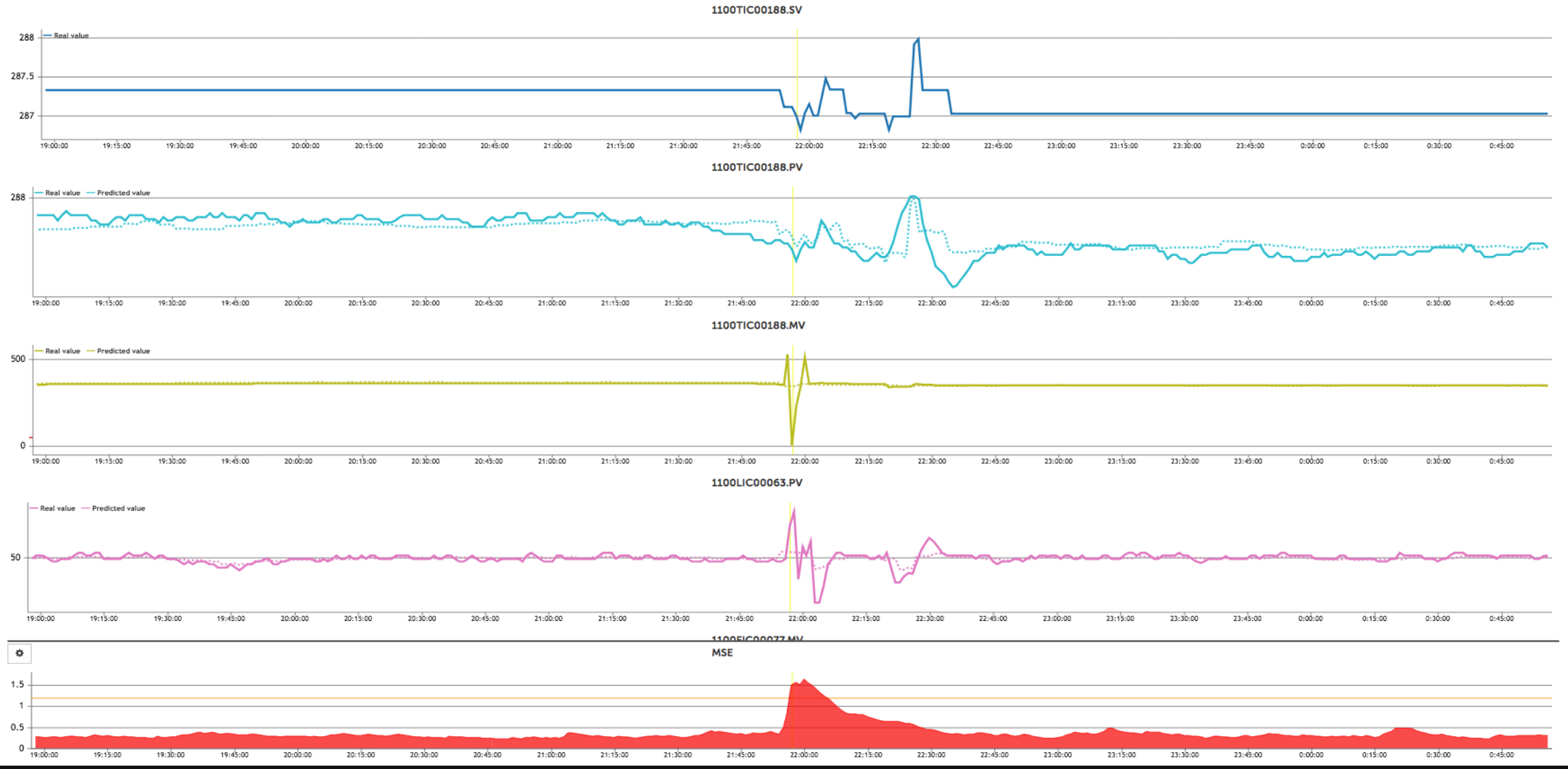


Monitoring | History | Events | Models

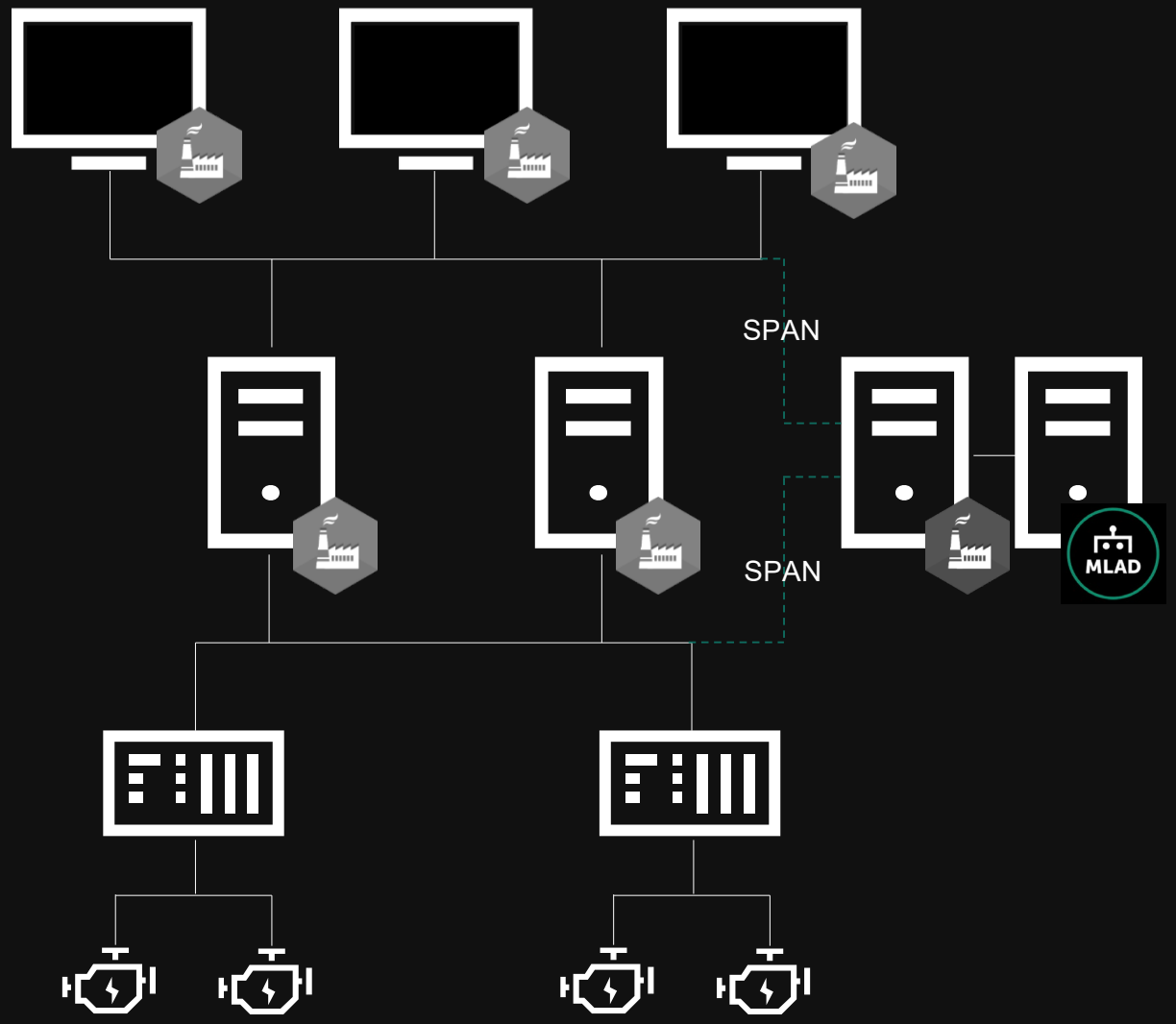
Taneco two-step resnet pv-sv dense-decoder model

Services | About | Help | Login

6 hours | MSE | Sorted Tags | Date: 2017-12-26



Machine Learning for Anomaly Detection



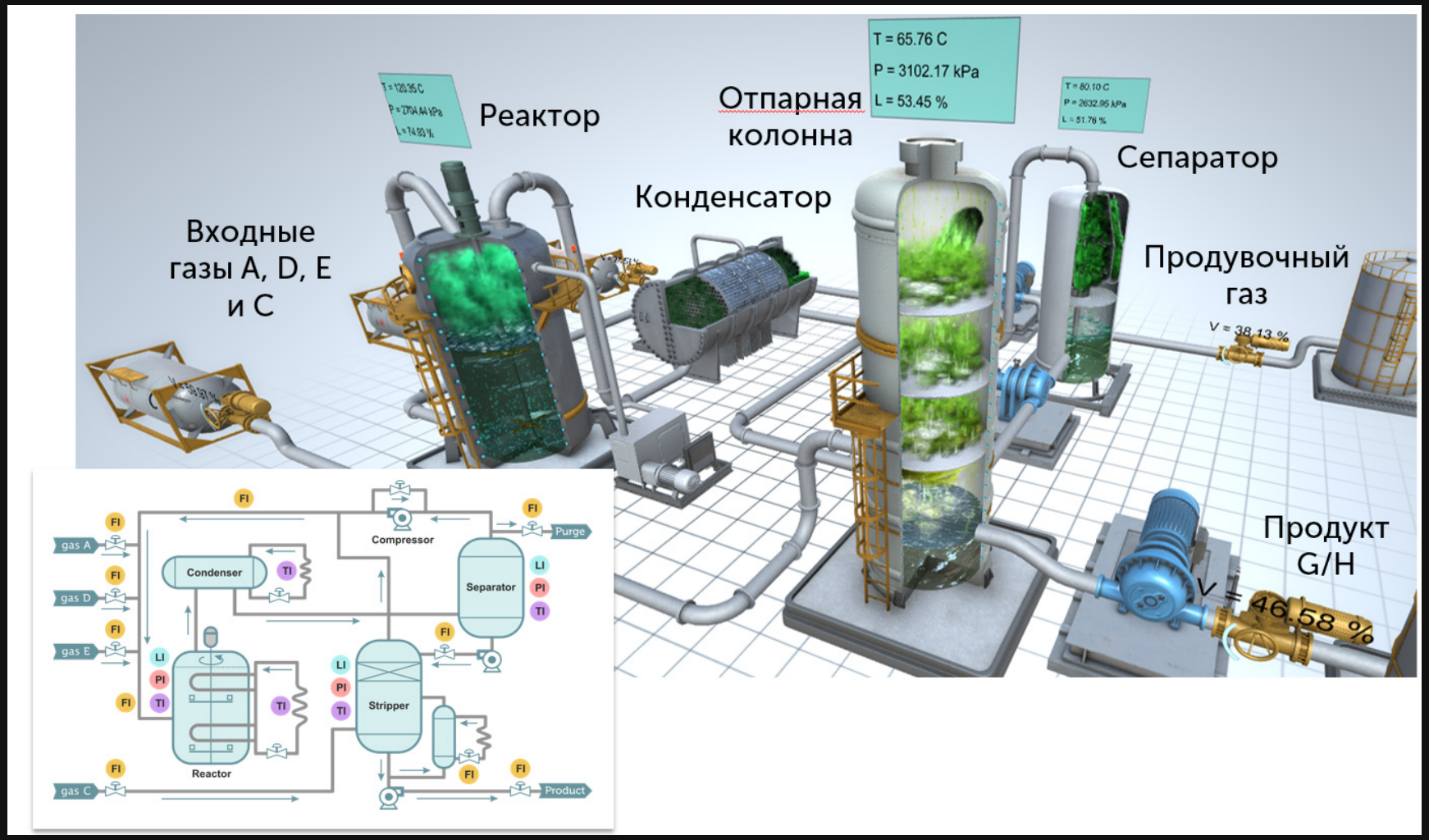
KASPERSKY lab

Machine Learning for Anomaly Detection

- Работает по принципу неразрушающего контроля
- Не требует дополнительного измерительно-диагностического оборудования
- Обнаруживает аномалии вне зависимости от причин их возникновения
- Интерпретирует найденные аномалии
- Не требует ручного написания правил

Ценность решения

- Раннее обнаружение аномалий
- Ретроспективный анализ эффективности контроля процессов
- Интерпретация аномалий
- Обнаружение редких аномалий (трудноуловимых для оператора)



Разница между временем обнаружения аномалии с помощью MLAD и срабатыванием ПАЗ — 3 часа 8 минут

KASPERSKY lab

Какую пользу от KICS for Networks и MLAD можно получить помимо киберзащиты?

KASPERSKY lab

Установка ЭЛОУ-АВТ-7

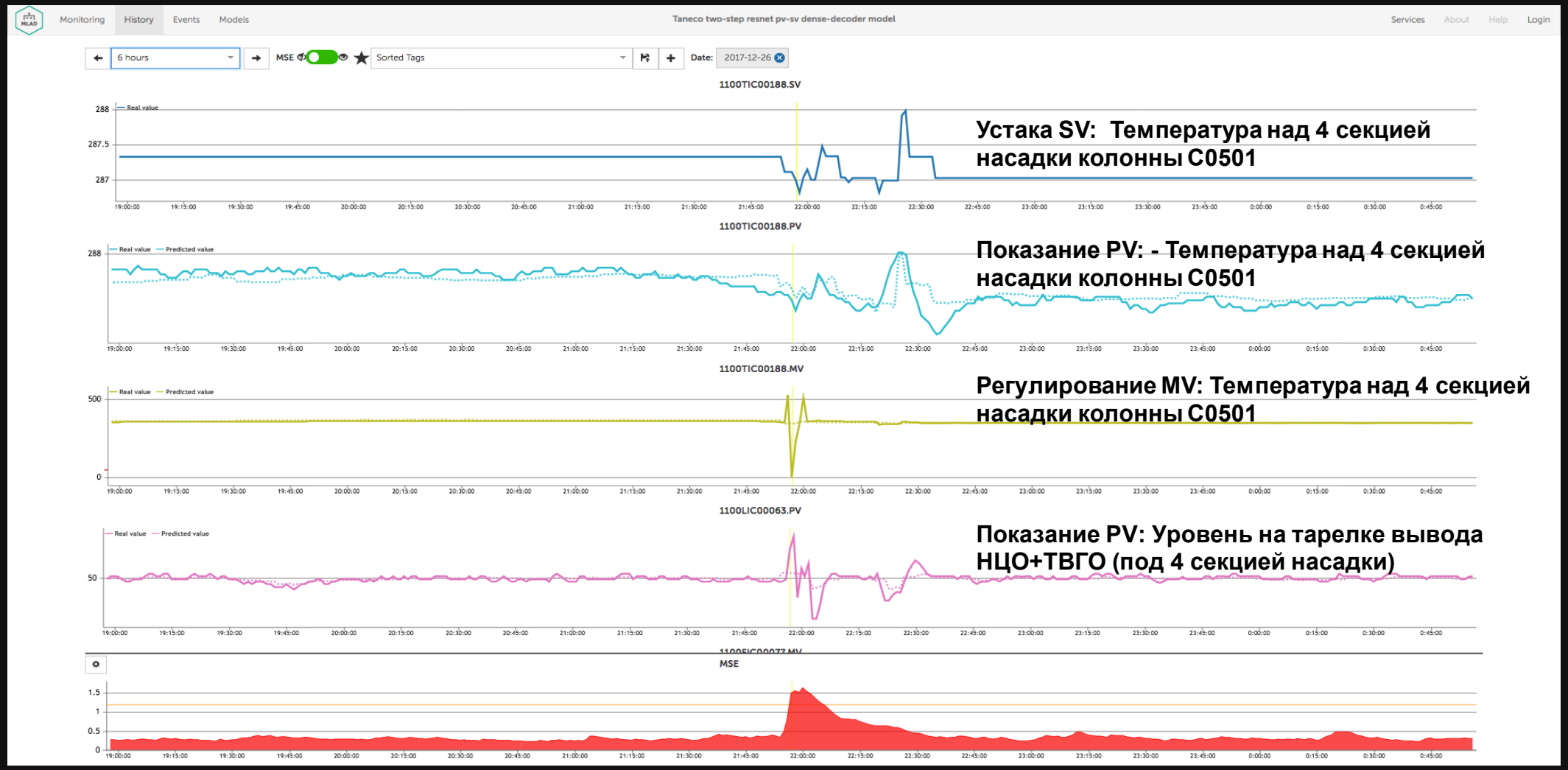
- Электрообессоливающая установка, печи, атмосферные и вакуумные колонны
- Происходит разделение нефтепродуктов по фракциям

- Обучение на исторических данных (6 месяцев)
- Онлайн мониторинг
- Автоматическое раннее обнаружение аномалий в техпроцессах
- Автоматическая интерпретация аномалий

Обнаружены различные типы аномалий:

- Отклонения технологического процесса, связанные с периодами смены режимов
- Переводы контуров управления в ручной режим
- Ситуации, связанные с некорректными показаниями датчиков

Аномалия в температуре Вакуумной колонны



Ситуация связана с некорректным показанием расходомера в связи с забивкой коксовыми отложениями импульсных трубок

Каракулин Сергей
Sergey.Karakulin@kaspersky.com

KASPERSKY lab