ViPNet Coordinator IG. Инструкция к применению

Марина Сорокина,
руководитель продуктового направления по АСУ ТП

Новости

ViPNet Coordinator IG

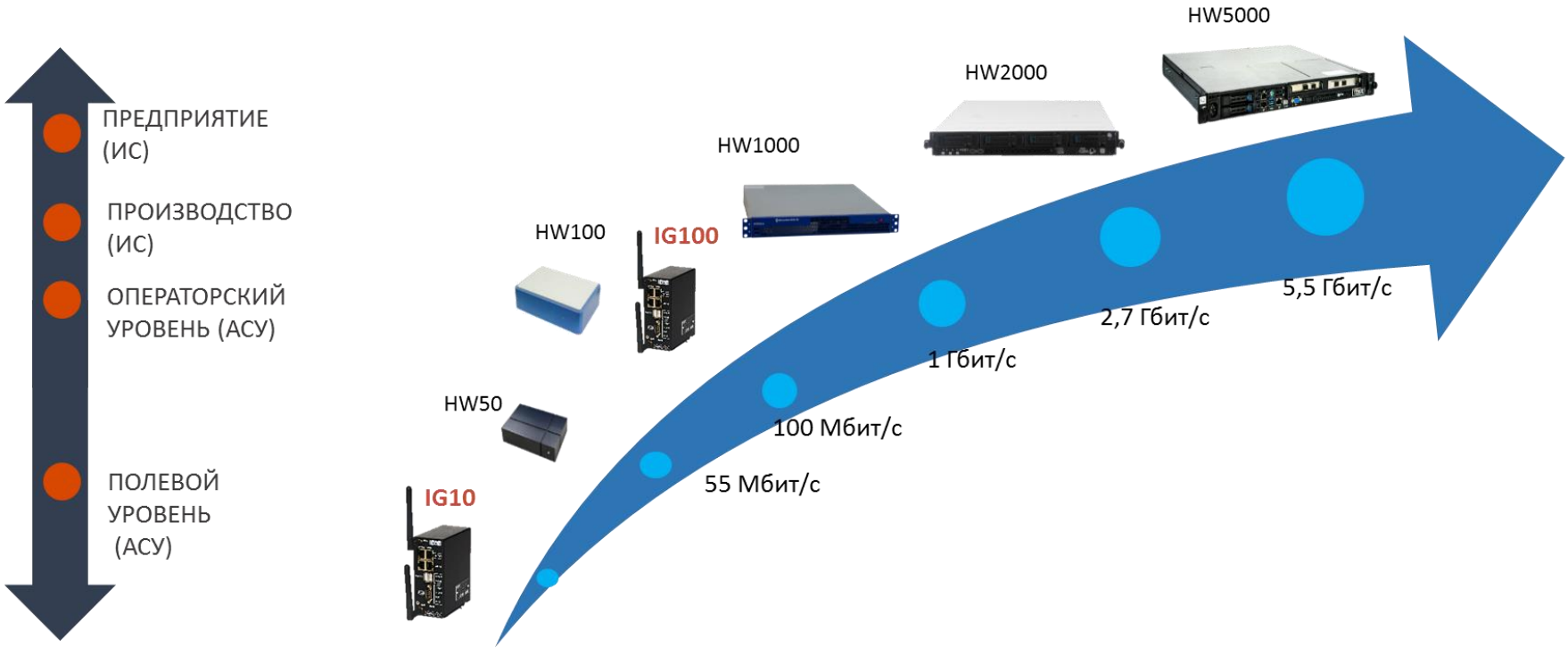
Выпуск релиза ViPNet Coordinator IG 4.2.3

- Поддержка новой аппаратной платформы – IG100 I1
- Поддержка GPIO
- Фильтрация протокола Modbus
- Функционирование как МЭ типа Д и типа А
- Режимы работы для МЭ типа Д – штатный, специальный режимы и режим регламентного обслуживания
- Цветовая индикация режимов работы

ViPNet Coordinator IG

	ViPNet Coordinator IG10	ViPNet Coordinator IG100
Платформа	IG10 I1	IG100 I1
Количество туннелей	• 5 туннелей • без ограничений	• 5 туннелей • без ограничений
Дополнительные беспроводные модули	• Wi-fi - модуль • GSM-модуль (3G)	• Wi-fi - модуль • GSM-модуль (3G)
Поддержка интерфейсов	• Ethernet • Ethernet + Serial interface	• Ethernet • Ethernet + Serial interface

ViPNet Coordinator IG 4.2.3



Сценарий 1
Сегментация (режим МЭ)

Сегментация (режим МЭ)

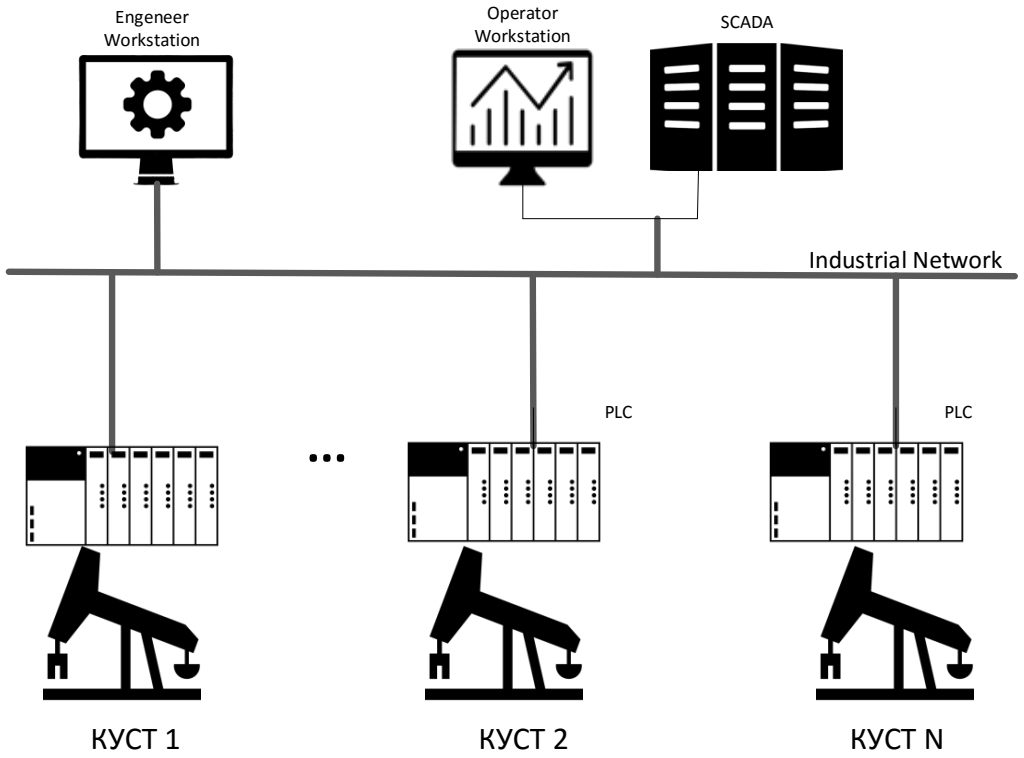
Задача:

Есть АСУ ТП по управлению нефтяными кустами, расположенная внутри контролируемой зоны.

Контроллеры кустов передают информацию в центральный офис в SCADA-сервер. Операторы отслеживают состояние АСУ ТП с АРМ оператора, подключающего к SCADA-серверу.

Управление конфигурацией контроллеров осуществляется с рабочего места инженера.

Требуется обеспечить информационную безопасность с АСУ ТП.



Сегментация (режим МЭ)

Модель угроз:

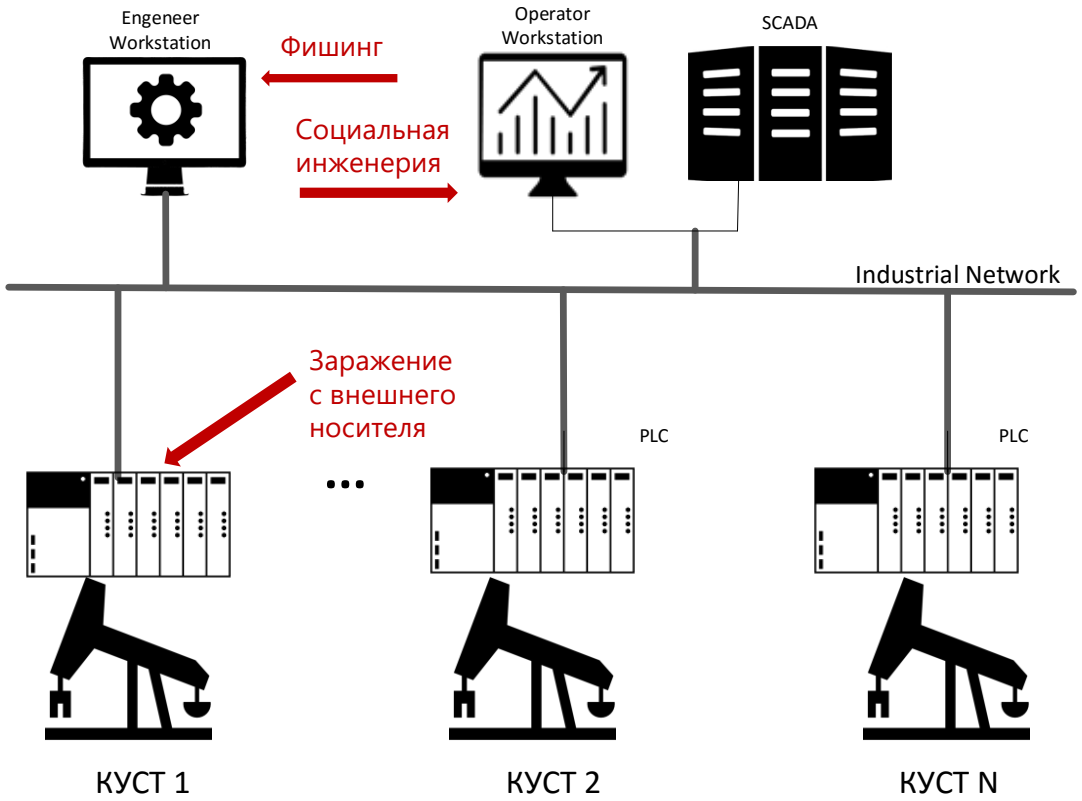
Угроза изменения конфигурации

Угроза неправомерного действия в каналах

Угроза перехвата данных

Угроза подмены сетевого доступа

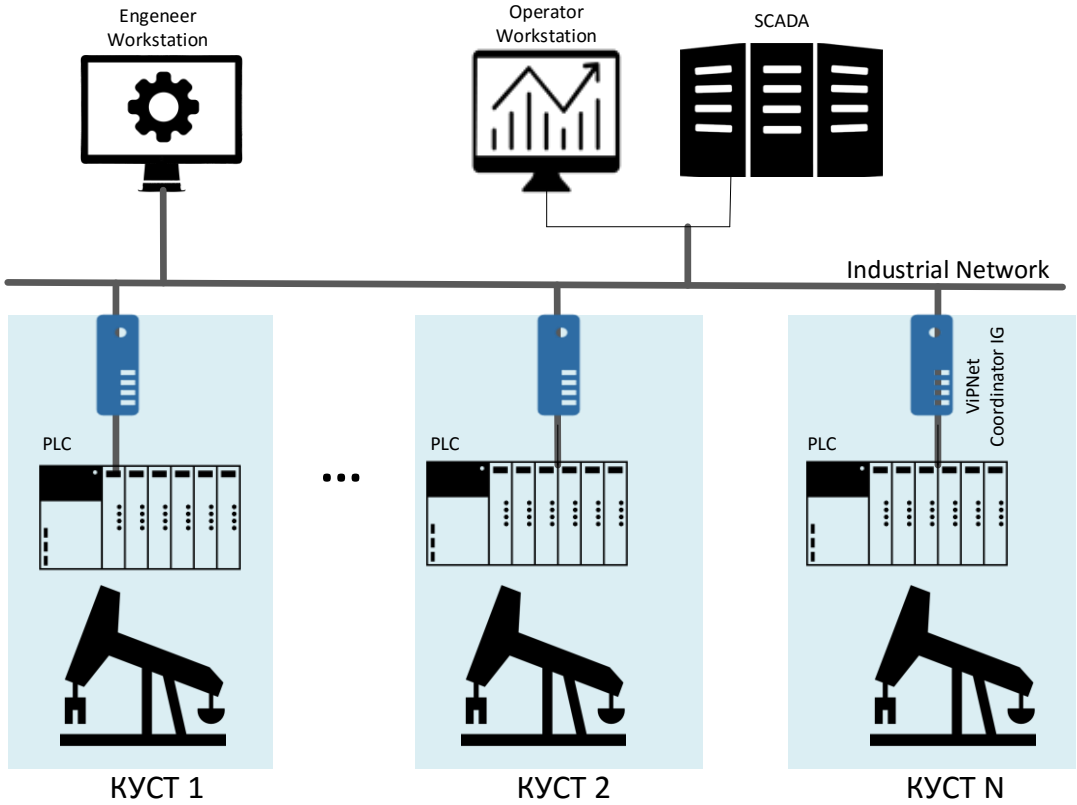
Угроза перехвата управления АСУ ТП



Сегментация (режим МЭ)

Решение

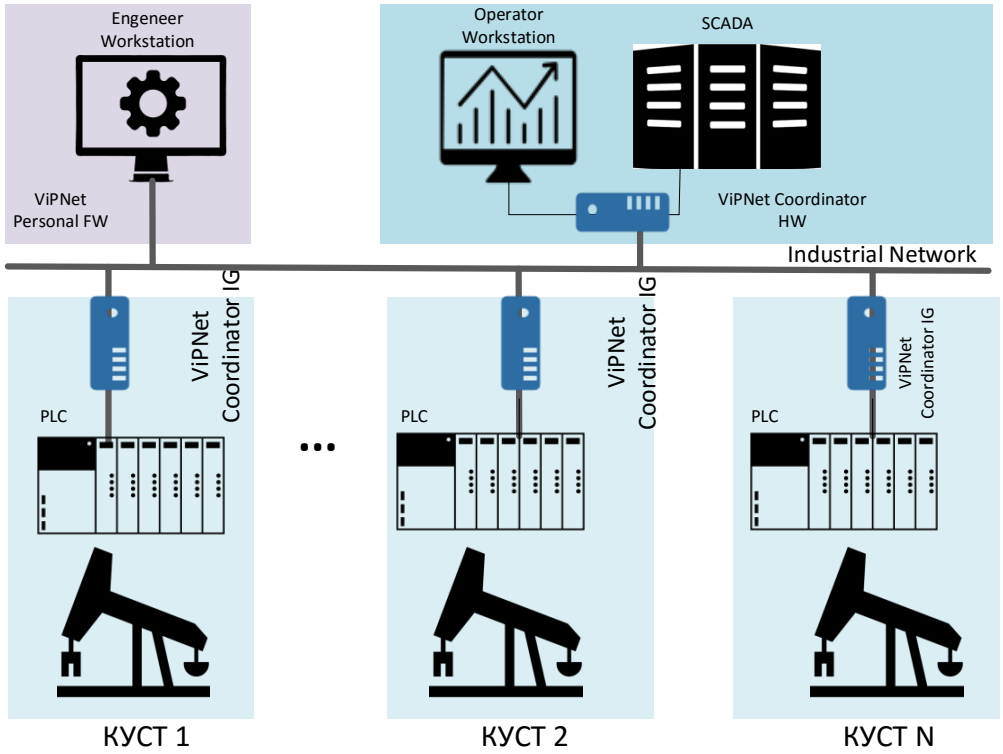
1. Осуществляем сегментацию сети АСУ ТП на уровне автоматизации
2. Защищаем сегменты от несанкционированного доступа из технологической сети.



Сегментация (режим МЭ)

Решение:

1. Осуществляем сегментацию сети АСУ ТП на уровне автоматизации
2. Защищаем сегменты от несанкционированного доступа из технологической сети.
3. Осуществляем сегментацию на уровне оперативно-диспетчерского управления

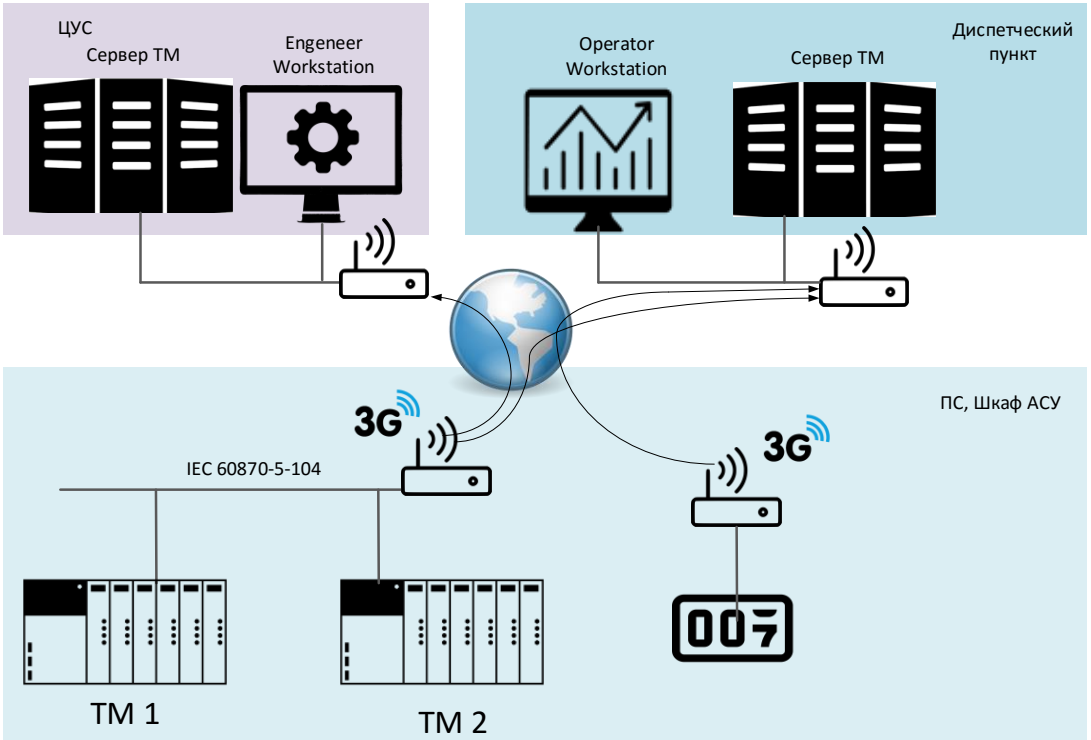


Сценарий 2
Сегментация и защита каналов Подстанции (МЭ + VPN)

Сегментация и защита каналов ПС (МЭ + VPN)

Задача:

Есть подстанция 6-35 кВт. Для передачи информации используются арендованные каналы или беспроводные сети.



Сегментация и защита каналов ПС (МЭ + VPN)

Модель угроз:

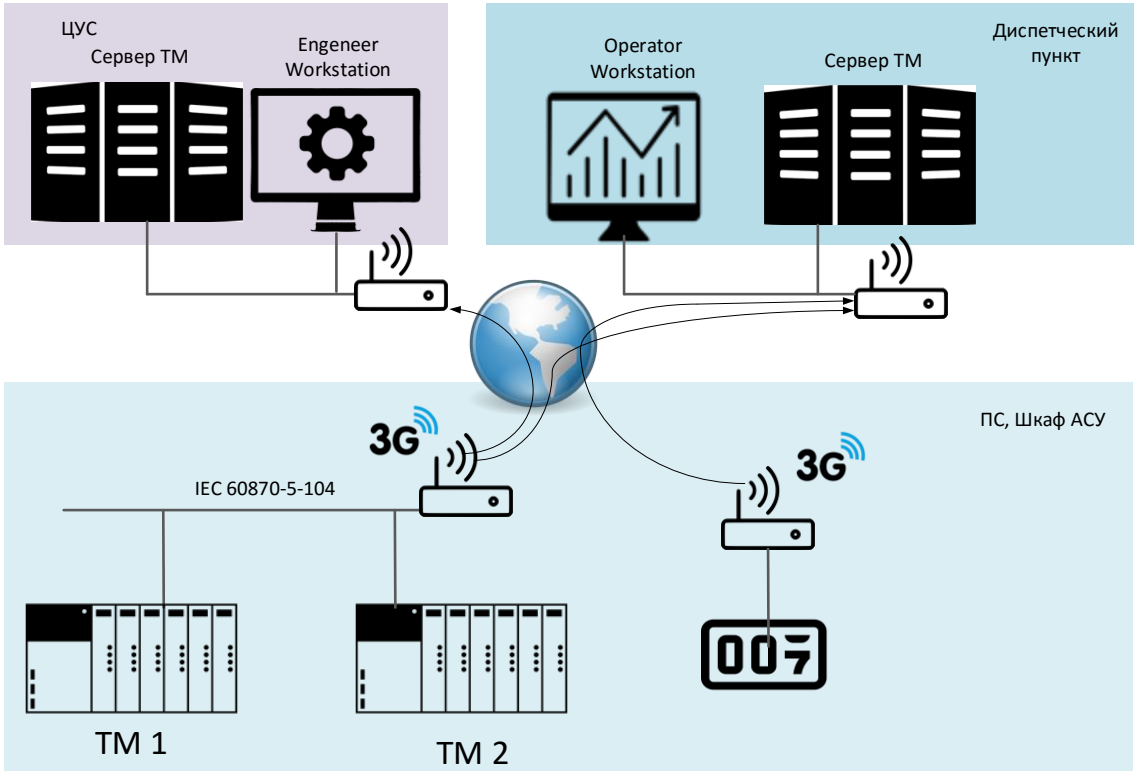
Угроза изменения конфигурации

Угроза неправомерного действия в каналах

Угроза перехвата данных

Угроза подмены сетевого доступа

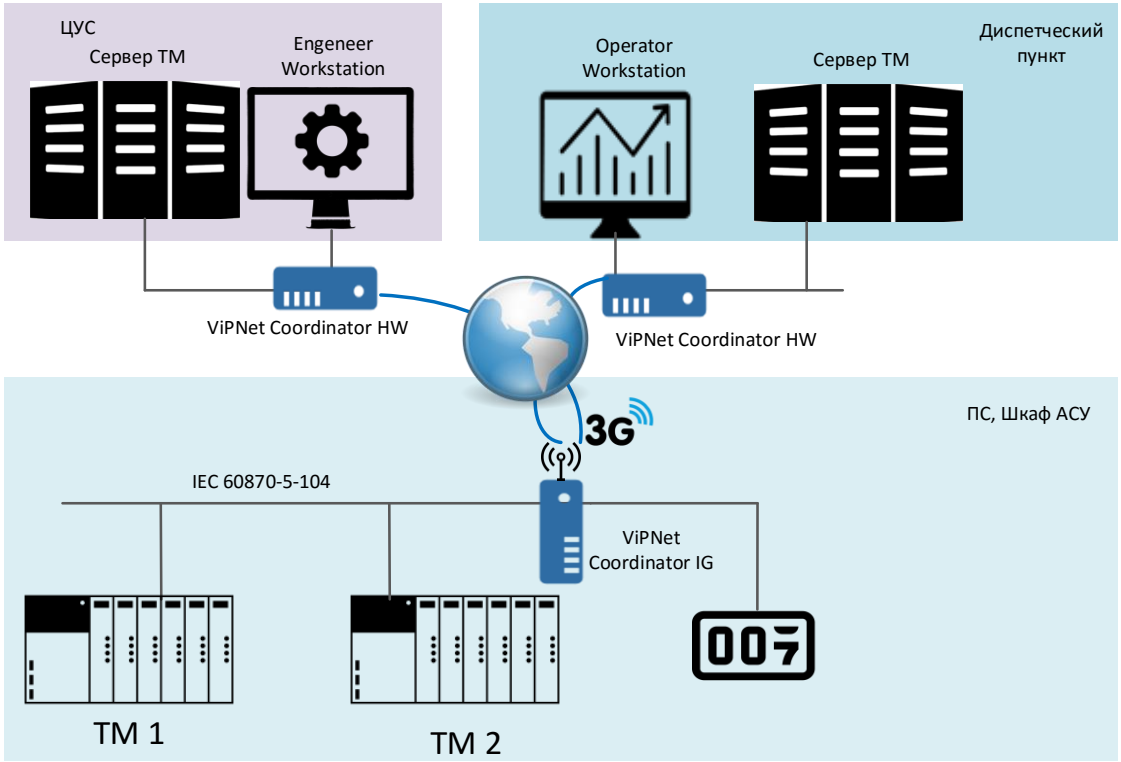
Угроза перехвата управления АСУ ТП



Сегментация и защита каналов ПС (МЭ + VPN)

Решение:

1. Осуществляем сегментацию сети
2. Защищаем сегменты от несанкционированного доступа из технологической сети.
3. Защищаем каналы передачи информации между сегментами с помощью VPN



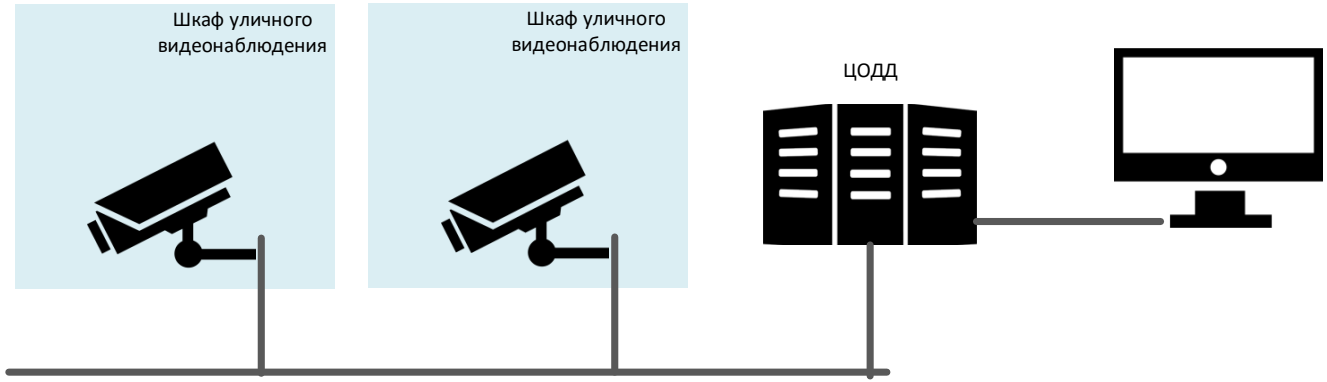
Сценарий 3
Защита каналов для Умного города (МЭ + VPN + GPIO)

Сегментация и защита каналов (МЭ + VPN + GPIO)

Задача:

Есть система уличного видеонаблюдения. Для передачи данных используются проводные арендованные сети.

Требуется обеспечить информационную безопасность.



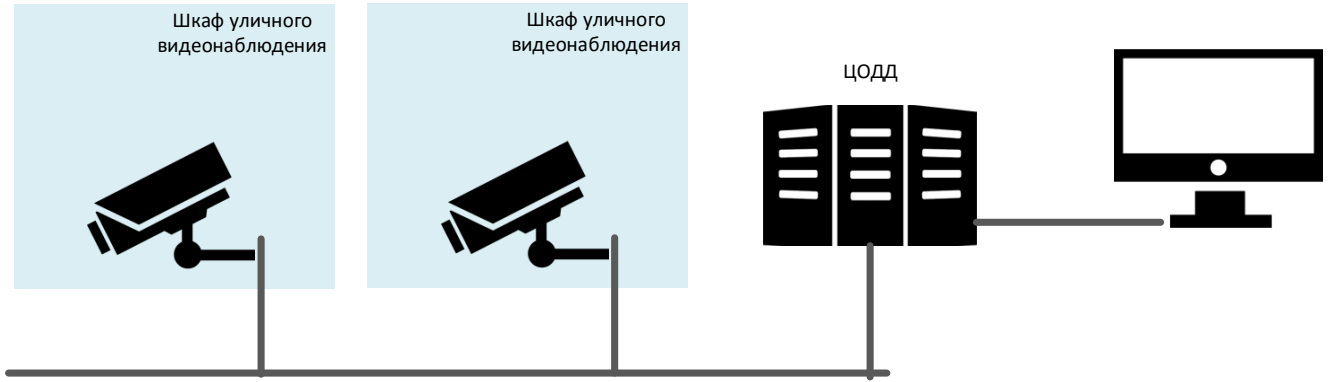
Сегментация и защита каналов (МЭ + VPN + GPIO)

Модель угроз:

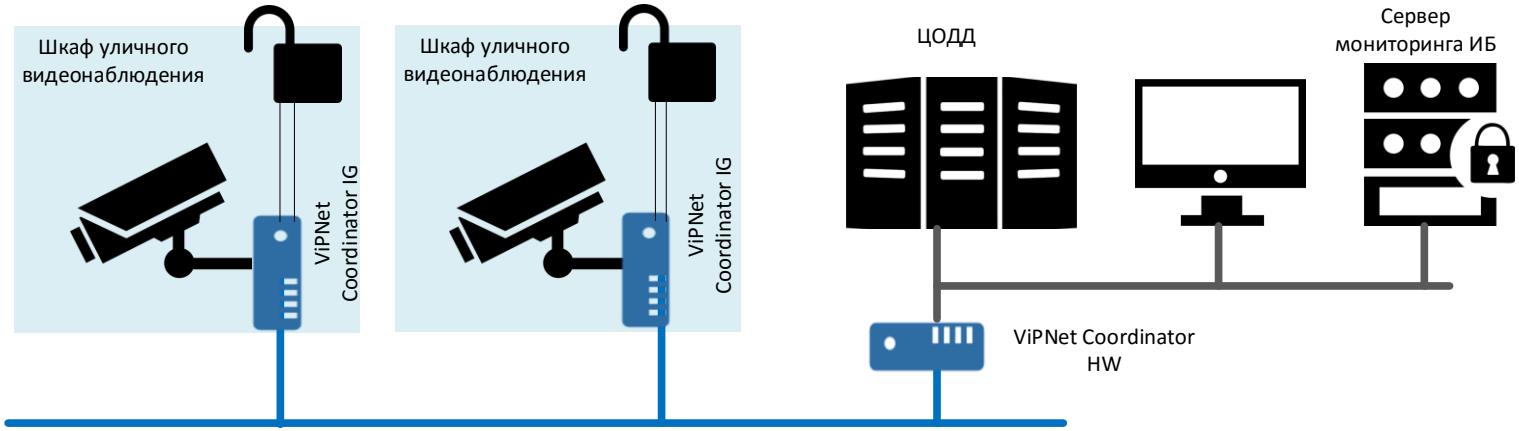
Угроза неправомерного действия в каналах

Угроза перехвата данных

Угроза подмены сетевого доступа



Сегментация и защита каналов (МЭ + VPN + GPIO)

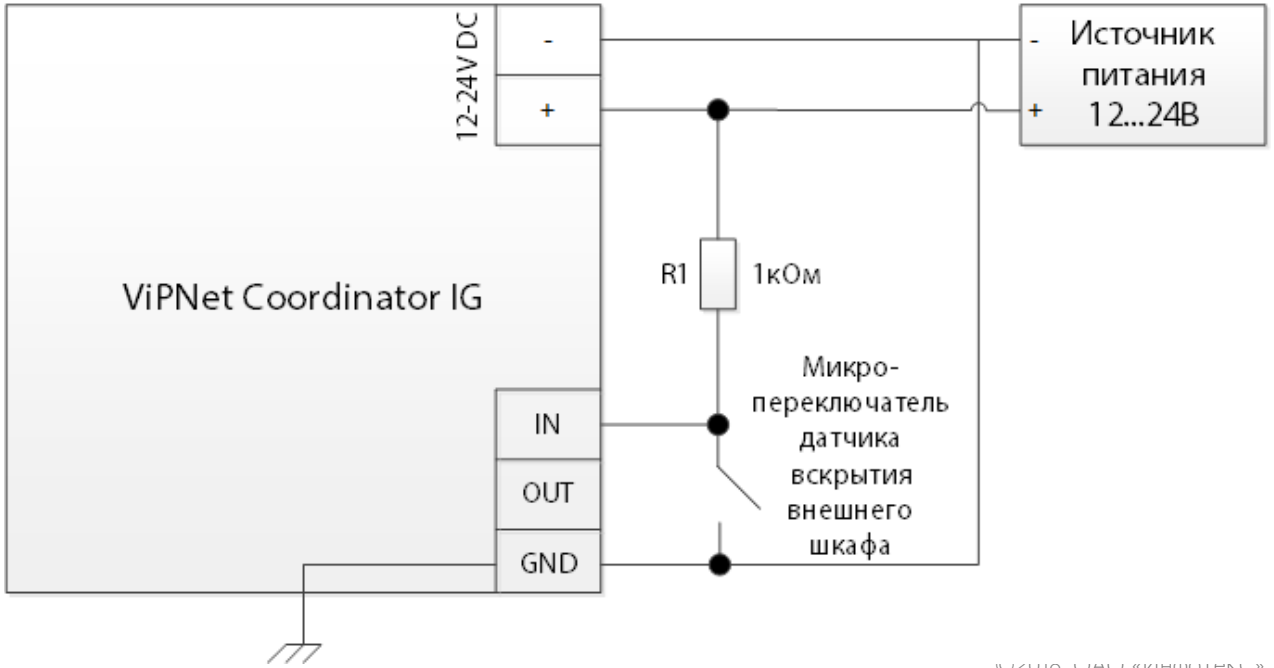


Решение:

1. Осуществляем сегментацию сети
2. Защищаем сегменты от несанкционированного доступа из интернета.
3. Защищаем каналы передачи информации между сегментами с помощью VPN
4. Подключаем датчик вскрытия шкафа, в который установлена система уличного видеонаблюдения, к входному порту GPIO ViPNet Coordinator IG и отслеживаем события открытия шкафа в центре мониторинга по syslog

Сегментация и защита каналов (МЭ + VPN + GPIO)

Подключение внешнего датчика вскрытия к портам GPIO



Сценарий 4
Защищенное обновление ПО ПТК Цифрового РЭС

Защищенное обновление ПО PLC

Задача:

Есть Цифровой РЭС.

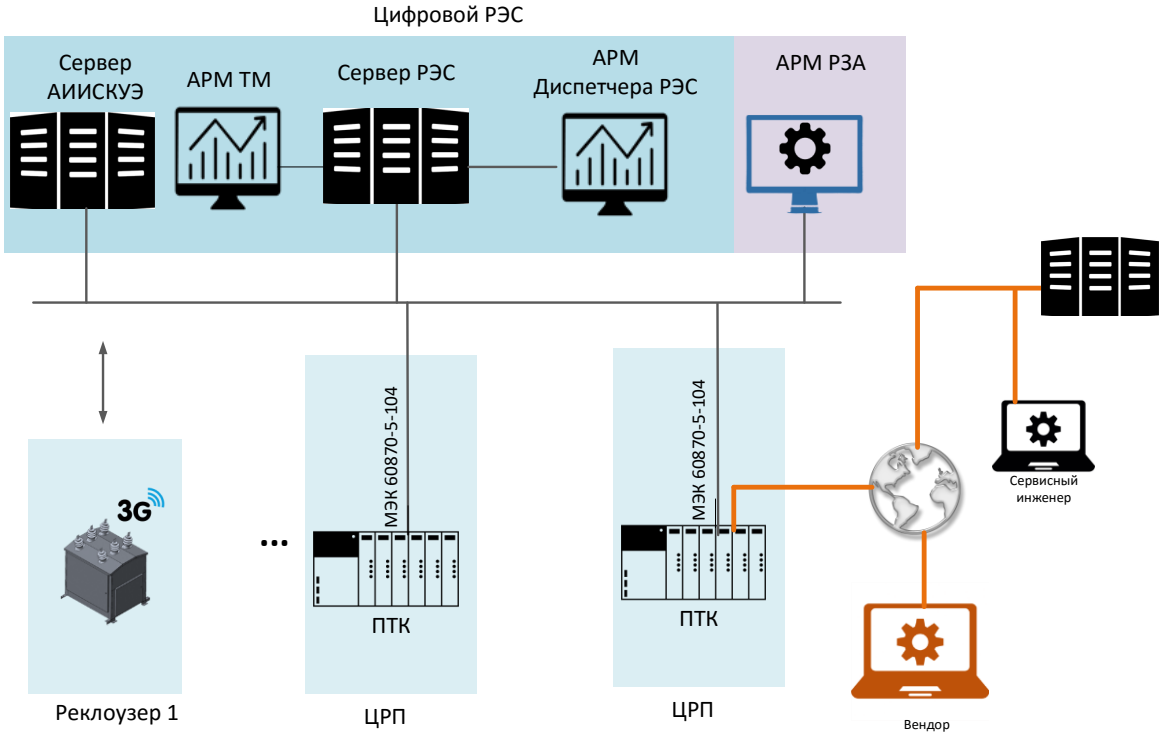
Передача данных в РЭС идет по протоколу МЭК 60870-5-104.

Обновление ПО ПТК осуществляет сервисным инженером из Репозитория ПО, расположенного в центральном сервисном центре.

Диагностику работы ПО ПТК осуществляет вендор.

Диагностика и обновление происходят по протоколу HTTP

Требуется обеспечить информационную безопасность.



Защищенное обновление ПО PLC

Модель угроз:

Угроза изменения конфигурации

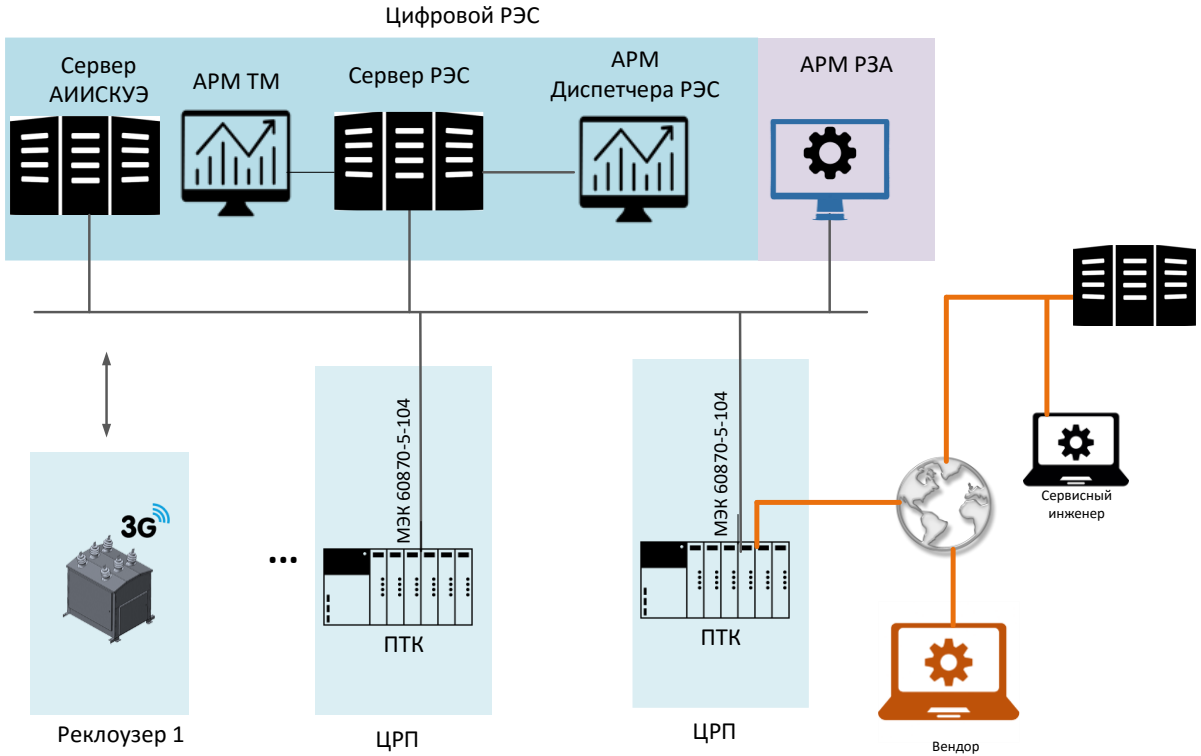
Угроза внедрения кода или данных

Угроза неправомерного действия в каналах

Угроза перехвата данных

Угроза подмены сетевого доступа

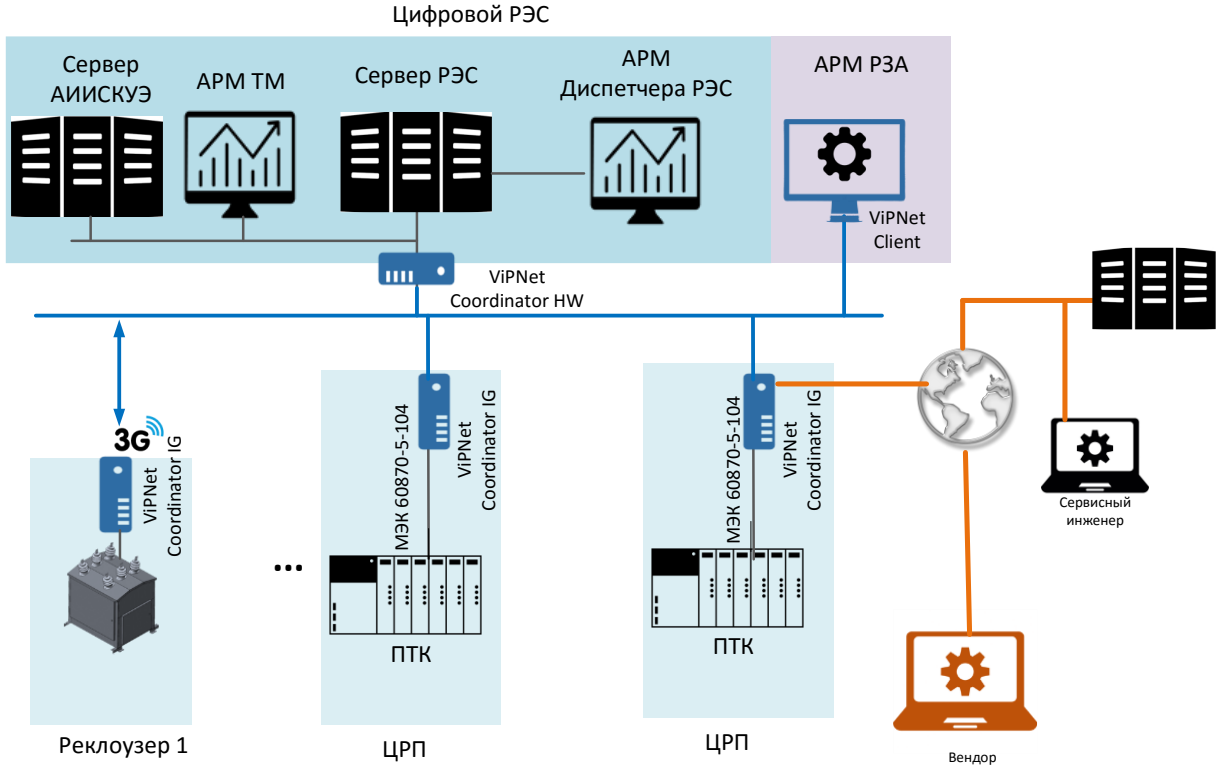
Угроза перехвата управления АСУ ТП



Защищенное обновление ПО PLC

Решение: часть 1

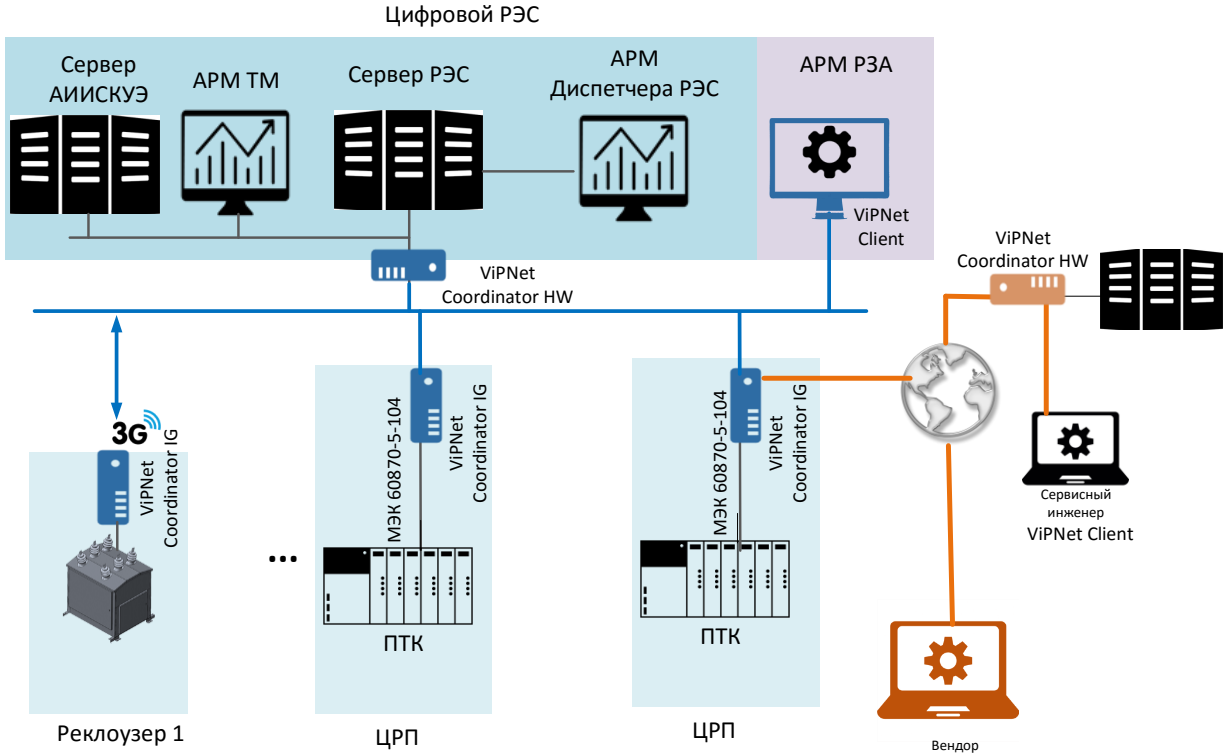
1. Осуществляем сегментацию сети
2. Защищаем сегменты от несанкционированного доступа из технологической сети.
3. Защищаем каналы передачи информации между сегментами с помощью VPN



Защищенное обновление ПО PLC

Решение: часть 2

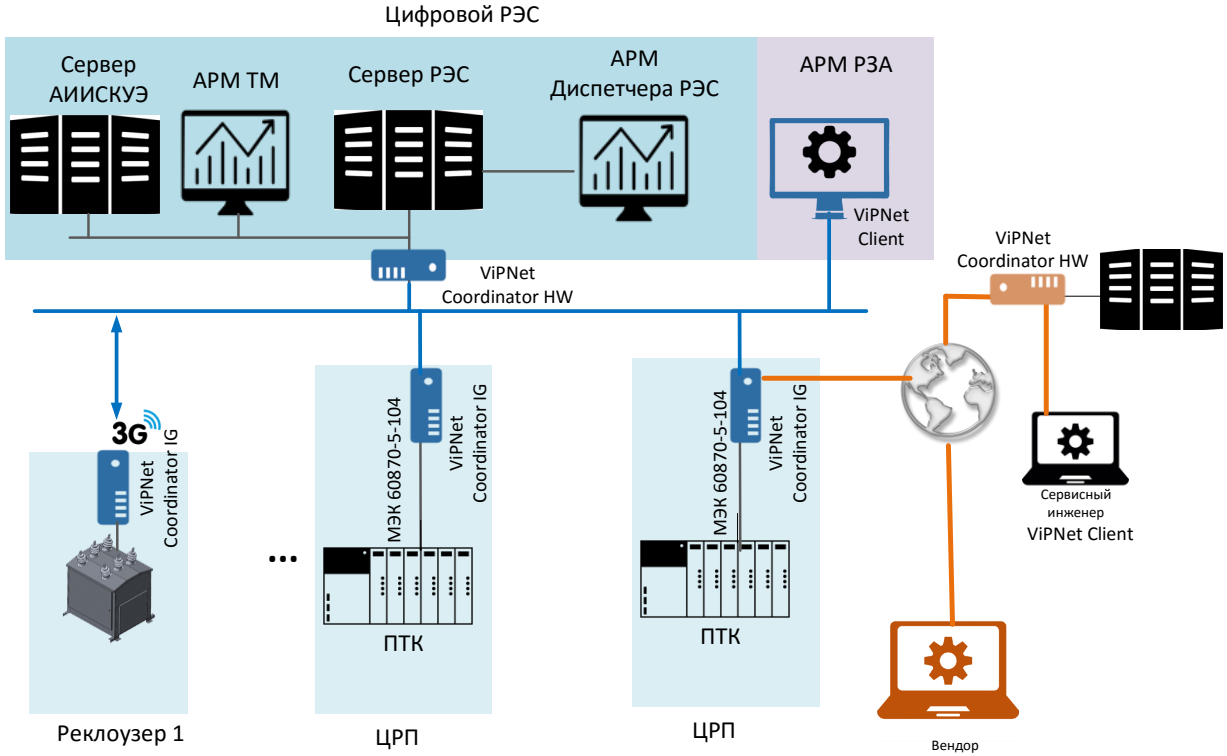
1. Устанавливаем защищенный канал от центрального сервисного центра до ЦРП и реклоузеров
2. Устанавливаем защищенный канал между мобильным АРМ Сервисного инженера, ЦРП и реклоузером



Защищенное обновление ПО PLC

Решение: часть 3

1. Регистрируем ViPNet Coordinator IG как МЭ типа Д
2. Настраиваем для штатного режима ViPNet Coordinator IG разрешающее правило МЭК 60870-5-104
3. Настраиваем для регламентного обслуживания разрешающие правила фильтрации МЭК 60870-5-104 и HTTP



Защищенное обновление ПО PLC

	МЭ типа Д
Штатный режим	Правила штатного режима: All protocol block, Modbus Enable
Режим регламентного обслуживания	Правила штатного режима: All protocol block, Modbus Enable, HTTP Enable

Сценарий 5
Разделение ПАЗ и АСУ ТП Нефтеперерабатывающего завода

Разделение ПАЗ и АСУ ТП

Задача:

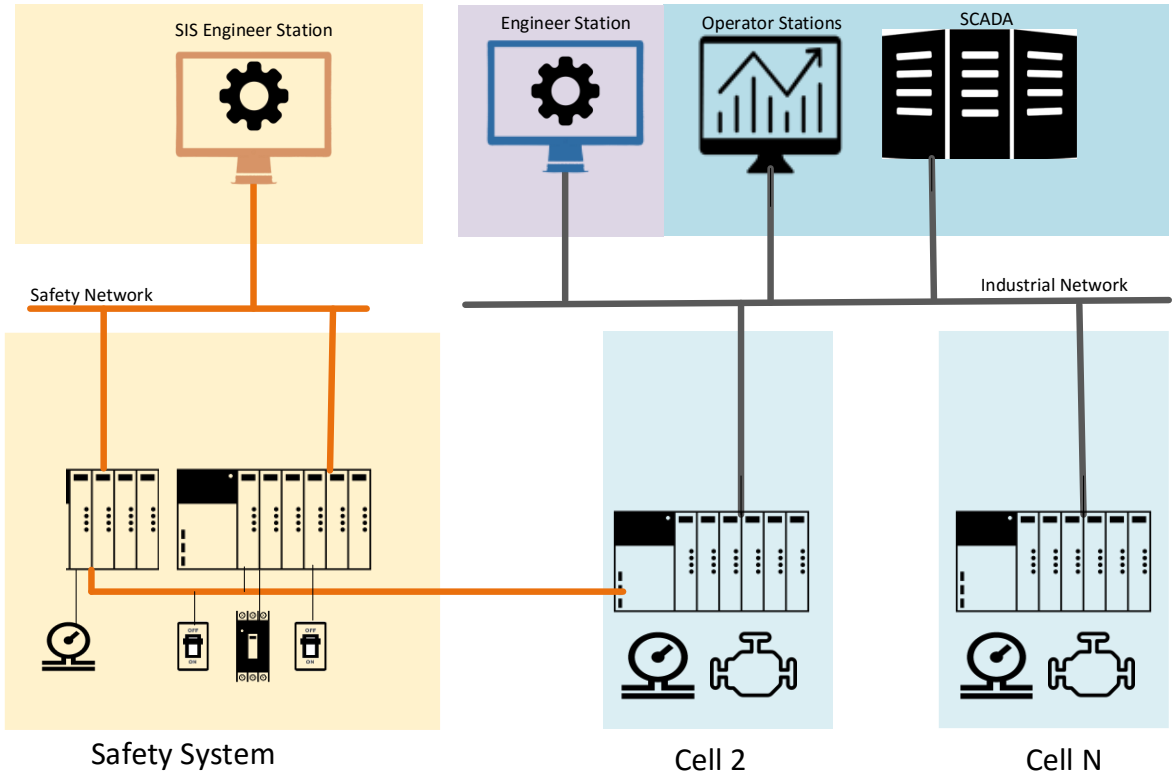
Есть нефтеперерабатывающий завод.

Передача в АСУ ТП идет по Modbus между контроллерами и SCADA.

ПАЗ с АСУ ТП связаны между собой по протоколу Modbus RTU.

Диагностика и обновление ПАЗ и АСУ ТП происходят по протоколу Modbus.

Требуется обеспечить информационную безопасность.



Разделение ПАЗ и АСУ ТП

Модель угроз:

Угроза изменения конфигурации АСУ ТП и ПАЗ

Угроза внедрения кода или данных в АСУ ТП и ПАЗ

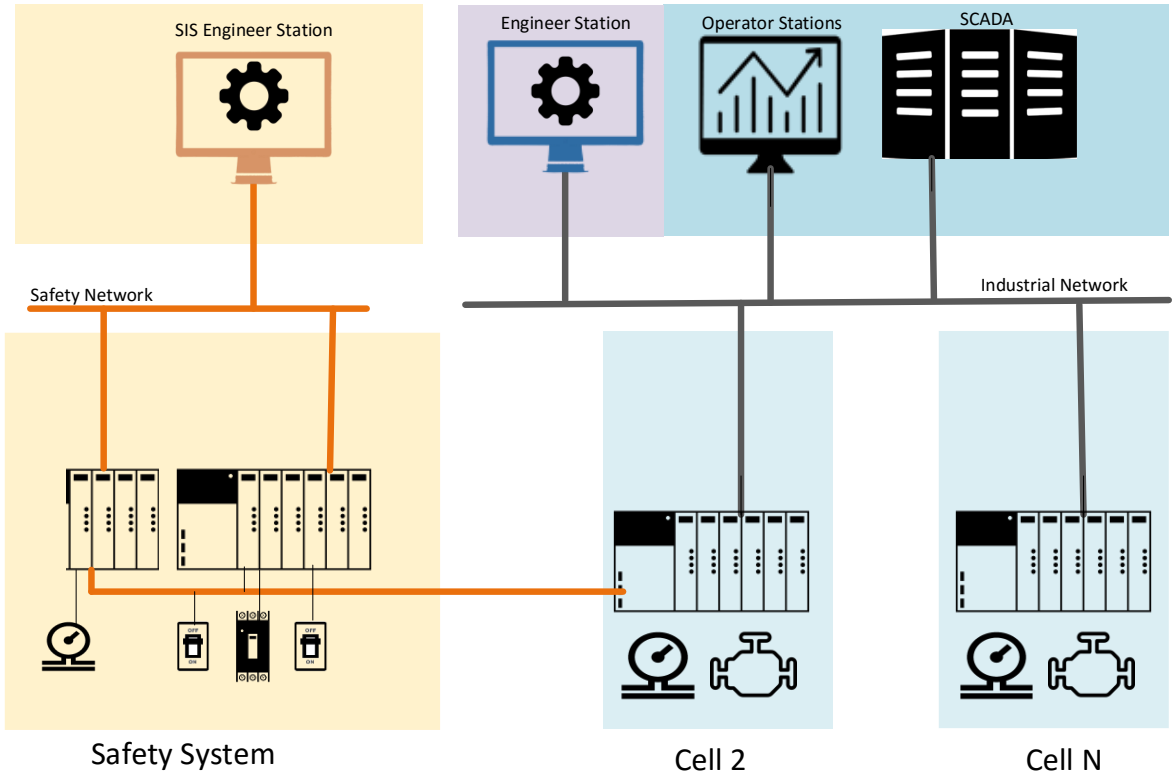
Угроза неправомерного действия в каналах

Угроза перехвата данных

Угроза подмены сетевого доступа

Угроза перехвата управления АСУ ТП

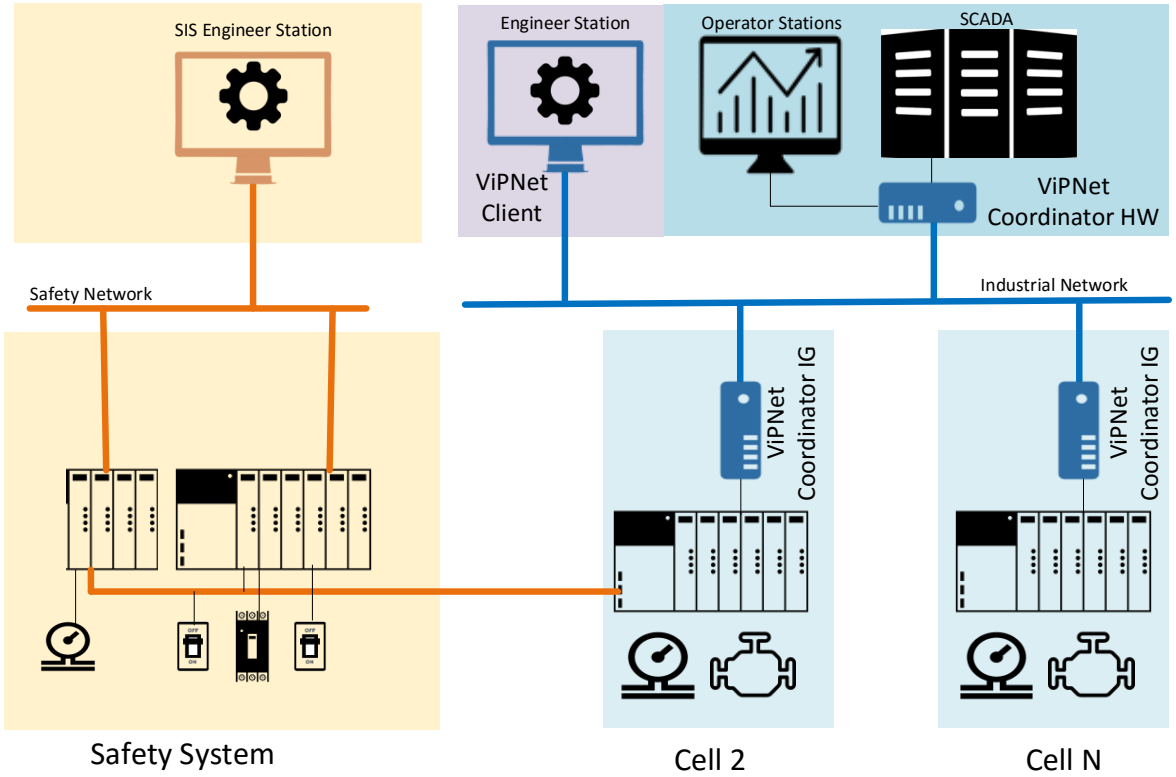
Угроза несанкционированного доступа в зону ПАЗ



Разделение ПАЗ и АСУ ТП

Решение: часть 1

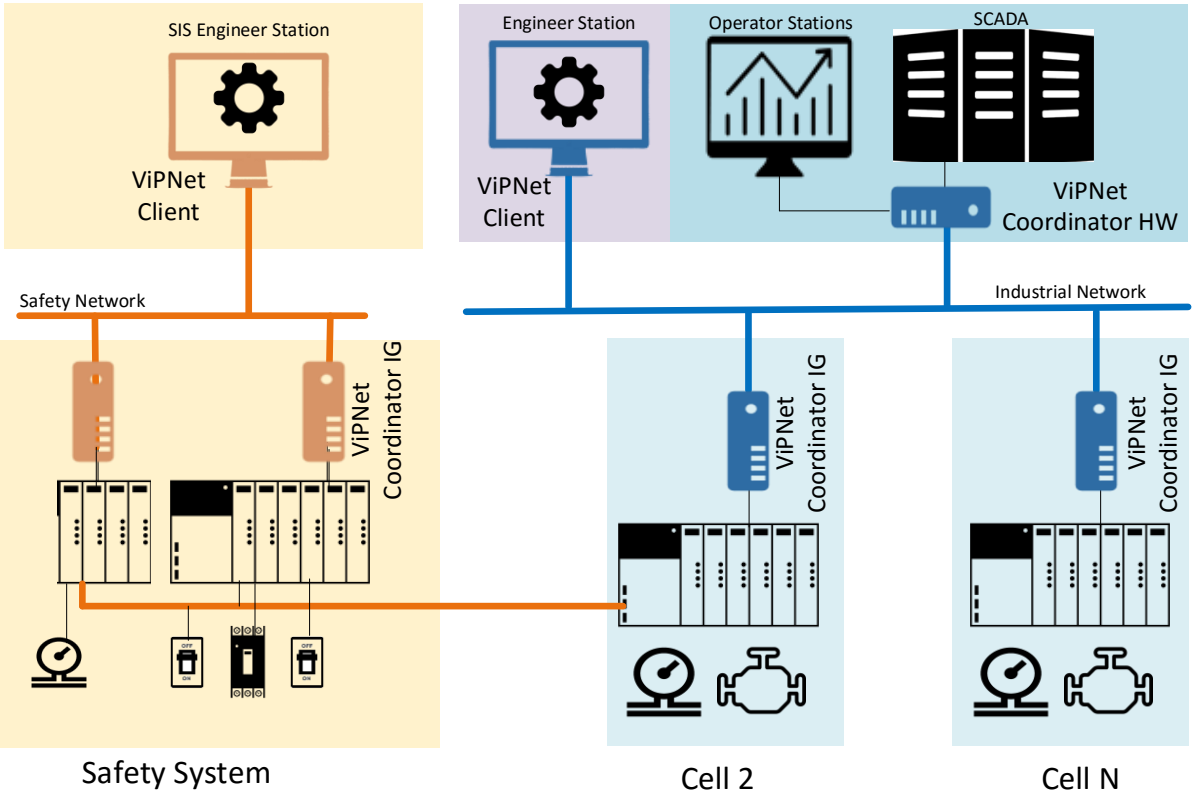
1. Осуществляем сегментацию сети АСУ ТП
2. Защищаем сегменты от несанкционированного доступа из технологической сети.
3. Защищаем каналы передачи информации между сегментами с помощью VPN



Разделение ПАЗ и АСУ ТП

Решение: часть 2

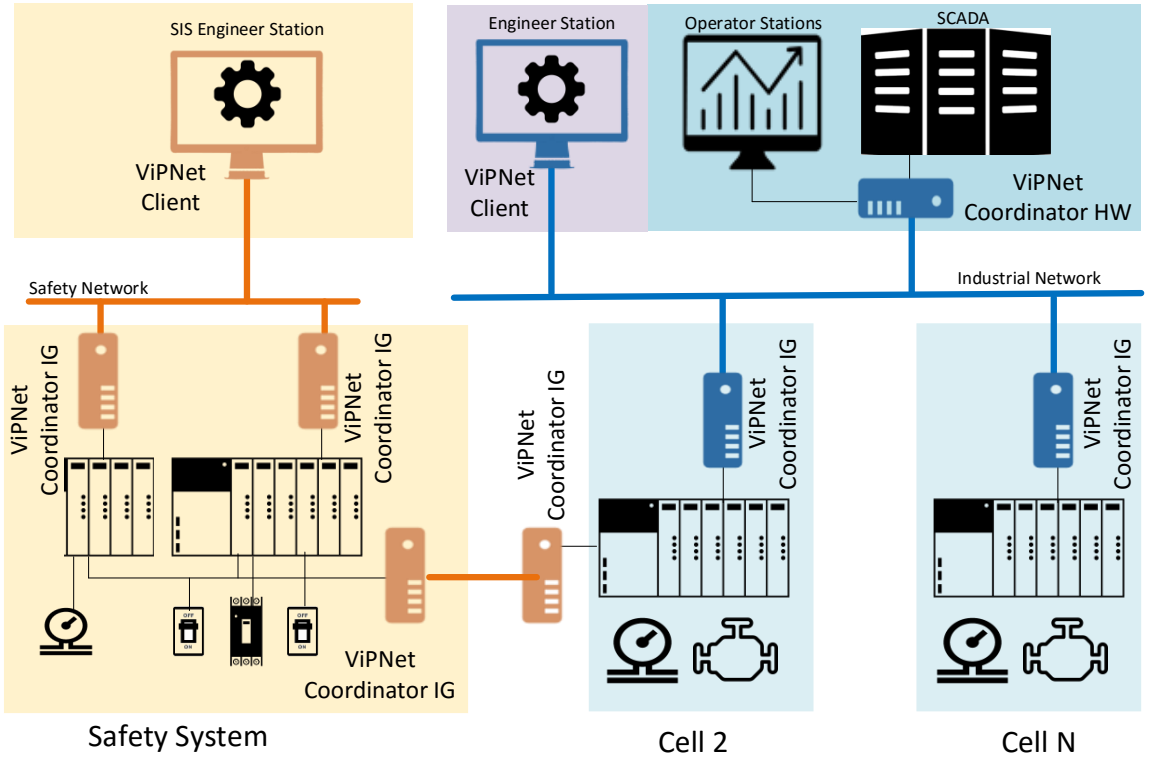
1. Осуществляем сегментацию сети ПАЗ
2. Защищаем сегменты от несанкционированного доступа из технологической сети.
3. Защищаем каналы передачи информации между сегментами с помощью VPN

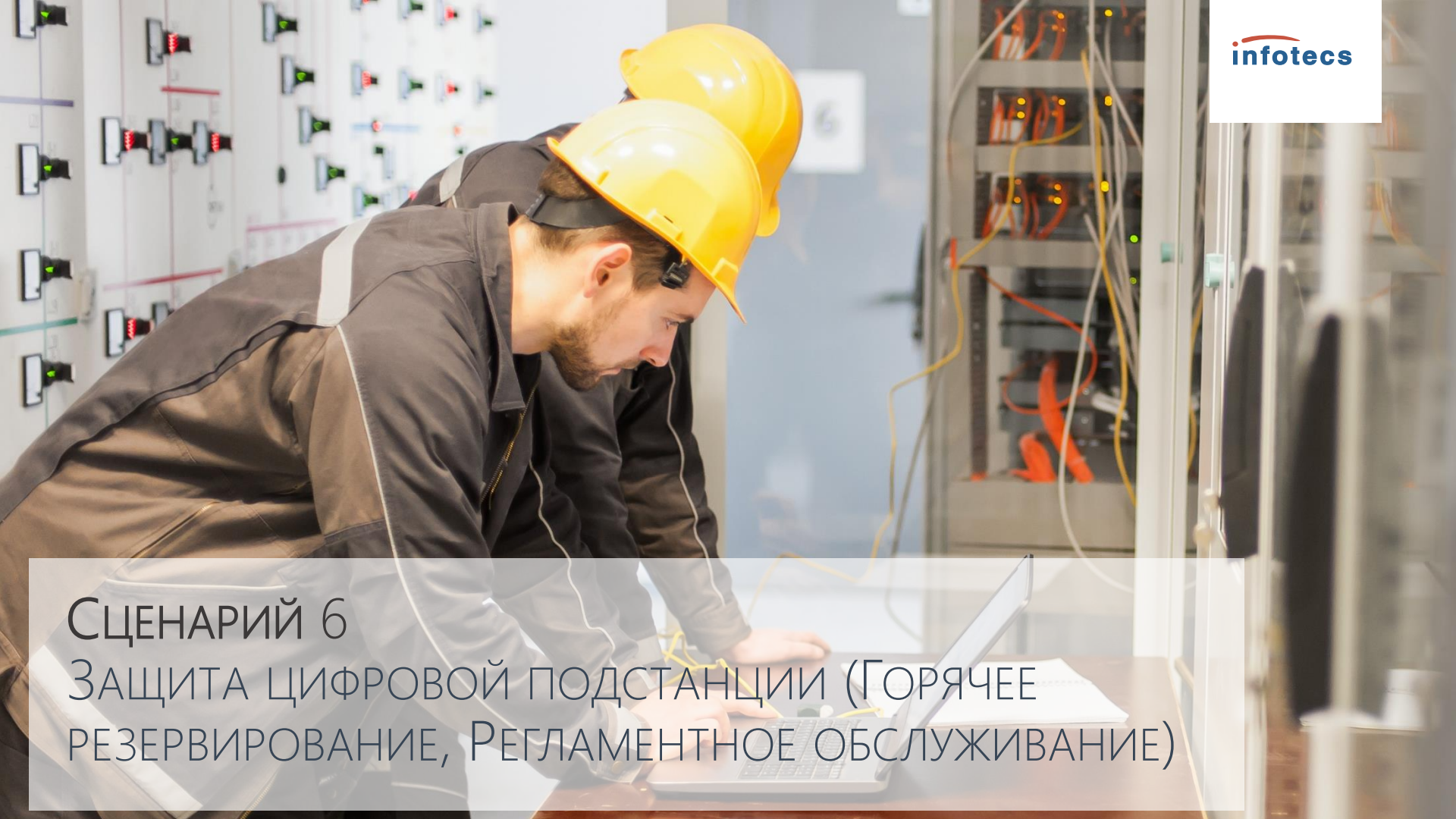


Разделение ПАЗ и АСУ ТП

Решение: часть 3

1. Отделяем ПАЗ от АСУ ТП с помощью двух ViPNet Coordinator IG в режиме шлюзов Modbus TCP/RTU. Один шлюз настроен как Modbus rtu-to-tcp, а второй как tcp-to-rtu
2. Защищаем канал между двумя ViPNet Coordinator IG между ПАЗ и АСУ ТП
3. Создаем одно разрешающее правило для протокола Modbus
4. Настраиваем DPI для Modbus на обоих ViPNet Coordinator IG: адрес устройства + коды команды





Сценарий 6
Защита цифровой подстанции (Горячее резервирование, Регламентное обслуживание)

Защита цифровой подстанции (Горячее резервирование, Регламентное обслуживание)

Задача:

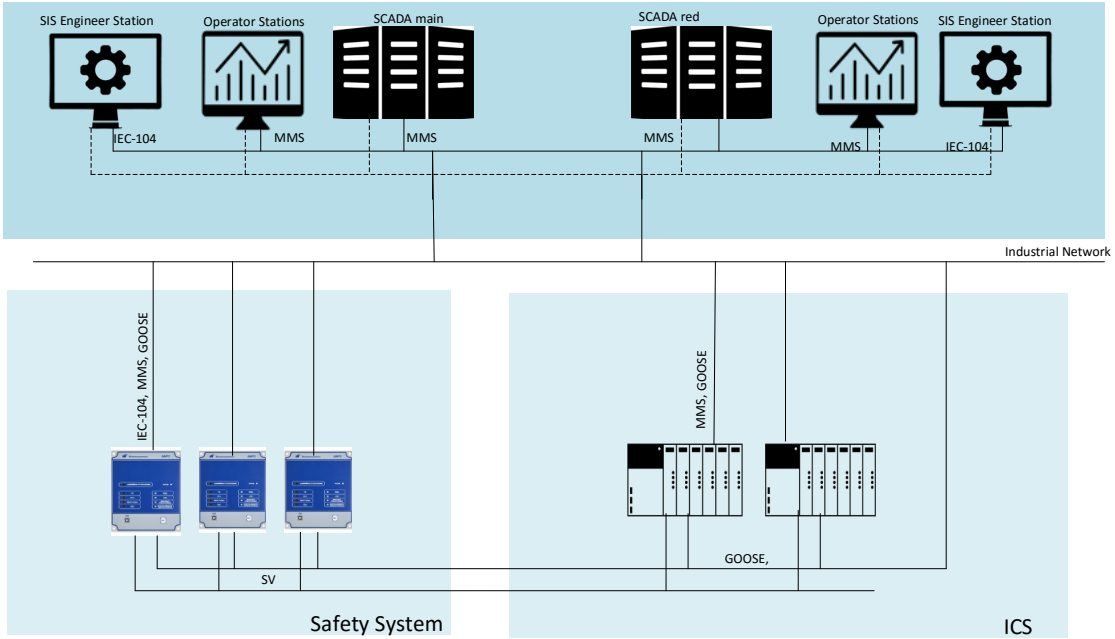
Есть Цифровая подстанция.

Передача информации между РЗА и оперативно-диспетчерским уровнем осуществляется по MMS и МЭК60870-5-104.

Передача информации между контроллером ТМ и оперативно-диспетчерским уровнем осуществляется по MMS и МЭК60870-5-104.

Устройства автоматизации конфигурируются по Mobdus

Требуется обеспечить информационную безопасность.



Защита цифровой подстанции (Горячее резервирование, Регламентное обслуживание)

Модель угроз:

Угроза изменения конфигурации АСУ ТП и РЗА

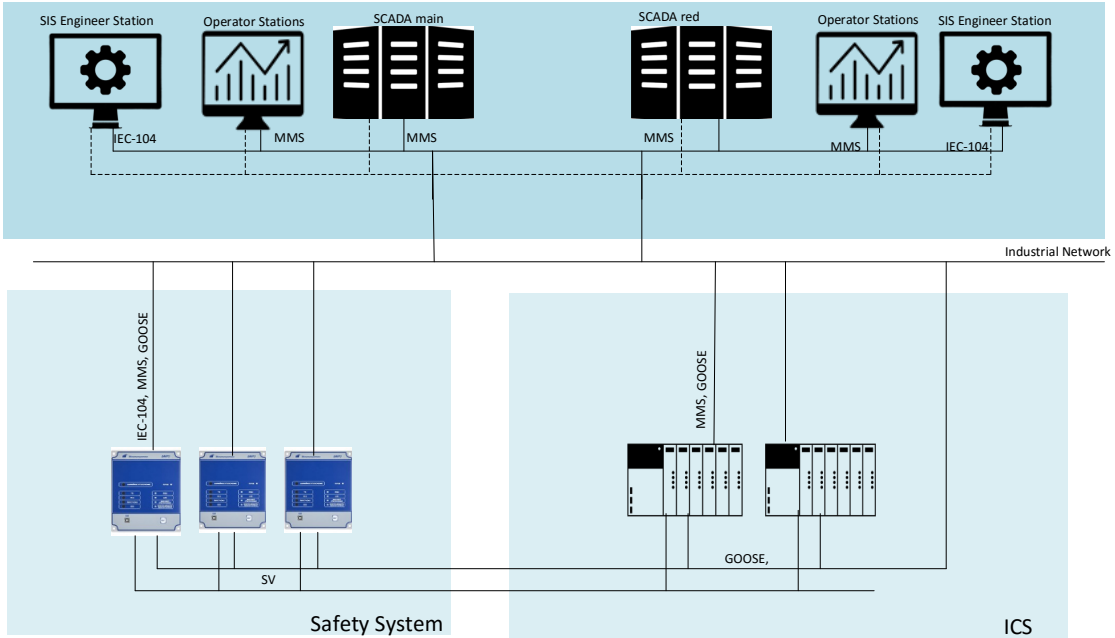
Угроза внедрения кода или данных в АСУ ТП и РЗА

Угроза неправомерного действия в каналах

Угроза перехвата данных

Угроза подмены сетевого доступа

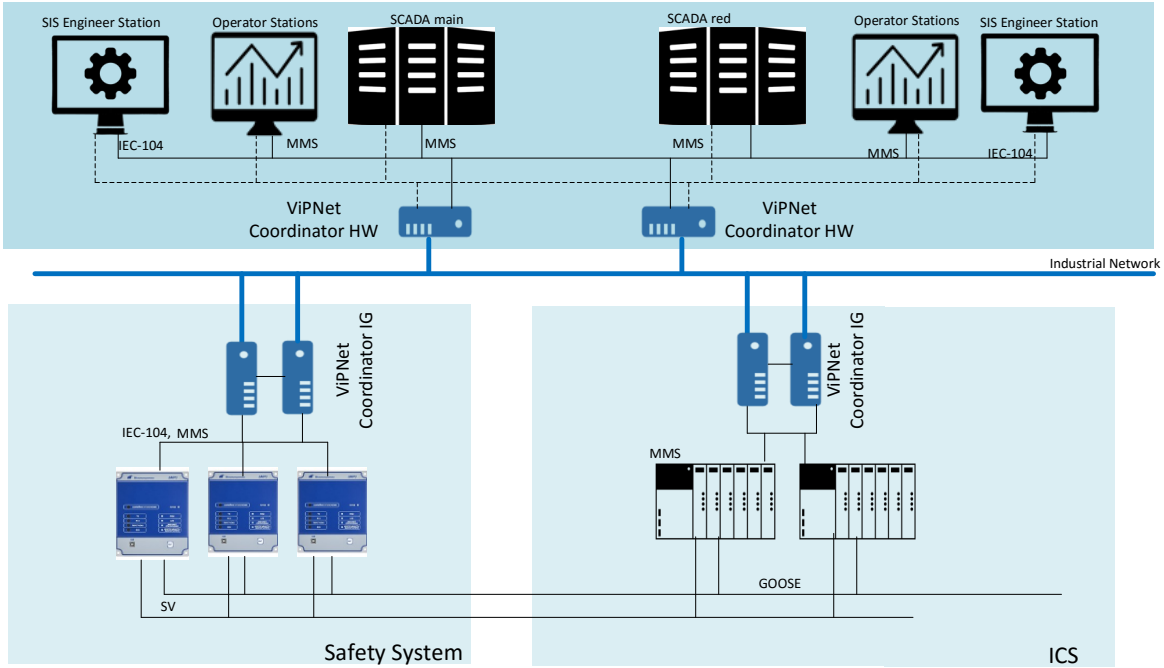
Угроза перехвата управления АСУ ТП и РЗА



Защита цифровой подстанции (Горячее резервирование, Регламентное обслуживание)

Решение: часть 1

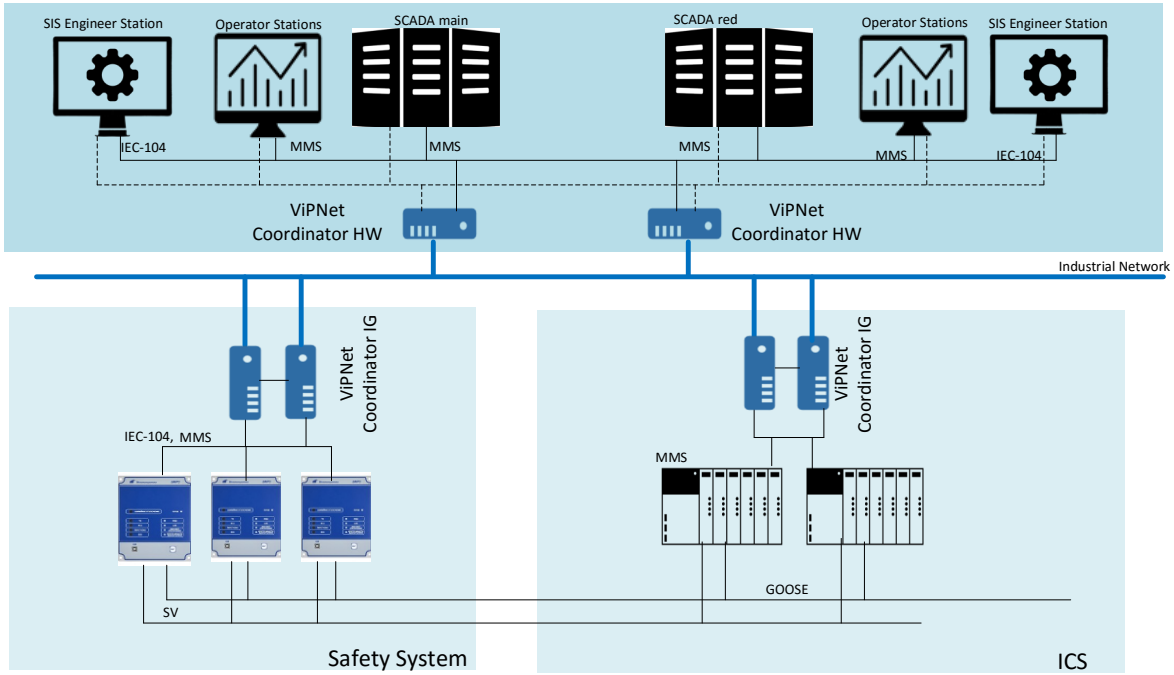
1. Разделяем сети MMS и GOOSE
2. Защищаем сегмент сети оперативно-диспетчерской службы от несанкционированного доступа



Защита цифровой подстанции (Горячее резервирование, Регламентное обслуживание)

Решение: часть 2

1. Защищаем сегмент РЗА от несанкционированного доступа, обеспечиваем горячий резерв
2. Подключаем «красную кнопку» аварийного режима к GPIO ViPNet Coordinator IG
3. Настраиваем фильтр для регламентных режимов ViPNet Coordinator IG для сегмента РЗА - Modbus разрешен
4. Настраиваем фильтр для специальных режимов ViPNet Coordinator IG для сегмента РЗА - разрешить все



Сценарий 7
Подключение старых устройств к системе мониторинга

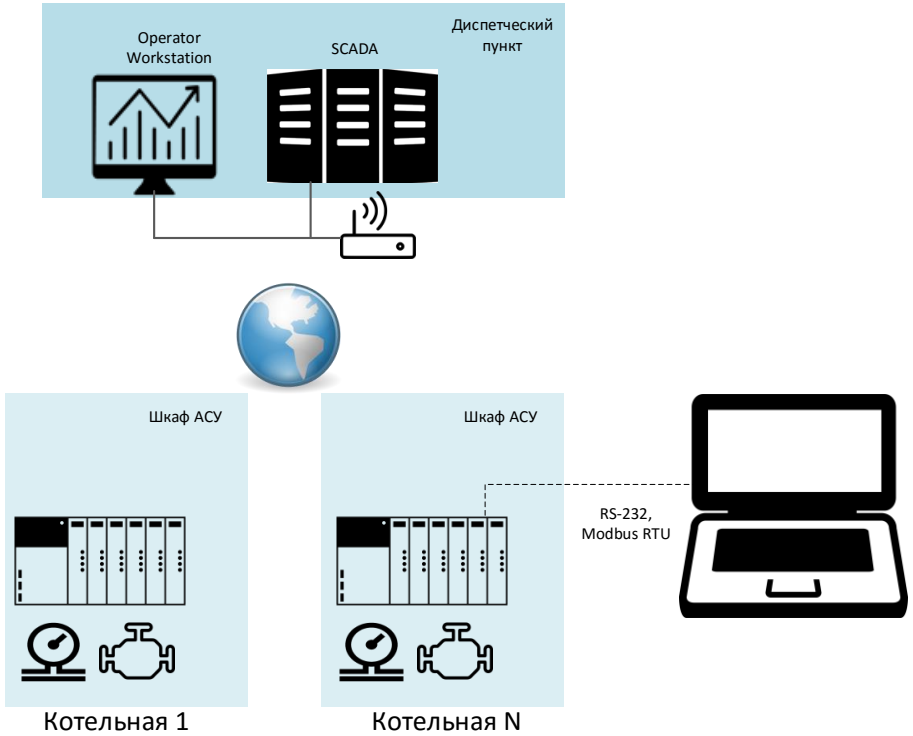
Подключение старых устройств к системе мониторинга

Задача:

Есть несколько Котельных. В шкафах котельных стоит контроллер, режимы работы которого можно отслеживать локально по Modbus RTU по интерфейсу RS-232/485 .

Планируется модернизация системы, в ходе которой мониторинг работы оборудования будет вестись дистанционно. В качестве канала передачи решено выбрать беспроводной канал GSM.

Требуется обеспечить информационную безопасность и минимизировать стоимость.



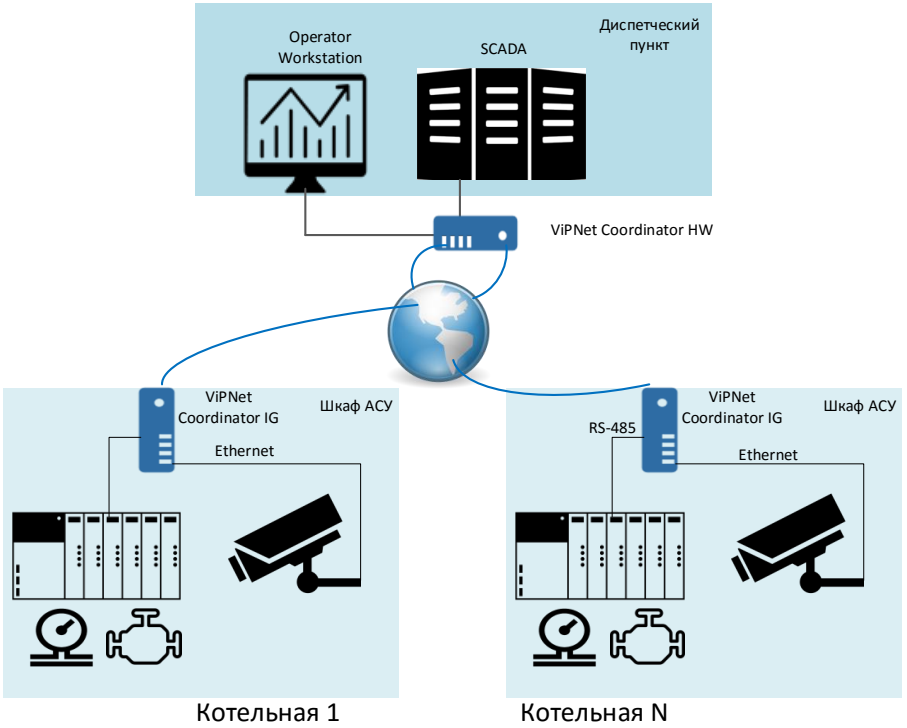
Подключение старых устройств к системе мониторинга

Решение:

В диспетчерском пункте устанавливается криптошлюз ViPNet Coordinator HW, который тунелирует оборудование сети.

В котельной устанавливается ViPNet Coordinator IG, к которому по RS-485 или RS-232 подключается имеющийся контроллер. Настраивается шлюз Modbus RTU/TCP. По Ethernet каналу подключает видеокамера наблюдения.

Устанавливается защищенный канал между ViPNet Coordinator HW и ViPNet Coordinator IG.



Суммируем сценарии:

- Защита цифрового периметра промышленной сети
- Сегментация сети и защита доступа к сегменту
- Удаленный защищенный доступ к сегменту и его оборудованию
- Защищенные каналы для беспроводных сетей
- Защищенный канал между сегментами сети, в том числе для распределенных систем
- Защищенный канал для последовательных сетей
- Телеуправление и телеконтроль - защищенный удаленный мониторинг и управление
- Телесервис – удаленное сервисное обслуживание
- Удаленный защищенный доступ с мобильных устройств для конфигурирования и обслуживания устройств внутри защищенного сегмента

Соответствие мерам Приказа ФСТЭК №239 и №31

Можно закрыть

~46%

мер


infotecs
Спасибо!
Marina.Sorokina@infotecs.ru
Марина Сорокина