Платформа граничных вычислений Siemens Industrial Edge

Перспективы и безопасность

Александр Лифанов

SIEMENS

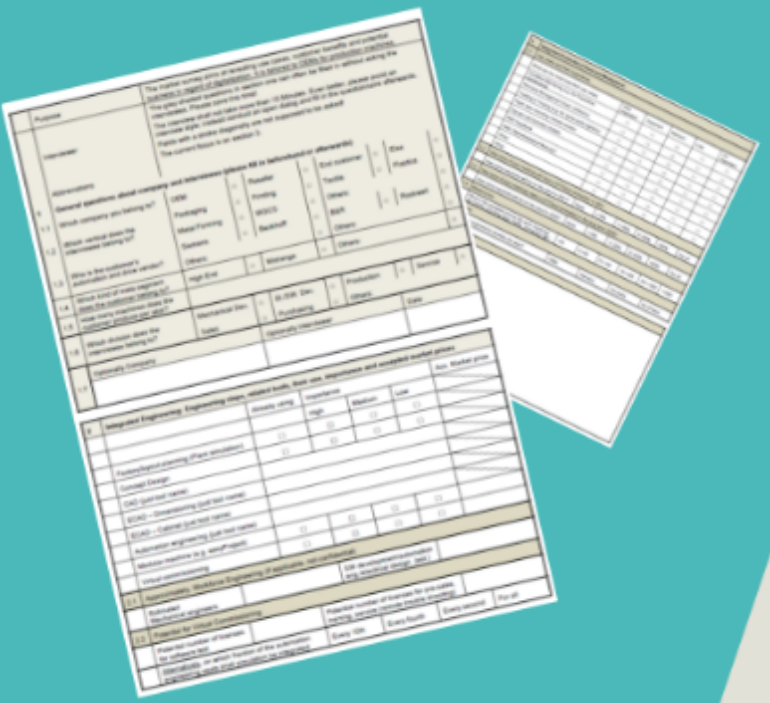
Industrial Edge Архитектура и назначение

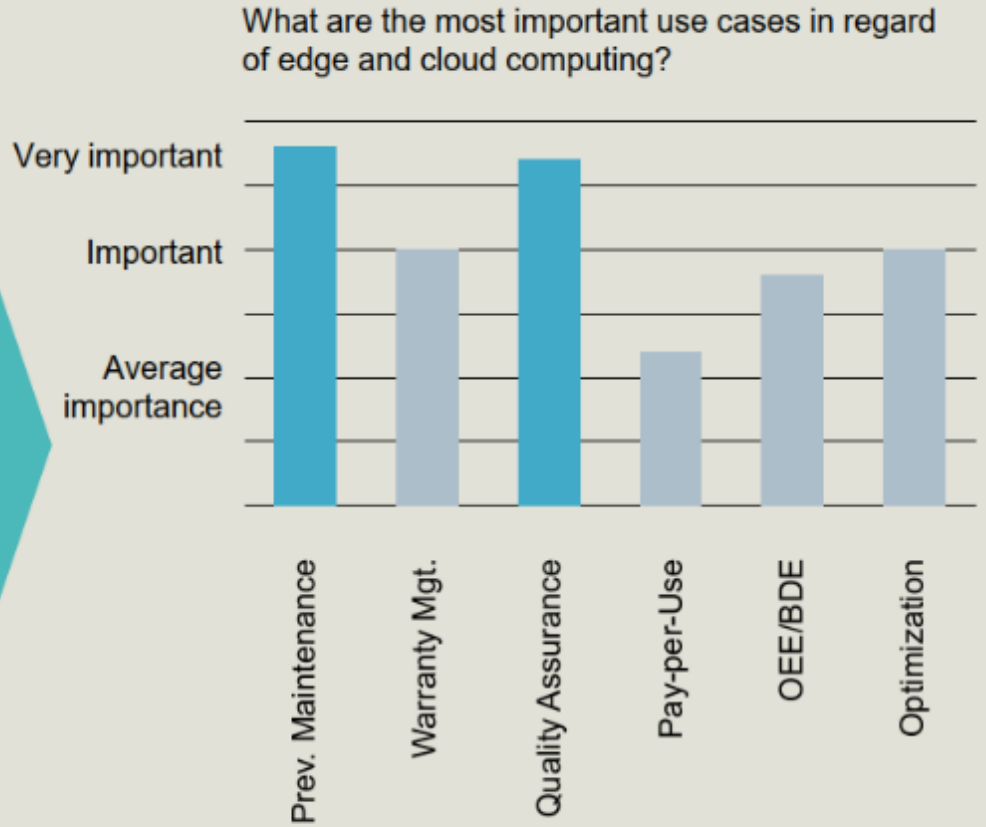
SIEMENS

Industrial Edge
Драйверы появления

Customer interviews:

- More than 70 customer interviews





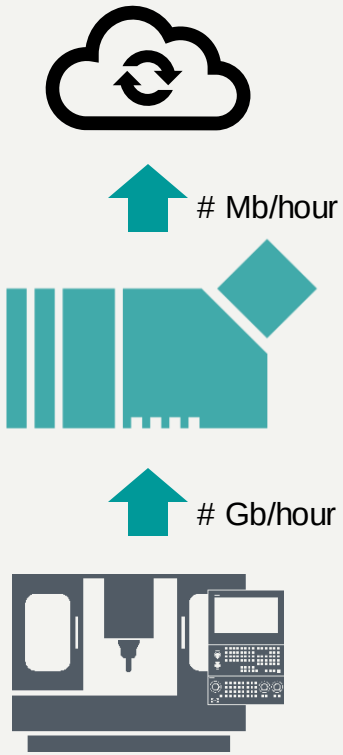
Example OEE

Example Prev. Maintenance (on the basis of high frequent drive/controller data)

SIEMENS

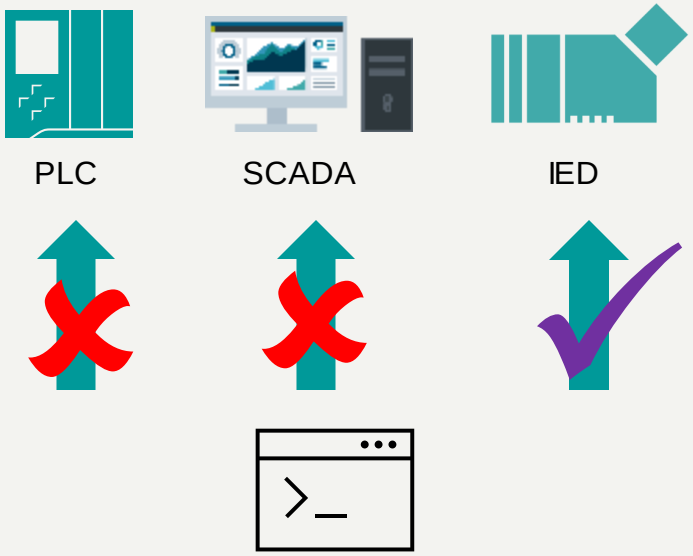
Industrial Edge
Драйверы появления

1. Обработка (прореживание) высокочастотных данных



2. «Не трожь работающую систему»

(уменьшение воздействия непроизводственных алгоритмов на производящие системы)

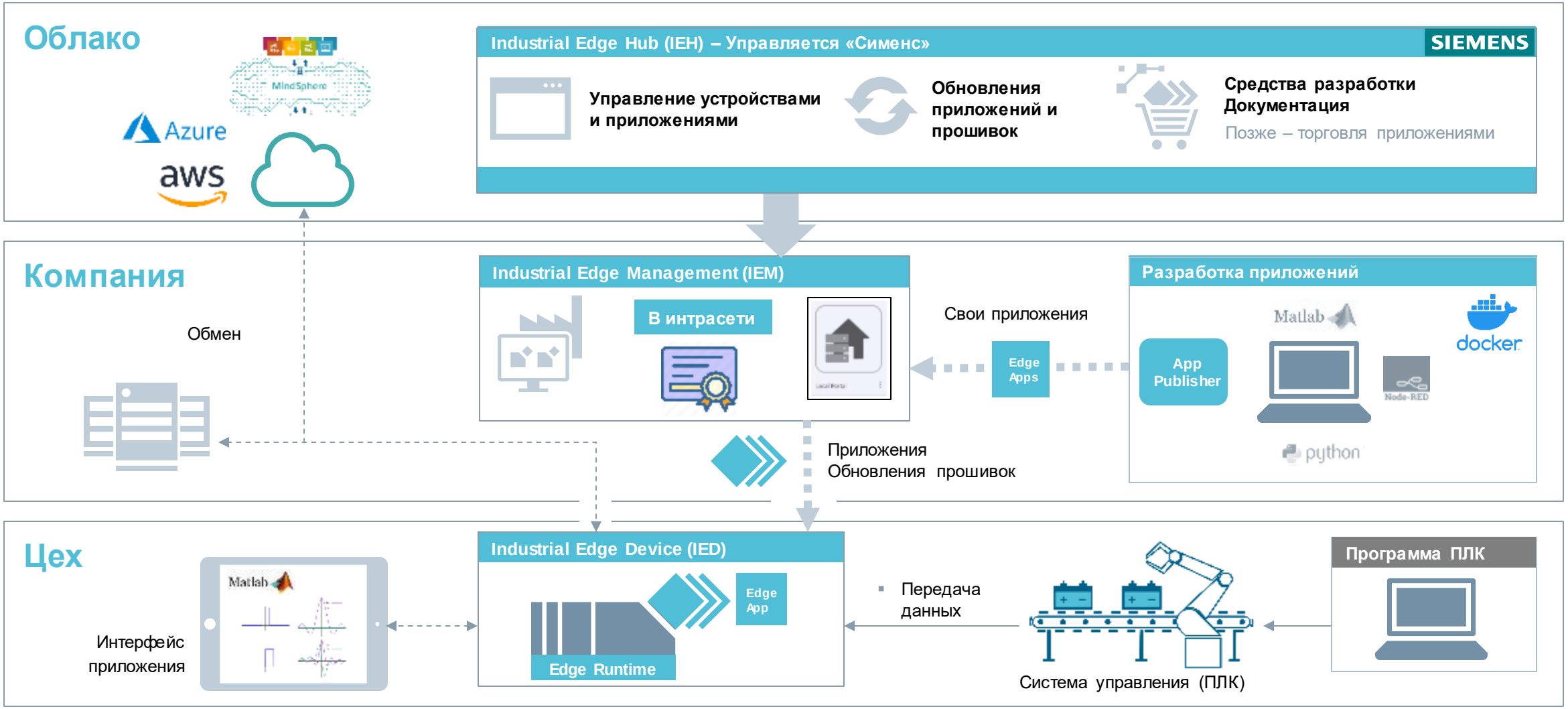


3. Территориально распределенные задачи

(замена поездок на удаленный доступ)

SIEMENS

Industrial Edge
Архитектура системы



SIEMENS

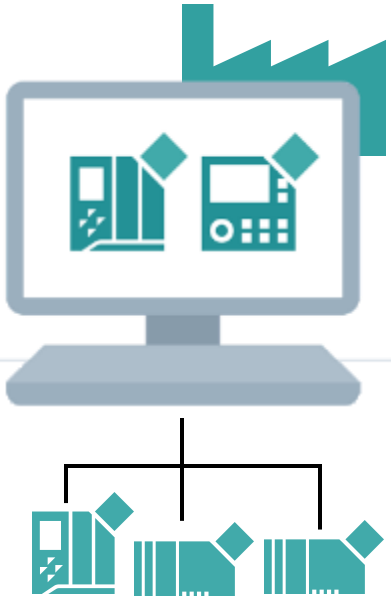
Industrial Edge
Варианты развертывания

Масштабы системы

Unified Comfort Panel – выпуск с 04/2020

Остальные устройства – нет понимания

Ограниченно доступно с 09/2020
В России пока не поставляется (legal issue)



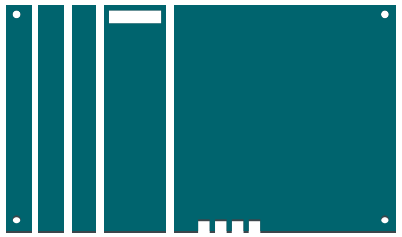
План на версию 2.0 – осень-зима 2021

Локальное управление — **Управление в интрасети** — **Управление в облаке** — **Интеграция с ИТ**

SIEMENS

Industrial Edge
Основные платформы для IED

Промышленные ПК как чисто Edge-устройства



EDGE

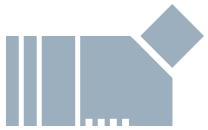
Контроллеры с Edge-функциональностью

Автоматика

EDGE

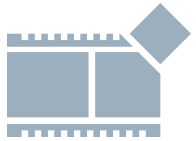
Будущие Edge-устройства

IPC127E



IPC227E
IPC427E

IPC647E



IOT2050

Open Controller

Unified
Comfort Panel

S7-1500
with TM MFP

SCALANCE/
RUGGEDCOM

SIEMENS

Industrial Edge
Облегчение труда разработчика

Разработчик – <u>много задач</u> помимо основной

Весь комплекс исходного кода для решения задачи
Классическая процедура разработки

Безопасность, связь, визуализация…

Сборка и развертывание

- Упр.контейнерами
- Упр.прошивками
- ОС
- HW – промПК

Поддержка ОС

- ОС
- HW – промПК

- HW – промПК

Проектирование плат, сборка в корпус

Большие трудозатраты до, в процессе и после запуска:
Разработка, обновление ОС, обновления прикладного ПО

VS.

Разработчик – <u>фокусиру-ется на основной задаче</u>

Приложения Edge

- …
- App SDK
- Data bus и семантика
- Магазин приложений
- Упр. приложениями
- Безопасность
- Упр. контейнерами
- Упр. прошивками
- OS – Linux
- HW – Simatic

Industrial Edge

Всё кроме прикладного кода разработано и отлажено

SIEMENS

Industrial Edge
Приложение Industrial Vulnerability Manager

Шаг 2: Edge-приложение Industrial Vulnerability Manager регулярно обновляет БД уязвимостей с центрального сервера, отправляя только номер лицензии.

SIEMENS

Более 80,000 компонентов:

open source initiative
ubuntu
debian
SIEMENS
Microsoft
И др.!
IBM
...

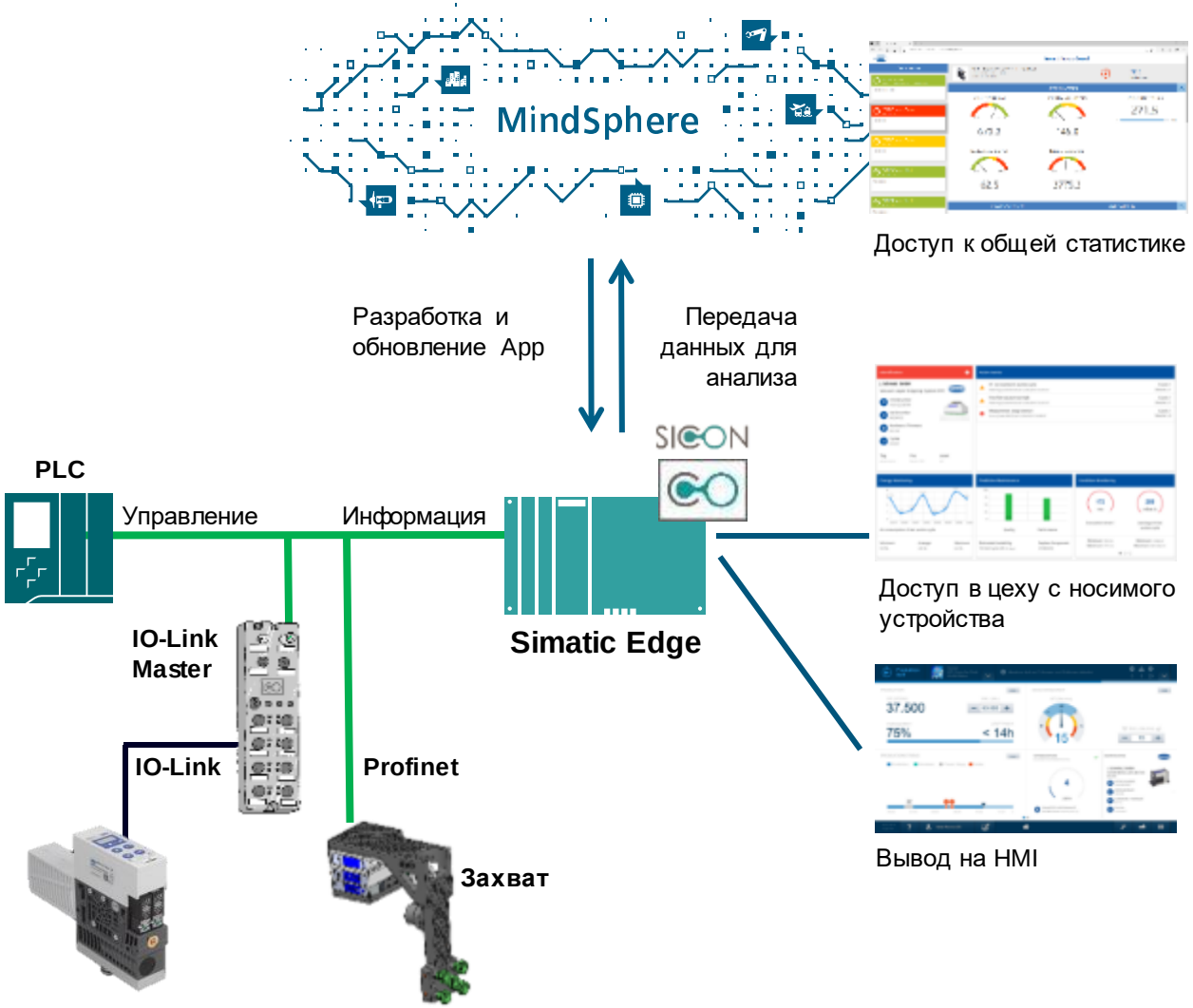
Условие:
Есть публичная информация об этом оборудовании и уязвимостях прошивок.

Детали:

- Industrial Vulnerability Manager скачивается и обновляется с сервера Siemens, работает внутри интрасети конечного пользователя.
- БД пополняется из официальных источников, от вендоров (вкл 3rd party) и из коммьюнити.
- Вся информация об оборудовании и его прошивках остается в интрасети предприятия.
- За реагирование на выдаваемые рекомендации отвечает пользователь.

SIEMENS

Industrial Edge
Пример применения: Schmalz

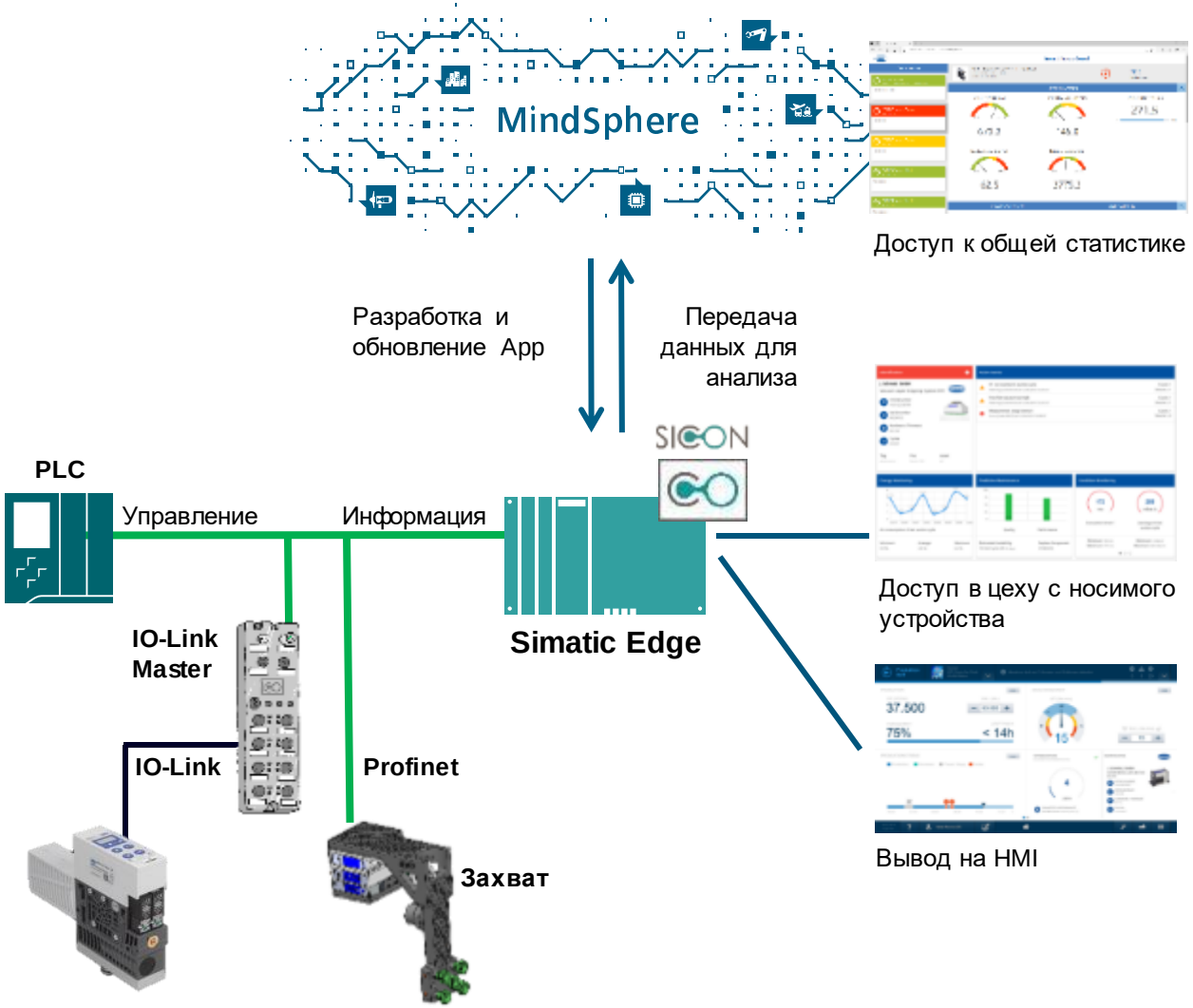


Schmalz – вакуумные захваты

- Проблема износа резины на присосках
- Проблема засорения фильтров вакуум-генераторов
- Предупредительное обслуживание оборудования заказчика

SIEMENS

Industrial Edge
Пример применения: Schmalz



Уровень облака

- Хранение телеметрии
- Удаленная техподдержка
- Анализ дефектов из исторических данных

Уровень Edge

- Агрегация и буферизация данных
- Местная аналитика
- Стандартные интерфейсы для данных и HMI
- Автоматическое подключение к Mindsphere

Уровень устройства

- Сбор, масштабирование, именование данных
- Формирование сообщений
- Связь через IO-Link или Profinet

SIEMENS

Industrial Edge Безопасность

SIEMENS

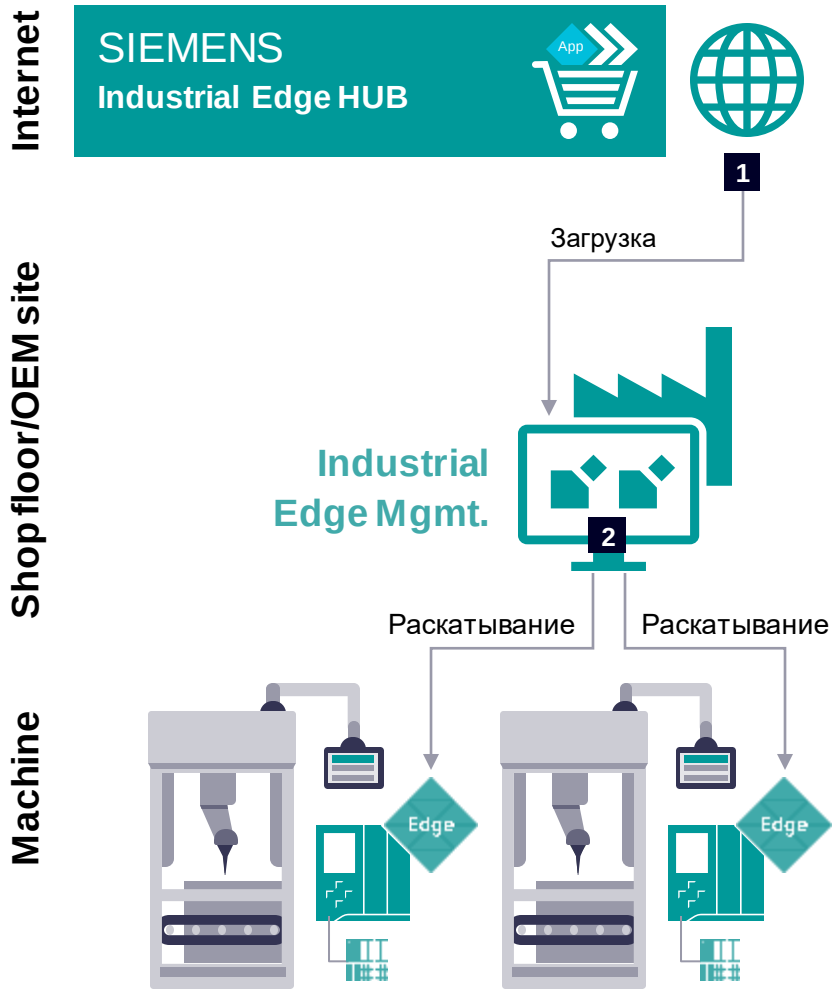
Industrial Edge
Компоненты безопасности отдельных элементов

Прикладное ПО	Изоляция контейнеров	Подписывание кода с сертификатами	Аутентификация с сертификатами	Безопасное подключение новых устройств
Операционная система	SE Linux	Root-доступ закрыт	Безопасная загрузка	Безопасные обновления
Аппаратура	Полное шифрование диска	Trusted Platform Module	Шифрование коммуникаций	Аппаратные сертификаты устройств

Запланирована сертификация Industrial Edge на соответствие IEC 62443.

SIEMENS

Industrial Edge
Направление коммуникаций



IE HUB

Обновления и приложения

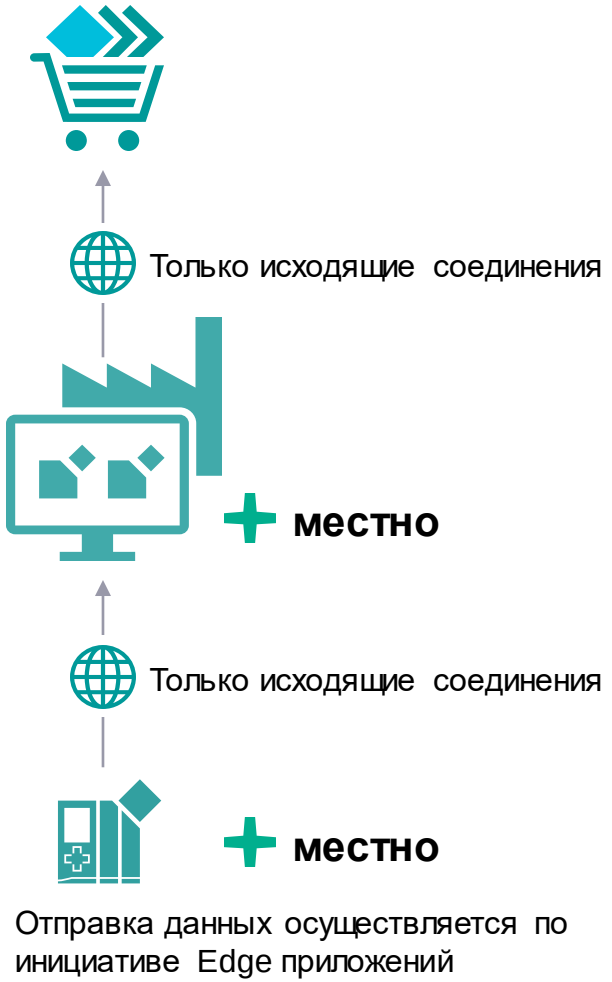
IE Management

Управление IED

Раскатывание приложений и конфигураций

IE Device

Исполнение приложений



Отправка данных осуществляется по инициативе Edge приложений

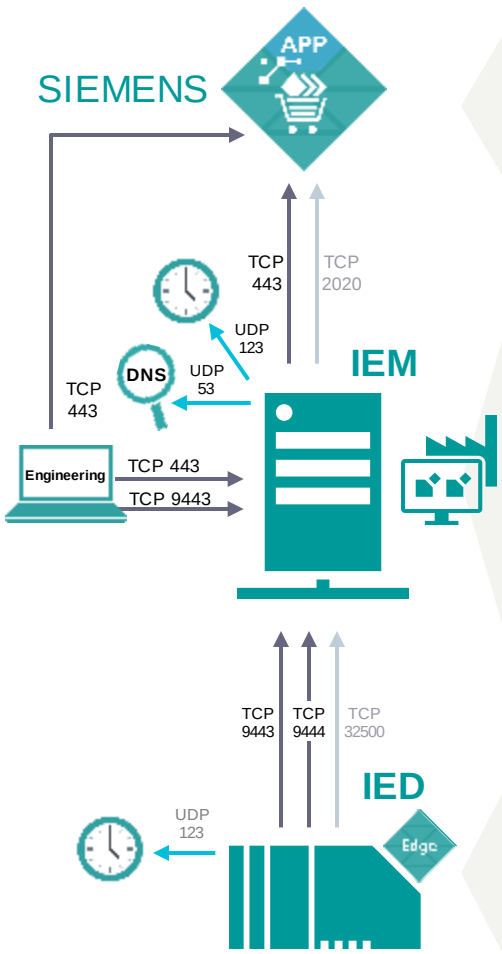
SIEMENS

Industrial Edge
Документированность соединений

Internet

Shop floor

Machine



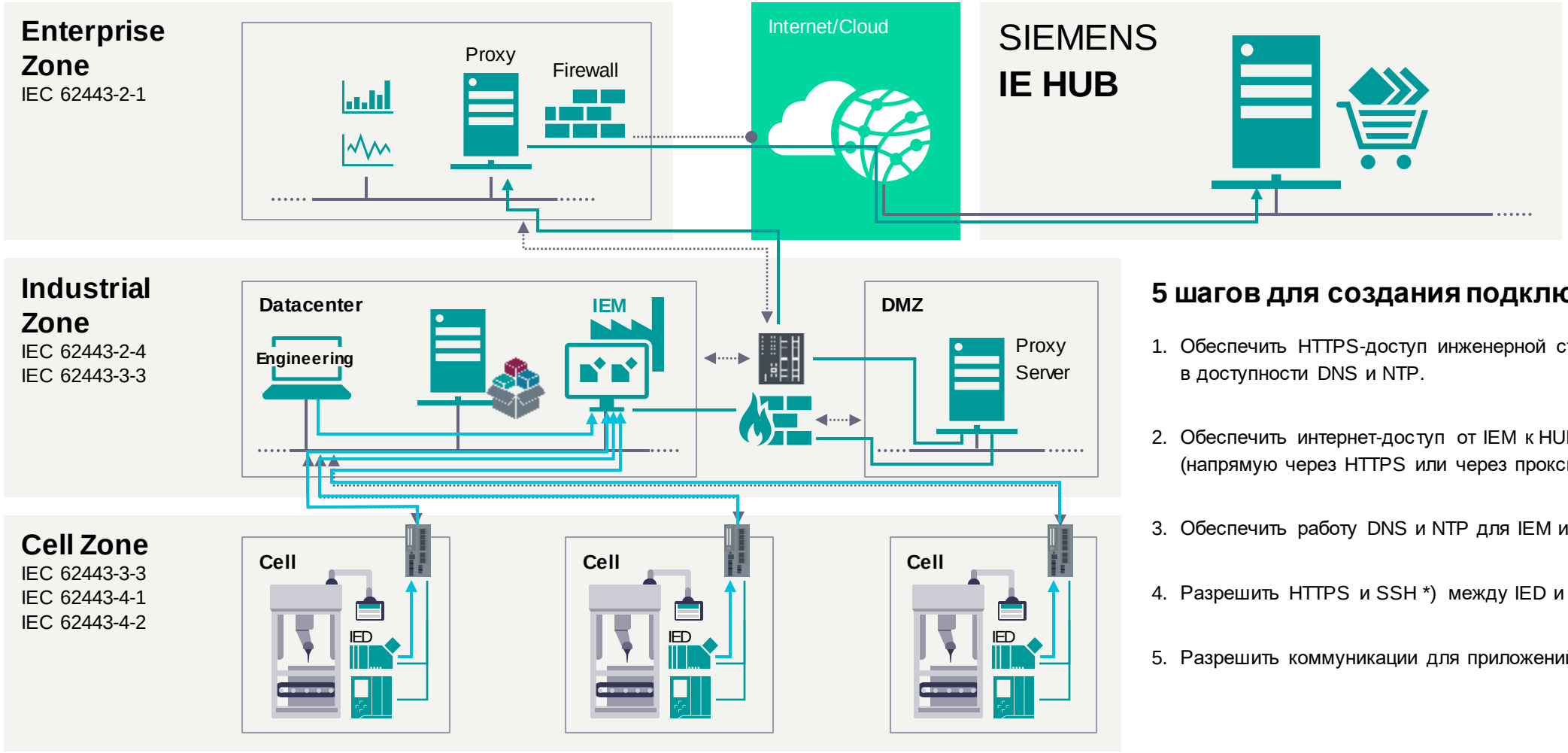
Dst. Port	Direction	Source	Destination	Mandatory	Description
TCP 443	Inbound	Engineering	iehub.eu1.edge.siemens.cloud	Recomm.	HTTPS access (Engineering ➔ HUB)
TCP 443	Inbound	IEM	portal.eu1.edge.siemens.cloud portalhub.eu1.edge.siemens.cloud artifacts.eu1.edge.siemens.cloud	Yes	HTTPS access (IEM ➔ HUB)
TCP 2020	Inbound	IEM	portal-relay.eu1.edge.siemens.cloud	No	Siemens remote support (IEM ➔ HUB)

Dst. Port	Direction	Source	Destination	Mandatory	Description
TCP 443	Inbound	Engineering	IEM	Yes	Configuration (OS UI)
TCP 9443	Inbound	Engineering	IEM	Yes	Configuration (Mgmt. UI)
TCP/ UDP 53	Outbound	IEM	DNS Server	Yes	Domain Name Resolution
UDP 123	Outbound	IEM	NTP Server	Yes.	NTP Time Synchronization
TCP 443	Outbound	IEM	portal.eu1.edge.siemens.cloud portalhub.eu1.edge.siemens.cloud artifacts.eu1.edge.siemens.cloud	Yes	HTTPS access (IEM ➔ HUB)
TCP 9443	Inbound	IED	IEM	Yes	Edge device access
TCP 9444	Inbound	IED	IEM	Yes	Edge device access
TCP 32500	Inbound	IED	IEM	No	SSH Tunnel (IED ➔ IEM)
TCP 2020	Outbound	IEM	portal-relay.eu1.edge.siemens.cloud	No	Siemens remote support (IEM ➔ HUB)

Dst. Port	Direction	Source	Destination	Mandatory	Description
TCP 443	Inbound	Engineering	IED	Yes	Configuration access (Device UI)
UDP 123	Outbound	IED	NTP Server	Yes	NTP Time Synchronization
TCP 9443	Outbound	IED	IEM	Yes	HTTPS access (IED ➔ IEM)
TCP 9444	Outbound	IED	IEM	Yes	HTTPS access (IED ➔ IEM)
TCP 32500	Outbound	IED	IEM	No	SSH Tunnel (IED ➔ IEM)

SIEMENS

Industrial Edge
Сетевая конфигурация для внутреннего IEM



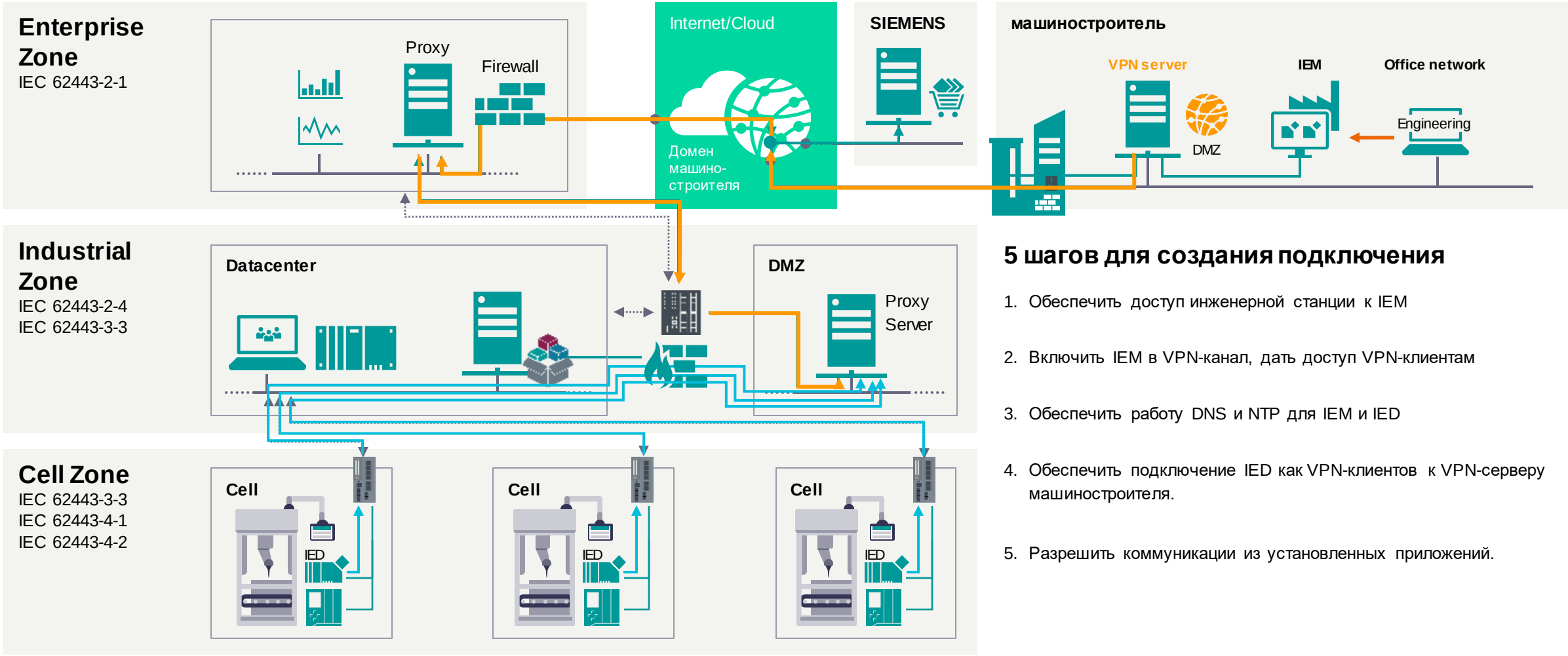
5 шагов для создания подключения

1. Обеспечить HTTPS-доступ инженерной станции к IEM. Убедиться в доступности DNS и NTP.
2. Обеспечить интернет-доступ от IEM к HUB (напрямую через HTTPS или через прокси сервер)
3. Обеспечить работу DNS и NTP для IEM и IED
4. Разрешить HTTPS и SSH *) между IED и IEM
5. Разрешить коммуникации для приложений

*) Если это необходимо для работы с приложением

SIEMENS

Industrial Edge
Сетевая конфигурация для внешнего IEM



5 шагов для создания подключения

1. Обеспечить доступ инженерной станции к IEM
2. Включить IEM в VPN-канал, дать доступ VPN-клиентам
3. Обеспечить работу DNS и NTP для IEM и IED
4. Обеспечить подключение IED как VPN-клиентов к VPN-серверу машиностроителя.
5. Разрешить коммуникации из установленных приложений.

SIEMENS

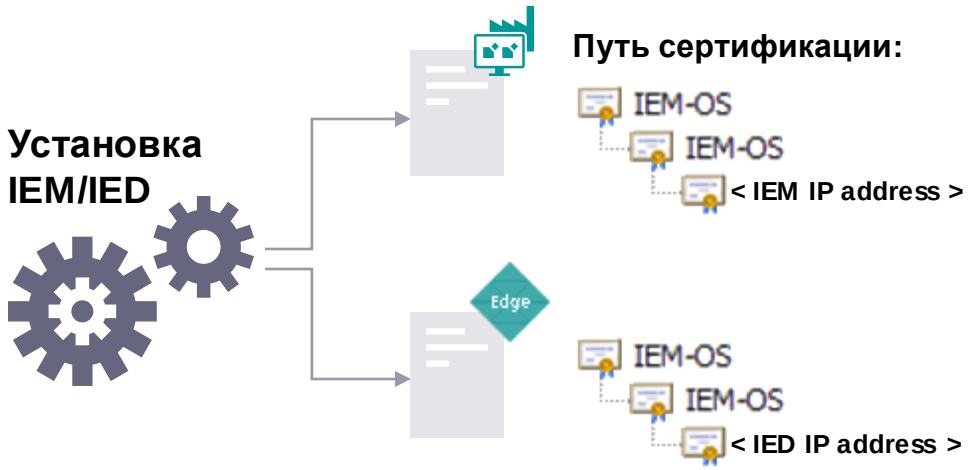
Industrial Edge
Подключение новых платформ IED

Примечание: Схема может меняться в зависимости от местной конфигурации

SIEMENS

Industrial Edge
Управление цифровыми сертификатами

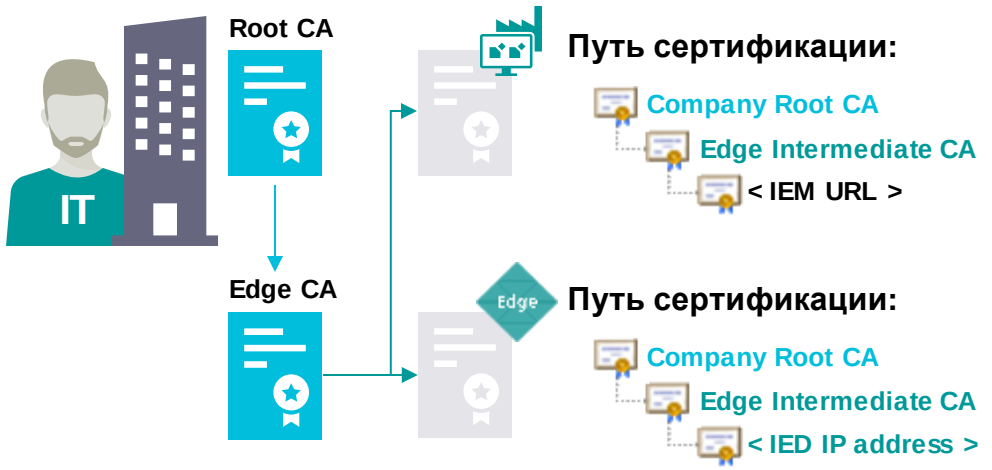
Режим по умолчанию



Обычно сертификаты создаются в процессе установки

- \+ Просто
- − Позже нет подтверждения принадлежности
- − Необходимо интегрировать IEM CA с инфраструкт.

Сертификаты от PKI



Создание сертификатов через PKI

- − Более сложная настройка
- \+ Подтверждает принадлежность организации
- \+ Не нужна интеграция с IEM Root CA

SIEMENS

Industrial Edge
Контроль установки новых приложений

Разработчик не проверен Siemens

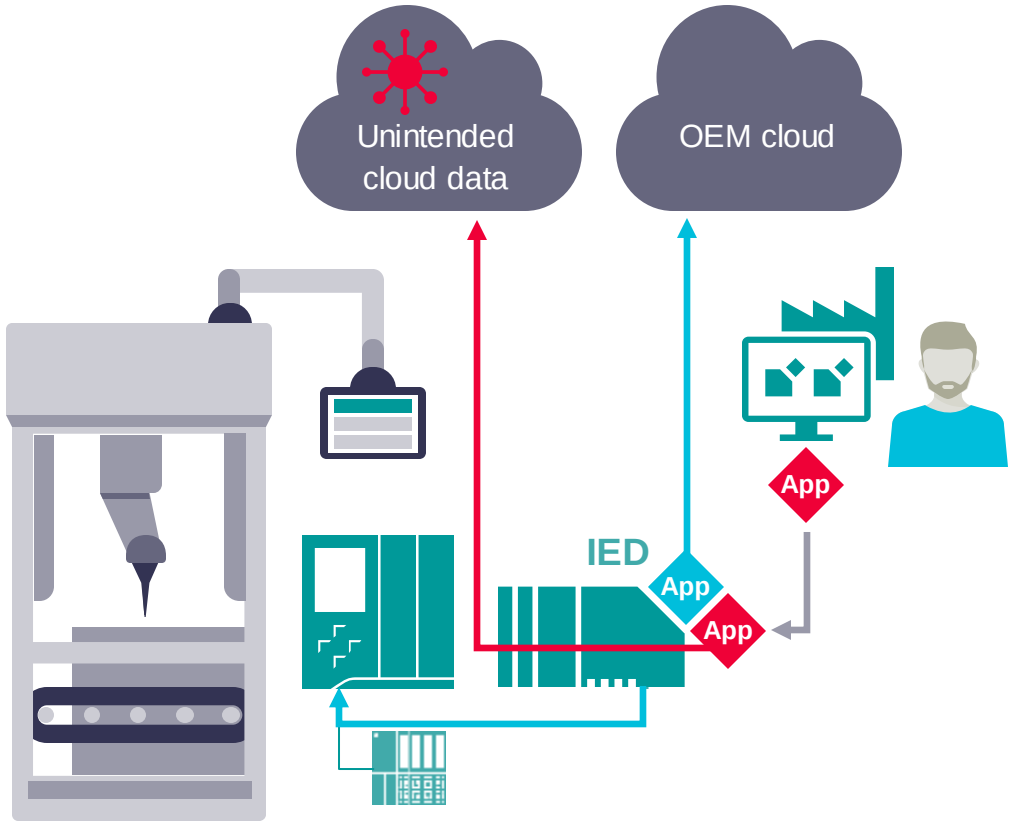
Приложение открывает порт 33123 на вход

Функция: При установке приложений выдаются предупреждения безопасности

SIEMENS

Industrial Edge

Сетевая конфигурация – Открытые порты полезных приложений



Проблема: возможна утечка данных изнутри приложения

Рекомендация:
Защита ячеек файрволлами

SIEMENS

Contacts

Alexander Lifanov

IPC, HMI, Industrial Edge
RC-RU DI FA AS

Bol.Tatarskaya Street, 9
115184 Moscow
Russian Federation
Mobile +7 916 480 09 23

E-mail Alexander.Lifanov@siemens.com