Защита индустриальных систем. Стоит ли овчинка выделки?

Назим Латыпаев

Системный инженер
nlatypae@cisco.com

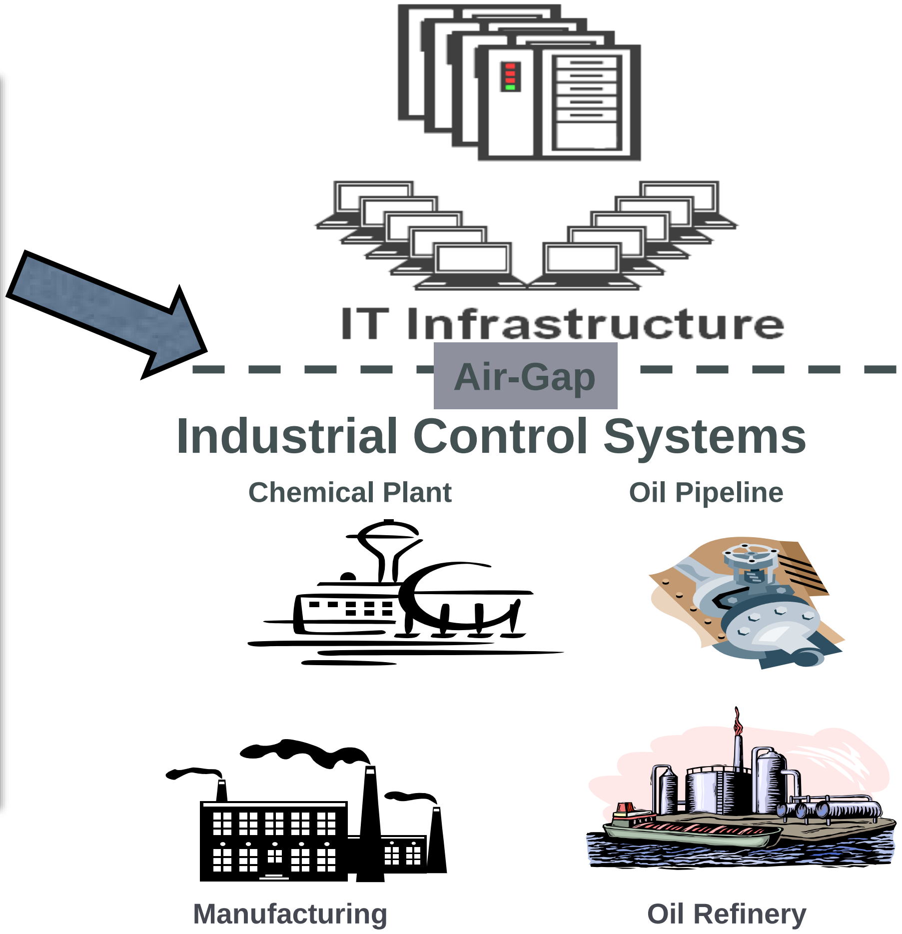
29 апреля 2016 г.

Вместо предисловия…

1. Риски вирусных заражений.
2. Физическая блокировка АРМ
3. Отсутствие сегментации производственных сетей
4. Множественные точки входа в сеть АСУТП
5. Отсутствие парольной политики
6. Проблемы с обновлением ПО сети АСУТП
7. Недекларируемые возможности в промышленном оборудовании

Индустриальная сеть, история…

- Индустриальные системы жили в совершенно другом мире от IT.
- Enterprise сеть была отделена от производства и не было никаких связей.
- Сетевый технологии были проприетарными и отвязанными от товарных/сырьевых систем.
- Подход быстро изменился...



Общие уязвимости

- Хрупкий стек TCP/IP – NMAP, Ping Sweep сканы
- Отсутствие или слабая аутентификация
- Плохой дизайн – хабы, сеть в виде гирлянды
- Сервера IA на Windows – патчи и уязвимости
- Ненужные сервисы в сети – FTP, HTTP и т.д.
- Открытый доступ в сеть, нет port security, отсутствие физического ограничения доступа к оборудованию
- Ограниченный аудит и мониторинг доступа к IA устройствам
- Неавторизованное использование HMI, IA систем для доступа в интернет, загрузки музыки и фильмов.
- Отсутствие опыта работы с IA системами и сетями, много белых пятен.

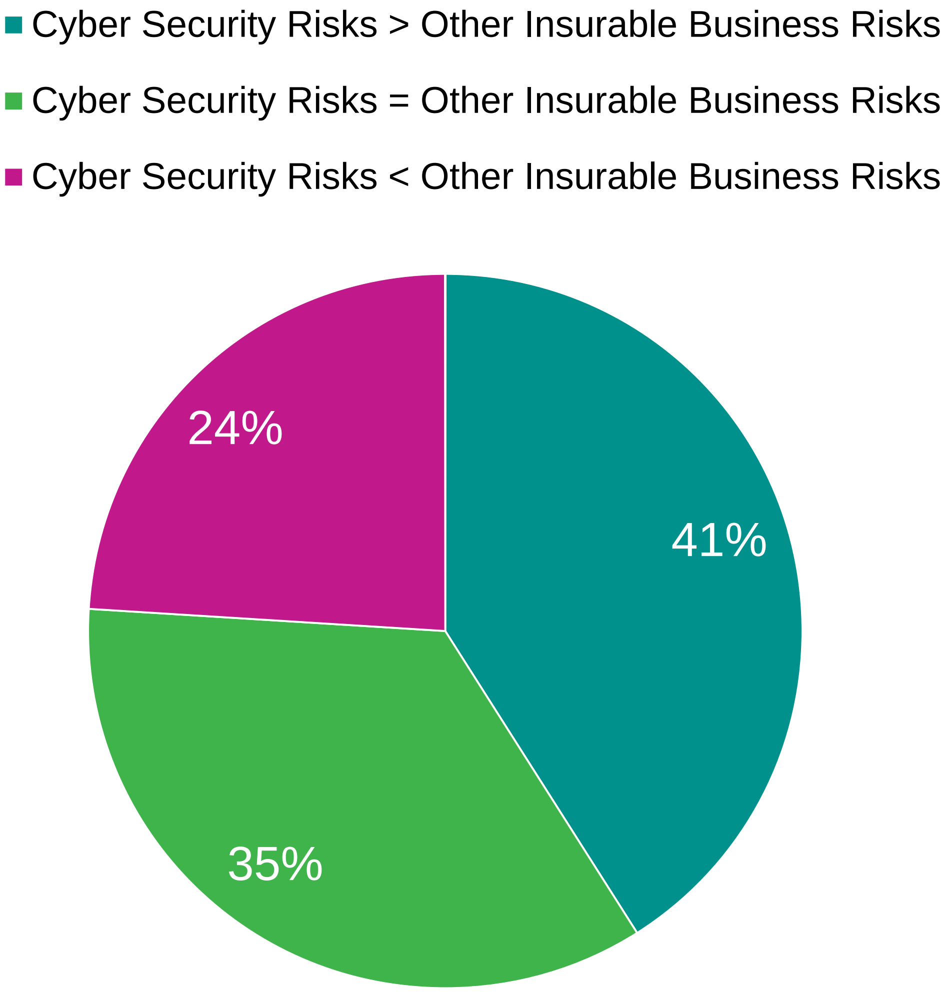
Нефтяная компания – нарушение процесса нефтепереработки

- **Conficker (KIDO) заражение НПЗ** – неопубликовано
- **Описание** – **Cyber Assault**. Вирус поразил Windows компьютеры и продолжал распространение. Привел к нарушению трафика DCS контроллеров, приведшего к их остановке.
- **Вектор Атаки**– Вирус принесен на Flash USB носителе контрактника от вендора (предположительная причина)
- **Уязвимость** – Уязвимость на Windows хостах, соединенных с DCS контроллерами.
- **Ущерб**– НПЗ потерял контроль над производством на целый день. Финансовые потери более UK£ 500,000

Stuxnet Virus – Направленная кибер атака

- **Описание**– **Cyber Assault** Высоко организованная и ресурсоемкая атака на объекты иранской ядерной программы.
- **Вектор Атаки**– Инфицированная USB Flash подключена в Windows PC, подключенный к производственной сети.
- **Уязвимость** – Siemens контроллеры, подключенные к центрифугам на иранском заводе по обогащению урана.
- **Ущерб**– Вирус перехватил управление контроллером и изменял скорость вращения центрифуги заставляя изнашиваться шестерни, приводя к дорогому и длительному ремонту. Также нанесен политический ущерб.

Кибер атаки стоят компаниям миллионы $



10.4% YoY Увеличение стоимости (2013-2014)

$7.6M Средняя годовая стоимость кибер преступления

$163M Средний максимальный потенциальный риск

$500M Максимальный потенциальный риск

7

Индустриальные кибер атаки существуют – последствия критичны!

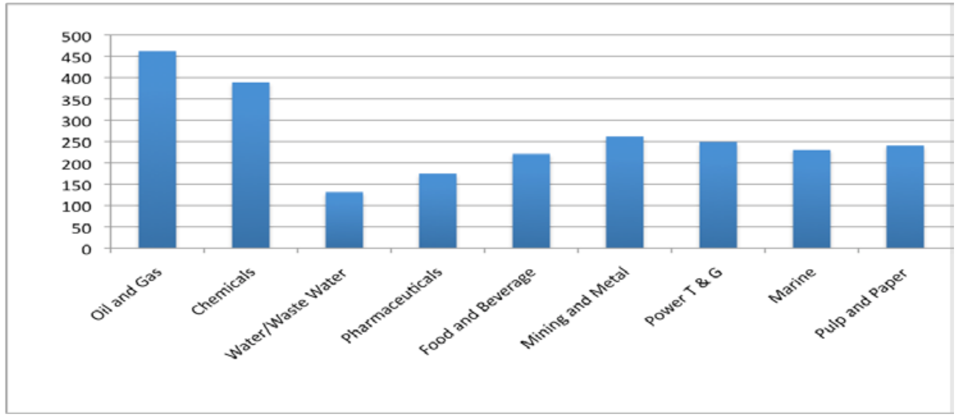
Существуют уязвимости

- Wurldtech’s Achilles платформа идентифицировала более 750 уязвимостей в индустриальном оборудовании
  - Более 70% уязвимостей приводили к потере контроля или потере видимости оборудования.

- Wurldtech создала и поддерживает Delphi – крупнейшую в мире базу уязвимостей индустриальных сетей

Последствия

- Потеря производства
- Сопутствующие потери и отсрочки
- Безопасность людей, повреждение оборудования, удар по репутации.



Смена парадигмы в кибербезопасности промышленной сети

- Принимаемые организационные и технические меры защиты информации должны обеспечивать доступность обрабатываемой в АСУ ТП (исключение неправомерного блокирования) информации, ее целостность (исключение неправомерного уничтожения, модифицирования информации), а также, при необходимости, конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации)
- Организационные и технические меры защиты информации должны быть согласованы с мерами по промышленной, физической, пожарной, экологической, радиационной безопасности, иными мерами по обеспечению безопасности АСУ ТП и управляемого (контролируемого) объекта и (или) процесса и не должны оказывать отрицательного (мешающего) влияния на штатный режим функционирования АСУ ТП

Продукты по промышленной ИБ

Безопасность промышленных сетей от Cisco

OT-centric Security

ISA 3000

Fog Data Services

IoT Сеть как Сенсор

IR Portfolio

ISE

IE Portfolio

ASA H

IoT Физическая безопасность

3000 and 6000 Series
WDR IP Cameras

IDENTIV

ICPAM
Physical Access Control

IoT Сервисы Безопасности

Потребность в специализированных МСЭ/IPS

Для промышленного применения, АСУ ТП, подстанций и т.п. требуется небольшой, монтируемый DIN-rail-type форм-фактор, способный работать в экстремальной окружающей среде

Новые модели Cisco ASA with FirePOWER Services

5506-X	5506W-X	5508-X 5516-X	5506H-X
			
Desktop Model	Integrated Wireless AP	Выше производительность	Для АСУ ТП
100% NGFW - поставляется с AVC	Wi-Fi может управляться локально или через Cisco WLC	1RU; новая платформа – лучшее сочетание цены и производительности	NGFW для критичных инфраструктур и объектов

Идеальна для замены Cisco® ASA 5505

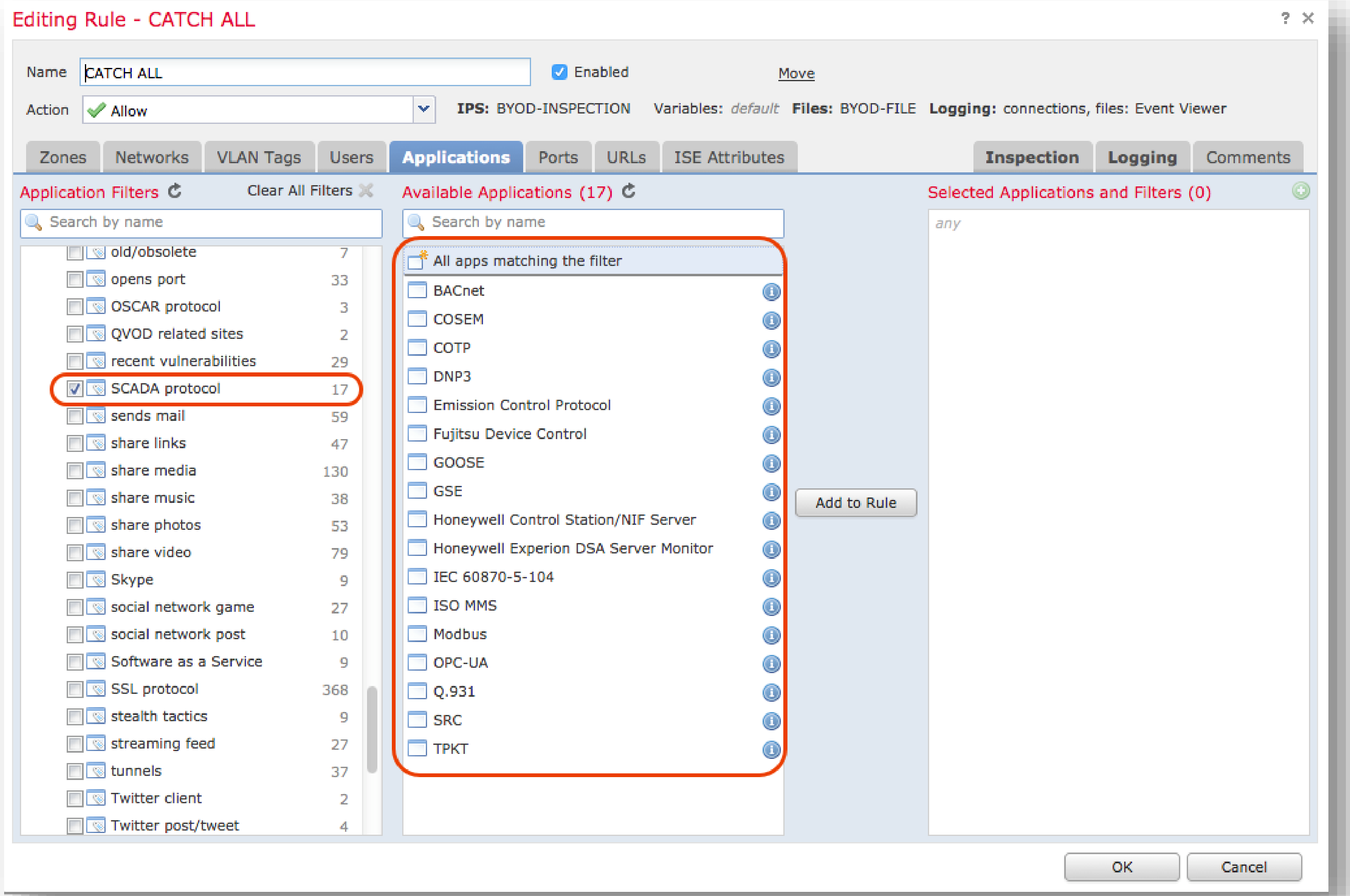
Специальные сертификаты на Cisco ASA 5506H-X

Сертификаты соответствия

IP40 per IEC 60529
KN22
IEC 61850-3
IEC 61000-6-5
IEC 61000-5
IEC 611000-4-18
IEEE 1613.1
IEEE C62.412
IEC 1613
IEC 61850-3
IEC 60068-2

Промышленный МСЭ/IDS Cisco ISA 3000

Поддержка промышленных протоколов

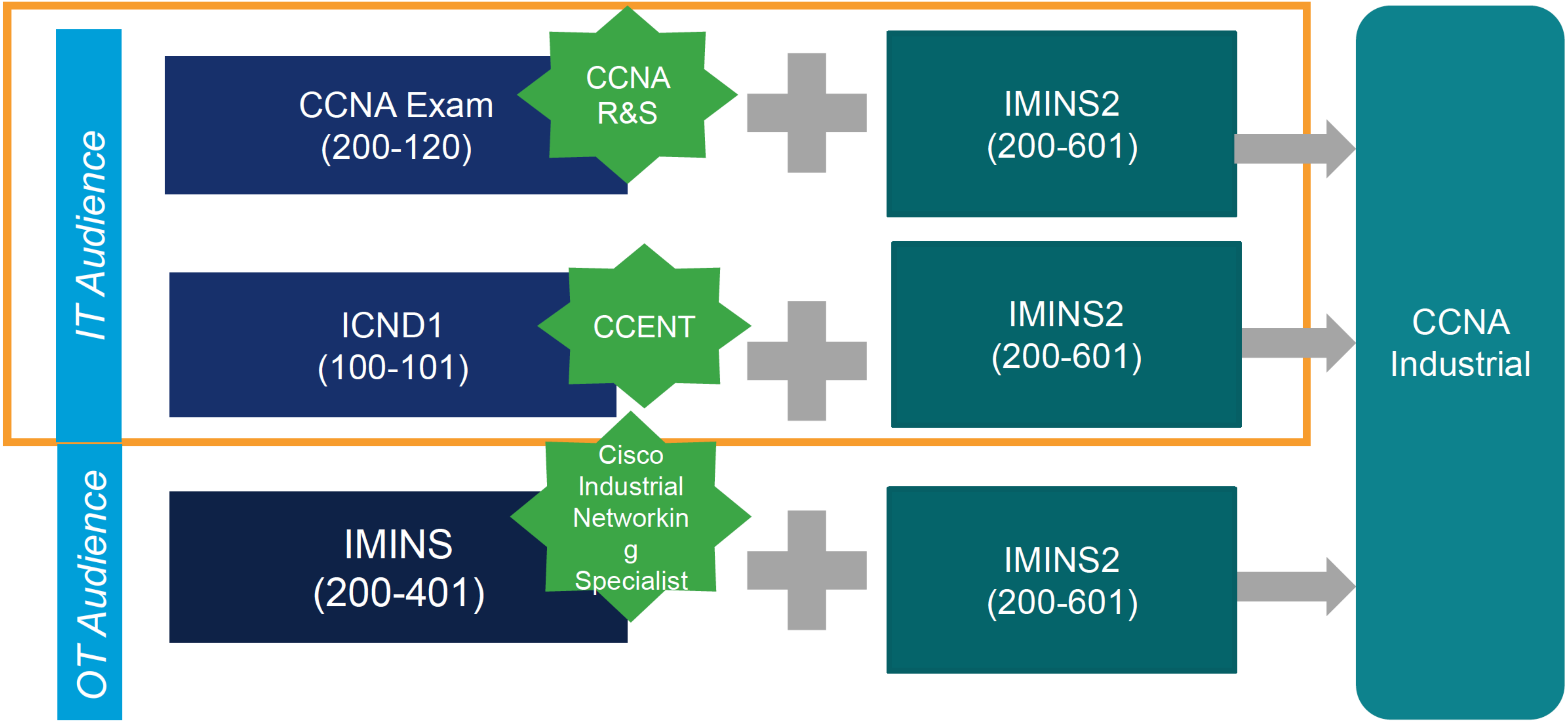


Отражение атак на промышленные системы

- Препроцессоры для промышленных протоколов, например, для Modbus, DNP3
- Возможность написания собственных сигнатур
- Свыше сотни встроенных сигнатур

CitectSCADA	**RSLogix**	**GE Sielco ScadaTec Sinapsi D**
OMRON	**DAQFactory**	**ATAC**
Kingview	**Beckhoff**	**WellinTech**
IGSS	**Measuresoft**	**Tridium**
Tecnomatix	**ScadaPro**	**Schneider Electric**
RealWin Iconics	**Broadwin**	**CODESYS**
Genesis	**Progea Movicon**	
Siemens	**Microsys**	
IntelliCom	**Sunway**	
Cogent	**Moxa**	

Новая сертификация CCNA Industrial



Резюме

Открытые вопросы

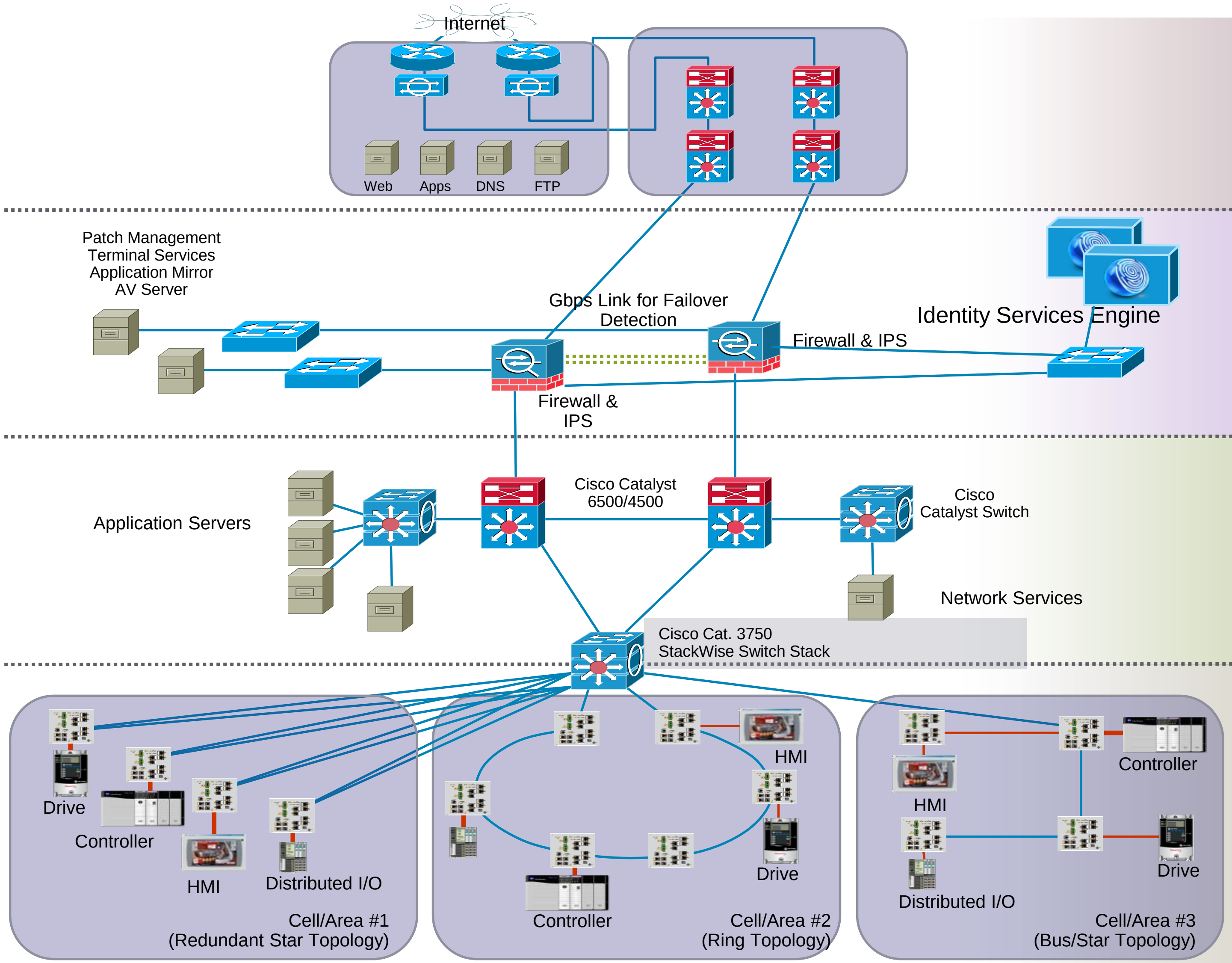
1. Есть ли у вас в сети АСУТП анти-вирусное ПО?
2. Блокируете ли вы физический доступ к АРМ?
3. Сегментированна ли ваша производственная сеть?
4. Уверены ли в целостности вашей сети АСУТП?
5. Парольная политика?
6. Как у вас обстоят дела с обновлением ПО сети АСУТП?
7. Уверены ли вы в вашем оборудовании?

Благодарю
за внимание

cisco

Архитектура безопасности

Архитектура Ethernet-to-the-Factory (ETTF)



Сеть предприятия
Уровни 4-5

Интеграция в сеть предприятия
UC
Wireless
Application Optimization

Буферная
зона
(DMZ)

Контроль доступа

Защита от угроз

Индустриальная
зона
Уровень 3

Сегментация

Мультисервисные сети

Безопасность приложений и управления

Cell/Area Zone
Уровни 0-2

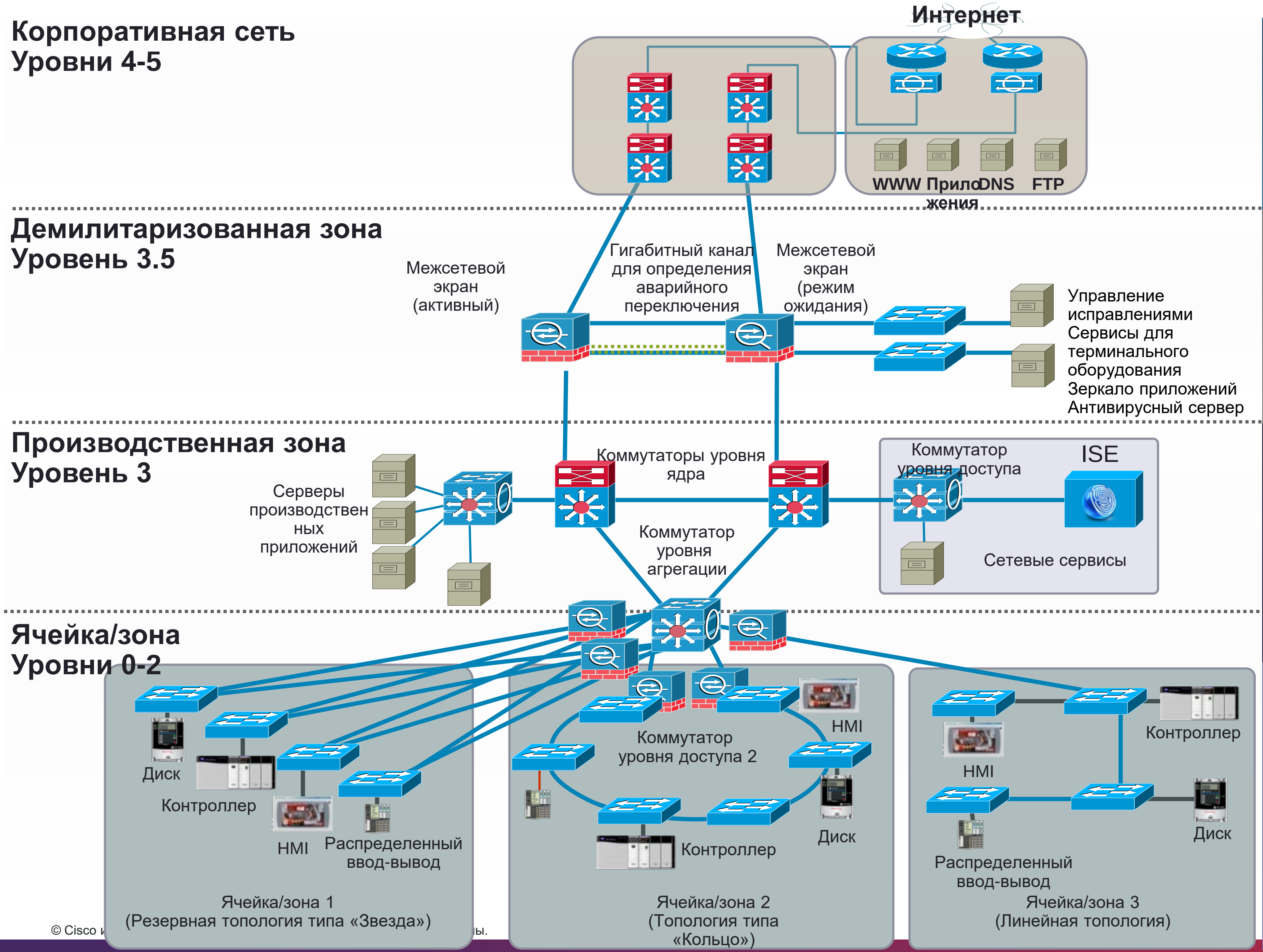
Контроль в реальном времени

Конвергенция

Multicast Traffic

Простота использования

Архитектура ИБ производства от Cisco



Защита от угроз в облаке

Применение политик для всей сети

Контроль доступа (на уровне приложений)

VPN и сервисы удаленного доступа

Межсетевой экран нового поколения

Система предотвращения вторжений (IPS)

Межсетевой экран с сохранением состояния

Защита и определение вторжений (IPS/IDS)

Системы управления физическим доступом

Усиленный межсетевой экран

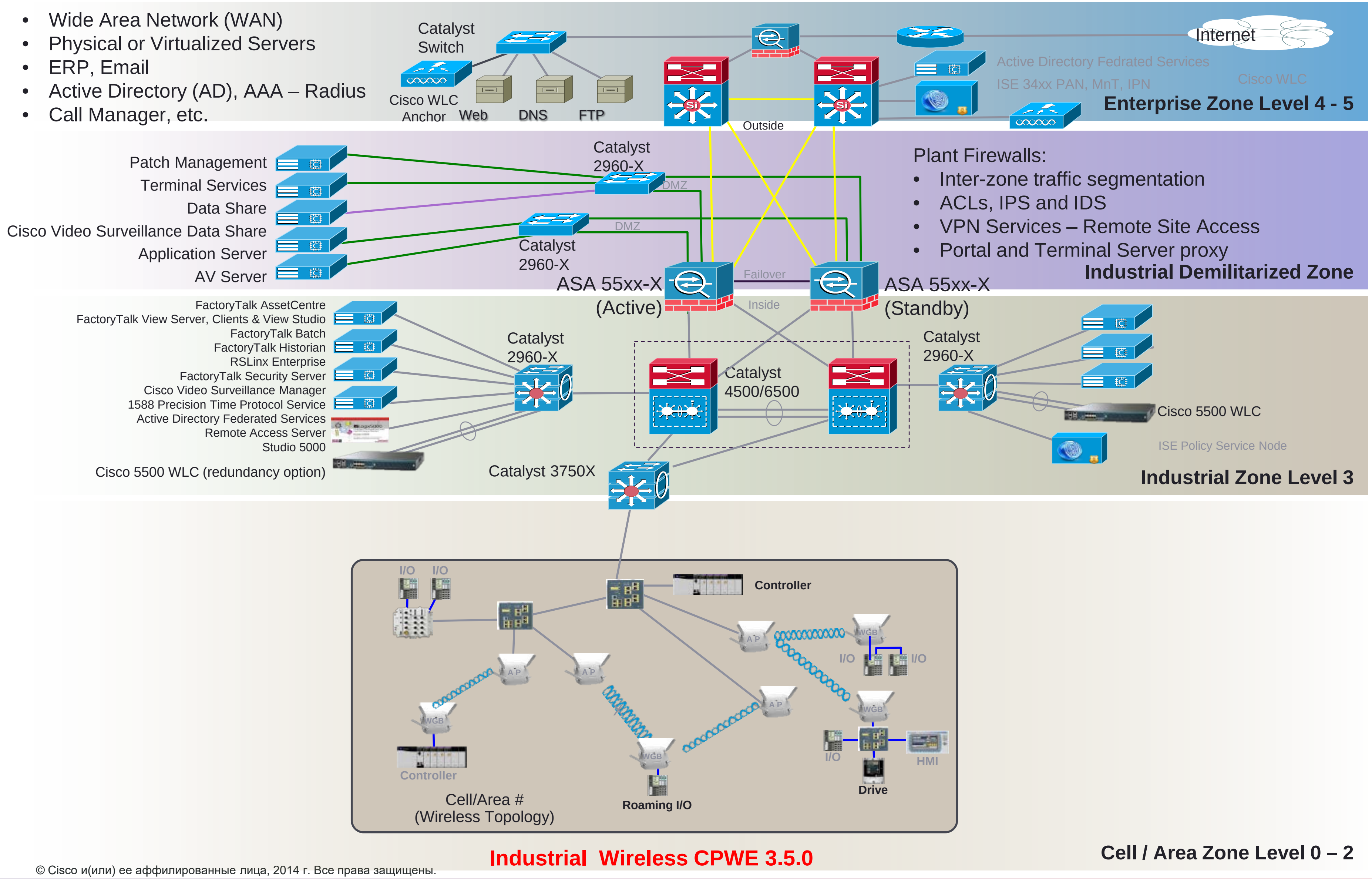
Усиленная система предотвращения вторжений (IPS)

Удаленный мониторинг и наблюдение

Управление ПО, конфигурацией и активами

Сервисы идентификации

Cisco Connected Factory 3.5.0 – беспроводная инфраструктура



БЛВС производства

Бизнес результат

Уменьшение затрат

Ключевые параметры

Factory Mobility

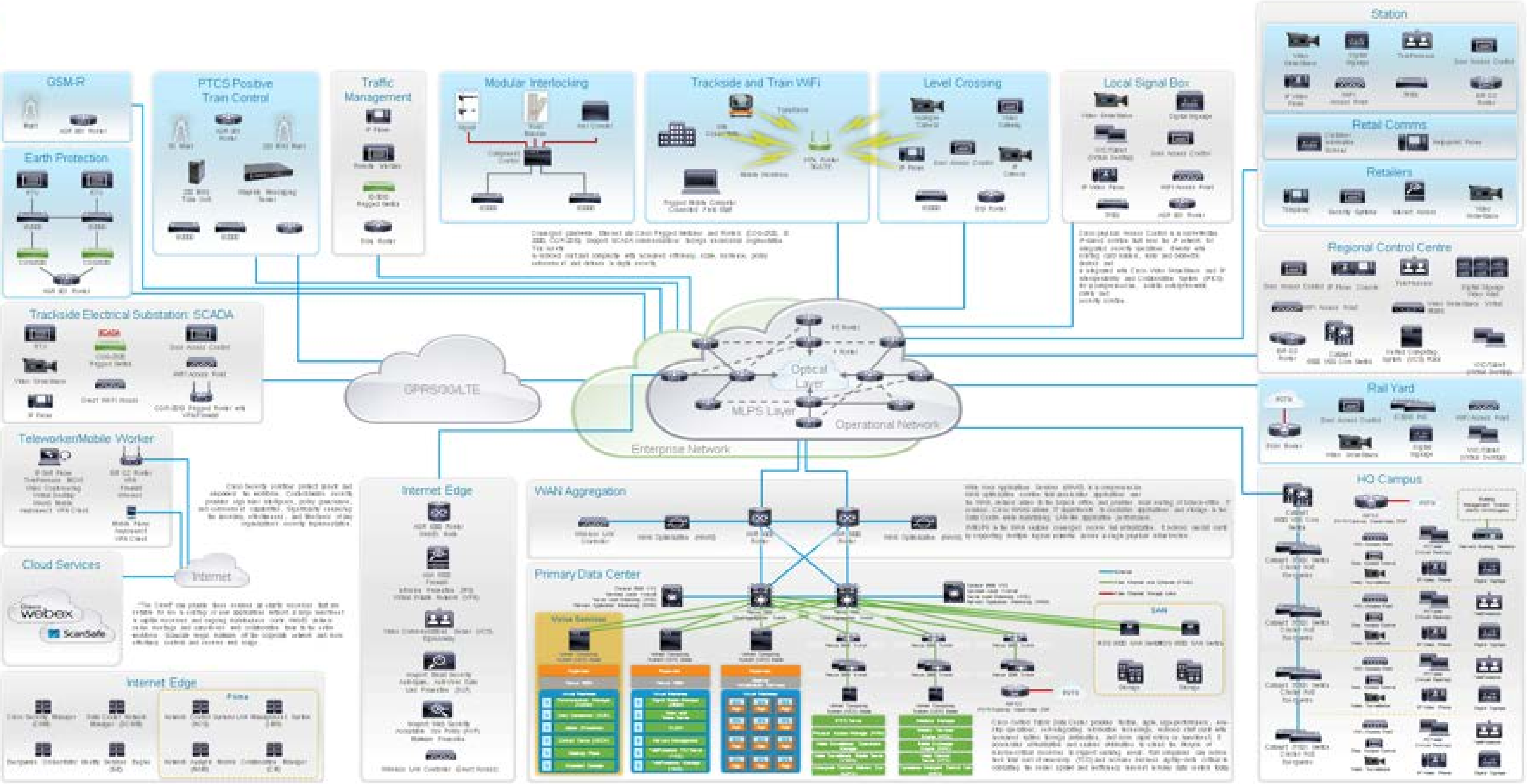
- Mobile Controls visibility
- Wireless tooling, I/O
- Asset Tagging
- Mobile video
- Mobile Apps

Продукты решения

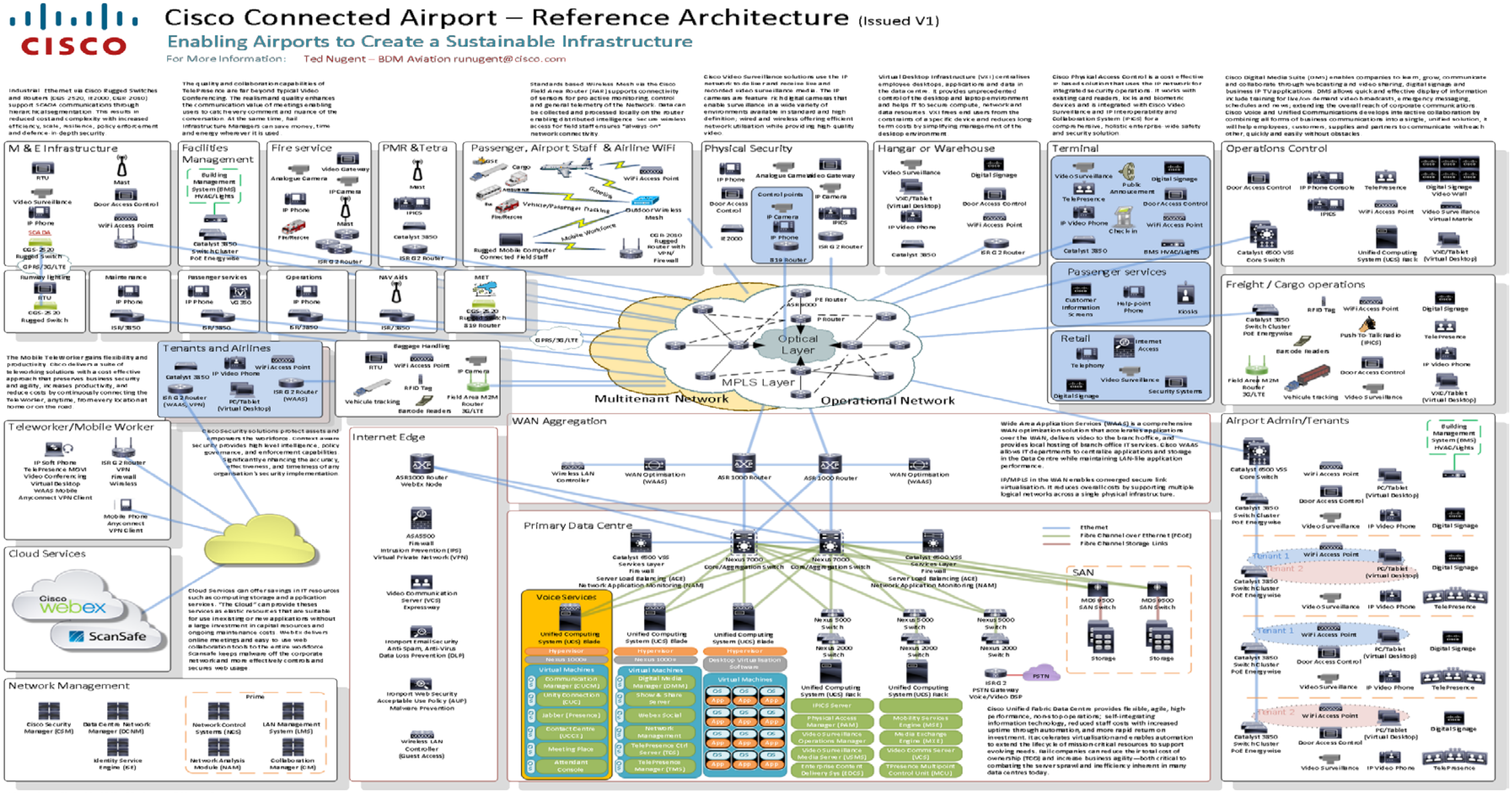
- **1552 AP, 2600 AP, WLC**
- **Stratix 5100 AP**
- Ent Mobility Svs Platform
- IOE Site surveys

CVD от Ноября‘14

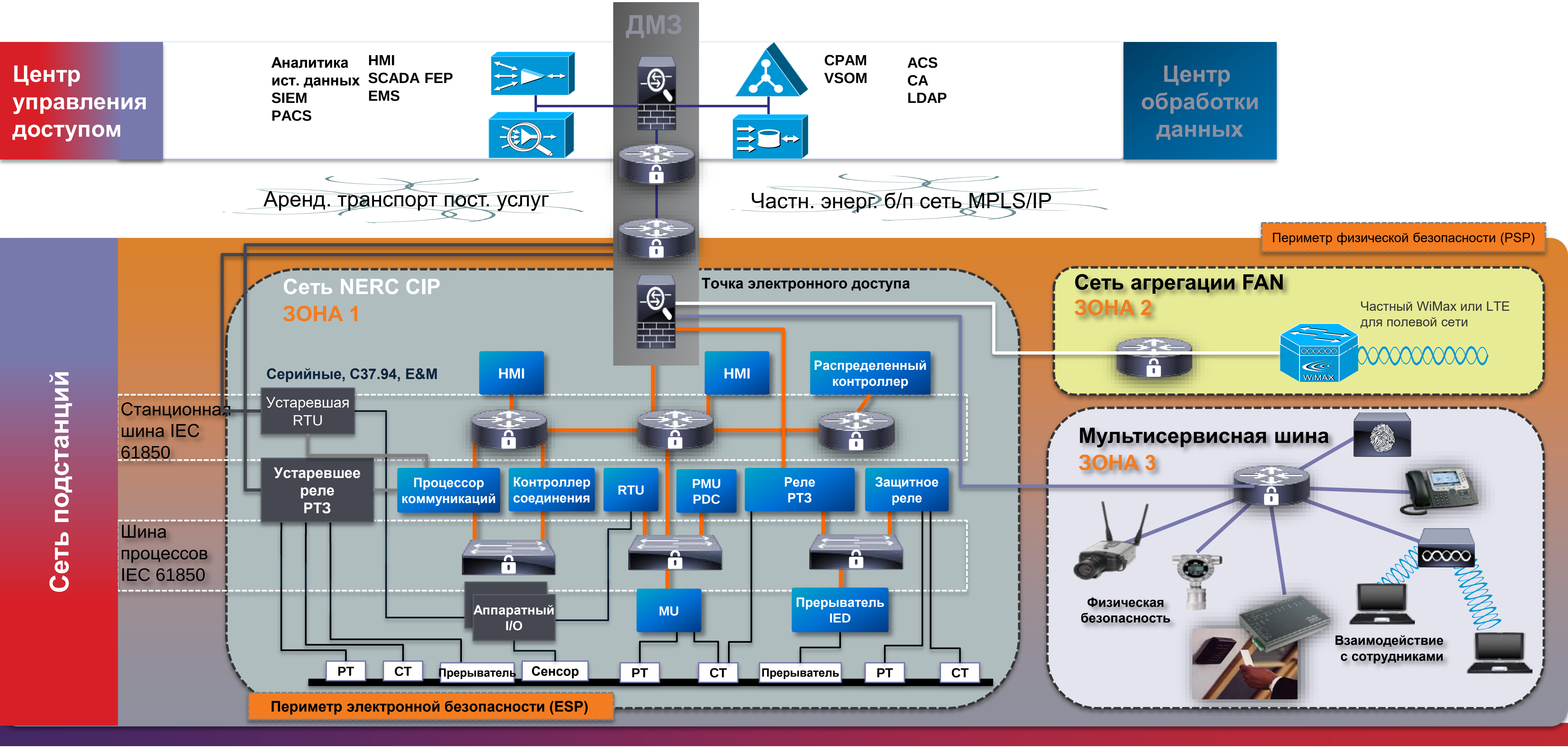
Архитектура ИБ железнодорожного транспорта от Cisco



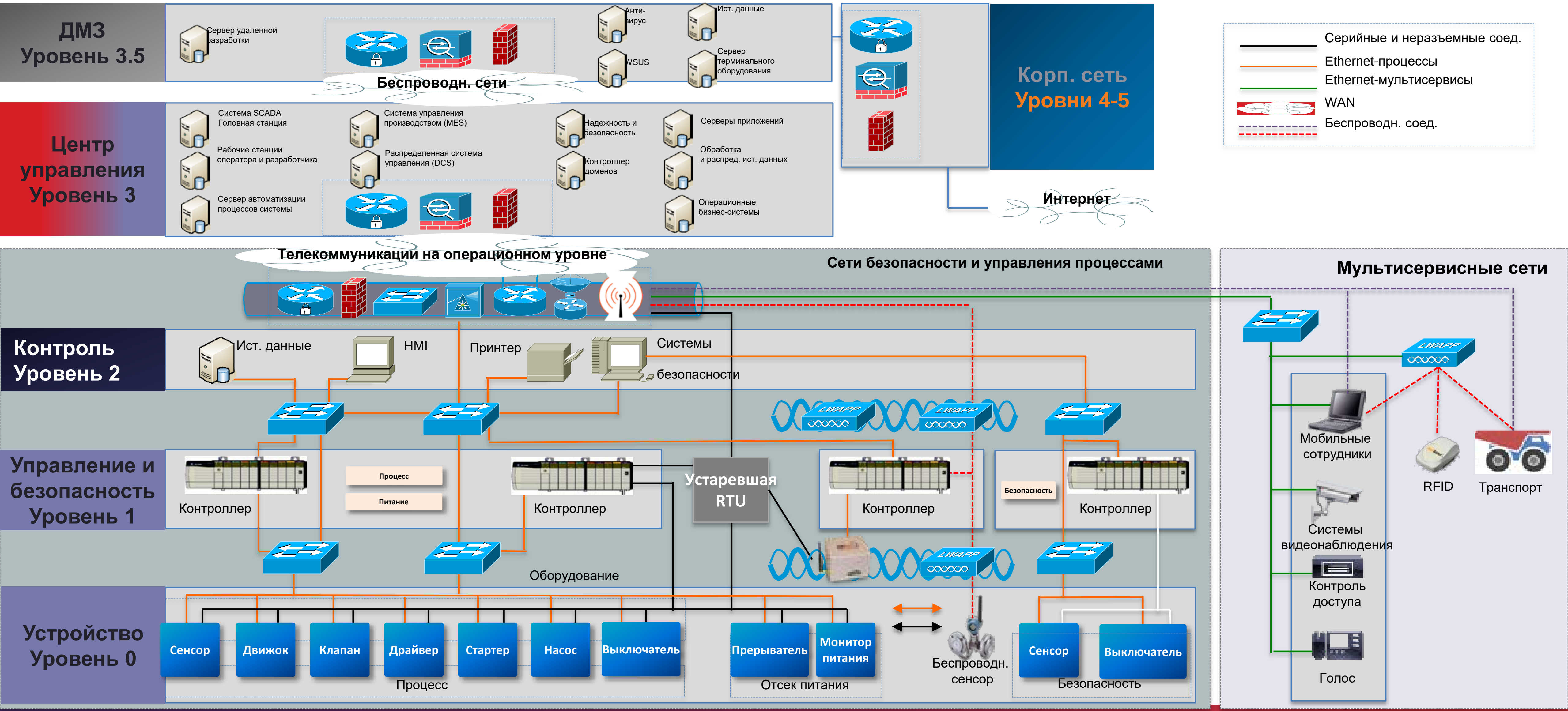
Архитектура ИБ аэропорта от Cisco



Архитектура ИБ цифровой подстанции от Cisco



Архитектура ИБ нефтеперерабатывающего завода от Cisco

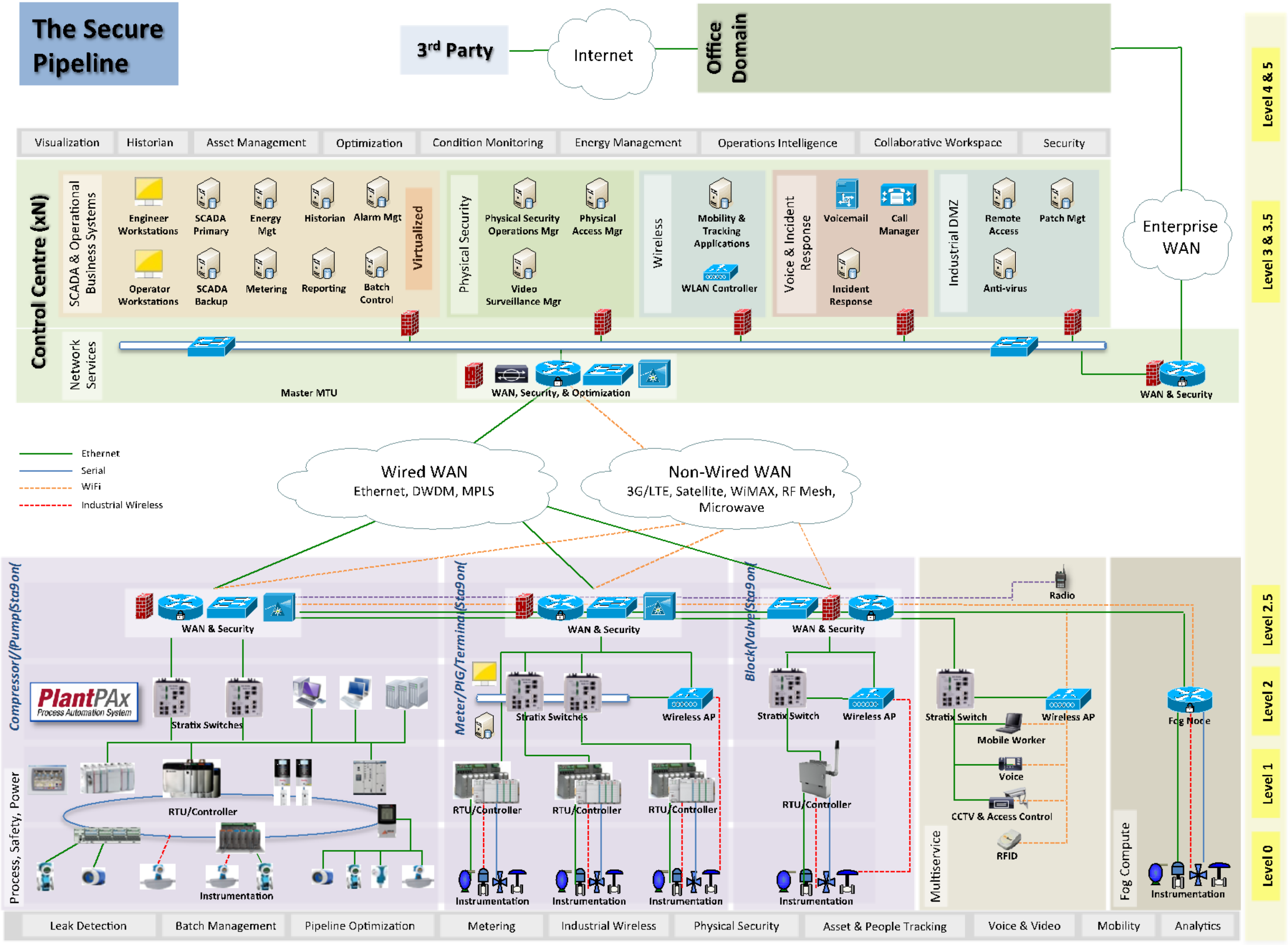


Архитектура ИБ трубопровода от Cisco и Rockwell

Rockwell Automation

Совместная функциональная архитектура целостной трубопроводной инфраструктуры.

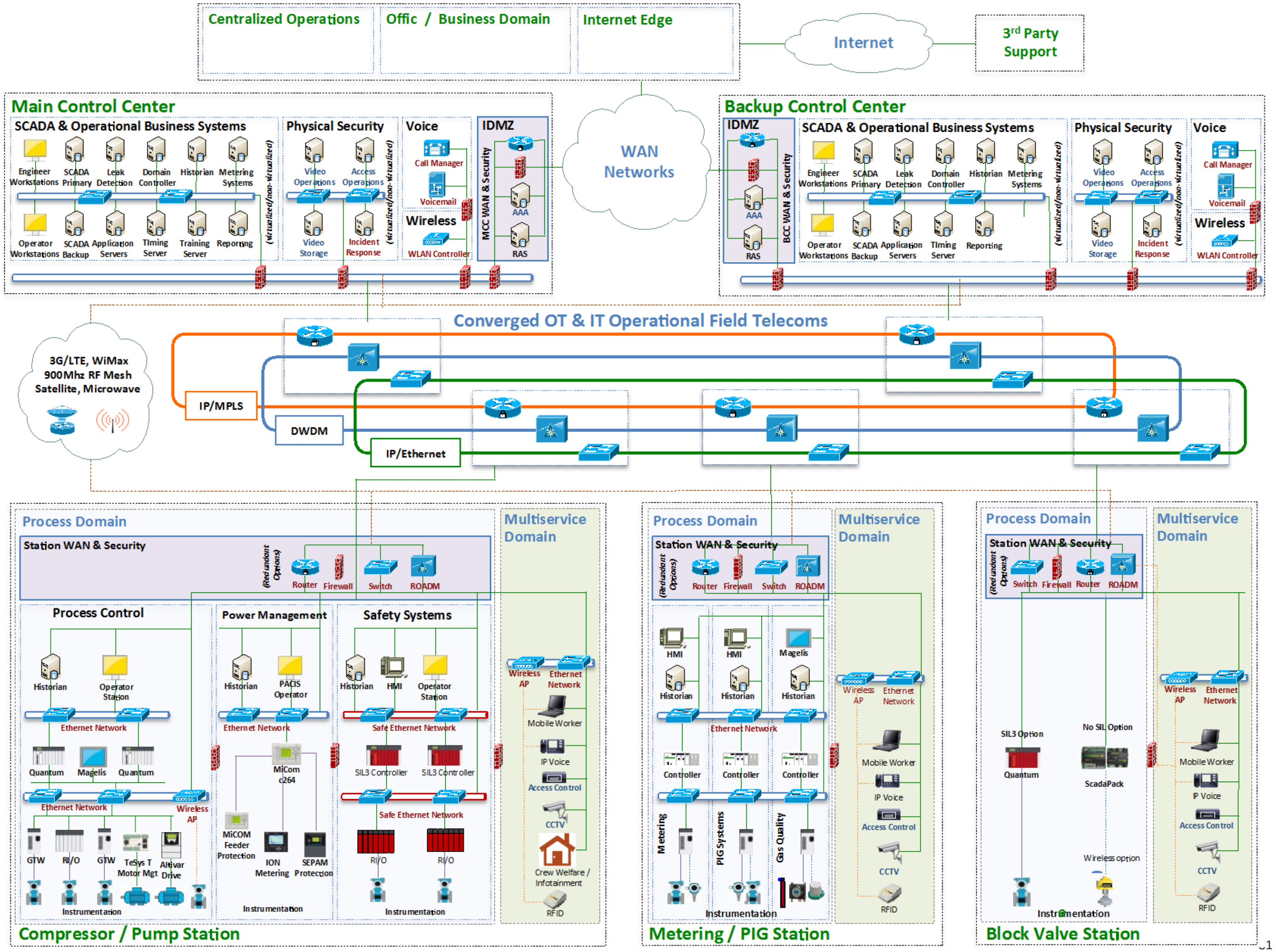
- Гибкий, модульный подход, подерживающий этапную трансформацию **Нефте-Газового трубопровода**
- Виртуализация контрольной комнаты
- Конвергентное WAN операционное взаимодействие
- Проводные и беспроводные сети трубопровода
- Интегрированные мульти-Сервисные системы
- IEC 62443 / ISA99 Модель безопасности



Архитектура ИБ трубопровода от Cisco и Schneider

Совместная функциональная архитектура целостной трубопроводной инфраструктуры.

- Гибкий, модульный подход, подерживающий этапную трансформацию **Нефте-Газового трубопровода**
- Виртуализация контрольной комнаты
- Конвергентное WAN операционное взаимодействие
- Проводные и беспроводные сети трубопровода
- Интегрированные мульти-Сервисные системы
- IEC 62443 / ISA99 Модель безопасности



Благодарю
за внимание