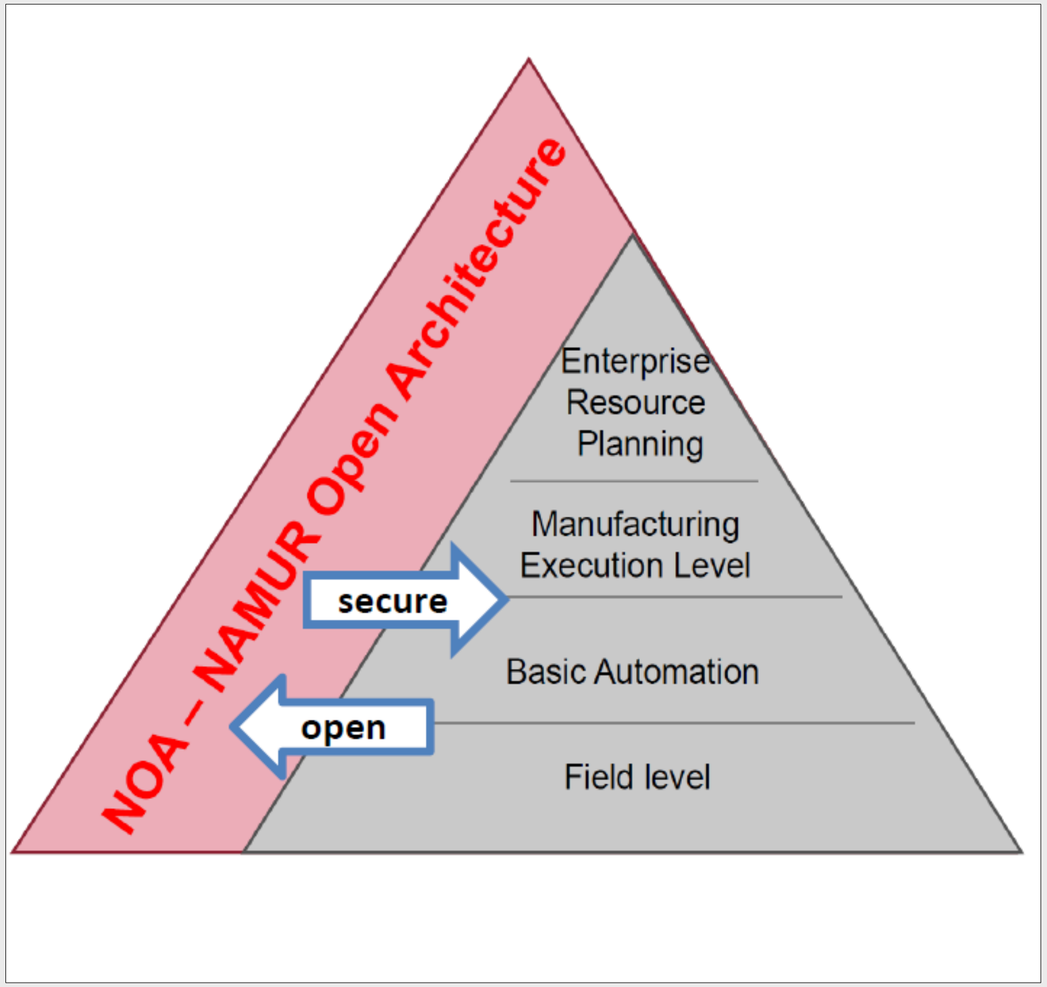
Стандарты открытых систем промышленной автоматизации в мире и России.
Где там кибербезопасность ?

Даренский Дмитрий
Руководитель практики промышленной кибербезопасности
Positive Technologies

NAMUR™ Open Architecture- NOA™

Международная ассоциация пользователей технологий автоматизации в перерабатывающих отраслях промышленности, представляющая интересы своих членов уже более 65 лет.



NOA использует традиционные системы автоматизации процессов и определяет новую область мониторинга и оптимизации.

Основные области применения:

- Мониторинг полевых устройств
- Управление предприятием
- Дополнительные измерения для оптимизации процессов

NAMUR Open Architecture- NOA

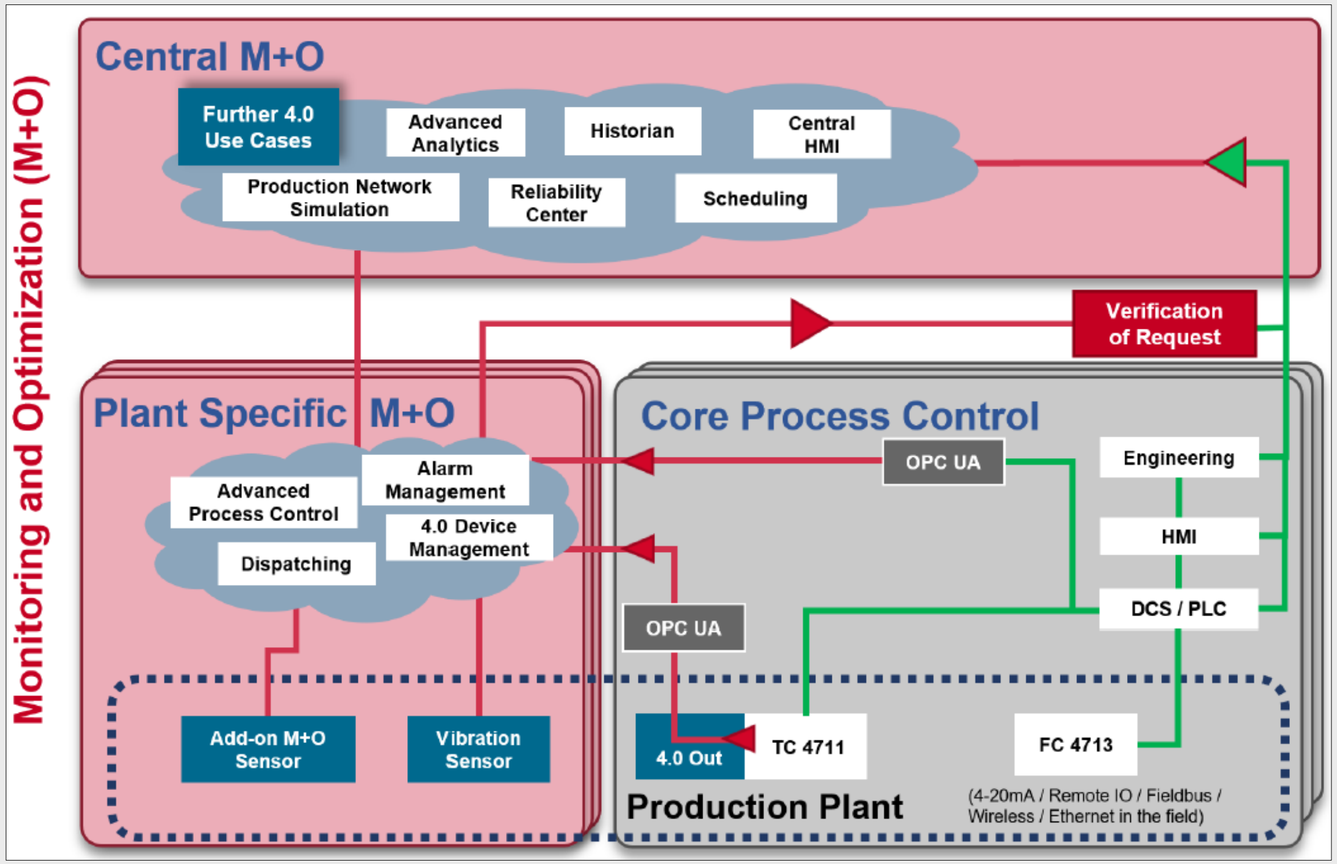
Основные элементы :

Стандартизированная информационная модель (NOA-IM)
основана на спецификациях OPC UA

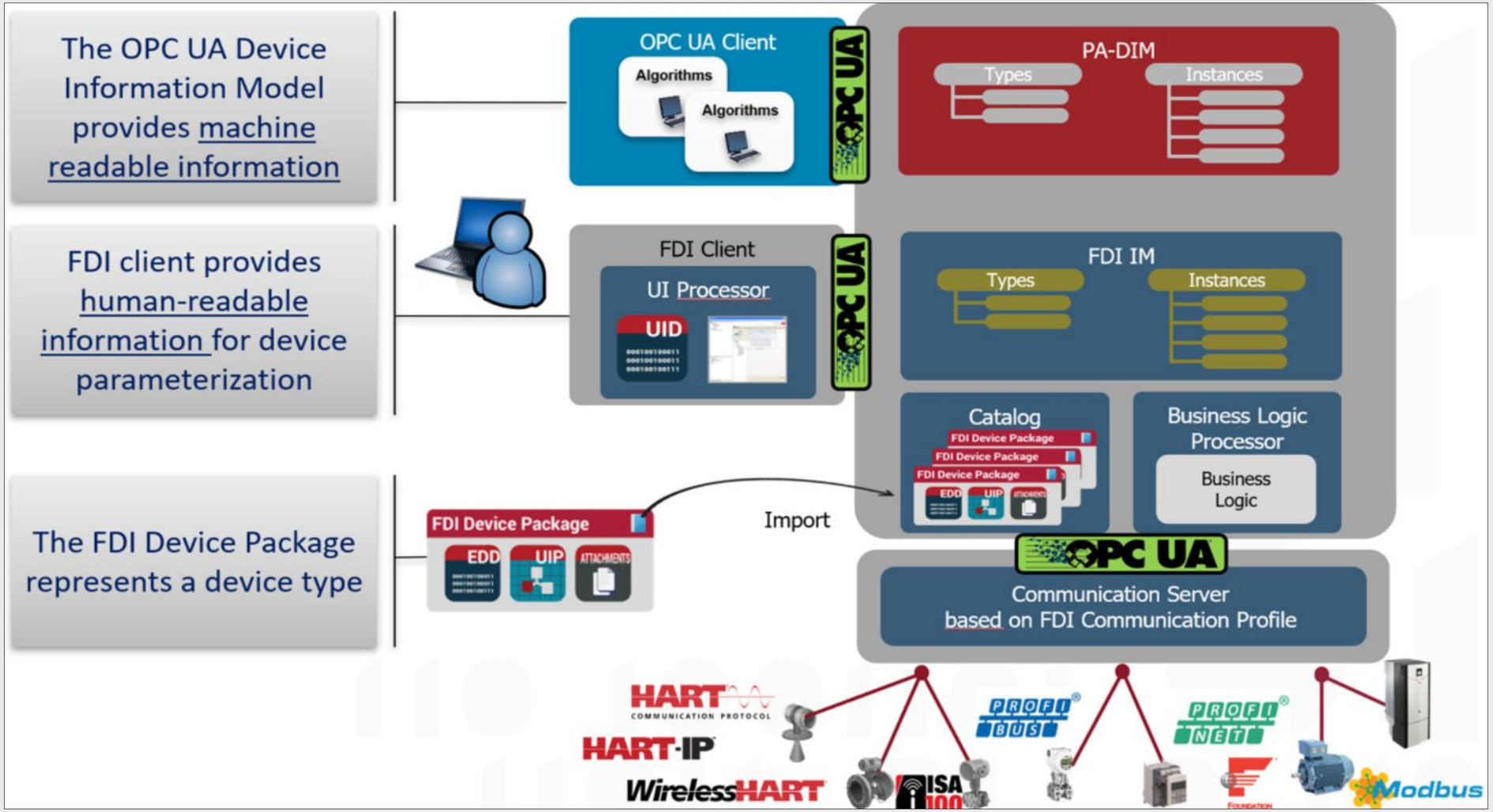
Диод NOA

Компонент проверки запросов NOA

Концеп Сервера агрегирования NOA



NAMUR™ Open Architecture- NOA™



Стандарт Open Process Automation ™ - O-PAS ™

Стандарт O-PAS™ - это “стандарт стандартов”, разработанный форумом Open Process Automation™ (OPAF).

Стандарт определяет открытую, совместимую и безопасную архитектуру для систем автоматизации промышленных процессов.

Стандарт Open Process Automation ™ - O-PAS ™

OPAS information model
Базируется на спецификациях AML
(соответствует ГОСТ Р МЭК 62714-1-2020)

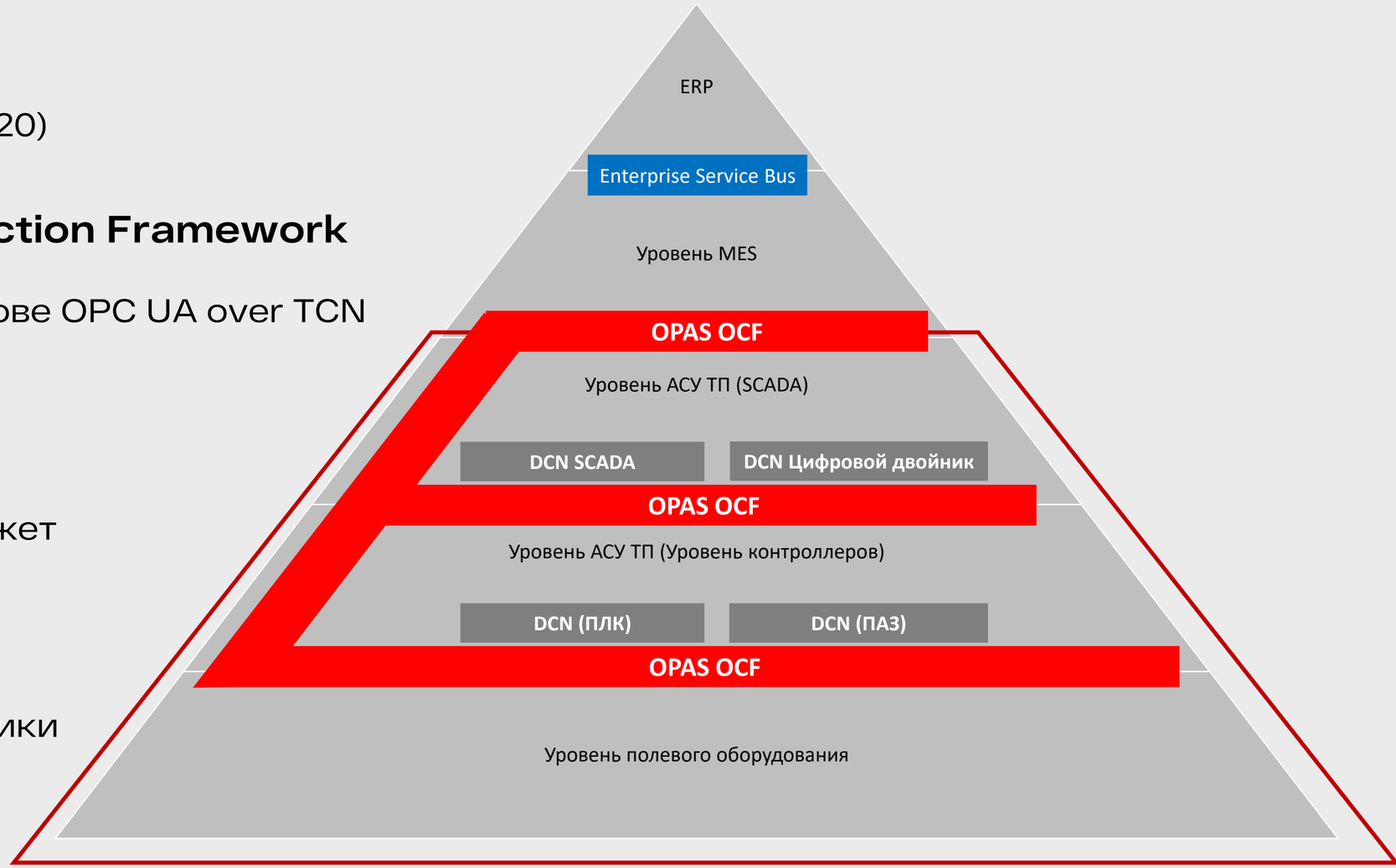
OPAS OCF – Open Platform Connection Framework

Унифицированная шина обмена на основе OPC UA over TCN

DCN-Distributed Control Node

Универсальный контейнер который может включать:

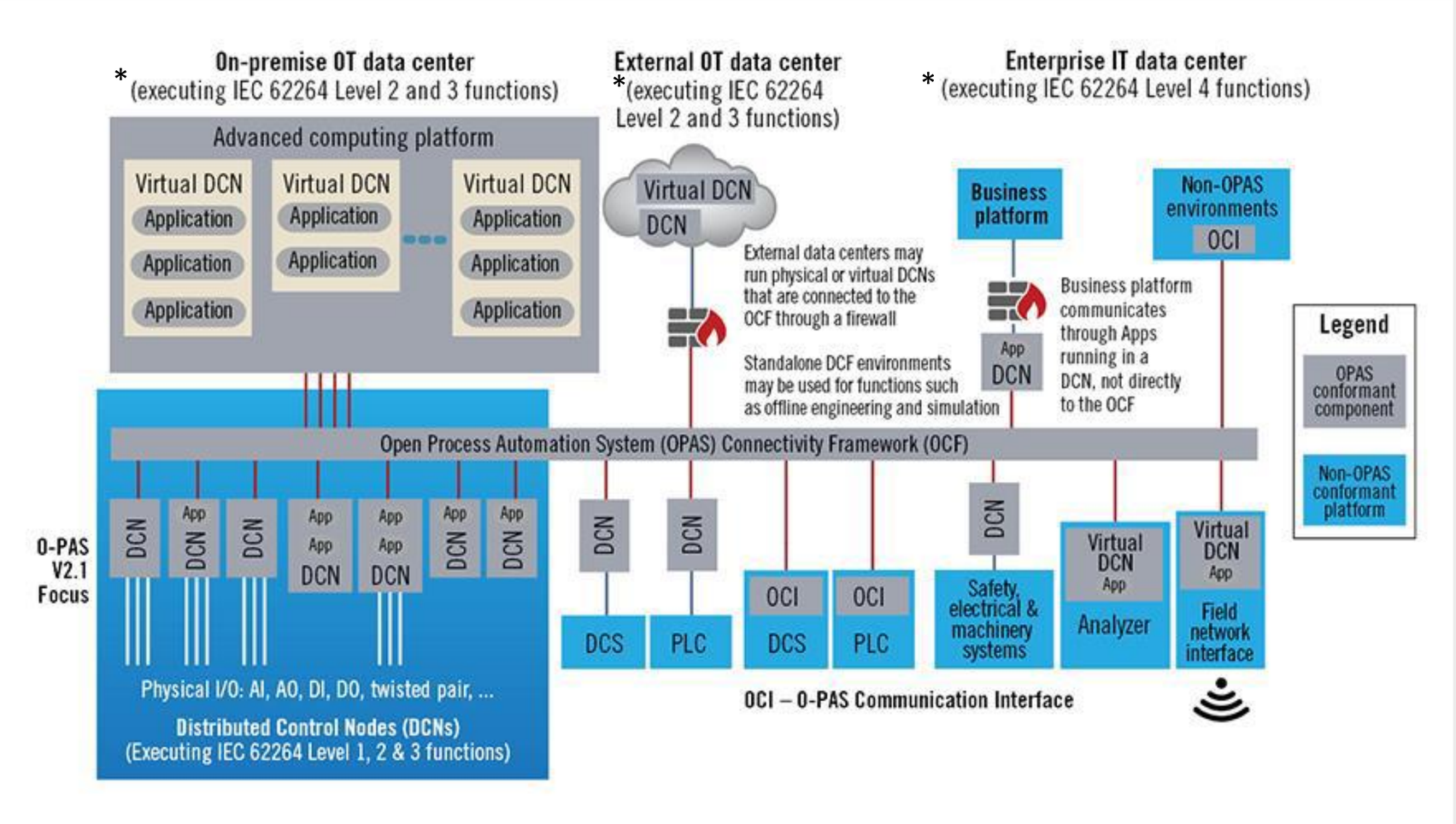
- ПЛК (IEC61131, IEC61499)
- Linux-приложение (например SCADA)
- Приложения безопасности
- Приложения мониторинга и диагностики



Стандарт Open Process Automation ™ - O-PAS ™

Атрибуты качества компонентов

1. Общеприменимость
2. Доступность
3. Совместимость
4. Конфигурация
5. Обнаруживаемость
6. Возможность развития
7. Гибкость
8. Взаимозаменяемость
9. Функциональная совместимость
10. Ремонтопригодность
11. Управляемость
12. Модульность
13. Портативность
14. Надежность
15. Устойчивость
16. Возможность повторного использования
17. Безопасность
18. Масштабируемость
19. Защищённость
20. Соответствие стандартам
21. Тестируемость
22. Прослеживаемость
23. Удобство использования



* Соответствует ГОСТ Р МЭК 62264-2014. Национальный стандарт российской федерации. Интеграция систем управления предприятием.

Область стандартизации O-PAS Part -2 Security

Ключевое понятие O-PAS Part -2 Security - **Уровни безопасности**. В соответствии с положениями стандарта ANSI/ISA-62443 описывает три уровня безопасности и кем они обеспечиваются

Возможности SL (SL-C):
уровень безопасности, который может обеспечить компонент при правильной настройке.

Определяется поставщиком продукта. Это можно продемонстрировать с помощью тестирования на соответствие или сертификации.

Целевой уровень безопасности (SL-T):
желаемый уровень безопасности для конкретного решения автоматизации.

Определяется владельцем актива или системным интегратором/поставщиком услуг совместного владельцем актива на основе оценки рисков.

Достигнутый SL (SL-A):
фактический уровень безопасности для конкретного IACS после внедрения.

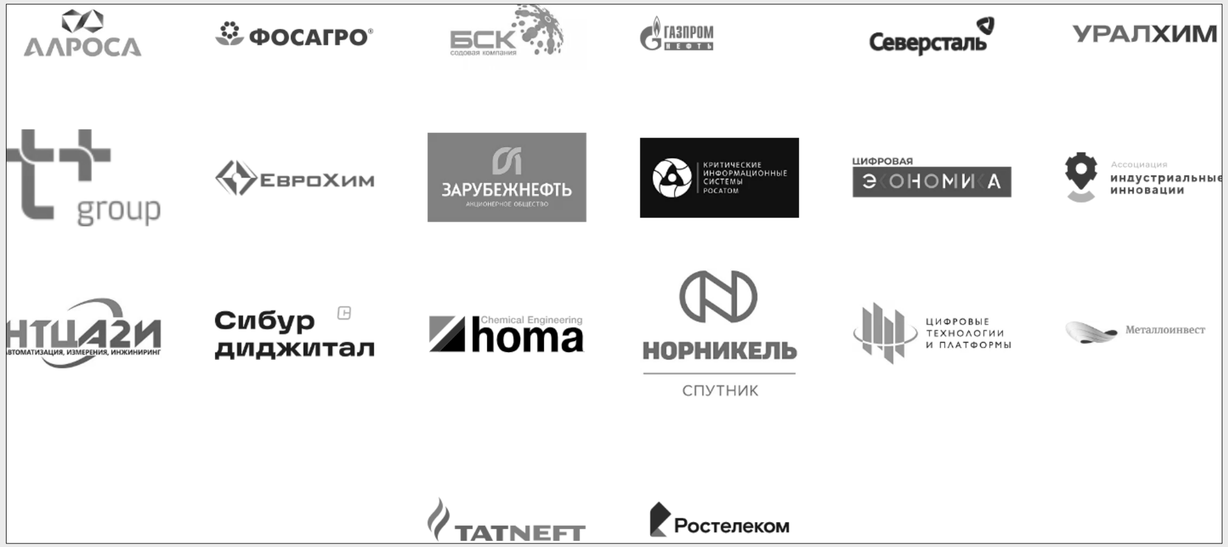
Может быть продемонстрирован системным интегратором/поставщиком услуг владельцу актива.

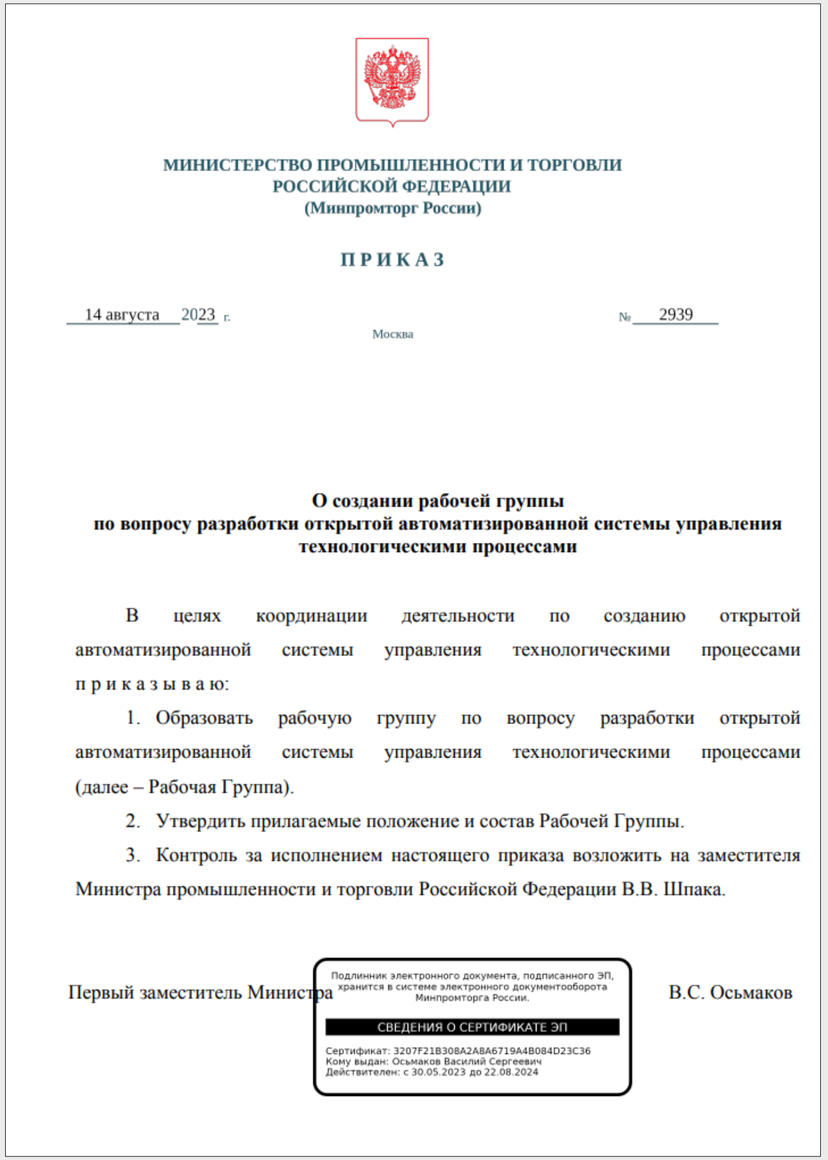
Важное уточнение:
Положения O-PAS Part -2 Security определяют требования только к уровню **SL-C**

- Identification
- Authentication
- Non-repudiation
- Authorization
- Integrity
- Anomaly Detection
- Confidentiality
- Segmentation
- Auditability/Accountability
- Availability
- Incident Response

МЕЖОТРАСЛЕВАЯ РАБОЧАЯ ГРУППА
Открытая АСУ ТП

Создана по инициативе Индустриальных центров компетенций (ИЦК) “Металлургия” и “Химия”, АНО “Цифровая экономика” и также Ассоциации “Индустриальные инновации”





МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(Минпромторг России)

ПРИКАЗ

14 августа 2023 г. № 2939

Москва

**О создании рабочей группы
по вопросу разработки открытой автоматизированной системы управления технологическими процессами**

В целях координации деятельности по созданию открытой автоматизированной системы управления технологическими процессами п р и к а з ы в а ю:

1. Образовать рабочую группу по вопросу разработки открытой автоматизированной системы управления технологическими процессами (далее – Рабочая Группа).
2. Утвердить прилагаемые положение и состав Рабочей Группы.
3. Контроль за исполнением настоящего приказа возложить на заместителя Министра промышленности и торговли Российской Федерации В.В. Шпака.

Первый заместитель Министра В.С. Осьмаков

Подлинник электронного документа, подписанного ЭП, хранится в системе электронного документооборота Минпромторга России.

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 3207F21B30BA2A8A6719A4B084D23C36
Кому выдан: Осьмаков Василий Сергеевич
Действителен: с 30.05.2023 до 22.08.2024

МЕЖОТРАСЛЕВАЯ РАБОЧАЯ ГРУППА
Открытая АСУ ТП

Цели создания рабочей группы

Вендорная независимость

вендорная независимость конечного решения

Открытость решений

открытость решений, систем и их компонентов для управления и улучшения силами заказчика

Универсальность архитектуры

универсальность архитектуры, принципов организации взаимодействия между компонентами решений и систем, модульная совместимость и взаимозаменяемость, модульная масштабируемость

Универсальность (индустриальные отраслевые стандарты)

универсальность по отношению к индустриальным отраслевым стандартам и межотраслевая применимость конечного решения

МЕЖОТРАСЛЕВАЯ РАБОЧАЯ ГРУППА Открытая АСУ ТП

Основной фокус деятельности

Рабочая группа определит спецификации, технические требования и стандарты открытой, совместимой, защищенной архитектуры автоматизации технологических процессов.

Приоритетной задачей является подбор стандартов и протоколов из числа существующих отраслевых стандартов.

В случае отсутствия применимых стандартов Рабочая группа будет разрабатывать требования и привлекать к работе организации по разработке стандартов с целью создания нового стандарта.

Стандарты

Отраслевые и межотраслевые стандарты в области ОАСУ ТП

Программный ПЛК

Открытый виртуальный программный ПЛК

Среда разработки АСУ ТП

Открытая виртуальная универсальная сквозная среда разработки АСУ ТП

ОВ ОСРВ

Открытая виртуальная операционная система реального времени (ОВ ОСРВ)

Протокол передачи данных

Открытый универсальный промышленный протокол передачи данных

Универсальный конвертор

Открытый универсальный конвертор типовых промышленных протоколов передачи данных для обеспечения обратной совместимости ОАСУТП с действующими АСУ ТП

МЕЖОТРАСЛЕВАЯ РАБОЧАЯ ГРУППА Открытая АСУ ТП

Основные разрабатываемые требования

1.Спецификации, технические требования и стандарты OpenАСУТП

1.1. Спецификации, технические требования и открытые стандарты промышленной автоматизации, охватывающих все отрасли промышленности и различные виды производств (непрерывные, дискретные и гибридные);
1.2. Единая информационная модель АСУТП (Уровни 0,1,2,3).

2. Аппаратное обеспечение (Hardware)

2.1. Требования к аппаратной части открытой IIoT-платформе для управления объектами промышленной автоматизации;
2.2. Требования к аппаратной части открытой распределенной системе управления (РСУ);
2.3. Требования и разработка микроэлектронных устройств для CPU (MIPS, RISC-V, ARM);
2.4. Требования и разработка микроэлектронных устройств для протоколов автоматизации (EtherCAT, ProfiBUS, ProfiNET);
2.5. Требования и разработка микроэлектронных устройств для модулей (DIO, AIO, высокоскоростного счета частоты HFC);
2.6. Требования и разработка для модулей рефлективной памяти (ReflectiveMemory);
2.7. Требования и разработка для модулей сбора и анализа данных процесса (Process data acquisition and analysis).

3. Программное обеспечение (Software)

3.1. Требования к программной части «Открытой IIoT-платформы для управления объектами промышленной автоматизации»
3.2. Требования к программной части «Открытой распределенной системы управления (РСУ)»
3.3. Требования и разработка «Открытой интегрированной среды разработки» (OpenIDE)
3.4. Требования и разработка «Открытого программного ПЛК» (OpenSoftPLC)
3.5. Требования и разработка открытых протоколов внутренней и внешней шины ПЛК
3.6. Контроль версий и изменений в проектах (локальный репозиторий, удаленный репозиторий)
3.7. Требования и разработка визуализации (WEB, HMI, SCADA)
3.8. Требования к ОСРВ для работы в АСУТП
3.9. Сбор и хранение данных процесса, диагностика и предиктивная аналитика

4. Информационная безопасность в OpenАСУТП

4.1. Требования к построения OpenАСУТП на объектах КИИ (ФЗ N187).

5. Функциональная безопасность

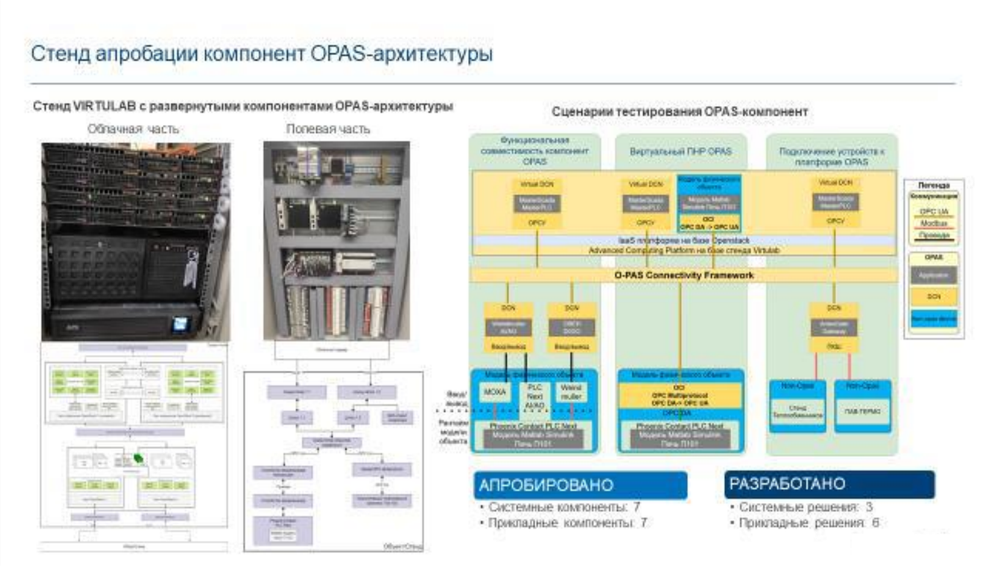
5.1. Требования к построению OpenАСУТП с УПБ (SIL).

МЕЖОТРАСЛЕВАЯ РАБОЧАЯ ГРУППА
Открытая АСУ ТП

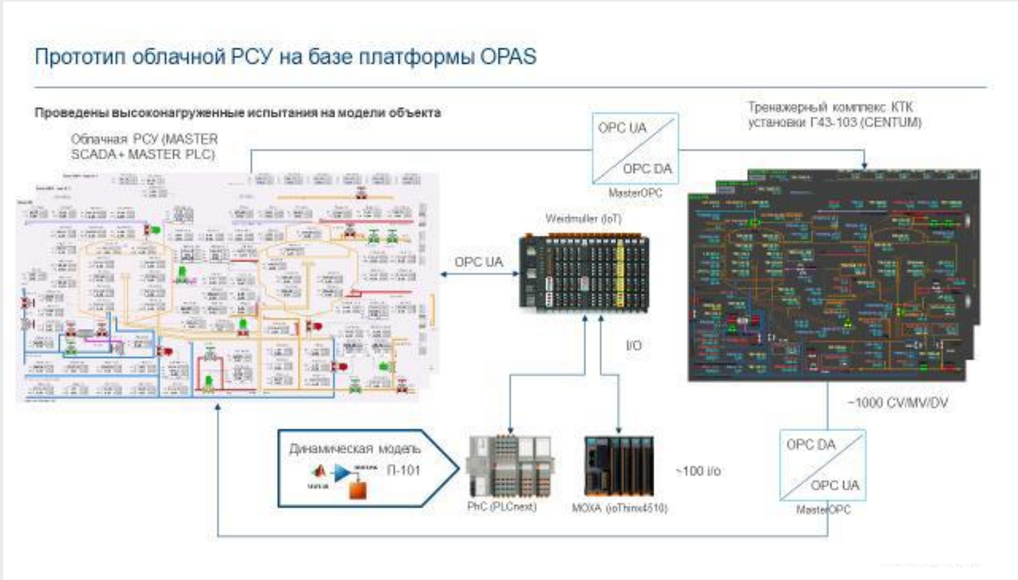
Первые результаты деятельности

Разработана типовая архитектура и схема сетевого взаимодействия системных платформ

Развернут стенд и произведена апробация компонент платформы на базе стандартов O-PAS



Разработан MVP: Развернут прототип **облачной РСУ** на базе стандартов O-PAS



Кибербезопасность в открытых стандартах

Развитие требований кибербезопасности в стандартах промышленной автоматизации

За рубежом

В России

Модель PERA
От PURDUE

- Сегментация сети
- Выделение DMZ
- Firewalls

Модель PERA
От PURDUE

Основополагающие требования ANSI/ISA-62443

- Identification & Authentication Control
- Use Control
- System Integrity
- Data Confidentiality
- Restricted Data Flow
- Timely Response to Events
- Resource Availability

Цели обеспечения безопасности O-PAS Part -2 Security

На базе Требований ANSI/ISA-62443

- Identification
- Authentication
- Non-repudiation
- Authorization
- Integrity
- Anomaly Detection
- Confidentiality
- Segmentation
- Auditability/Accountability
- Availability
- Incident Response

Open АСУ ТП

Что Будет/Должно учитываться ?:

- O-PAS Part -2 Security (?)
- ГОСТ-Р-МЭК-62443 (?)
- Требования 239 и 31 приказов ФСТЭК (?)
- Взаимодействие с НКЦКИ (?)
- Требования к доверенным ПАК ТК-167(?)
- РБПО (?)
- **Что ещё?**

Как началось — **Как стало** — **Как планируется**

1992 — 1999 — 2019 — 2023

Соотнесение со стандартами автоматизации в электроэнерегетике

Области соотнесения	O-PAS	NAMUR	Открытая АСУ ТП	ГОСТ Р 61850	ГОСТ Р 58651
Объектно-ориентированная информационная модель	Automation ML на базе XML	Спецификации OPC UA	Не определена Прототипы на базе AML	SCL на базе XML	CIM на базе XML
Объекты описания информационной модели	Основное оборудование и процессы	Устройства систем автоматизации, их функции	Не определены Объекты прототипа- основное оборудование	Устройства систем автоматизации, функции, параметрирование	Основное оборудование
Унификация информационного обмена	На базе OPC UA	На базе OPC UA	Не определены Прототипы на базе OPC UA	SV, Goose, MMS	TCP/IP
Требования к функциям безопасности ПО и оборудования	Определены, на базе IEC 62443	Не устанавливаются	Не определены	Не устанавливаются	Не устанавливаются
Требования к защищённости информационного обмена	Определены, на базе IEC 62443 и спецификации OPC UA	Определены, на базе IEC 62443 и спецификации OPC UA	Не определены	Не устанавливаются	Не устанавливаются
Требования к безопасности систем, создаваемых на основе стандарта	Не устанавливаются	Не определены	Не определены	Не устанавливаются	Не устанавливаются
Комплементарность национальным стандартам кибербезопасности КИИ	Отсутствует	Отсутствует	Отсутствует	Отсутствует	Отсутствует
Комплементарные национальные отраслевые стандарты безопасности	Отсутствуют	Отсутствуют	Отсутствуют	Отсутствуют	Отсутствуют

Текущая ситуация в понимании ИБ-отрасли

Открытые стандарты промышленной автоматизации устанавливают базовые требования к подходам по обеспечению и функциям кибербезопасности. Или как минимум стремятся к этому.

Стандарты в электроэнергетике частично пересекаются с открытыми стандартами промышленной автоматизации, но никаких базовых требований к функциям кибербезопасности не устанавливают

Нормативные требования в области безопасности КИИ слабо соотносятся со новыми и перспективными стандартами в области промышленной автоматизации

Обеспечение импортонезависимости и вендоронезависимости путём перехода на новый открытый технологический стек без учёта требований по кибербезопасности несёт большие риски. Но прямой перенос требований безопасности КИИ не возможен и контрпродуктивен

Обеспечение функций и мер безопасности в соответствии с требованиями по безопасности КИИ в АСУ ТП на базе нового открытого технологического стека – серьёзный вызов для предприятий, отрасли пром автоматизации, и регуляторов. Его преодоление возможно только совместными усилиями.

Кибербезопасность в жизненном цикле АСУ ТП на базе новых стандартов

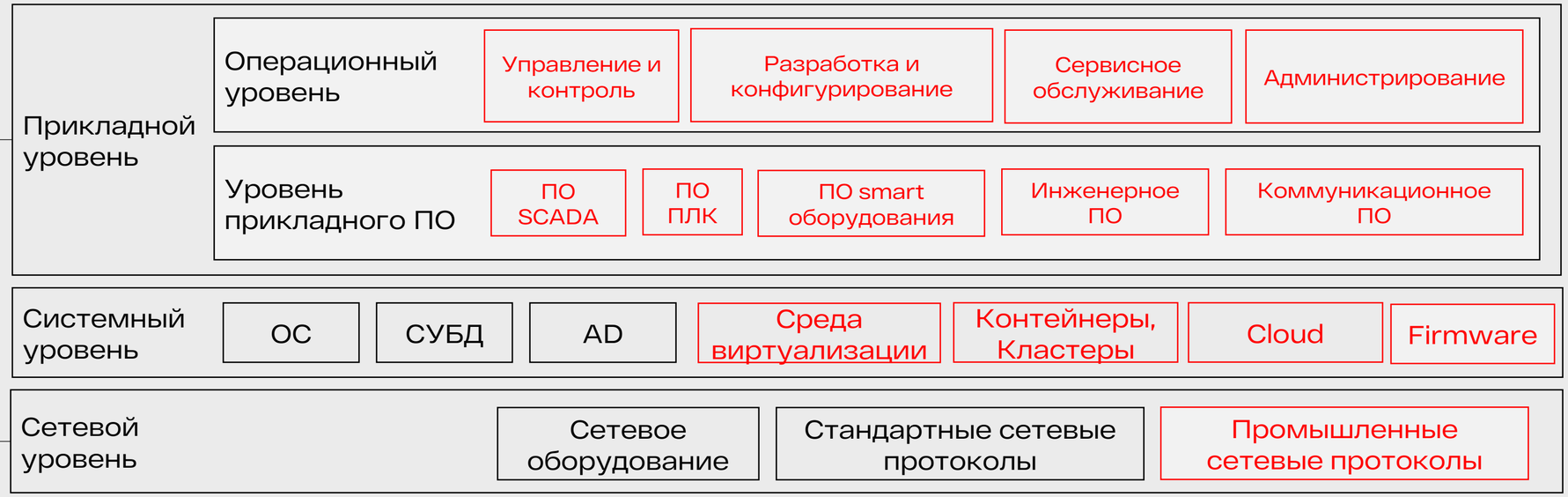
Application Security	Разработка компонент АСУ ТП		**PE AI** **PT BB** **DevSecOps IDE Plugins (free!)**	Построение и техническое обеспечение процессов безопасной разработки
		Эксплуатация АСУ ТП	**PT CS** **PT AF**	Защита контейнерных сред Межсетевое экранирование уровня приложений
Endpoint Detect & Response			**MaxPatrol EDR**	Обнаружение целевых и сложных угроз на конечных точках, реагирование
Incident management			**MaxPatrol SIEM**	Обнаружение и управление инцидентами безопасности
Vulnerability Management			**MaxPatrol VM**	Управление уязвимостями индустриальных систем, патч-менеджмент
Network Security			**PT ISIM**	Обнаружение вторжений и аномалий в технологической сети, Threat Hunting
Anti-Malware			**PT Sandbox**	Обнаружение и анализ вредоносного контента, вирусов, инструментов APT

Индустриальная экспертиза в продуктах PT

		Siemens	AdAstra	AVEVA	МПС	Rockwell	Yokogawa	Schneider Electric	«Атомик Софт»
MaxPatrol VM	▪ Сканеры SCADA, firmware ▪ Обнаружение уязвимостей	🕒	🕒	🕒	🕒	🕒	🕒	🕒	🕒
MaxPatrol SIEM	▪ Транспорты к проприетарному software и firmware ▪ Нормализации событий SCADA, Firmware ▪ Кейс-ориентированные корреляции	✓	✓	✓	✓	🕒	✓	🕒	🕒
PT ISIM	▪ Поддержка промышленных сетевых протоколов ▪ Детекты новых угроз и атак ▪ Цепочки инцидентов в технологическом трафике	✓	✓	✓	🕒	✓	✓	✓	✓
PT Sandbox	▪ Эмуляция технологических сред ▪ Обнаружение АСУ ТП-специфичного ВПО	✓	✓	✓	🕒	🕒	🕒	✓	🕒
MaxPatrol EDR	▪ Совместимость с промышленным hardware/software ▪ Сканирование, инвентаризация, ИТ- мониторинг на конечных узах АСУ ТП ▪ Правила обнаружения, работающие на конечных узлах АСУ ТП	🕒	🕒	🕒	🕒	🕒	🕒	🕒	🕒

Безопасность в рамках эксплуатации АСУ ТП

Покрытие функциями безопасности на базе решений и технологий PT



Какие кейсы безопасности в системах пром автоматизации уже можно решать с технологиями Positive Technologies

Прикладной уровень

- Легитимность и корректность пользовательских операций в среде исполнения
- Легитимности и корректность использования инженерного ПО, IDE-среды SCADA, проектов PLC и Safety
- Подмена/модификация конфигураций и проектов SCADA, PLC и Safety терминалов
- Деструктивные воздействия и операции изнутри и извне систем управления (саботаж, использование ресурсов не по назначению)

Сетевой уровень

- Обнаружение подключение к внешним сетям и интернет
- Обнаружение подключения к сети новых сетевых узлов/хостов
- Контроль целостности сети и сетевого обмена, обнаружение аномалий
- Ретроспективный анализ событий, инцидентов, изменений сети

Узнайте больше о Позитиве

habrahabr.ru/
company/pt

t.me/
positive_technologies

vk.com/
ptsecurity

t.me/
positive_investing

ptsecurity.com