КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КАК ПРИМЕНЯТЬ АНАЛИТИЧЕСКИЕ СРЕДСТВА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ ПРЕДПРИЯТИЙ ТЭК?

НИКОЛАЙ НАШИВОЧНИКОВ
ООО «Газинформсервис»

План доклада

01 Киберфизические системы

Киберфизические системы (Cyber-Physical System (CPS)) в ТЭК
Операционный мониторинг и анализ безопасности CPS - заинтересованные стороны
Практики расширенной аналитики (Advanced Analytics) CPS

02 Анализ безопасности киберфизических систем

Ключевые направления применения аналитических средств
Отличительные особенности системы операционного мониторинга и анализа
Комплексный анализ безопасности киберфизических систем

03 Практический опыт

Результаты апробации на реальном объекте ТЭК
Проблемные вопросы

04 Архитектурные решения аналитической платформы

Методология и реализация

05 Заключение

КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ
Cyber-Physical System (CPS)

Многообразие устройств (датчиков) со встроенными процессорами и средствами хранения данных

Интеграция систем разных производителей в огромные комплексы

Функционирование в рамках единой газотранспортной сети крупного предприятия

Актуальность эффективной системы операционного мониторинга и анализа киберфизических систем критической информационной инфраструктуры (КИИ) в эпоху четвертой промышленной революции (INDUSTRY 4.0)

Заинтересованные стороны

Собственник предприятия ТЭК

Стабильный доход за счет сокращения расходов

Эксплуатирующая организация

Контроль (governance) безопасности

Персонал ТЭК (Операторы)

Оптимизация процессов при заданных требованиях безопасности

Поставщики\Потребители продукции ТЭК

Безусловное выполнение контрактных обязательств

Производители\Интеграторы систем

Переход к комплексному анализу безопасности

Требования регуляторов

Промышленная безопасность

Экологическая безопасность

Информационная безопасность

Встроенная безопасность

- Жизненный цикл индустриальных CPS 10–30 лет
- Сложность своевременного устранения уязвимостей и обновления ICS/SCADA
- Разработчики индустриальных CPS ориентированы прежде всего на выполнение требований функциональной и промышленной безопасности
- Встроенные функции ИБ не развиты или отсутствуют

Информационная безопасность

Конфиденциальность

Целостность

Доступность

Приоритеты

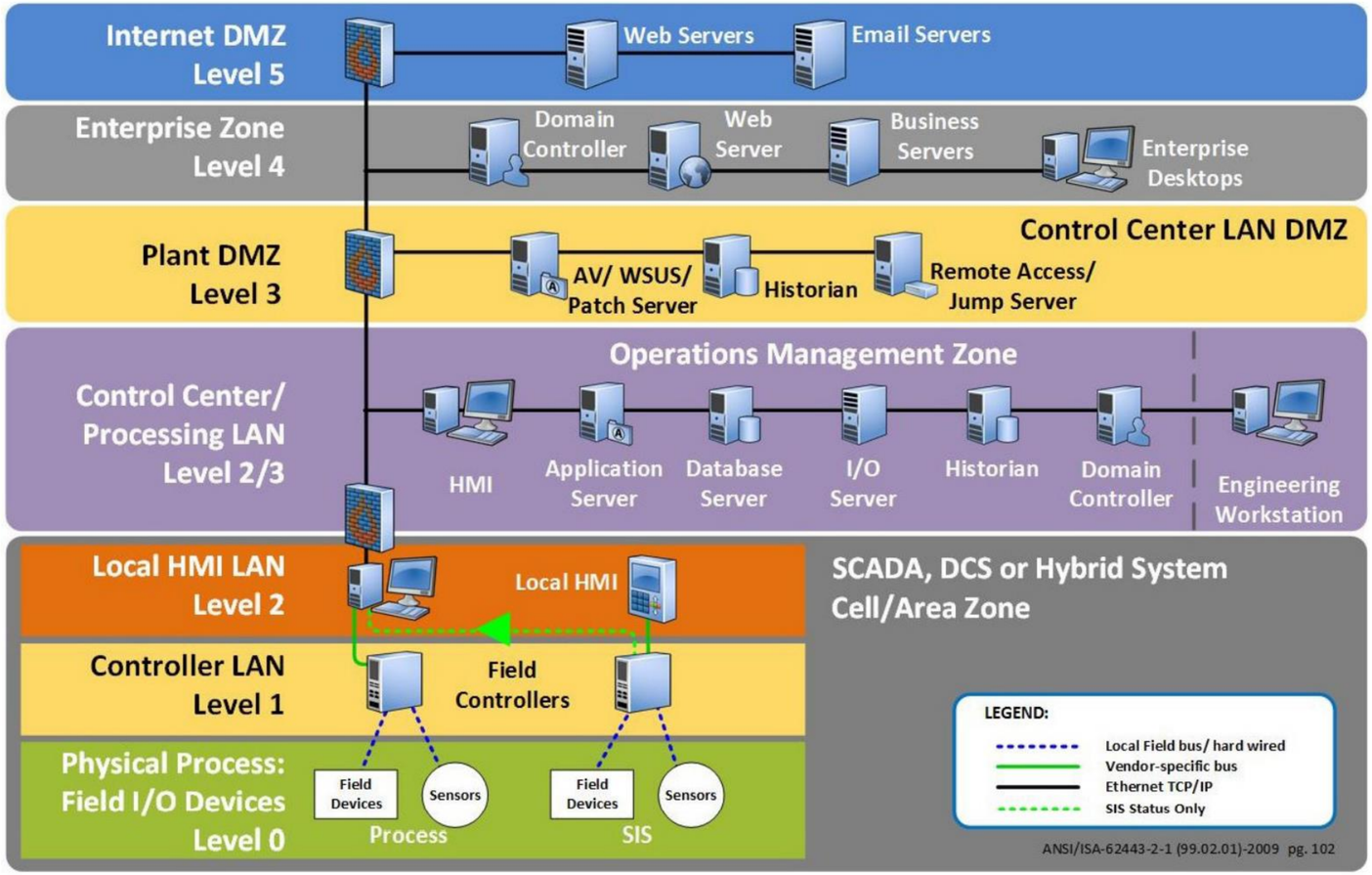
Функциональная безопасность

Доступность

Целостность

Конфиденциальность

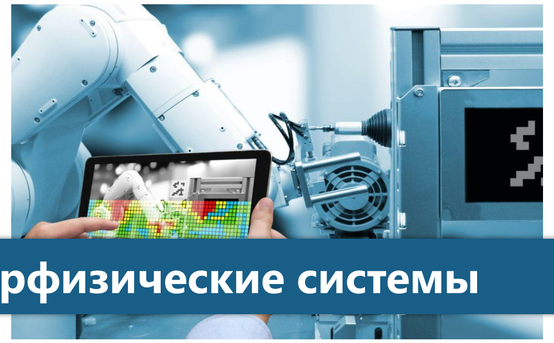
Типовая архитектура АСУ ТП



Применение аналитических средств

Ситуационные центры

Объекты ТЭК



Киберфизические системы

Система операционного мониторинга и анализа (СОМА)

Комплексный анализ

Выявление скрытых причинно-следственных связей компонентов и систем.
Выявление и прогнозирование аномалий в функционировании технологических объектов и ICS

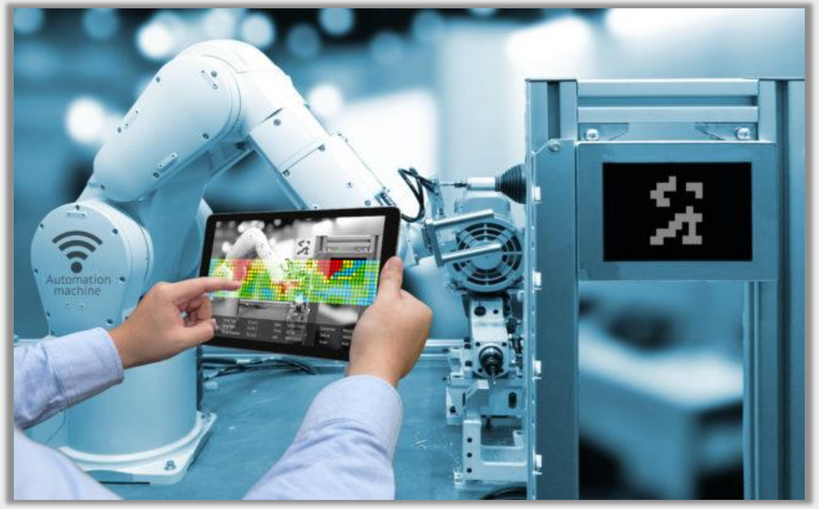
Практики анализа

Машинное обучение, сопоставление образцов, прогнозирование, визуализация, сетевой и кластерный анализ, интеллектуальный анализ данных/текста, анализ графов, обработка сложных событий, нейронные сети

Сложные методы и инструменты

Исследование данных или контента требует использование передовых методов и инструментов анализа данных

Отличительные особенности СОМА



Анализ безопасности по трем направлениям

Комплексный анализ сенсорных данных, ИТ-метрик и событий ИБ

Независимость СОМА от ПО ICS/SCADA

Инвариантность к алгоритмам управления ТП, реализованным в индустриальных приложениях конкретных производителей

Минимальное влияние СОМА на объект КИИ

Независимость от контура диспетчерского управления и систем автоматического управления ТП

Интероперабельность ICS/SCADA и СОМА

Сбор сигналов управления технологических процессов низкого уровня (direct access (DA)) из OPC–сервера SCADA согласно стандарту OPC DA

Комплексный анализ безопасности ICS/SCADA

ИТ-мониторинг

- Поиск аномалий, корреляций и скрытых зависимостей в работе оборудования инфраструктурного обеспечения
- Прогнозирование отказов, выхода из строя оборудования с целью оптимизации технического обслуживания и ремонта

ИБ

- Повышение эффективности процесса обеспечения защиты ICS/SCADA
- Мониторинг использования слабых мест SCADA
- Выявление аномальных действий пользователей; изменений настроек; нетипичного поведения CPS

Технологический процесс

- Поиск аномалий в работе компонентов ICS
- Прогнозирование отказов, выхода из строя компонентов технологического оборудования с целью оптимизации технического обслуживания и ремонта оборудования
- Исключение ошибок операторов

Комплексный анализ

- Задачи класса «больших данных»
- Режим, близкий к реальному времени
- Поведенческий анализ

Практический опыт применения аналитических средств

Подсистема сбора первичной информации

Подсистема анализа информации

Подсистема отображения информации

- СОДУ, АСУ ТП КЦ, САУ ГПА
- Системы энергообеспечения (АСУ Э, АСУ ЭСН)
- Системы промышленной безопасности
- Системы ИТСО

Сбор информации

Анализ ТП-параметров

Мониторинг ИТ-окружения

Сбор событий безопасности

Расчет ключевых показателей

Ретроспективные данные

Статистические показатели

Прогнозные показатели

Аномалии (отклонения) в ТП

Сложные инциденты безопасности

Положительные результаты апробации

Востребованность COMA при пусконаладочных работах

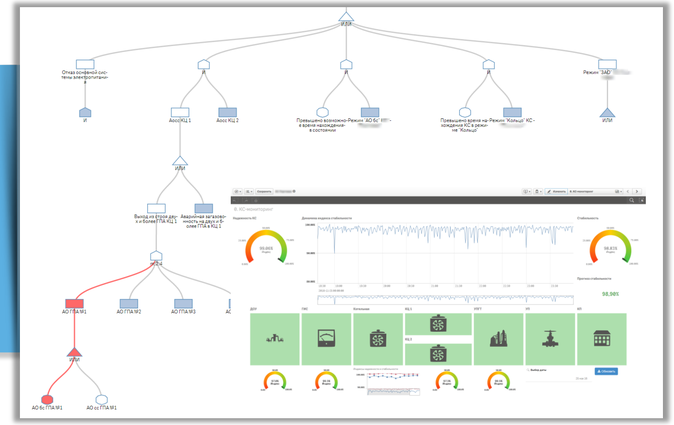
COMA наиболее востребованы во время испытаний и настройки совместного функционирования CPS на этапах опытной эксплуатации, ввода в строй и начала эксплуатации новых и модернизируемых объектов

01

02

Полезность статистических методов при обнаружении аномалий

Статистические индикаторы стабильности, модели деревьев отказов, методы визуального анализа в интерактивном режиме на основе ассоциативной модели данных в оперативной памяти позволили выявить ряд аномалий в технологических процессах



Перспективы применения COMA

В качестве перспективного направления применения COMA указаны задачи выявления аномального поведения операторов, объектов управления ICS, процессов работы SCADA

03

Проблемы готовности СОМА к промышленному применению

01 Проблема исходных данных

02 Проблема сложности объектов мониторинга и анализа

03 Проблема технико-экономического обоснования СОМА

04 Проблема игнорирования требований ИБ при разработке CPS (АСУ ТП)

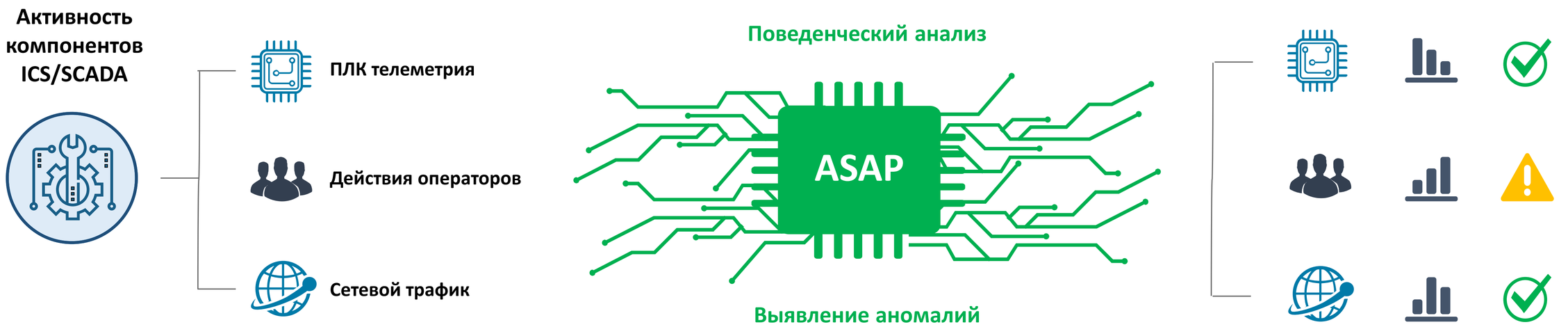
05 Проблема импортозамещения

Платформа расширенной аналитики безопасности Advanced Security Analytics Platform (ASAP)

01 Мониторинг поведения пользователей и объектов, построение моделей поведения и выявление аномалий посредством сложных статистических методов и машинного обучения

02 Предоставление расширенного набора инструментов для выявления признаков, расследования и сбора цифровых доказательств инцидентов ИБ

03 Прогнозирование поведения пользователей и объектов



Используемый подход Ankey ASAP

Хранилище данных (Data Warehouse/ Data Lake)

СБОР И ХРАНЕНИЕ

События ИБ от SIEM
Данные ICS/SCADA
Span-трафик

Данные обогащения:

- Нормативно-справочная и плановая информация
- Конфигурация ИТ-инфраструктуры и индустриальных объектов
- AD (домены, аккаунты)

Поведенческая аналитика (User and Entity Behavior Analytics (UEBA))

ТРАНСФОРМАЦИЯ И ПРОФИЛИРОВАНИЕ

Автоматическое формирование сессий пользователей.
Привязка событий ИБ к сессиям.
Предоставление методик для формирования моделей и профилей поведения пользователей, устройств и других сущностей

ОБНАРУЖЕНИЕ

Anomaly Detection
Выявление аномалий в наборах данных посредством использования алгоритмов машинного обучения и методов статистики

Risk Scoring
Оценка поведения пользователей и сущностей в соответствии с настроенными показателями

Реагирование на инциденты (Incident Response Platform (IRP))

РЕАГИРОВАНИЕ И РАССЛЕДОВАНИЕ

Информационно-аналитическая поддержка реагирования на инциденты ИБ, расследования и сбора цифровых доказательств инцидентов ИБ (use case/playbooks)

Предоставление инструментов расширенного визуального анализа для выявления признаков и формирования историй анализа (storytelling)

КАК ПРИМЕНИТЬ АНАЛИТИЧЕСКИЕ СРЕДСТВА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ ПРЕДПРИЯТИЙ ТЭК?

1. В соответствии с требованиями многоаспектного мониторинга безопасного функционирования объектов ТЭК применить комплексный подход к анализу, позволяющий определить степень взаимного влияния отдельных компонентов

2. В условиях дефицита специалистов набирать экспертизу в применении комплексной аналитики безопасности по частям: начинать с пилотов и апробированных методов аналитики, переходя потом к более сложным задачам и «изощренным» методам ML

3. При вводе в эксплуатацию и в начале эксплуатации технологических объектов, когда наблюдается наибольшее число аномалий в интегрируемых CPS, комплексная аналитика и инструменты расширенной аналитики наиболее востребованы

4. Промышленному характеру использования COMA должны соответствовать зрелые программные решения, разработанные на платформенных принципах и основанные на современных стеках технологий обработки больших данных

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

cto@gaz-is.ru