«Технологии QNX и КПДА в России»

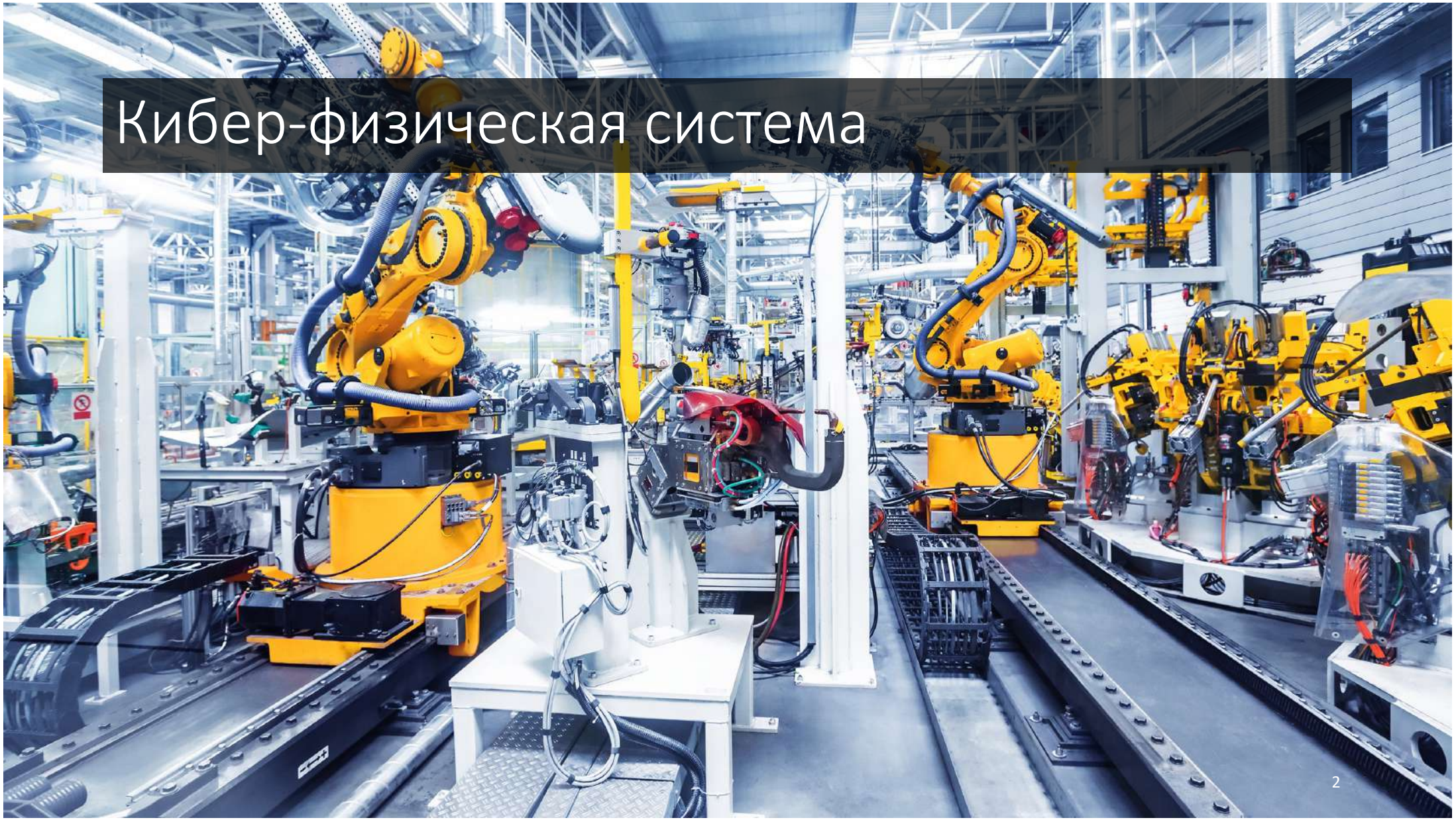
20 ноября 2019, Санкт-Петербург

Вопросы обеспечения информационной и функциональной безопасности в промышленных системах

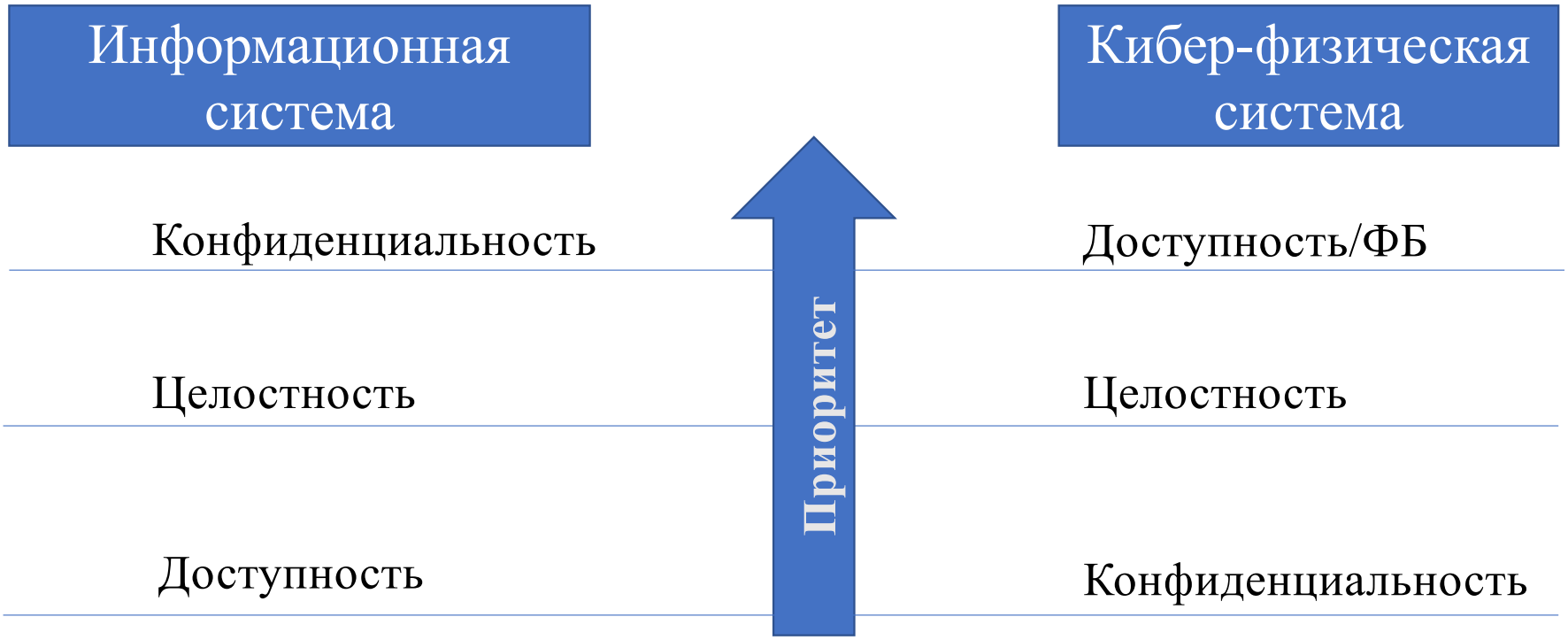
Сергей Зыль, ООО «СВД Встраиваемые Системы»

СВД Встраиваемые Системы

Кибер-физическая система

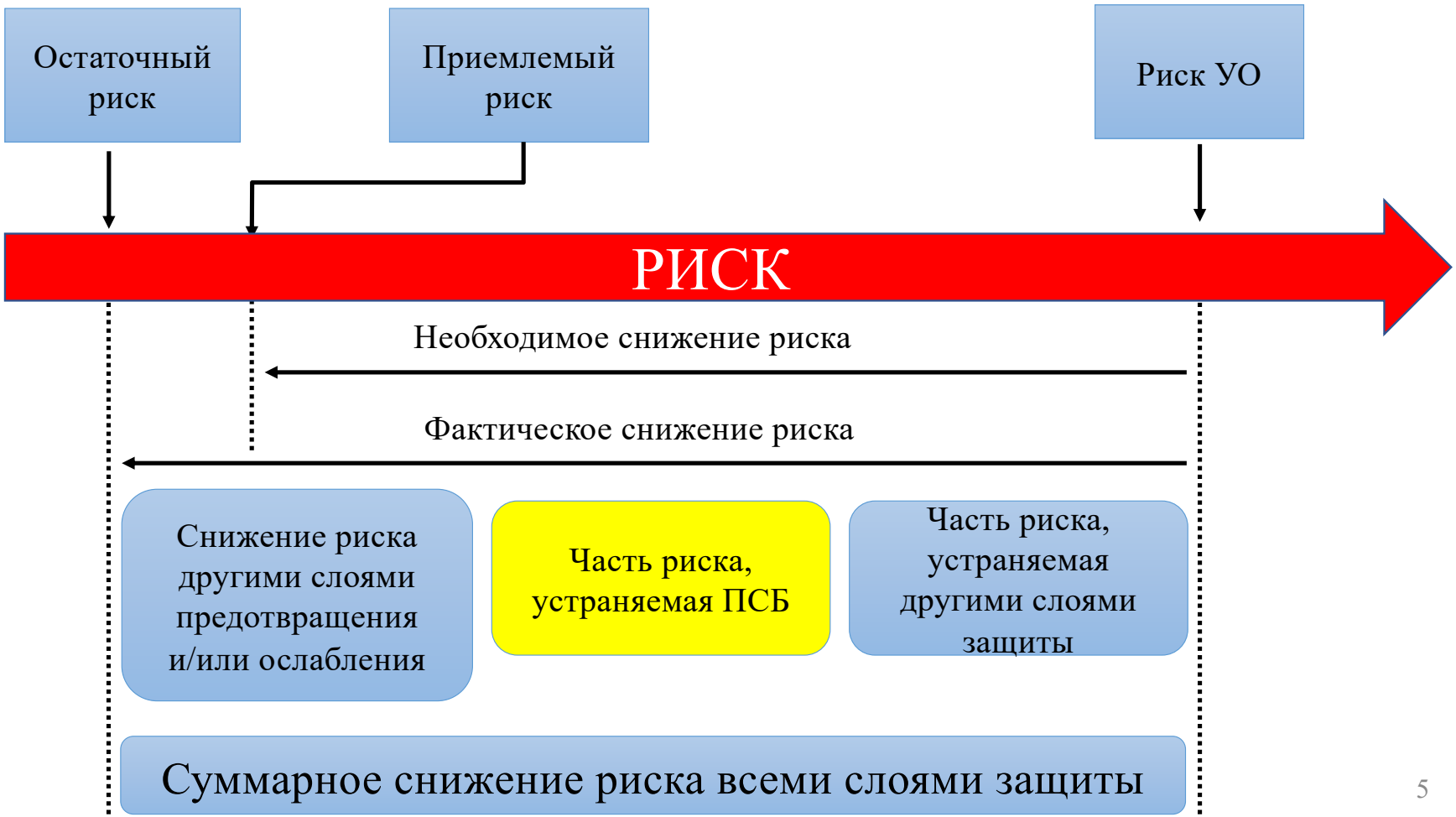


ISA/IEC 62443
Приоритетность задач кибербезопасности



Функциональная безопасность

ФБ – инструмент снижения риска



TÜV Rheinland: необходимость МЭК 61508

«Законодательная определенность»

«State-of-Art»

SIL
IEC 61508 / IEC 61511

IEC INTERNATIONAL ELECTROTECHNICAL COMMISSION

Международное признание

Планирование безопасности
разработчиками и эксплуатантами

Начало внедрения ФБ: формирование культуры безопасности

Safety Culture: примеры признаков

- Сильная зависимость от тестирования в конце разработки
- Руководство реагирует только тогда, когда возникают проблемы
- Система вознаграждения отдает предпочтение стоимости и графику работ, а не безопасности и качеству

- Интеллектуальное разнообразие ищут, ценят и включают во все процессы
- Системы вознаграждения наказывает тех, кто обходит вопросы, которые ставят под угрозу безопасность или качество
- Процесс обеспечивает систему сдержек и противовесов в процессах обеспечения безопасности, управления конфигурацией и др.

Результаты внедрения МЭК 61508

МЭК 61508

СВД ВСТРАИВАЕМЫЕ СИСТЕМЫ

Подготовка специалистов

«Проектирование программного и аппаратного обеспечения в соответствии с ГОСТ Р МЭК 61508»

Аккредитован в СДС ФБ
(Рег. № РОСС RU.31461.04ИДД0)

Кибербезопасность

Уровни защиты (SL) по ISA/IEC 62443

Защита против **намеренного** вторжения с использованием **специализированных** средств и **расширенных ресурсов** (недружественные государства, террористы)

Защита против **намеренного** вторжения с использованием **специализированных** средств (хактивисты, хакеры выс. квал.)

Защита против **намеренного** вторжения с использованием **простых** средств (хакеры ср. квал., инсайдеры)

Защита против **несистемных или случайных вторжений** (хакеры низ. кв., ошибки персонала)

Уязвимости СРВ: Закладки («бэкдор»)

Назначение закладки	Наличие умысла предоставить доступ нарушителю	
	Намеренно	**Не преднамеренно**
Не вредоносное	Для обеспечения удалённого технического сопровождения	Средства анализа и верификации, непреднамеренно оставленные в работоспособном состоянии
Вредоносное	Спроектирован предприятием-разработчиком (или его сотрудниками) для скрытого использования СРВ после ввода в эксплуатацию	Неизвестный предприятию-разработчику бэкдор, оставленный сотрудником для личного пользования (например, по легкомыслию)

Типовые проблемы ИБ в системах реального времени

- Оставлены пароли по умолчанию
- Не выполняется периодическая смена паролей
- Отключены аудит и регистрация
- Оставлено диагностическое ПО и диагностические учетные записи (возможно, даже без паролей)

СВД ВСТРАИВАЕМЫЕ СИСТЕМЫ

Противодействие ВКП: Методы разработки

- Безопасное программирование
- Статический анализ исходных текстов

Олег Игоревич Большаков

Мастер-класс: Приёмы безопасного программирования при разработке ПО для ЗОСРВ «Нейтрино»

Секция 2
14:00-14:30

Противодействие ВКП: ПК АВЗ

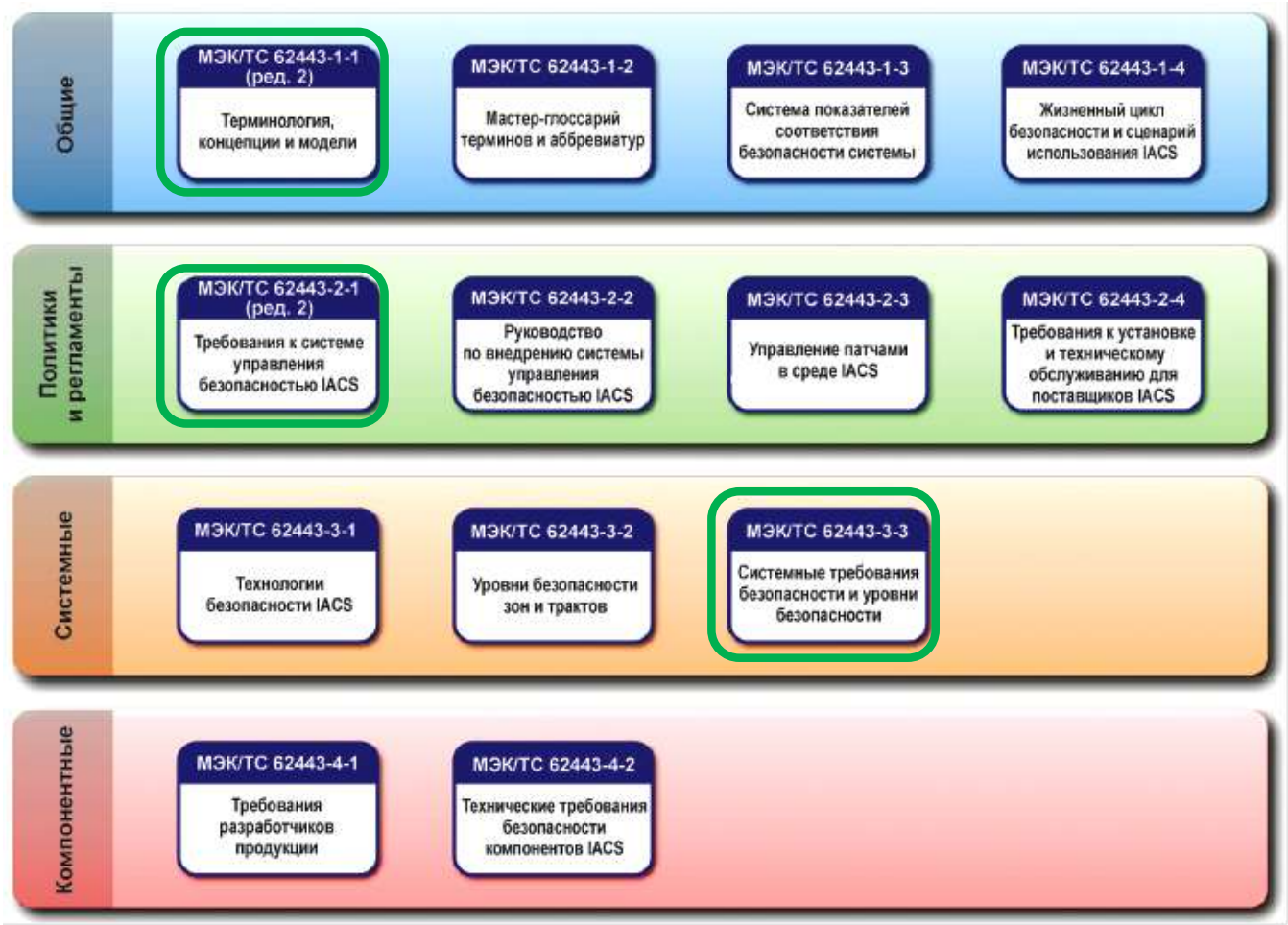
- Проверка модулей для включения в состав среды исполнения
- Проверка файлов, получаемых по коммуникационным каналам
- Проверка отчуждаемых носителей данных

ПК АВЗ: Поиск диагностических и уязвимых модулей

Противодействие ВКП: ЗОСРВ «Нейтрино»

- Эталонные контрольные суммы ОПО и СПО/ФПО
- Механизм замкнутой программной среды – «чёрные» и «белые» списки
- Контроль источника запуска программных модулей
- Рандомизация размещения адресного пространства
- др.

Стандарты ISA/IEC 62443



ГОСТ Р МЭК 56205-2014

Терминология, концептуальные положения и модели

ГОСТ Р МЭК 62443-2-1-2015

Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики

ГОСТ Р МЭК 62443-3-3-2016

Требования к системной безопасности и уровни безопасности

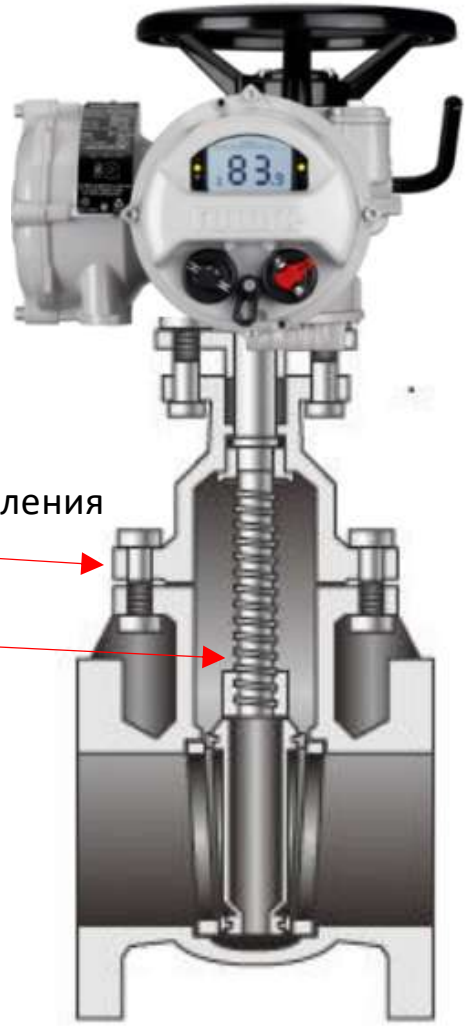
Промышленный интернет вещей (IIoT)

- Рост применения IIoT в различных отраслях является основным источником роста проблемы ИБ безопасности в киберфизических системах

Зачем нужен промышленный интернет вещей (IIoT)?

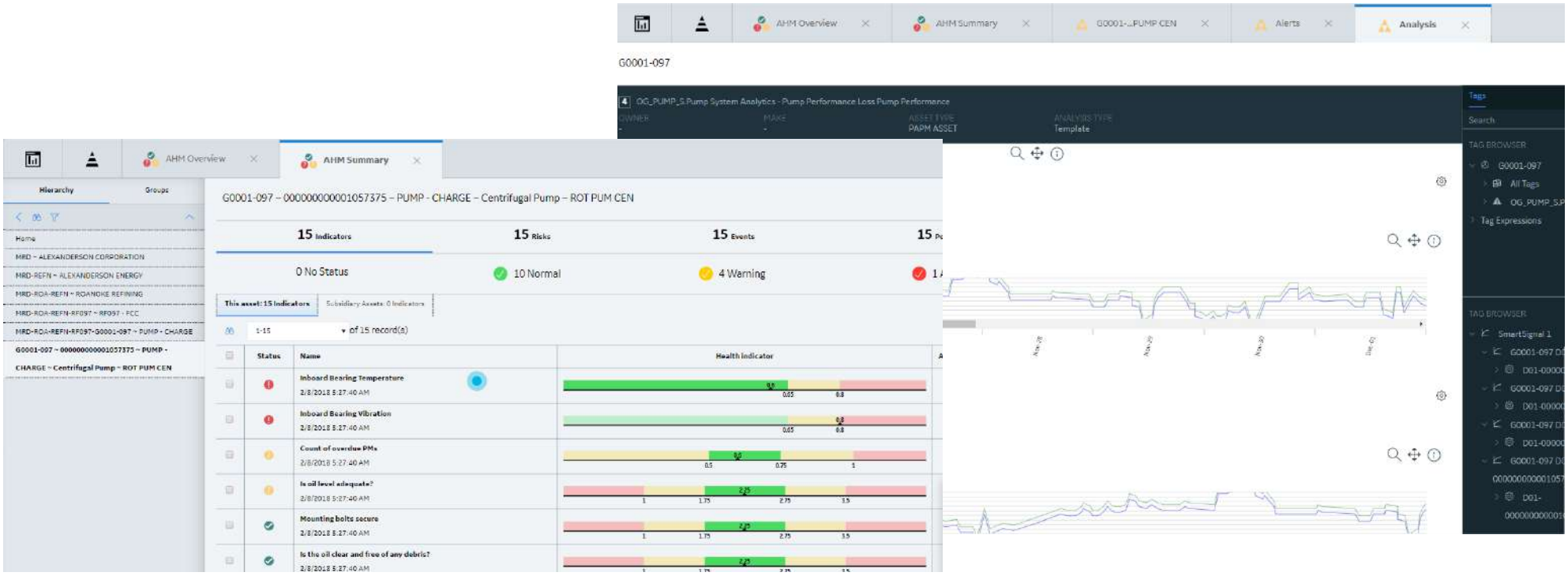
Предиктивный анализ:

- Контроль вибрации
- Контроль крутящего момента



- Отказы оборудования в результате постепенного износа
- У разработчиков накоплена статистика отказов
- Многие отказы можно предотвратить

Пример работы системы предиктивной диагностики эффективности насоса центрифуги



Выводы

- Функциональная и информационная безопасность – обязательные качества киберфизических систем
- Высокая эффективность и рентабельность решений IIoT ведет к росту их внедрения и – как следствие – к росту рисков ИБ
- Меры ФБ и ИБ не могут быть «добавлены» в конце проекта: они должны быть запланированы **ДО** начала проекта, а затем должны быть тщательно реализованы и поддерживаться в актуальном состоянии

Спасибо за внимание!

Сергей Николаевич Зыль

ООО «СВД Встраиваемые Системы»

СВД ВСТРАИВАЕМЫЕ СИСТЕМЫ