kaspersky

Kaspersky Industrial Cybersecurity Conference 2020

Сергей Соловьев

Руководитель Центра компетенций, ООО «Сименс»

#KasperskyICS

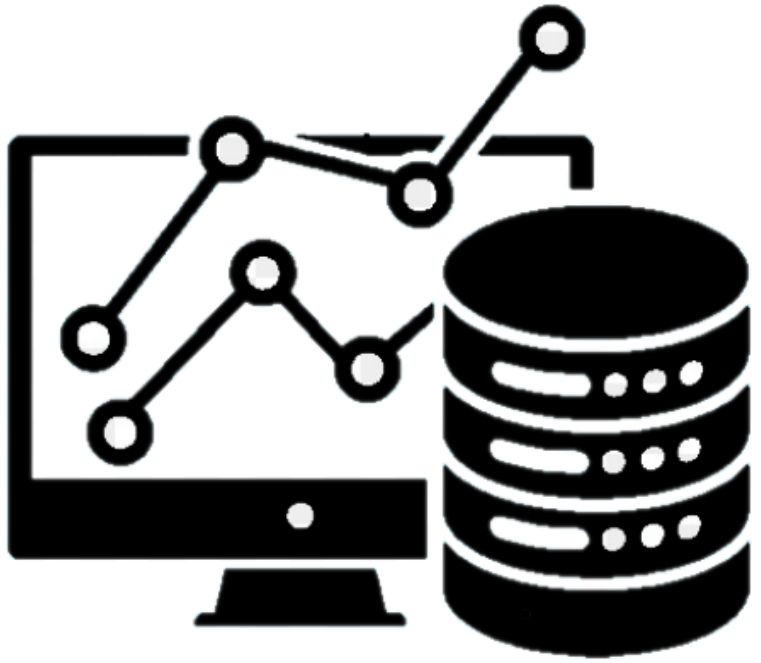
Чат конференции: https://kas.pr/kicscon

SIEMENS
Ingenuity for life

Обеспечение кибербезопасности современных SCADA-систем для критических инфраструктур в эпоху цифровизации

SCADA: какие буквы теперь главные?

SIEMENS
Ingenuity for life



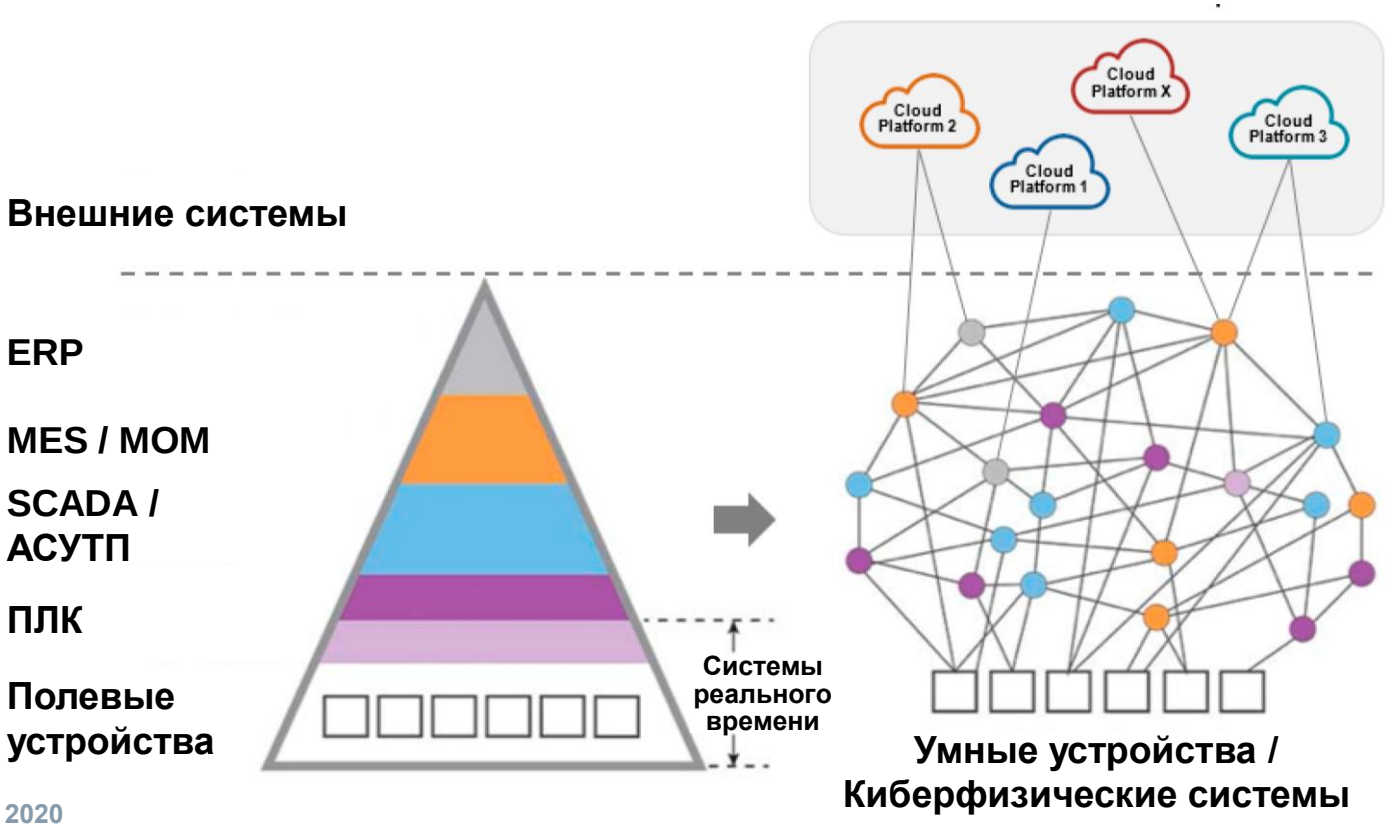
SCADA

sC**A**D**A**

Acquisition?
Analytics?

Тезис #1:

Пирамиды больше нет (скоро точно не будет), Cloud и Edge проникают, киберфизические системы крепнут и обрастают связями



Облачные платформ приложен

Периферийн вычислени

SIMATIC Industrial Edge

Распределённые управление и обработка данных

WinC OA

На основе: Monostori, L.; Kádár, B.; Bauernhansl, T.; Kondoh, S.; Kumara, S.; Reinhart, G.; Sauer, O.; Schuh, G.; Sihn, W.; Ueda, K. Cyber-physical systems in manufacturing. CIRP Ann. 2016

Тезис #2:

Интеграция всего со всем, углубление интеграции, вертикальная интеграция, горизонтальная интеграция, ещё больше интеграции

НСИ

ERP

Цифровые двойники

ТОиР

Оперативное управление производством

Энергоучёт и энергоменеджмент

Склад и логистика

Мониторинг и контроль персонала

Контроль охраны труда

Противоаварийная защита

Локальное позиционирование

Экологический контроль

ГИС

Планирование

Идентификация и прослеживаемость

Управление техпроцессом

Видеонаблюдение

Иллюстрация тезиса #2:
WinCC OA – Основные поддерживаемые протоколы и технологии

SIEMENS
Ingenuity for life

dnp

Modbus

IEC
МЭК 61850
МЭК 61400
МЭК 60870

PROFINET®

SIMA S7
SIEMENS

CERTIFIED FOR COMPLIANCE OPC FOUNDATION
OPC UA™

EtherNet/IP™

MindSphere

MQTT.ORG

ASHRAE BACnet™

ADO, XML, XML Parser, XML-RPC-Interface, TCP, Websockets, Open API, …

Тезис #3:

Аналитика позволяет выжать всё самое вкусное из данных разных видов, сортов и происхождения

Временные ряды (параметры процесса)
Видеопоток
Геоданные
Параметры окружающей среды
…

Тренды
Алармы
КПЭ
Прогноз
Оптимизация
Принятие решений

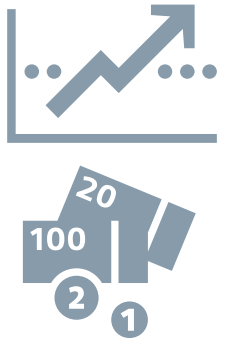


Иллюстрация тезиса #3:
WinCC OA SmartSCADA

SIEMENS
Ingenuity for life

Что можно сделать:

- Расчёт и анализ КПЭ
- Выявление причинно-следственных связей
- Поддержка при принятии решений
- Системная оптимизация

Что для этого есть:

- Инструменты, библиотеки и шаблоны
- Алгоритмы машинного обучения
- Интерфейс к языку R
- Сценарии пользователя
- Open API
- Интеграция с цифровыми двойниками

Тезис #4:

Многоуровневая, распределённая, … – этих слов уже мало, чтобы описать архитектуру современной SCADA-системы

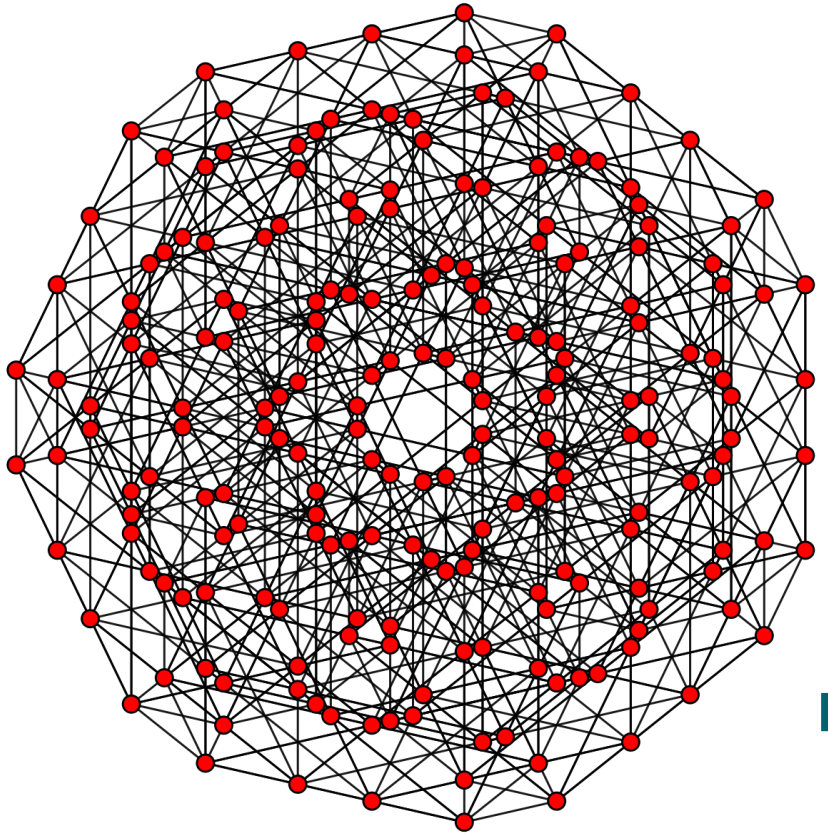
SIEMENS
Ingenuity for life

Масштабируемая

Динамически реконфигурируемая

Адаптивная

Робастная



Мультиплатформенная

Гетерогенная

Резервированная

Катастрофоустойчивая

Иллюстрация тезиса #4:
Аппаратные платформы и операционные системы, поддерживаемые WinCC OA

SIEMENS
Ingenuity for life

Raspberry Pi

IoT2040

Nanobox IPC

PC

Server

Data Center

До **10 млн. внешних тегов**, до **2 048 серверов** в распределённых системах
Резервирование и **катастрофоустойчивые конфигурации 2x2**

Windows 10 · Windows Server 2016 · Windows Server 2019 · Red Hat · openSUSE · CentOS · iOS · Android

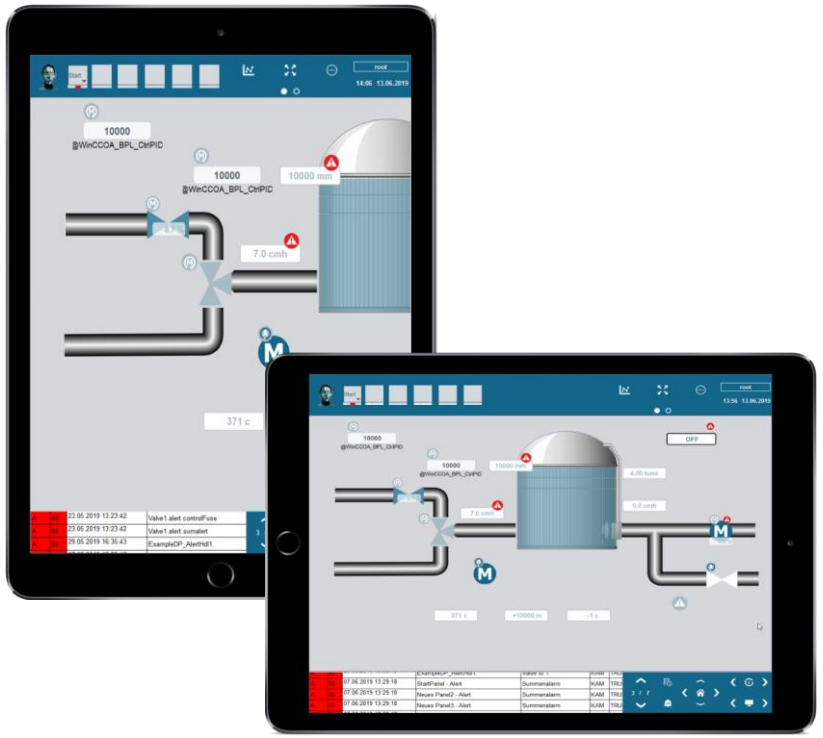
+ средства виртуализации, скоро – поддержка Astra Linux и SIMATIC Industrial OS

Тезис #5:

Мобильные устройства и носимая электроника в контуре SCADA – это актуальный User Experience, а не ошибка при предоставлении прав доступа

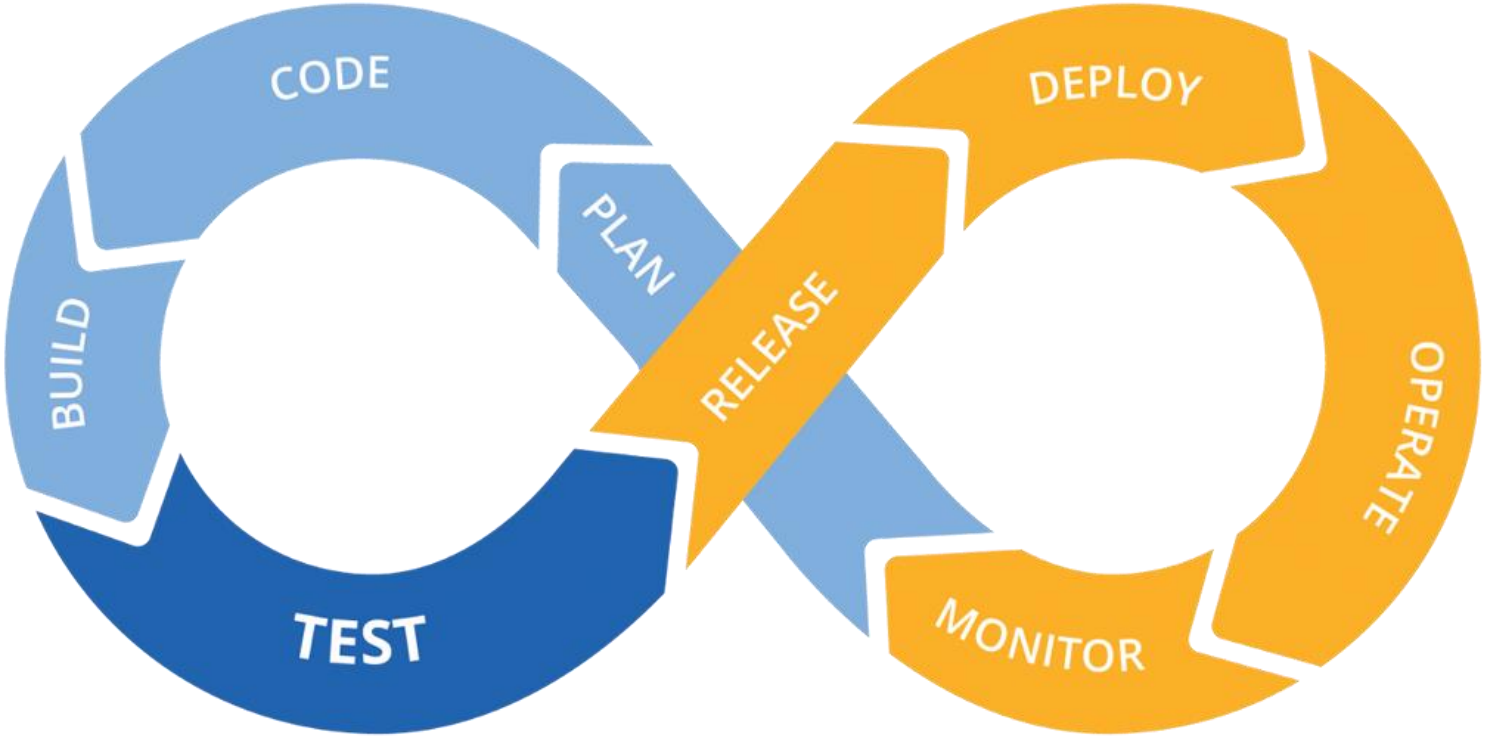
Иллюстрация тезиса #5:
Мобильные клиенты WinCC OA для iOS и Android, интеграция с SiWatch (умные часы, браслеты, каски, носимые метки)

SIEMENS
Ingenuity for life



Тезис #6:

Инжиниринг, внедрение и сопровождение SCADA-проектов – не просто Drag&Drop и использование Wizard’ов, а полноценный DevOps



Цепочка ценности SCADA: вчера, сегодня завтра

SIEMENS
Ingenuity for life

Вчера

1. **Подключение** оборудования и систем (ПЛК, RTU, КИП, АСУТП/ПАЗ…),
2. **Визуализация** состояния, трендов, предупредительная и аварийная сигнализация
3. Удалённое **управление** установкой / оборудованием / техпроцессом

Цель: обеспечить прозрачность и ситуационную осведомлённость для своевременного принятия решений по поддержанию требуемых производственных показателей и/или показателей эффективности

Завтра (сегодня?)

1. **Интеграция** источников данных и сопряжённых информационных систем
2. **Обработка** данных с использованием аналитики, моделирования, оптимизации
3. Запуск и **использование** информационных **сервисов**. Адаптация / модификация к меняющимся требованиям

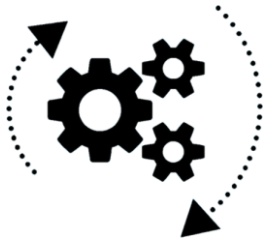
Цель: построение сквозных информационных цепочек, обеспечивающих целевое управление производственными и/или инфраструктурными активами и операциями, с использованием традиционных и новых бизнес-моделей

SCADA и облако: отличительные особенности

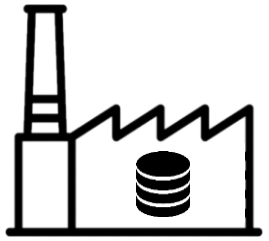
SIEMENS
Ingenuity for life

SCADA – платформа для оперативного управления и интеграции производственных систем и инфраструктуры предприятия

Сбор и обработка данных в режиме реального времени

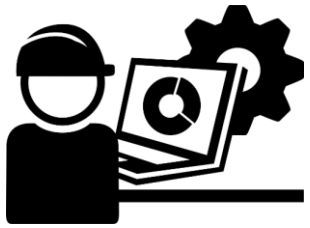


Замкнутые контуры управления



Локальное хранение данных в

Функциональная безопасность

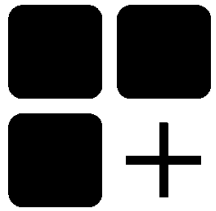


Контроль критических процессов

Выполнение спец./корп. требований

Облако – экосистема готовых приложений для запуска цифровых сервисов и построения кооперационных цепочек

Озеро данных



Экосистема готовых приложений

Совместная обработка данных из различных источников

Цифровые сервисы и кооперационные цепочки

Использование моделей знаний (семантика, онтология)

Комплексный подход к кибербезопасности SCADA

Аспекты обеспечения кибербезопасности SCADA:

- Обеспечение безопасности **процесса разработки самой SCADA**;
- Безопасность **SCADA как компонента** решения / ландшафта информационных систем;
- **Процессы инжиниринга, внедрения и эксплуатации** решения.

Охват:

- **Установки / системы / производства** в целом;
- Информационные **сервисы**;
- **Сквозные цепочки** обеспечения продуктивности / кооперации.

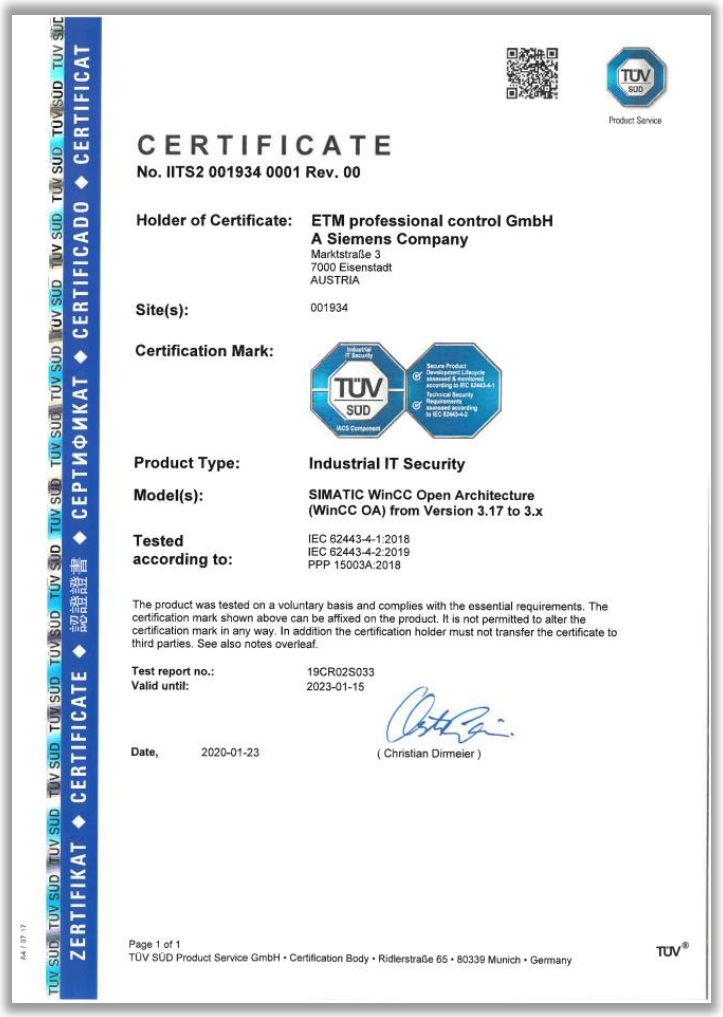
SIEMENS
Ingenuity for life

Комплексная концепция Siemens основана на стандарте

МЭК 62443

Сертификация по МЭК 62443-4-1 и МЭК 62443-4-2

SIEMENS
Ingenuity for life



CERTIFICATE
No. IITS2 001934 0001 Rev. 00

Holder of Certificate: ETM professional control GmbH
A Siemens Company
Marktstraße 3
7000 Eisenstadt
AUSTRIA

Site(s): 001934

Certification Mark:

Product Type: Industrial IT Security

Model(s): SIMATIC WinCC Open Architecture (WinCC OA) from Version 3.17 to 3.x

Tested according to: IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003A:2018

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: 19CR02S033
Valid until: 2023-01-15

Date, 2020-01-23 (Christian Dirmeier)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

4-1: Уровень зрелости процессов разработки – ML 3

4-2: Выполнение требований к уровням безопасности:

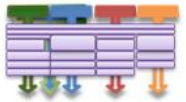
	SL-C 1	SL-C 2	SL-C 3	SL-C 4
Общее количество требований МЭК 62443-4-2	50	92	116	122
Количество релевантных требований (WinCC OA)	32	49	61	66
Количество выполненных требований (WinCC OA)	32	48	57	60
Выполнение требований	**100%**	**98%**	**93%**	**91%**

Процессы инжиниринга, внедрения и эксплуатации систем на базе WinCC OA

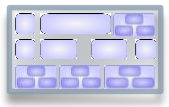
SIEMENS
Ingenuity for life

- **Руководство по обеспечению безопасности:**
  - Базируется на международных стандартах **IEC 62443/ISA99, ISO/IEC 15408**, **ISO/IEC 17799**, **ISO/IEC 27001**, **NA 67**, **NA 103**, **NA 115** и др.

Основные подходы

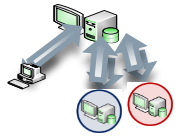


- **Многоуровневая защита**

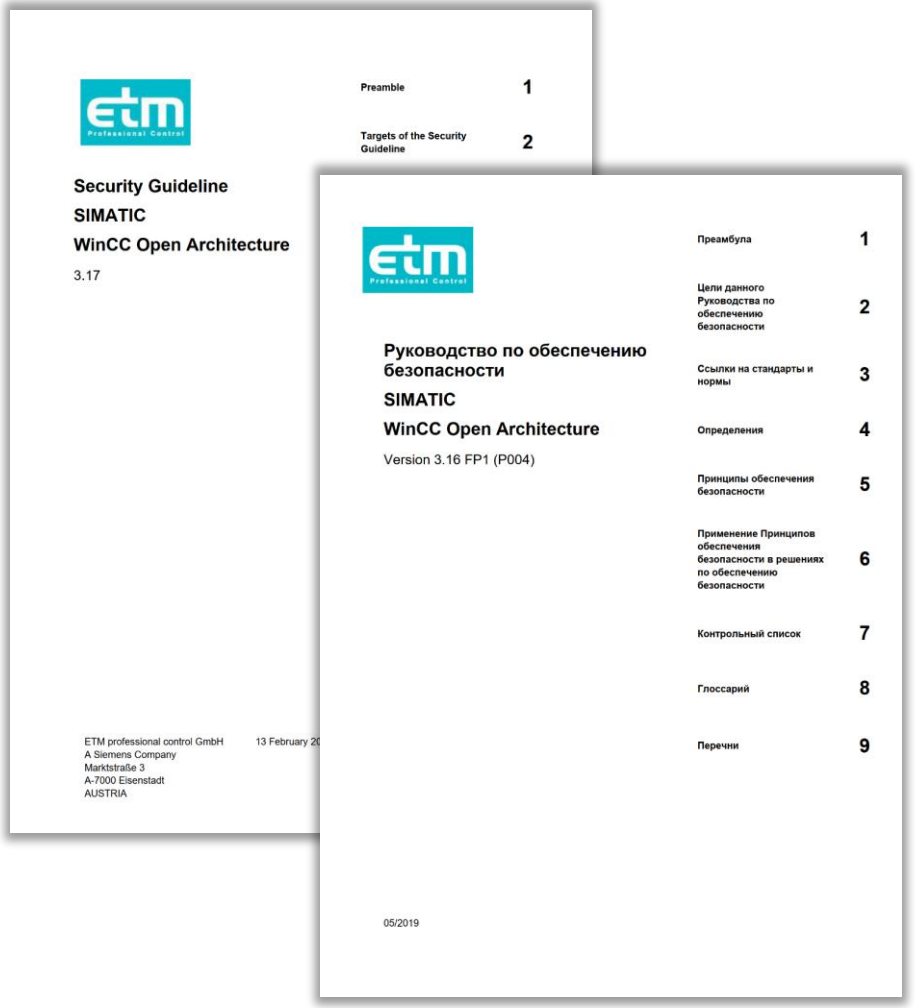


- **Сегментация на ячейки безопасности**

- **Управление правами пользователей в зависимости от выполняемых задач**



- **Централизация однотипных операций**



V3.14, V3.15, V3.16 – доступны на русском языке.

Технологии и механизмы обеспечения безопасности в составе WinCC OA

SIEMENS
Ingenuity for life

Шифрование панелей, сценариев и библиотек

SSL-шифрование при передаче данных

Разграничение уровней доступа

Аутентификация менеджеров WinCC OA на стороне сервера (сертификаты X509)

Контрольные суммы для обеспечения целостности при передаче данных

HTTPS для обмена данными с веб- и мобильными приложениями

Интеграция с Active Directory и другими системами авторизации

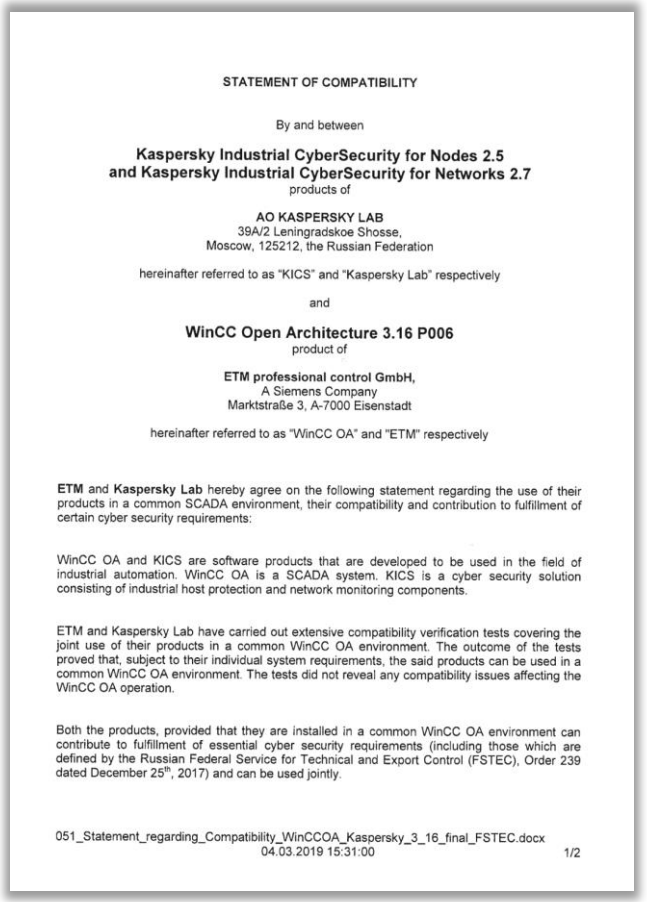
Поддержка протокола сетевой идентификации **Kerberos**

Создание и проверка электронных подписей (**Crypto API**)

Использование средств обеспечения безопасности SCADA и НСЗ: совместимость WinCC OA и KICS

SIEMENS
Ingenuity for life

- Компании **ETM Professional Control GmbH** (дочерняя компания Siemens AG, разработчик WinCC OA) и **АО «Лаборатория Касперского»** проводят регулярное тестирование совместимости системы WinCC OA и решения Kaspersky Industrial CyberSecurity (KICS).
- **Актуальные версии продуктов, успешно прошедших тестирование:**
  KICS for Networks 2.5,
  KICS for Nodes 2.7,
  WinCC OA 3.16.
- В настоящее время идёт тестирование **текущих версий продуктов**.



STATEMENT OF COMPATIBILITY

By and between

Kaspersky Industrial CyberSecurity for Nodes 2.5 and Kaspersky Industrial CyberSecurity for Networks 2.7
products of

AO KASPERSKY LAB
39A/2 Leningradskoe Shosse,
Moscow, 125212, the Russian Federation

hereinafter referred to as "KICS" and "Kaspersky Lab" respectively

and

WinCC Open Architecture 3.16 P006
product of

ETM professional control GmbH,
A Siemens Company
Marktstraße 3, A-7000 Eisenstadt

hereinafter referred to as "WinCC OA" and "ETM" respectively

ETM and **Kaspersky Lab** hereby agree on the following statement regarding the use of their products in a common SCADA environment, their compatibility and contribution to fulfillment of certain cyber security requirements:

WinCC OA and KICS are software products that are developed to be used in the field of industrial automation. WinCC OA is a SCADA system. KICS is a cyber security solution consisting of industrial host protection and network monitoring components.

ETM and Kaspersky Lab have carried out extensive compatibility verification tests covering the joint use of their products in a common WinCC OA environment. The outcome of the tests proved that, subject to their individual system requirements, the said products can be used in a common WinCC OA environment. The tests did not reveal any compatibility issues affecting the WinCC OA operation.

Both the products, provided that they are installed in a common WinCC OA environment can contribute to fulfillment of essential cyber security requirements (including those which are defined by the Russian Federal Service for Technical and Export Control (FSTEC), Order 239 dated December 25th, 2017) and can be used jointly.

051_Statement_regarding_Compatibility_WinCCOA_Kaspersky_3_16_final_FSTEC.docx
04.03.2019 15:31:00 1/2

Apart from benefiting from WinCC OA and KICS security features, additional measures may be necessary in order to implement a holistic, state-of-the-art industrial security concept. The exact set of measures depends on various circumstances and is specific to a particular production/operational environment. Such measures may, among others, include installation and use of other products, appropriate product configurations and implementation of certain organizational measures.

AO Kaspersky Lab
Date: 21.03.2019
Name:
Andrey Tikhonov
Title:
Chief Operating Officer

ETM professional control GmbH
Date: 05.03.2019
Name:
Dr. Bernhard Reichl
Title:
Chief Executive Officer

051_Statement_regarding_Compatibility_WinCCOA_Kaspersky_3_16_final_FSTEC.docx
04.03.2019 15:31:00 2/2

SCADA-системы нового поколения

Интеграция

Аналитика

Периферийные вычисления

Облачные платформы

Цифровизация

Сквозные сервисы

Повышение эффективности

Цифровые кооперационные цепочки

Кибербезопасность

Спасибо за внимание!

SIEMENS
Ingenuity for life

Сергей Соловьёв
Руководитель Центра компетенций
Канд. техн. наук

ООО «Сименс»

Управление «Цифровое производство»