Частные вопросы кибербезопасности АСУ ТП. Теория и практика применения МЭК 62443.

Владимир Карантаев

Руководитель направления
Кибербезопасности АСУ ТП

E-mail: v.karantaev@rt-solar.ru

Ростелеком
Солар

План доклада.

- Обзор нормативно-технических документов, посвященных кибербезопасности промышленных систем автоматизации. Структура серии стандартов IEC 62443
- Уровень зрелости серии стандартов IEC 62443
  - Существующая система сертификации
- Основные концепции заложенные в серии стандартов МЭК 62443: МЭК 62443-1-1, МЭК 62443 -2-1, МЭК 62443-3-3
  - Преимущества применения доменной модели на практике

Ростелеком
Солар

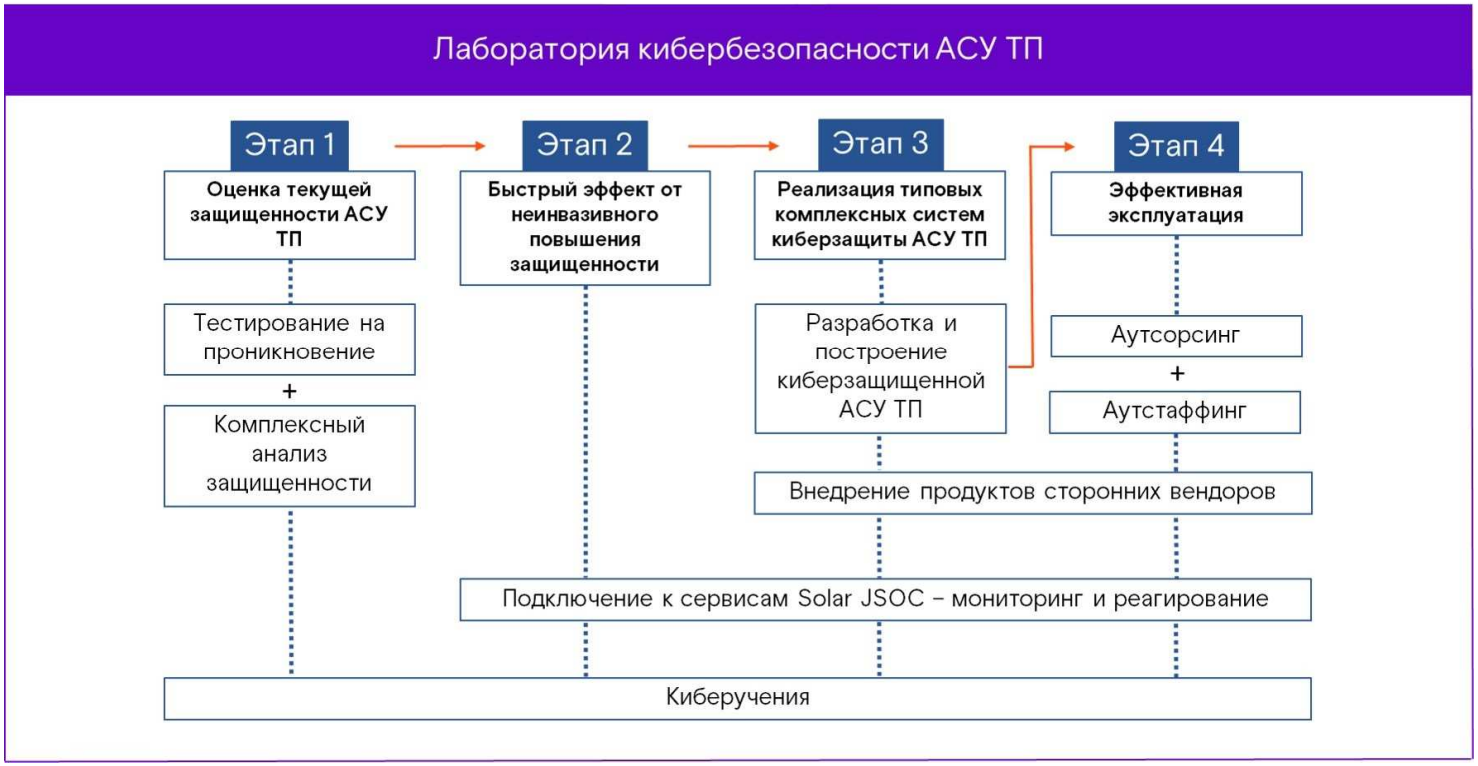
- Высокопрофессиональная команда с реальным опытом проектов по построению АСУ ТП, защиты АСУ ТП полного цикла
- Лаборатория кибербезопасности АСУ ТП с собственной лабораторной и методической базой
- В составе команды эксперты МЭК, IEEE, комитетов Росстандарта

Рабочая группа 15 ТК 57

- Создана почти 10 лет назад
- 121 эксперт-участник группы
- Эксперты из 21 страны
- 18 проектов стандартов
- Три очных встречи в год

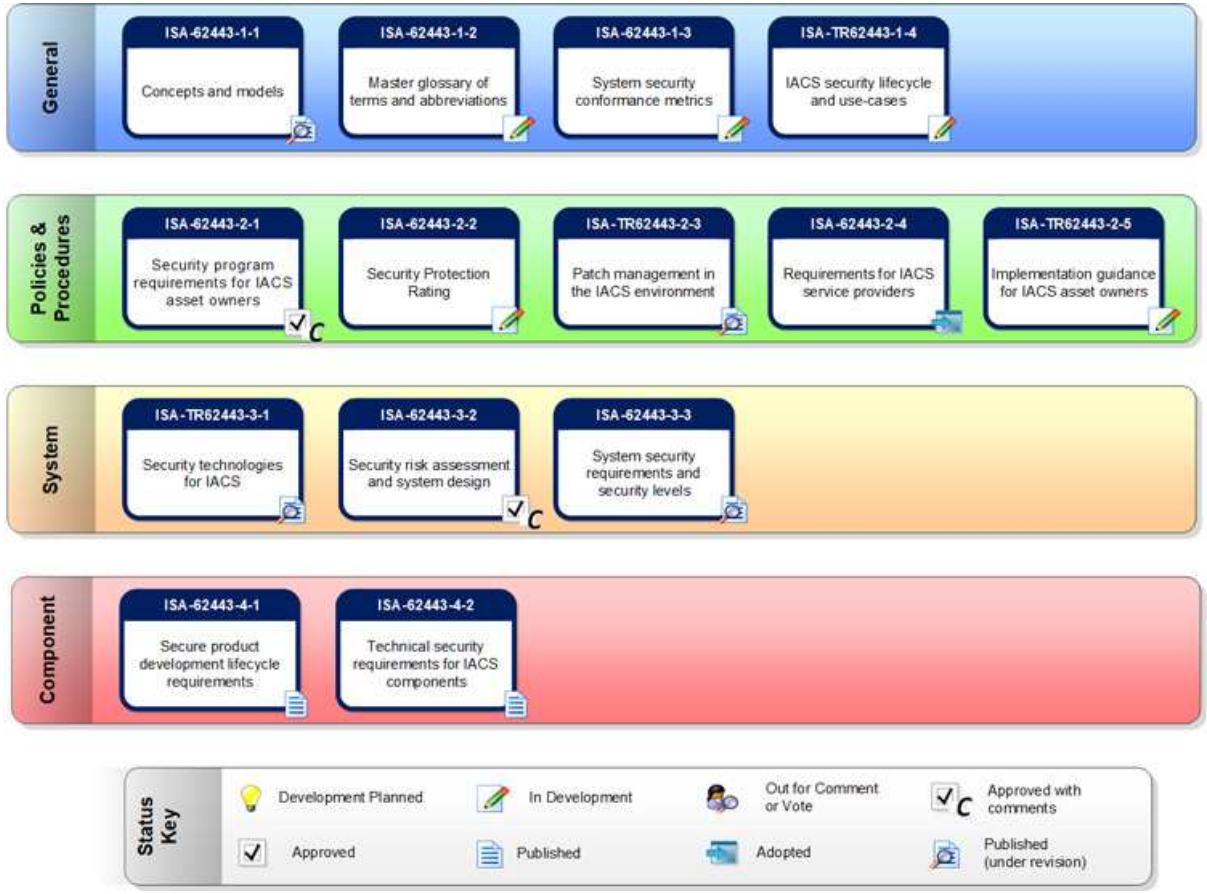
Цель группы: Разработка серии стандартов, предлагающих реализацию мер защиты телекоммуникационных протоколов, определенных ТК 57 МЭК

Повышение киберзащищенности АСУ ТП



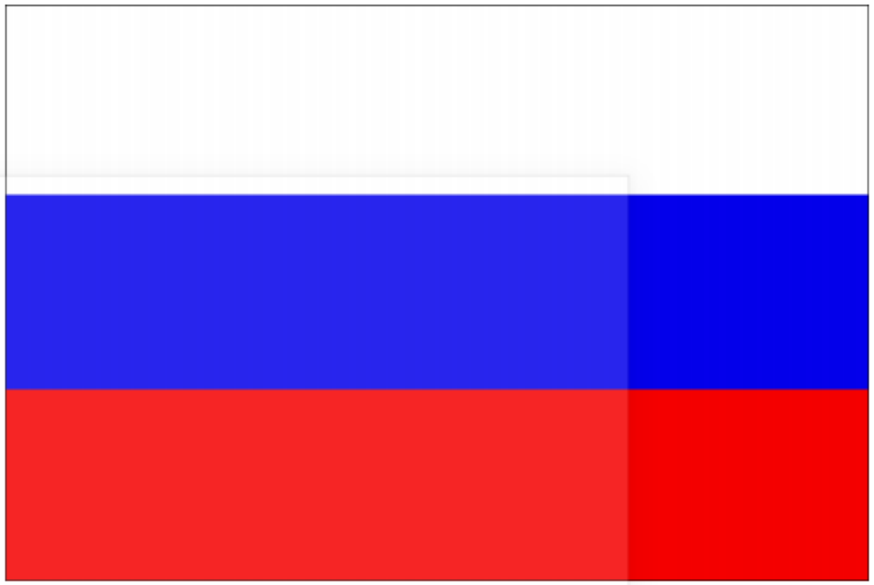
Ростелеком
Солар

Серия стандартов IEC 62443



Ростелеком
Солар

Части серии IEC 62443 гармонизированные в РФ



- **ГОСТ Р 56205-2014 IEC/TS 62443- 1- 1:2009**

«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».

Ростелеком
Солар

Система сертификации:
ISASecure conformance certification programs The ISA Security Compliance Institute (ISCI)

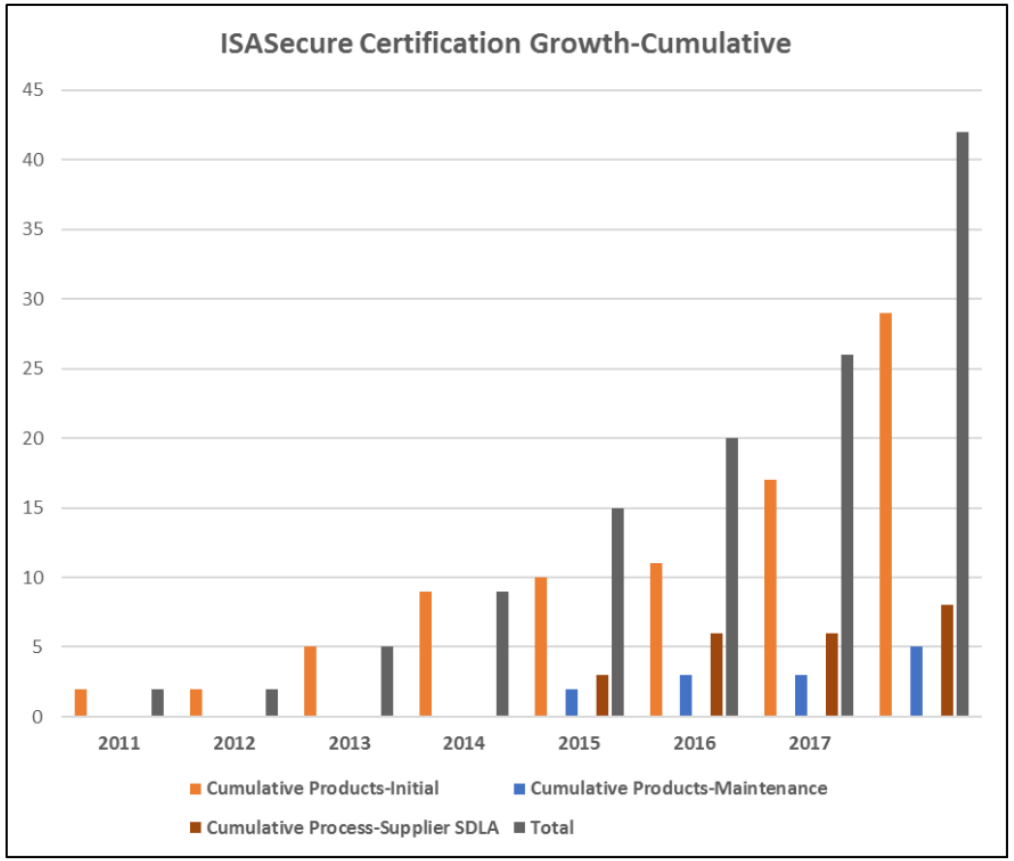
The ISA Security Compliance Institute (ISCI) предлагает три ISASecure сертификационных программы оценки соответствия серии стандартов ISA/IEC 62443:

- Сертификация ISASecure Security Development Lifecycle Assurance (SDLA) – обеспечивает соответствие процессов разработки требованиям безопасности, указанным в стандартах ISASecure на основе стандарта ISA / IEC 62443-4-1.

- Сертификация ISASecure System Security Assurance (SSA) применяется к промышленным системам управления (ICS) (АСУ ТП) и гарантирует, что требуемые функции безопасности могут быть поставлены для построения защищенного решения. Компоненты в системе подвергаются испытанию на надежность в этой программе сертификации на основе стандартов ISA / IEC 62443-3-3 и ISA / IEC 62443-4-1.

- ISASecure Embedded Devices Security Assurance (EDSA) certification – применяется к компонентам (встроенным устройствам) промышленных систем управления (ICS, АСУ ТП) и гарантирует, что требуемые функции безопасности компонент базируются/основаны на стандартах ISA/IEC 62443-4-2 и ISA/IEC 62443-4-1

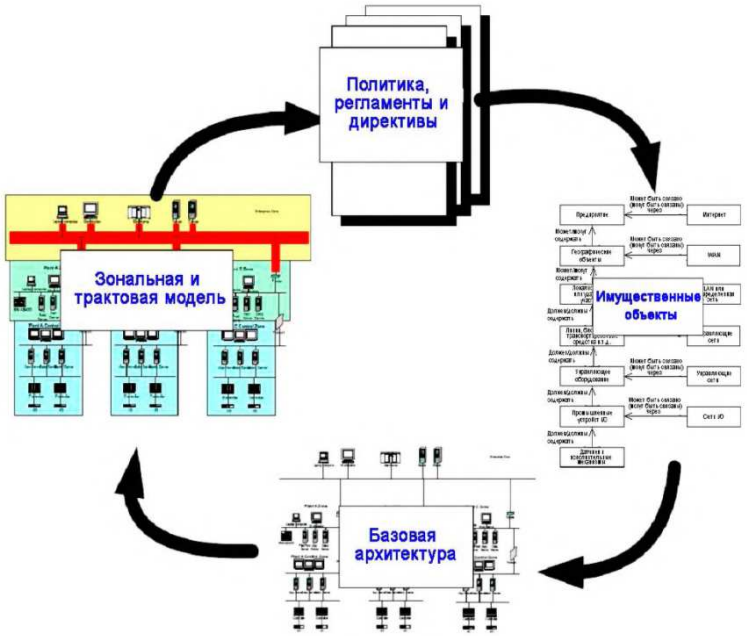
Статистика объема сертификаций на соответствие IEC 62443



Ростелеком
Солар

White Paper ISASecure Institute: Securing Control Systems using IEC 62443 Standards

Основные концепции IEC 62443



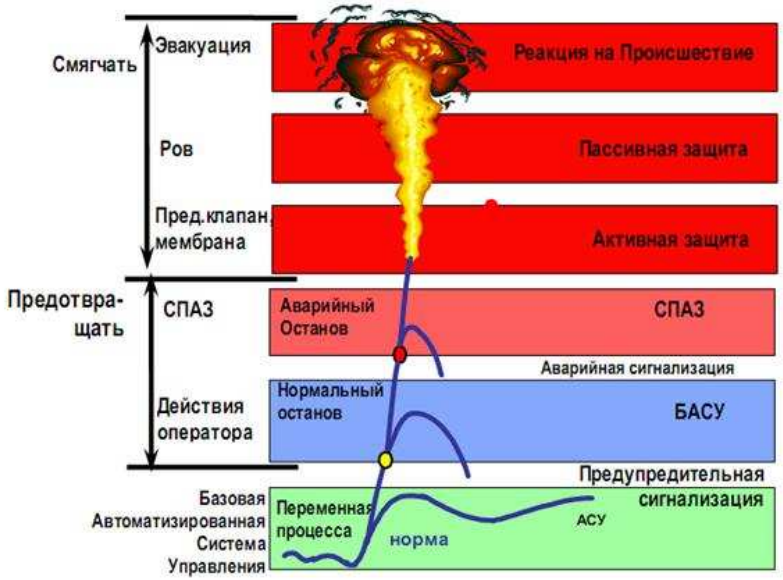
Оцениваются риски:

- HSE – риски (промышленной безопасности, охраны труда и окружающей среды).

- Финансовые риски:
  - Риски экономических потерь от простоев производства
  - Риски экономически потерь от снижения качества продукции
  - Риски кражи информации, отнесенной к коммерческой тайне. (Секреты производства)

Ростелеком
Солар

РСУ и ПАЗ как объект защиты

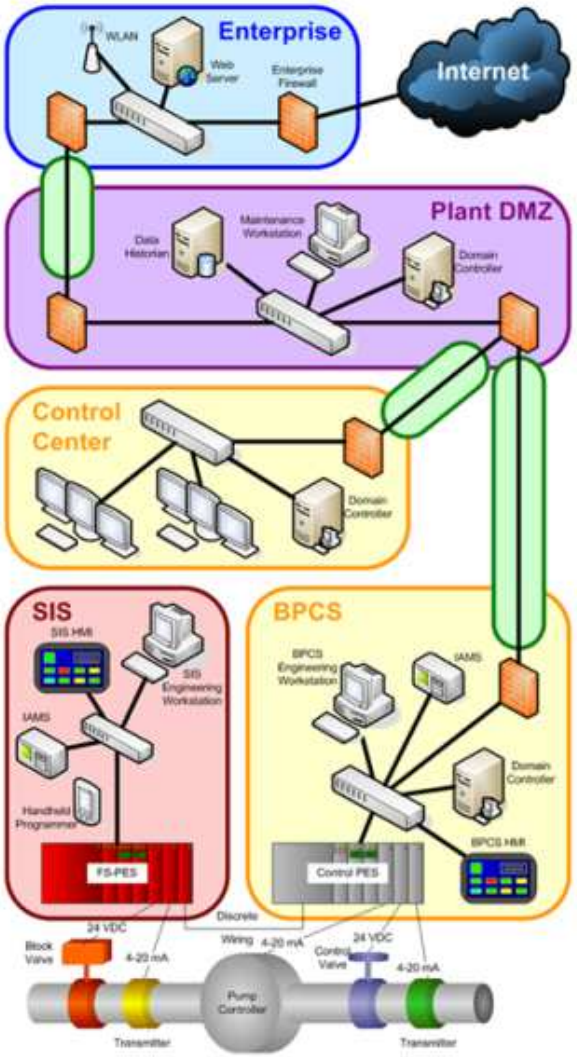


- СПАЗ наиболее критичная система с точки зрения наступления HSE рисков (промышленной безопасности, охраны труда и окружающей среды (HSE).
- Для идентификации опасностей и экологических аспектов, оценки HSE рисков и возможностей, а также определения необходимых мер используются методики: HAZID/ENVID, HAZOP, FMEA, QRA, SIL, LOPA, ESHIA, JRA и др. Результаты документируется (ведомости и реестры HSE рисков и экологических аспектов)

Вариант архитектуры №1

ISA-TR84, описывает 4 типа архитектур:

- ПАЗ и РСУ реализуются в виде отдельных зон «воздушный зазор» ,
- ПАЗ и РСУ реализуются частично сопряженными
- ПАЗ и РСУ реализуются в виде двух зон
- ПАЗ и РСУ реализуются в виде одной зоны



- ISA-TR84.00.09, 2013. Security Countermeasures Related to Safety Instrumented Systems (SIS)
- Safety & Security - Is a Physically Separation of the SIS Necessary?

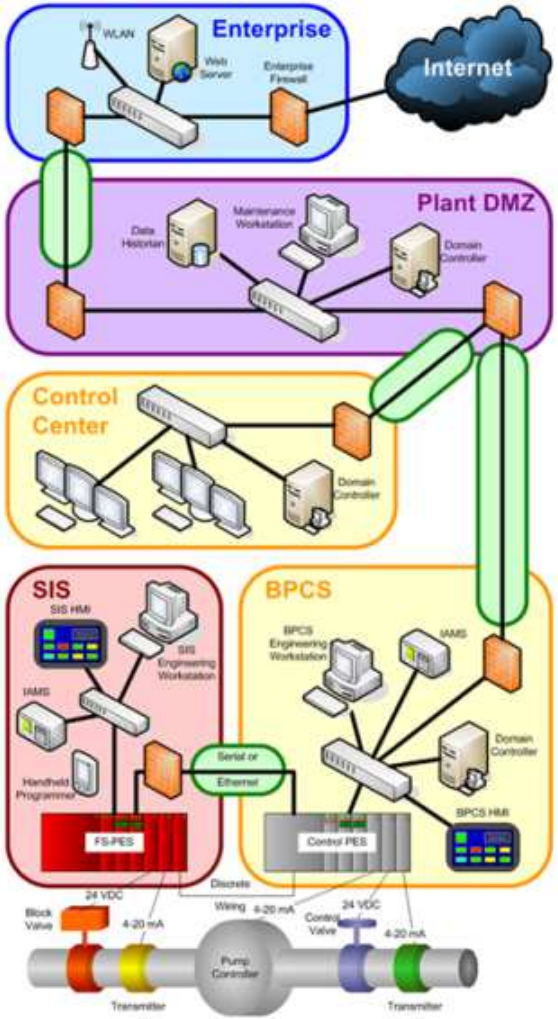
Ростелеком
Солар

Вариант архитектуры №2

- Компоненты Уровня операторского (диспетчерского) управления.
- Компоненты уровня автоматического управления: РСУ + Компоненты уровня ввода/вывода (полевой).
- Компоненты уровня автоматического управления: ПАЗ + Компоненты уровня ввода/вывода (полевой).

Образуют отдельные объекты критической информационной структуры.

Категория считается по последствиям для каждого ОКИИ.



- ISA-TR84.00.09, 2013. Security Countermeasures Related to Safety Instrumented Systems (SIS)
- Safety & Security - Is a Physically Separation of the SIS Necessary?

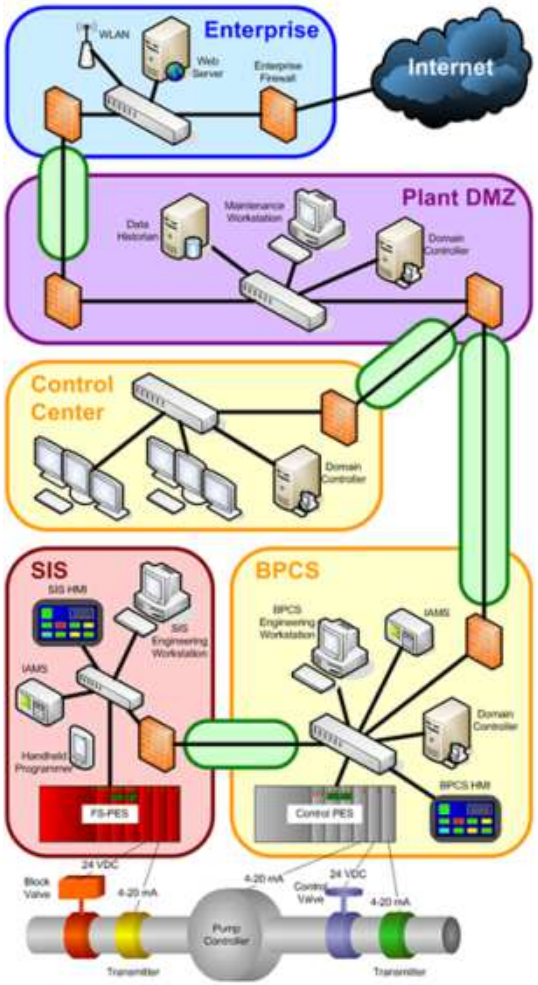
Ростелеком
Солар

Вариант архитектуры № 3

- Компоненты Уровня операторского (диспетчерского) управления.
- Компоненты уровня автоматического управления: РСУ + Компоненты уровня ввода/вывода (полевой).
- Компоненты уровня автоматического управления: ПАЗ + Компоненты уровня ввода/вывода (полевой).

Образуют отдельные объекты критической информационной структуры.

Категория считается по последствиям для каждого ОКИИ.



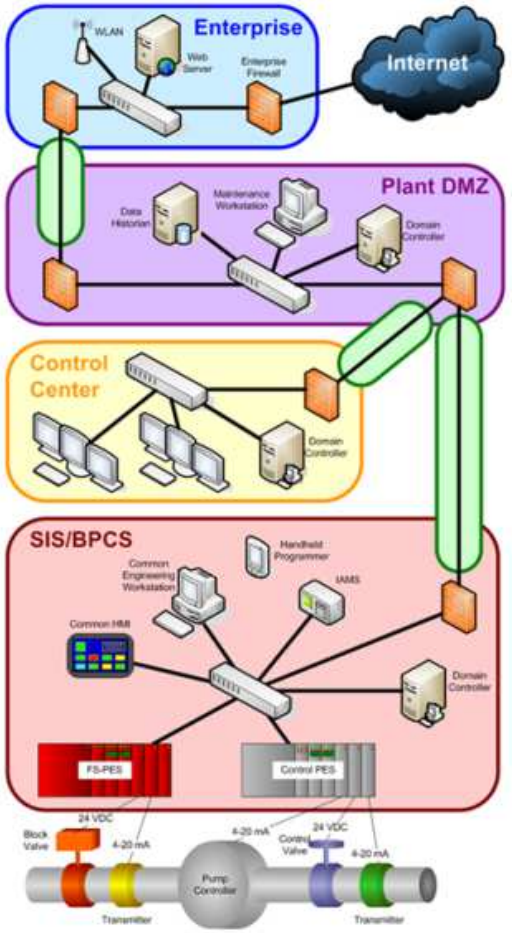
- ISA-TR84.00.09, 2013. Security Countermeasures Related to Safety Instrumented Systems (SIS)
- Safety & Security - Is a Physically Separation of the SIS Necessary?

Ростелеком
Солар

Вариант архитектуры № 4

- Компоненты Уровня операторского (диспетчерского) управления
- Компоненты уровня автоматического управления: РСУ и ПАЗ
- Компоненты уровня ввода/вывода (полевой)

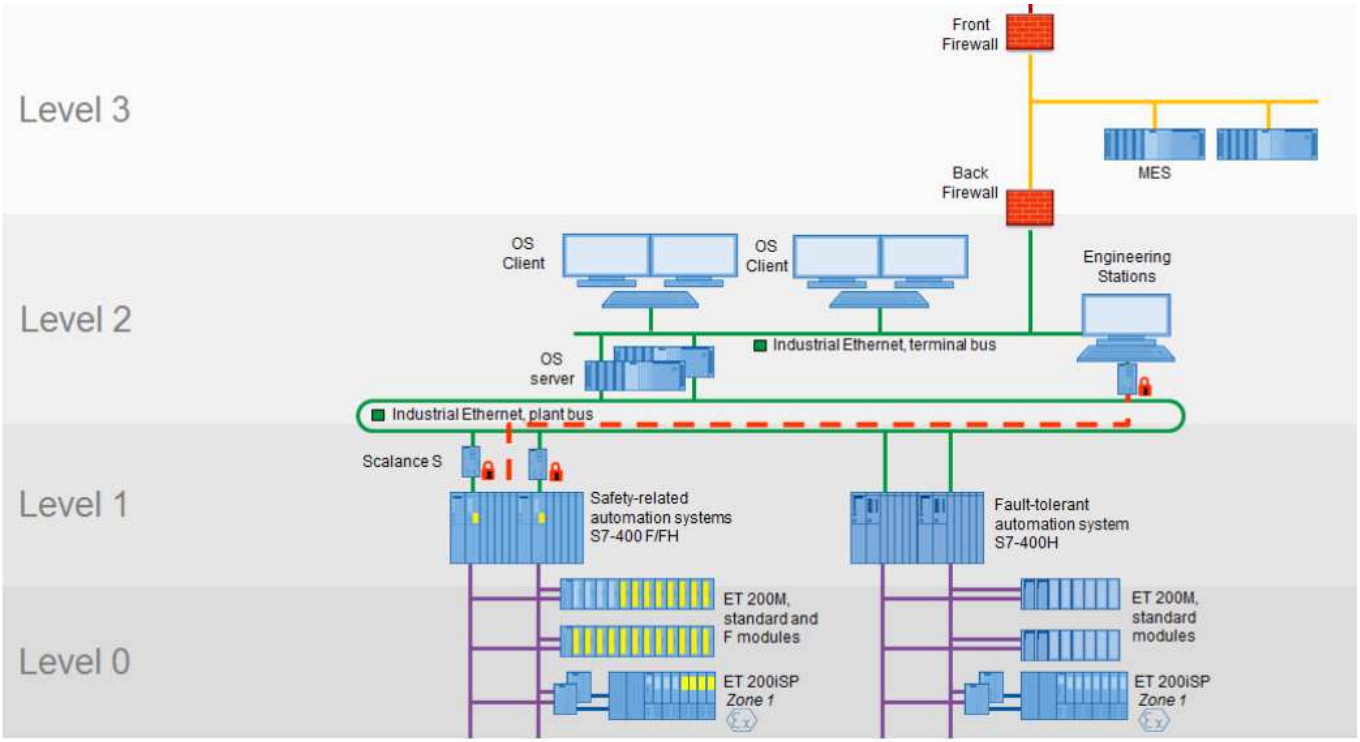
Образуют Объект критической информационной структуры. Категория считается по последствиям максимально критичного компонента ПАЗ.



- ISA-TR84.00.09, 2013. Security Countermeasures Related to Safety Instrumented Systems (SIS)
- Safety & Security - Is a Physically Separation of the SIS Necessary?

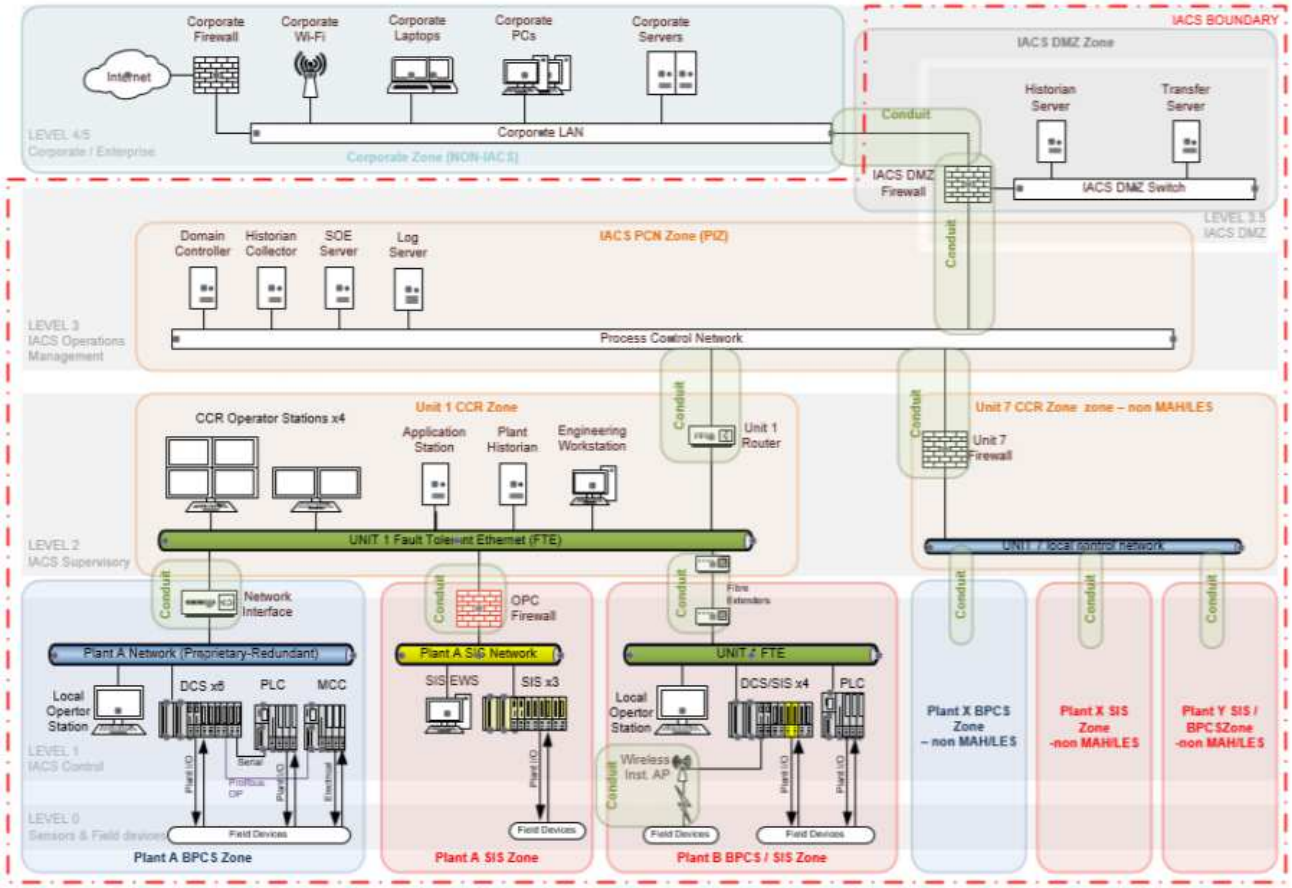
Ростелеком
Солар

Практический пример архитектуры ПАЗ и РСУ



- Safety & Security - Is a Physically Separation of the SIS Necessary?

Использование доменной модели МЭК 62443



Ростелеком Солар

Cyber Security for Industrial Automation and Control Systems (IACS) EDITION 2 http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf

Выводы

1. Системы должны разрабатываться с учетом анализа угроз функциональной надежности и информационной безопасности.
2. Реализация концепции Secure by design (встроенных средств защиты информации в промышленных системах автоматизации) и требований безопасной разработки выглядит наиболее перспективно с учетом необходимости удовлетворять требования по функциональной надежности и безопасности, наличия требований по быстродействию телекоммуникационных протоколов и оптимальности затрат.
3. Формирование комплексного предложения по кибербезопасности IIoT возможно на основе сформированных экосистемных партнерств.

Частные вопросы кибербезопасности АСУ ТП. Теория и практика применения МЭК 62443.

Владимир Карантаев

Руководитель направления
Кибербезопасности АСУ ТП

E-mail: v.karantaev@rt-solar.ru

Ростелеком
Солар