Вопросы обеспечения информационной безопасности РЗА

Владимир Карантаев, к.т.н.

Руководитель РГ 4 D2 РНК СИГРЭ

Автор блога: «Безопасность данных и коммуникаций в SmartGrid»

vladimir.karantaev@gmail.com

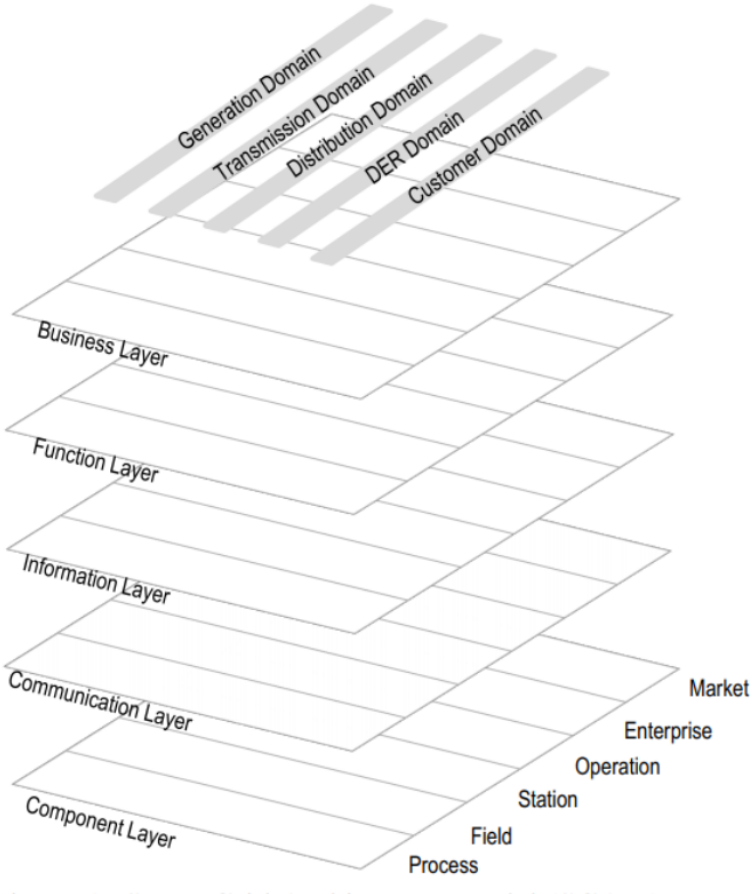
Структура доклада

- Методология оценки рисков на уровне архитектуры систем Smart grid.
- Оценка рисков, модель угроз на объектовом уровне.
- О роли экспертных сообществ.
- Возможные источники требований ИБ и ФБ
- МЭК 15408 «Общие критерии», SDLC «Цикл безопасной разработки», IEC 62351, IEC 61508, IEC 62443, IEC 62056.
- Возможные технические подоходы к реализации систем защит: сегодня, завтра.
- Необходимость гармонизации подходов.

О необходимости оценки рисков на уровне архитектуры систем Smart grid

- IEEE определение Smart Grid как концепции «полностью интегрированной,саморегулирующейся и самовосстанавливающейся элек-троэнергетической системы, имеющей сетевую топологию и включающей в себя все генерирующие источники, магистральные и распределительные сети и все виды потребителей электрической энергии, управляемые единой сетью информационно-управляющих устройств и систем в режиме реального времени».

Smart Power Grids — Talking about a Revolution // IEEE Emerging Technology Portal, 2009.



Общий принцип объединения подходов ИБ и ФБ

Моделирование угроз кибербезопасности в разрезе функциональной безопасности объектов электроэнергетики. Д. Даренский http://rza-expo.ru/doc/rza_materialy3.pdf

О роли экспертных сообществ СИГРЭ, РНК СИГРЭ, МЭК

Выводы:

- Результаты деятельности недоиспользованы.
- Завышенные ожидания от предполагаемых результатов деятельности.

Предложения:

- Провести GAP-анализ состояния разработки отечественных нормативно-технических документов.
- Авторизовать запрос на создание зеркальной рабочей группы к D 2.46 «Cybersecurity: future threats and impact on Electric Power Utility
- organizations and operations».

- **Рабочая группа CIGRE Working Group the B5.38:**

The Impact of Implementing Cyber Security Requirements using IEC 61850 CIGRE Working Group the B5.38, August 2010.

О требованиях кибербезопасности систем РЗА. Г.С. Нудельман 2012

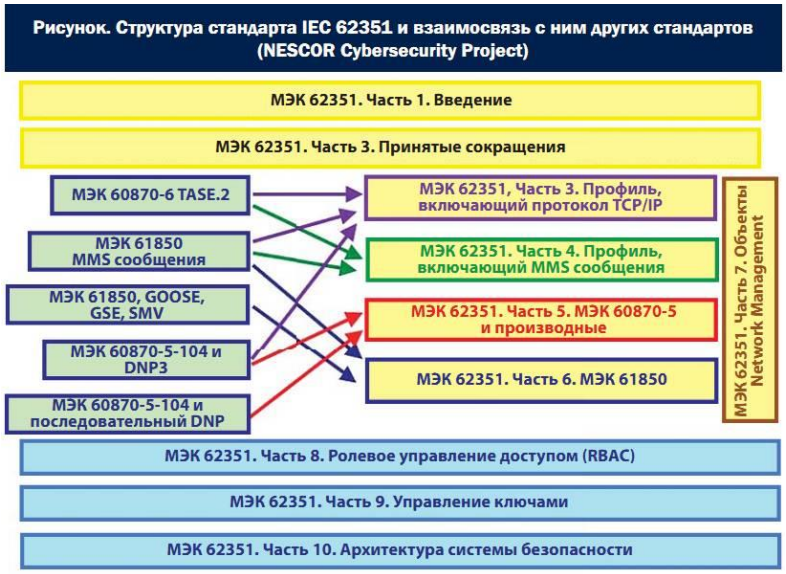
https://www.ruscable.ru/article/O_trebovaniyax_kiberbezopasnosti_sistem_RZA/

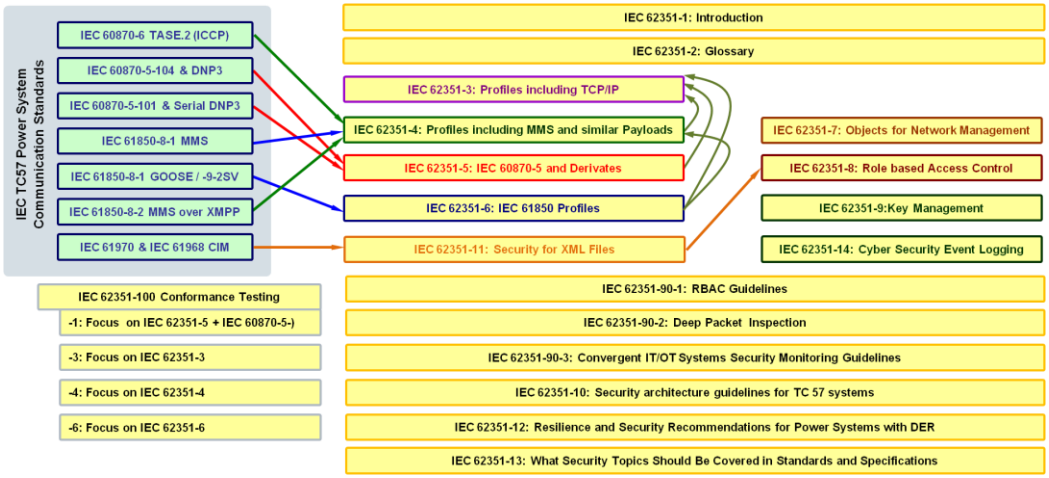
- **Рабочая группа ПРГ-2 B5/D2 РНК СИГРЭ:**

Предложения по корректировке нормативно-правовых актов.

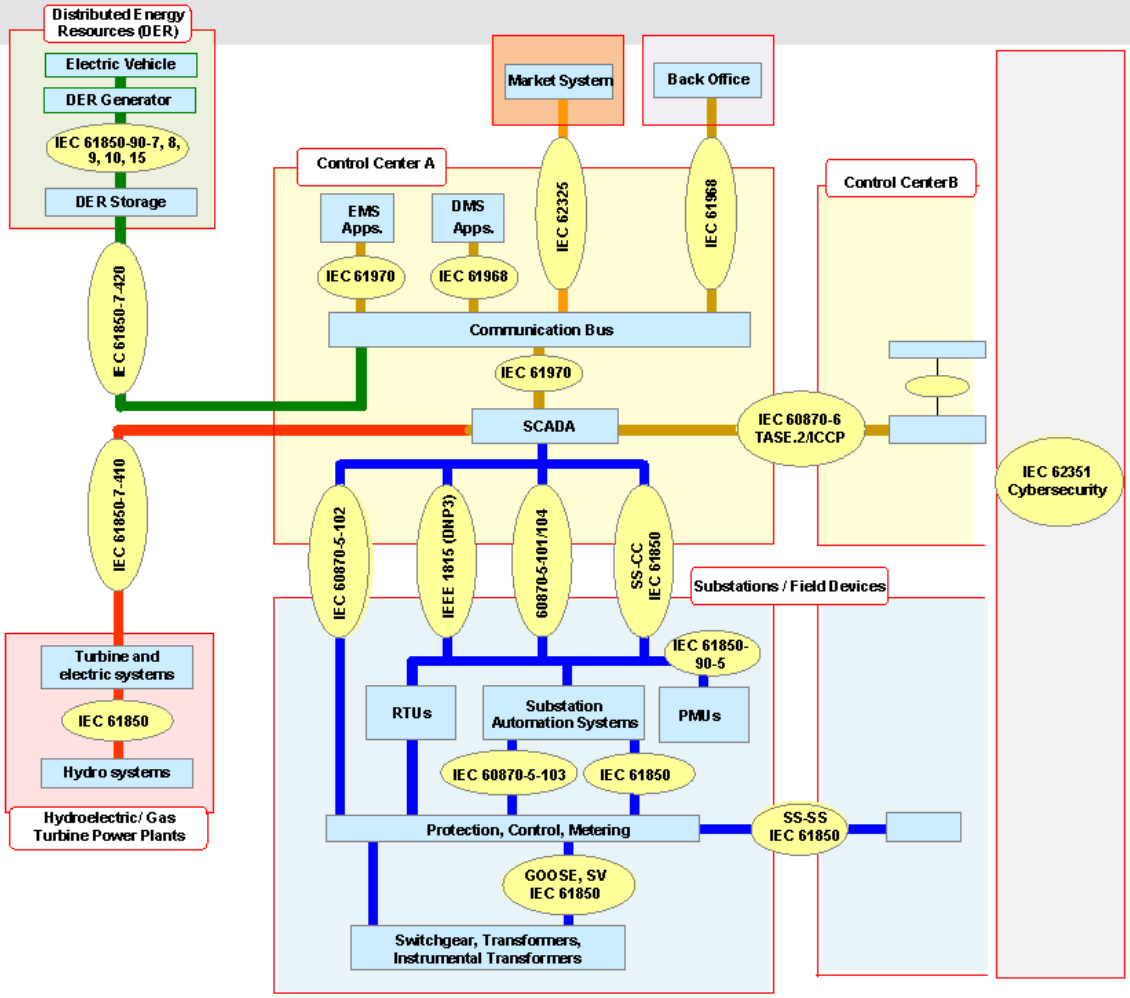
Методика моделирования угроз ФБ и ИБ

Развитие стандарта МЭК 62351

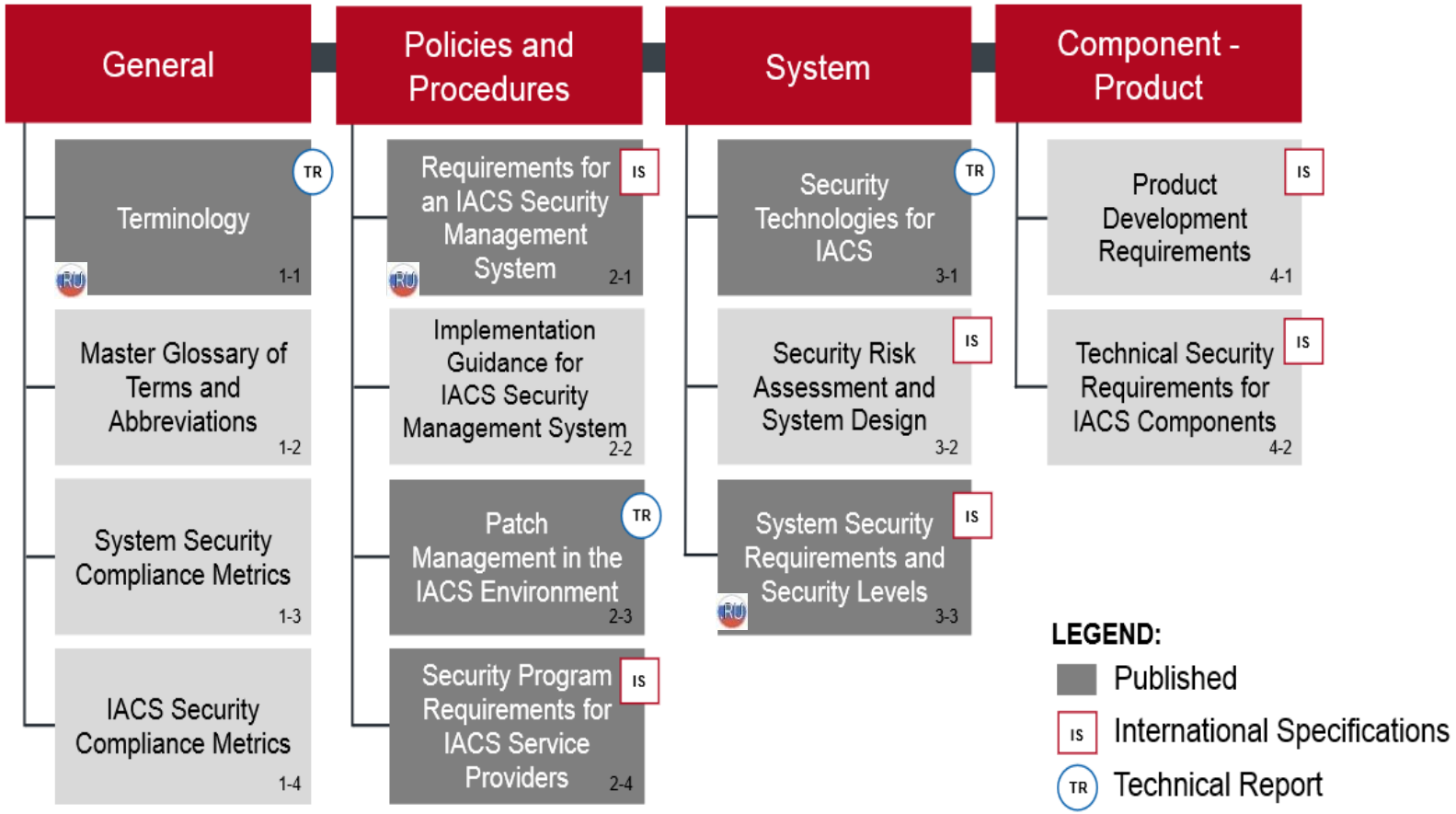




IEC TC57 WG15 Architecture of Information Standards



Серия стандартов IEC 62443



ГОСТ Р МЭК 62443

- **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».

Вопросы кибербезопасности ИЭС ААС

Повышение общего уровня информатизации энергетической сферы приводит к повышению риска возникновения ущерба (технического и экономического) от противоправных действий.

Особенности ИЭС ААС:

- работа в непрерывном активном режиме;
- приоритет задачи сохранения функциональности системы над задачей обеспечения ее информационной безопасности;

При реализации концепции информационной безопасности следует учитывать:

- IEC 62351.
- INL Cyber Security Procurement Language 2008.
- ISO/IEC 27000.

ОСНОВНЫЕ ПОЛОЖЕНИЯ КОНЦЕПЦИИ ИНТЕЛЛЕКТУАЛЬНОЙ ЭНЕРГОСИСТЕМЫ С АКТИВНО-АДАПТИВНОЙ СЕТЬЮ

Анализ рисков информационной безопасности

IEC:

ISA/IEC 62443 series
Серия ГОСТ Р МЭК 62443
Серия ГОСТ Р ГОСТ Р МЭК 61508

NIST:

NIST 800-30
NIST 800-39
And over

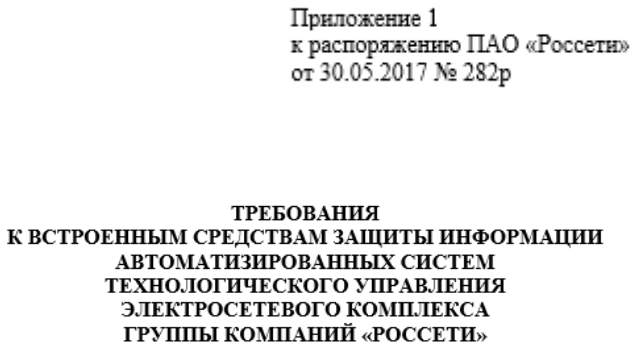
ISO:

ISO/IEC 15408-1,2,3
Information technology -- Security techniques -- Evaluation criteria for IT security
ISO/IEC 2700x series
Information technology -- Security techniques

NERC CIP:

Standard CIP–002

Требования ПАО Россети



Приложение 1
к распоряжению ПАО «Россети»
от 30.05.2017 № 282р

ТРЕБОВАНИЯ
К ВСТРОЕННЫМ СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ
ТЕХНОЛОГИЧЕСКОГО УПРАВЛЕНИЯ
ЭЛЕКТРОСЕТЕВОГО КОМПЛЕКСА
ГРУППЫ КОМПАНИЙ «РОССЕТИ»

Отличительные черты:

- Методология «Общих критериев»

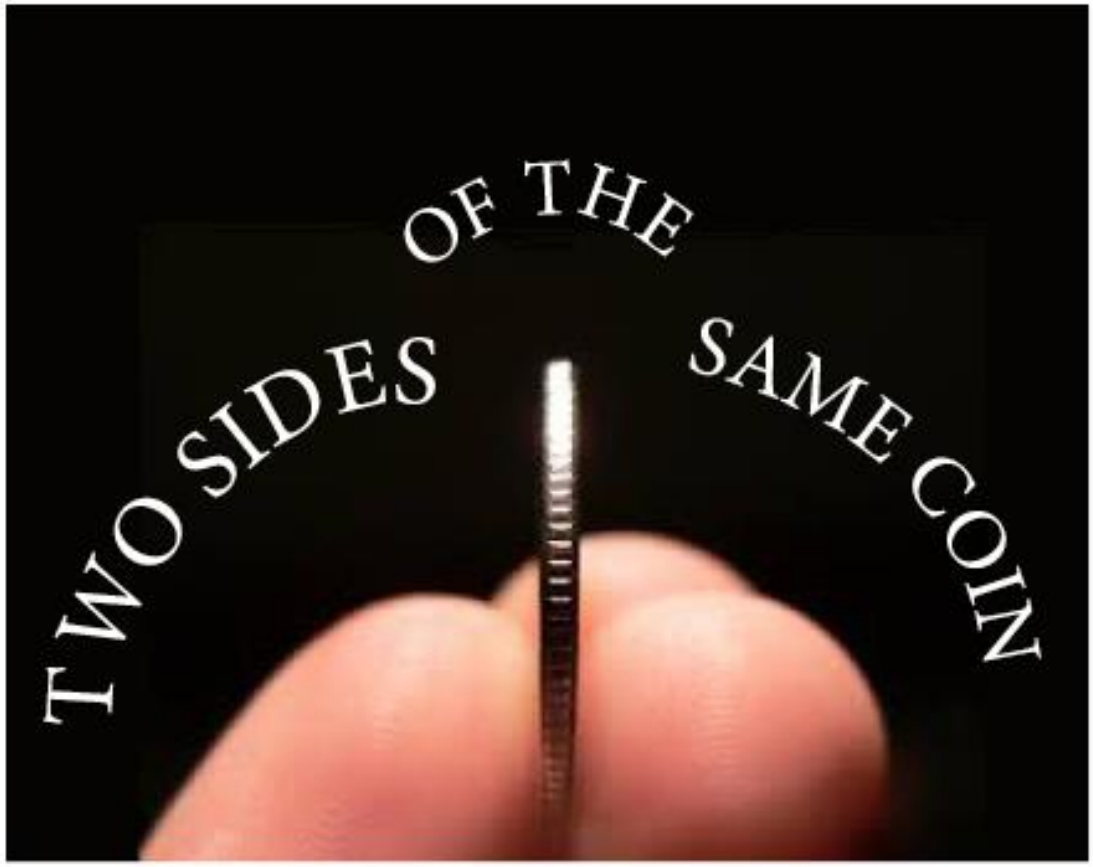
(Сертификация на ОУД).

- Следование трендам регулятора – ФСТЭК России.
- Требования доверия сформулированы в соответствии с ГОСТ Р ИСО/МЭК 15408-3 и представлены в виде оценочного уровня доверия ОУД 4+ (усиленный).

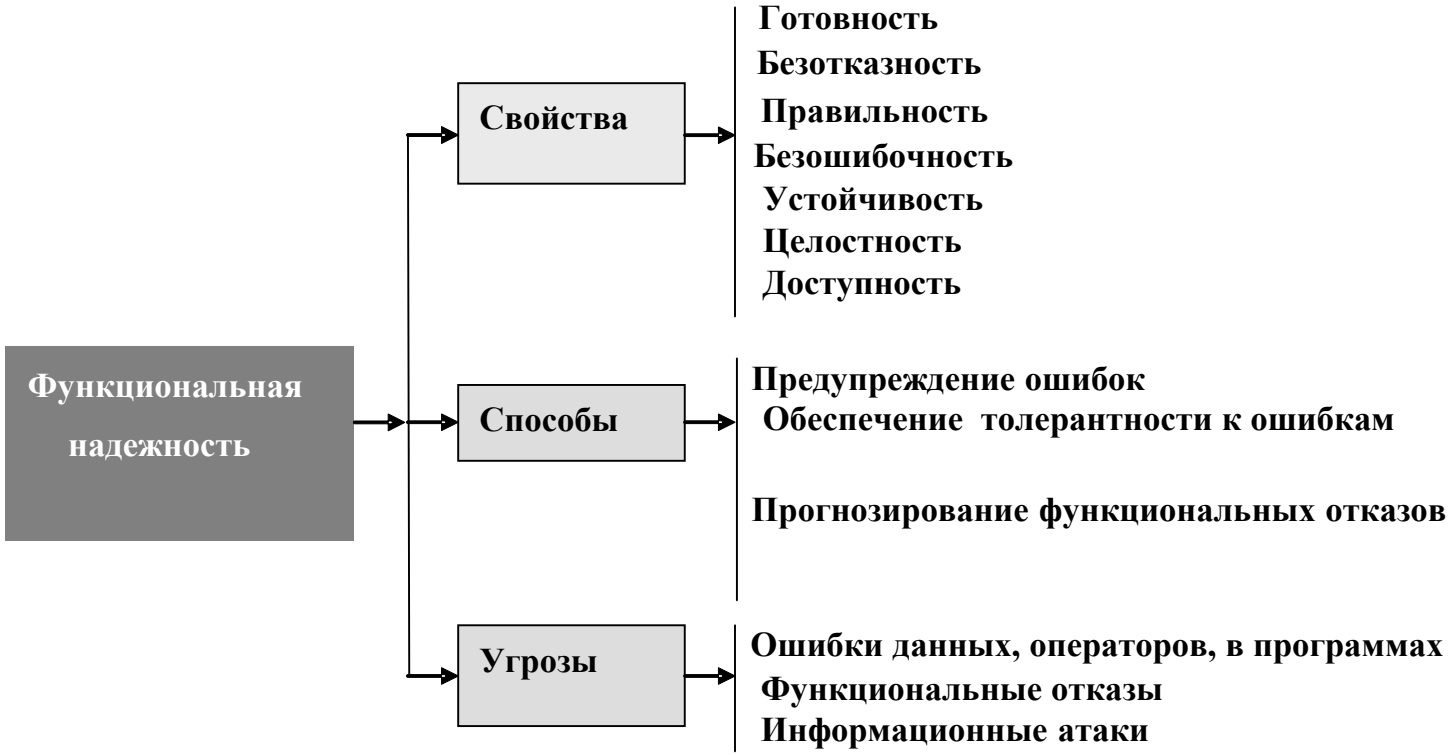
Требования доверия :

- Оценка уязвимостей (AVA)

Информационная безопасность и функциональная безопасность



ТРАКТОВКА ФУНКЦИОНАЛЬНОЙ НАДЕЖНОСТИ



д.т.н. И.Б.ШУБИНСКИЙ

УГРОЗЫ ФУНКЦИОНАЛЬНОЙ НАДЕЖНОСТИ

- ПРОГРАММНЫЕ ОШИБКИ: *системные, алгоритмические, ошибки кодирования*;
- СБОЙНЫЕ ОШИБКИ *функционального характера*;
- ОШИБКИ ЧЕЛОВЕКА-ОПЕРАТОРА;
- ОШИБКИ ВО ВХОДНЫХ ДАННЫХ;
- СИСТЕМАТИЧЕСКИЕ ОШИБКИ;
- ОШИБКИ ПО ОБЩЕЙ ПРИЧИНЕ;
- ОШИБКИ ВСЛЕДСТВИЕ ИНФОРМАЦИОННЫХ АТАК;
- ОТКАЗЫ ТЕХНИЧЕСКИХ СРЕДСТВ

д.т.н. И.Б.ШУБИНСКИЙ

Требования к процессу разработки ПО

Методология: Классический риск-ориентированный подход

Управление процессом создания безопасного ПО

Российская федерация:

- ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».
- ГОСТ Р ИСО/МЭК 27034-1. Безопасность приложений

Международные методологии:

- MS SDL,
- OWASP Secure SDLC Cheat Sheet.
- Cisco Security Development Life Cycle

Прогнозируемый результат:

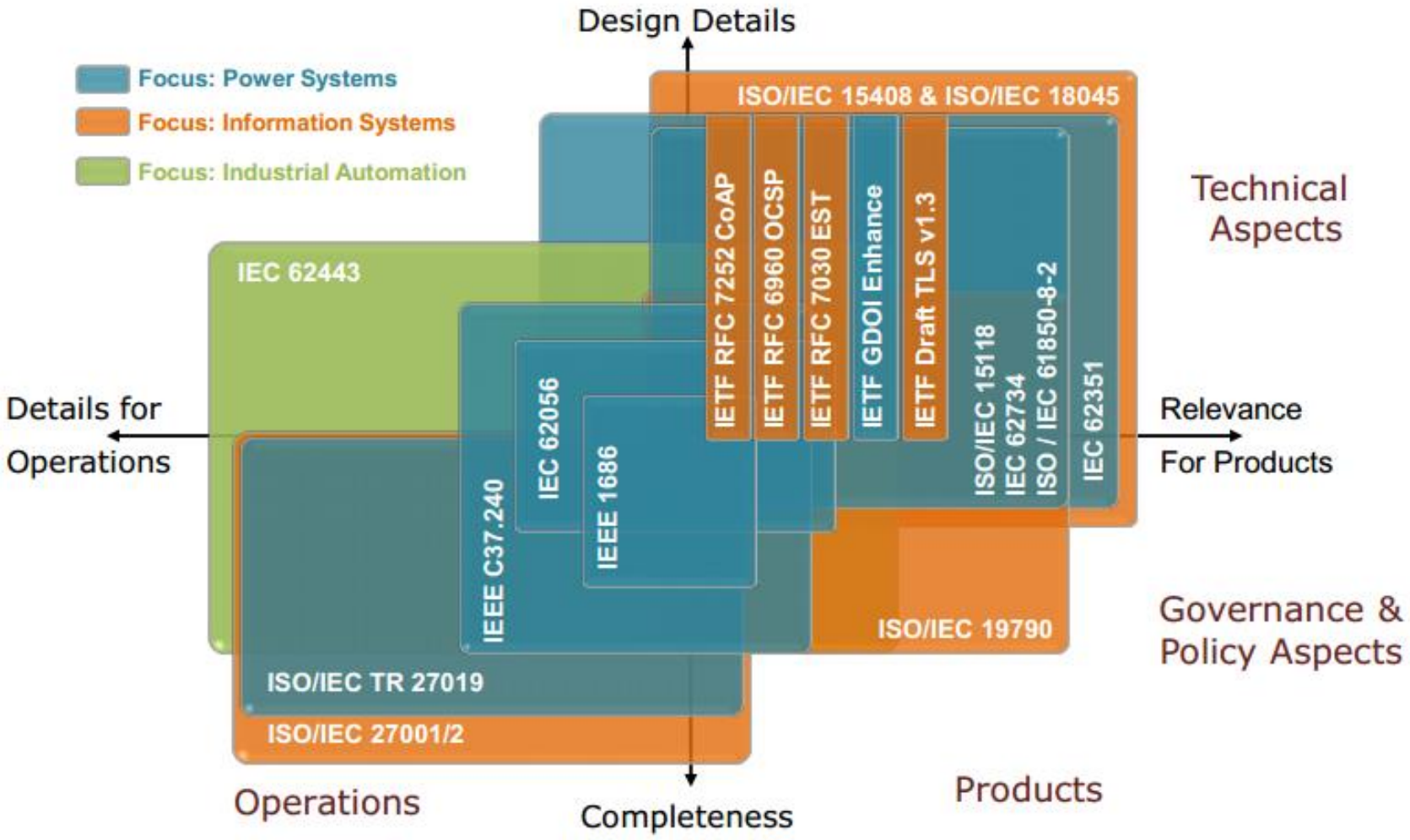
- Повышение качества ПО.
- Сокращение совокупной стоимости разработки.
- Повышение защищенности конечного продукта.
- Повышение надежности

Методы обеспечения функциональной безопасности

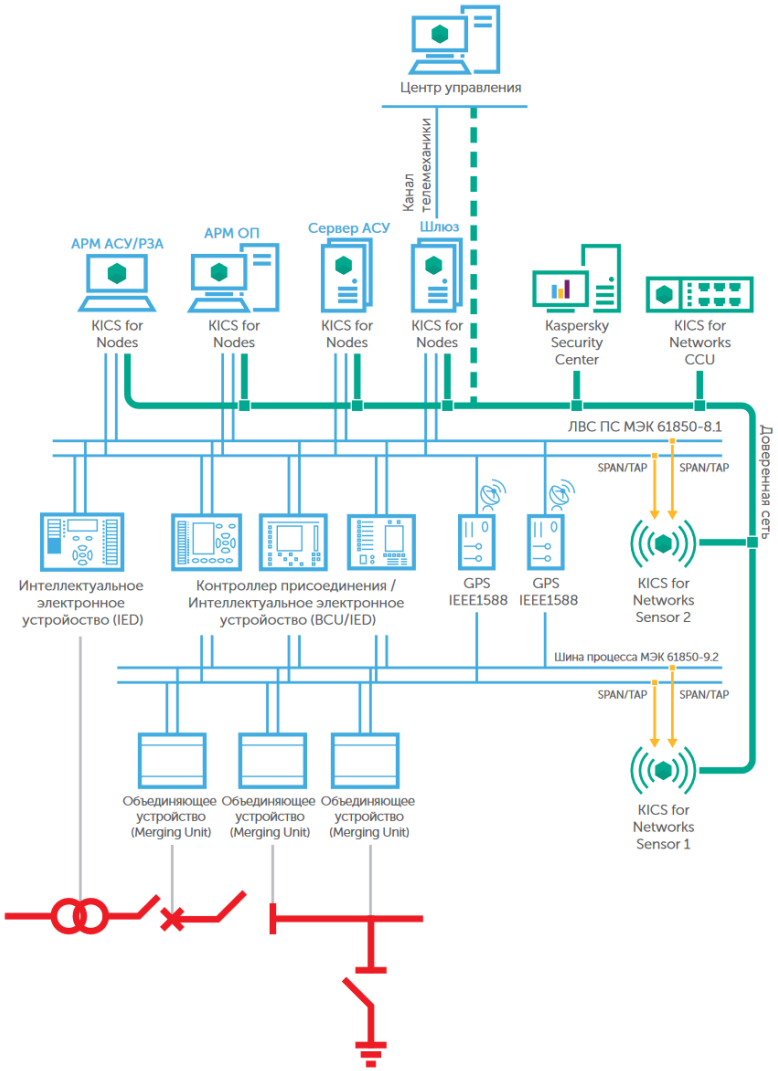
- ГОСТ Р МЭК 61508-3-2012 «Требования к программному обеспечению»

- Защита от случайных и систематических отказов.
- Повышение надежности.

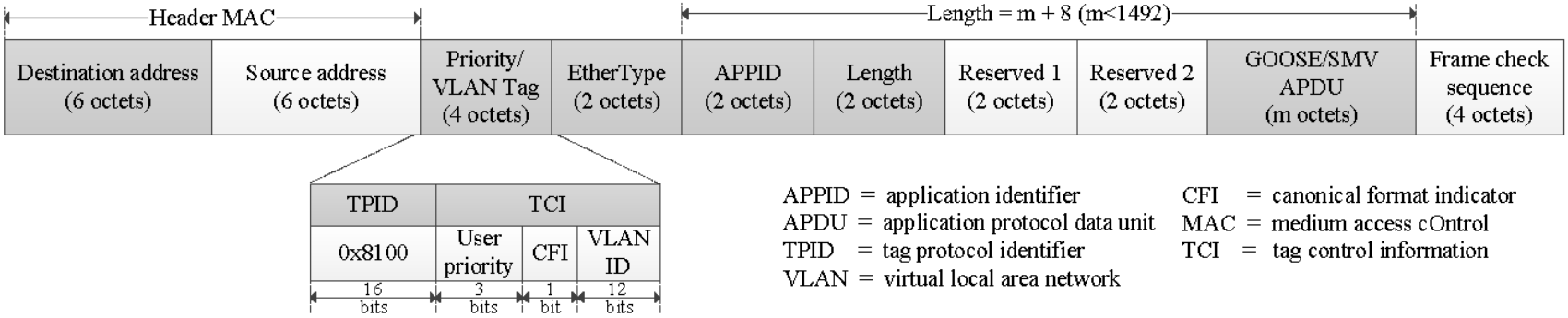
Необходимость гармонизации



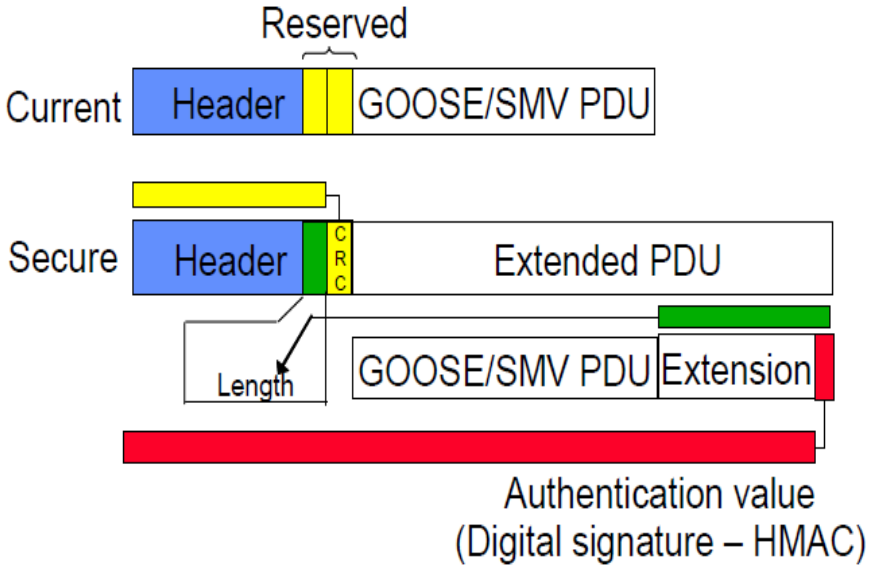
Сегодня. «Закрыть» периметр «повысить наблюдаемость»



Завтра. Защищенный пакет GOOSE/SV?

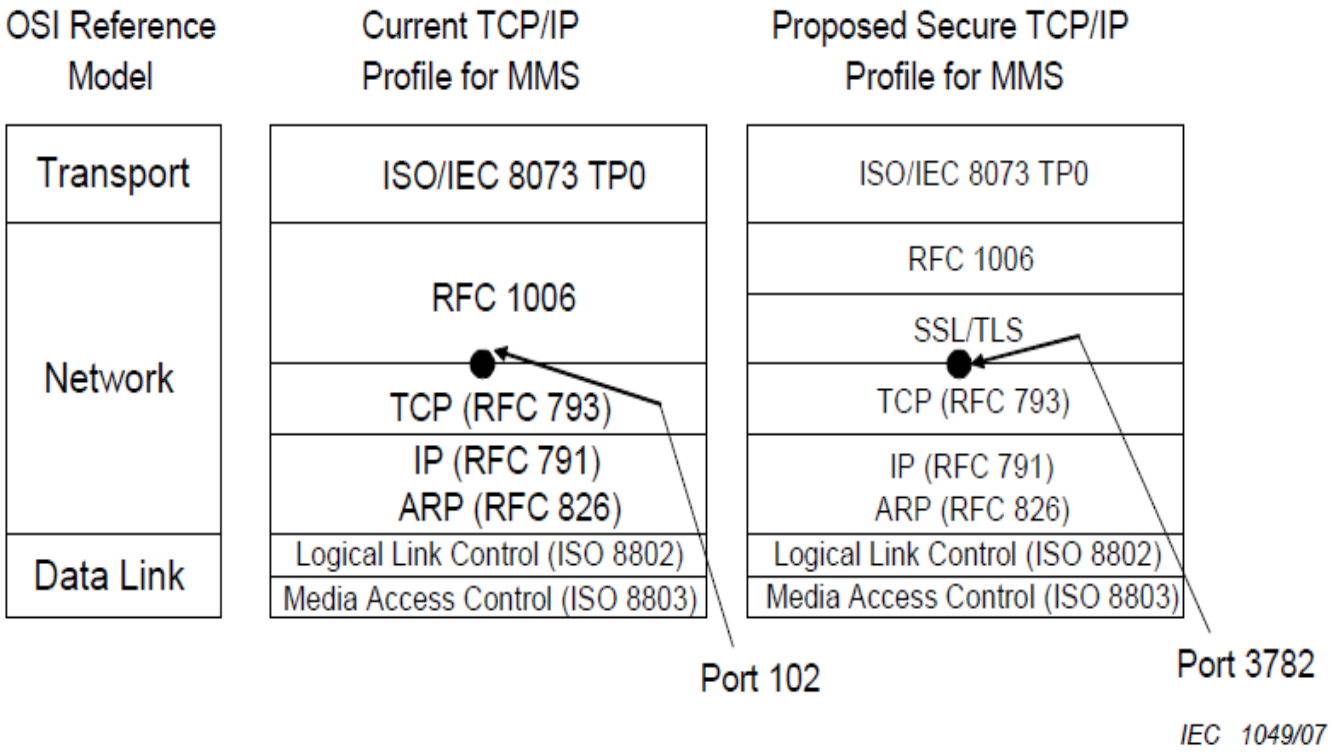


APPID = application identifier
APDU = application protocol data unit
TPID = tag protocol identifier
VLAN = virtual local area network
CFI = canonical format indicator
MAC = medium access cOntrol
TCI = tag control information



IEC 617/07

Завтра. Защищенный профиль MMS?



Краткосрочные и долгосрочные задачи:

- Наладить взаимодействие между ТК16 и ТК 26.
  Создать смешанную группу экспертов
- Осуществить гармонизацию стандарта МЭК 62351.
- Усилить активное присутствие экспертов РФ в профильном комитете ТК 57 МЭК.
- Организовать и провести НИР для комплексной оценки возможного влияния кибератак на устойчивость энергосистемы.
- Организовать и провести НИР и НИОКР для оценки реализуемости заложенные в стандарте концепции.
- Организовать и провести НИР и НИОКР по разработке типовых ПТК в киберзащищенном виде.

Выводы:

- Важной задачей является задача разработки инженерных методик расчета функциональной надежности.
- Системы должны разрабатываться исходя из анализа угроз функциональной надежности и информационной безопасности.
- В условиях необходимости удовлетворять комплексу требований по функциональной надежности, безопасности, наличия требований по быстродействию телекоммуникационных протоколов, оптимальности затрат реализация концепции «secure by design» (встроенных средств защиты информации в промышленных системах автоматизации), требований безопасной разработки – выглядит наиболее перспективно.

Вопросы обеспечения информационной безопасности РЗА

Владимир Карантаев, к.т.н.

Руководитель РГ 4 D2 РНК СИГРЭ

Автор блога: «Безопасность данных и коммуникаций в SmartGrid»

vladimir.karantaev@gmail.com