Вопросы реализации киберзащищенной цифровой подстанции на основе российских технологий

Владимир Карантаев

к.т.н. MBA

эксперт IEC, IEEE, CIGRE

Автор блога: https://smartgridib.blogspot.com/

Екатеринбург 11 Июля, 2019

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

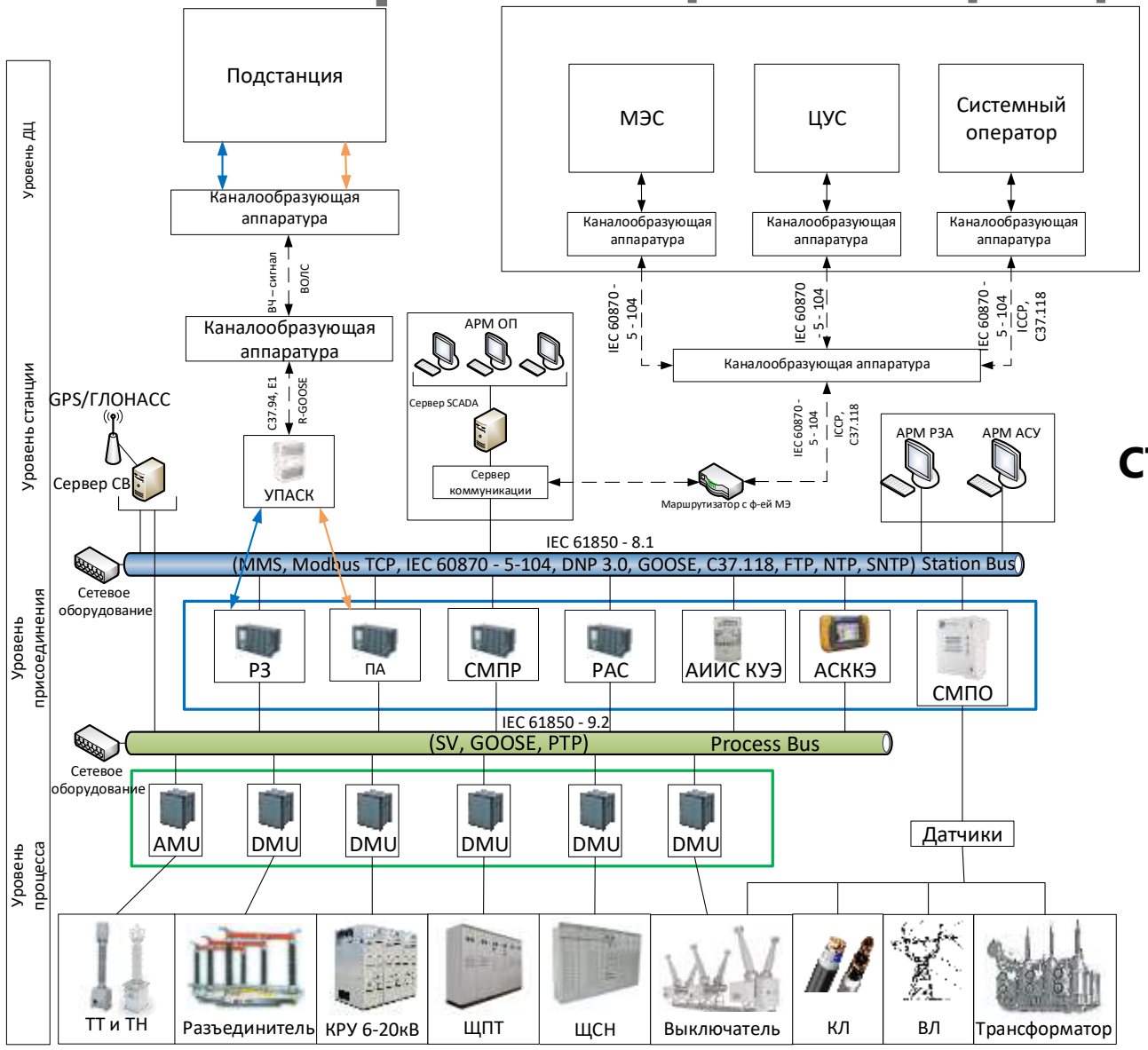
IEC

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

Основа реализации концепции цифровой трансформации



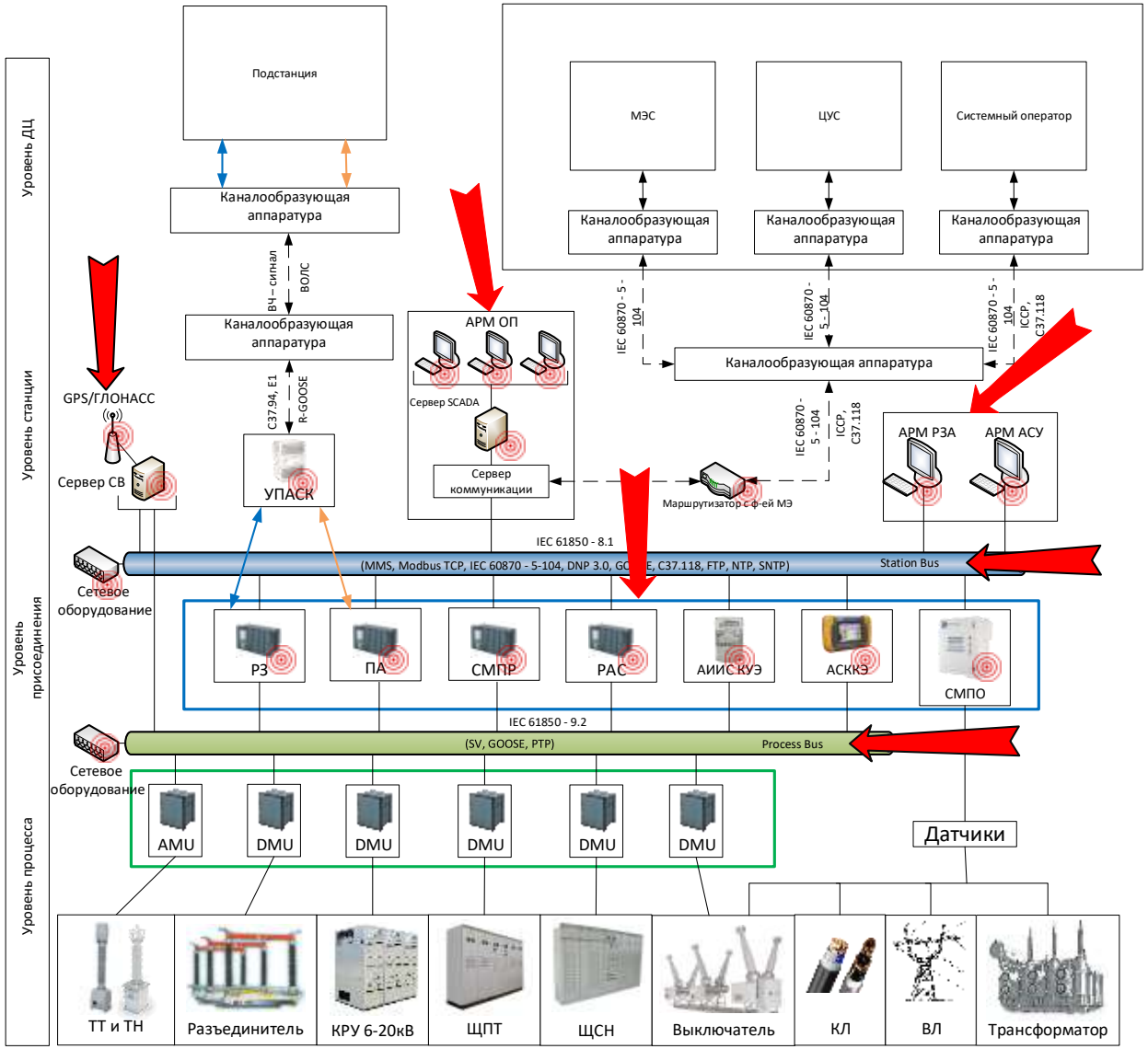
Цифровая подстанция:

Автоматизированная подстанция, оснащенная взаимодействующими в режиме единого времени цифровыми информационными и управляющими системами и функционирующая без присутствия постоянного дежурного персонала.

СТО 34.01.-21-004-2019 «Цифровой питающий центр».

Под «цифровой» подстанцией (ЦПС) понимается подстанция с высоким уровнем автоматизации управления, в которой практически все процессы информационного обмена между элементами ПС, обмена с внешними системами, а также управления работой ПС осуществляются в цифровом виде на основе протоколов МЭК.

Модель угроз ЦПС



Виды возможных атак:

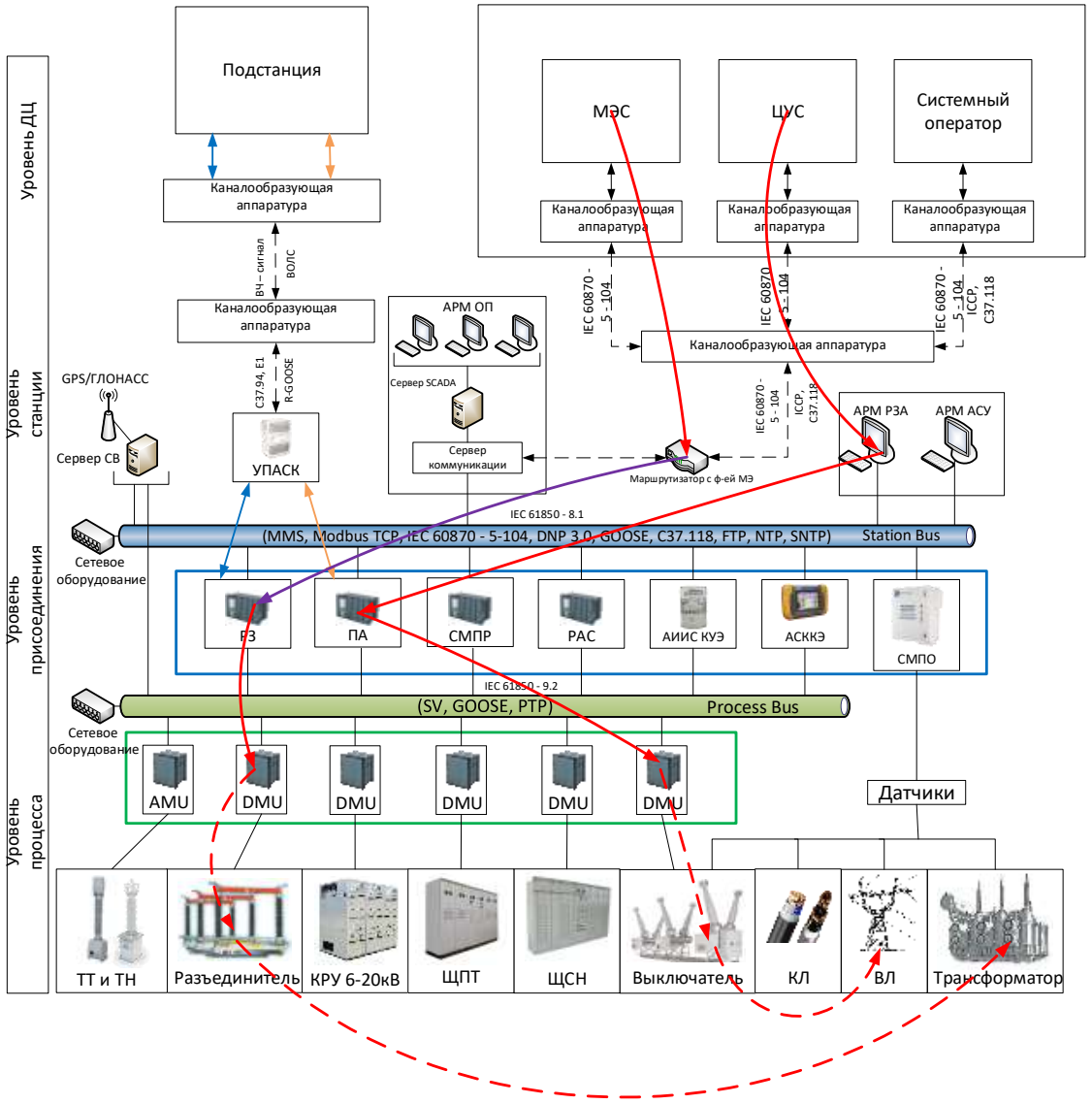
- GPS|ГЛОНАСС Spoofing
- GOOSE Spoofing
- MITM MMS
- MITM МЭК 60870 - 5 – 104
- Brute Force
- Риски успешных APT с ущербом кибер- и физическим характеристикам ЦПС и SmartGrids (ААС ЕЭС, Цифровым сетям

Возможные вектора воздействия:

Атаки на Endpoints

Атаки на протоколы

Пример дерева атаки



Сценарий №1:

Шаг 1: С уровня МЭС захват маршрутизатора
Шаг 2: Атака на протокол MMS
Шаг 3: Передача управляющего воздействия на РЗ
Шаг 4: Управление разъединителем под нагрузкой

Сценарий №2:

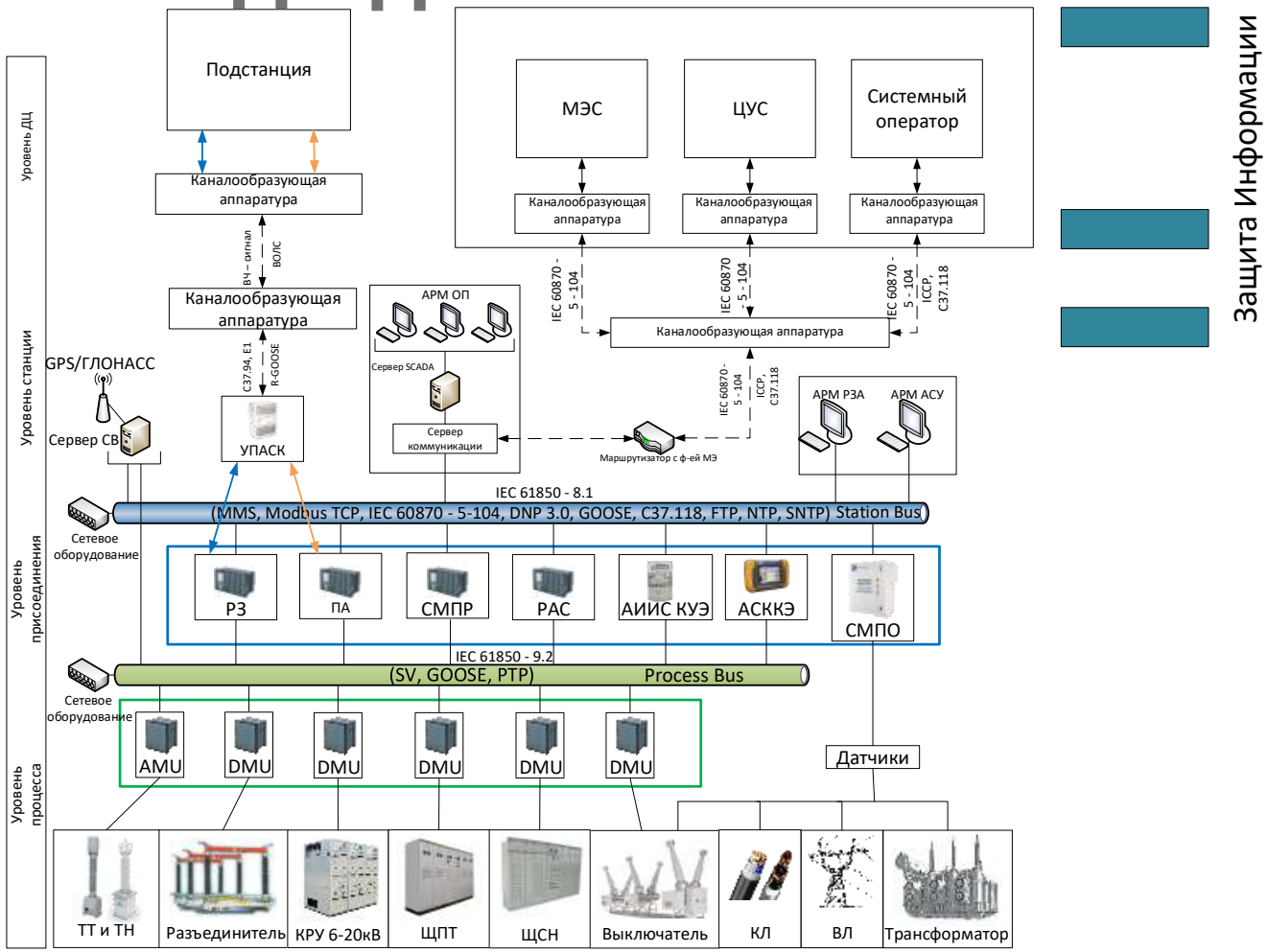
Шаг 1: С уровня ЦУС захват АРМ РЗА
Шаг 2: Изменение конфигурации ПА
Шаг 3: Передача управляющего воздействия на DMU Силового выключателя
Шаг 4: Отключение линий

Атака на протоколы

Атака на цифровую систему

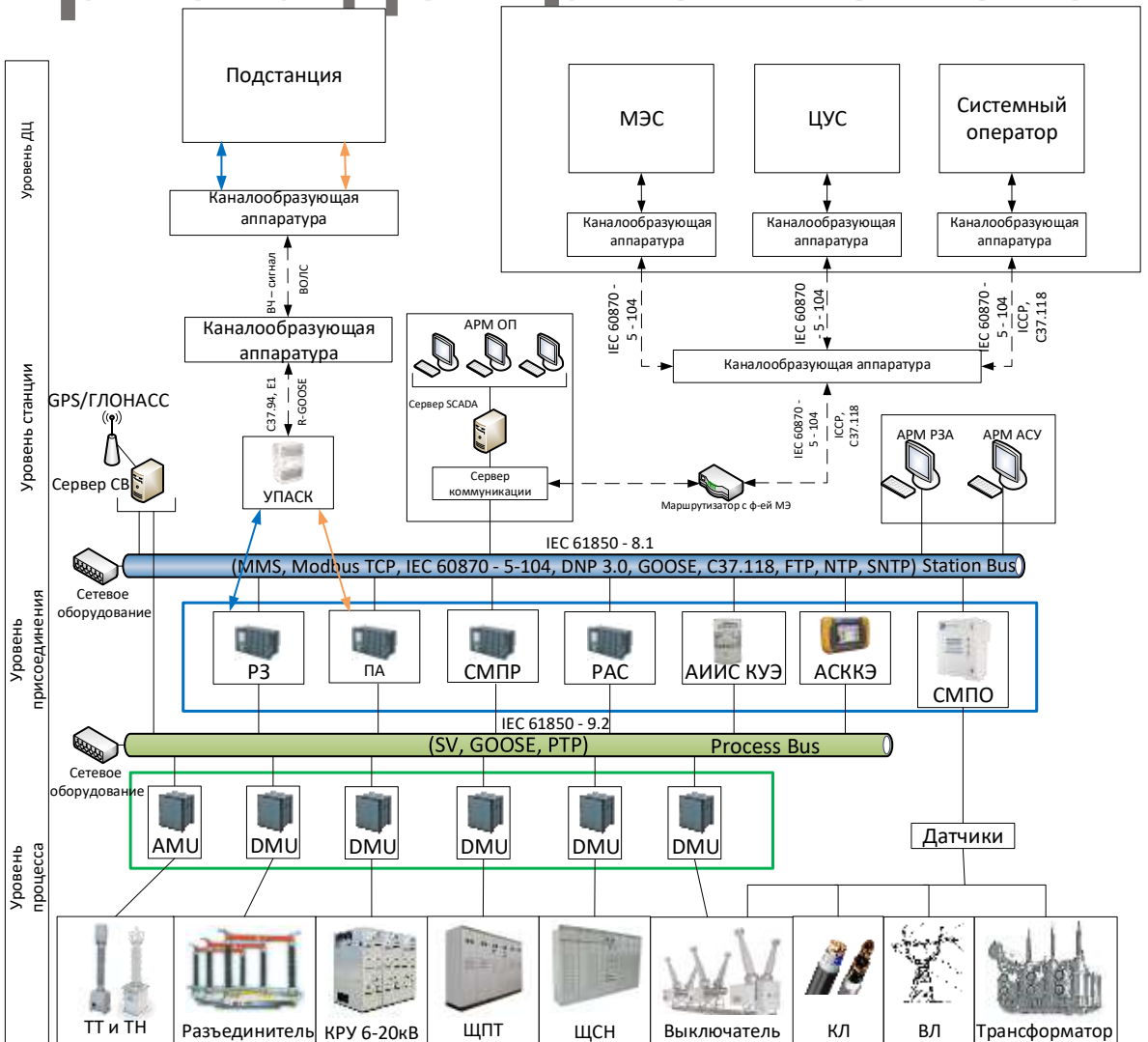
Воздействие на физический уровень

Что делать? Сегодня снизить уровень риска до достижимо низкого



- «Закрыть периметр»
- «Повысить наблюдаемость» – мониторинг состояния защищенности
- Применение положений МЭК 62443
- Сегментация и внедрение элементов многоуровневой защиты

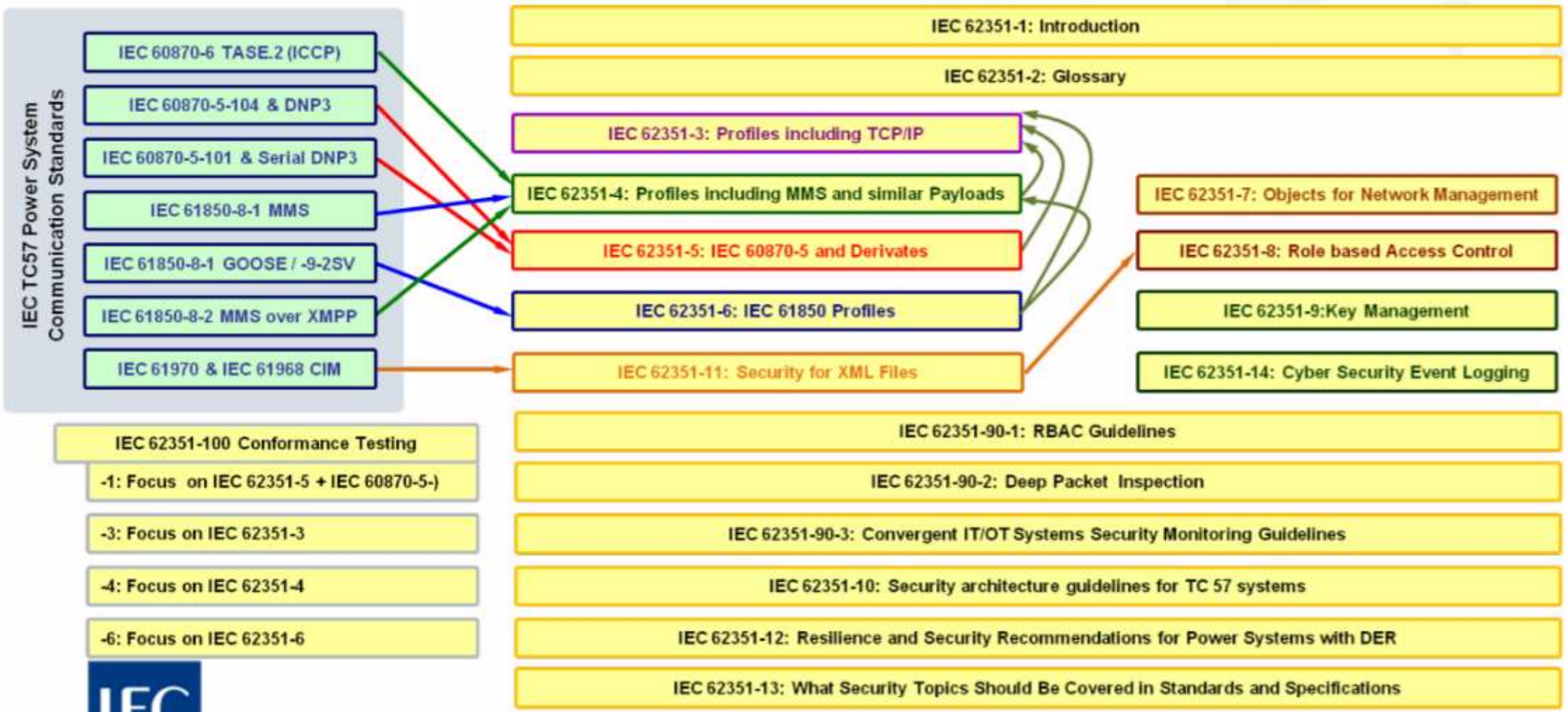
Что делать? Завтра добиться снижения уровня риска до приемлемого



КИБЕРБЕЗОПАСНОСТЬ

- Реализовать на практике принцип многоуровневой защиты
- Эффективно комбинировать применение наложенных и встроенных СЗИ
- Реализовать модель безопасности на уровне объекта (ЦПС)
- Реализовать модели безопасности на уровне каждого типа EndPoint:
  - АРМ
  - Сервер
  - Терминал РЗА
  - Контроллер присоединения
  - Активное сетевое оборудование всех уровней и т.д.
- Доверенные коммуникации
- Внедрить практики безопасной разработки (SDL)
- Разработать и внедрить методики оценки соответствия

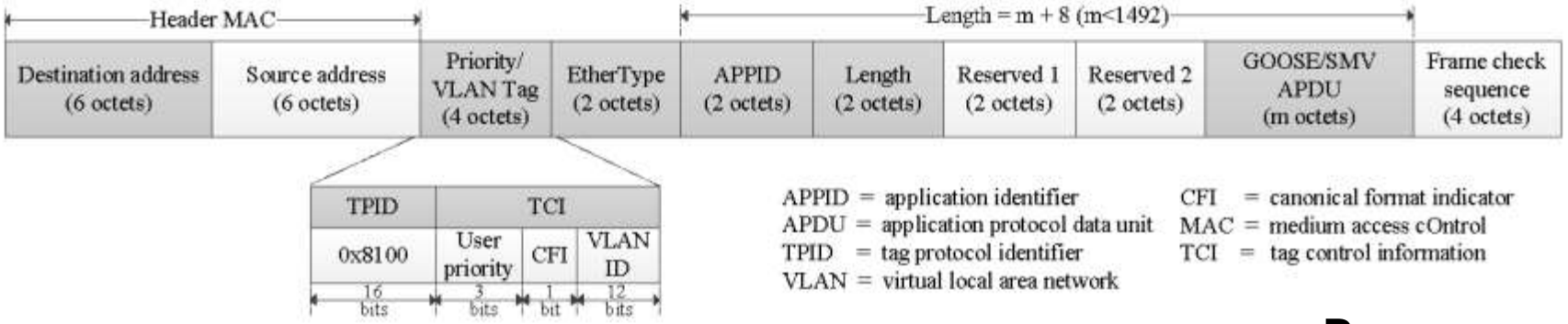
Нормативно-техническое регулирование

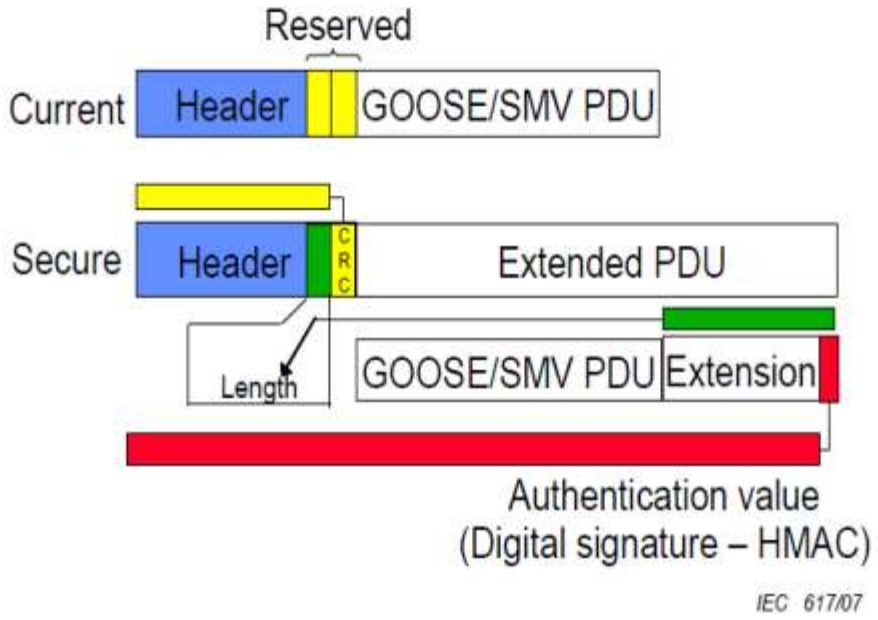


ЗАВТРА. Разработка доверенных систем технологического уровня

- Российские CPU и микроконтроллеры
- Доверенные операционные системы
- Аутентификация устройства
- Аутентификация пользователя устройств
- Доверенная загрузка устройства
- Доверенные обновления
- Встроенный МЭ
- Логирование событий безопасности
- Контроль целостности ПО устройства
- Защищенные протоколы обмена (TLS, защищенный 104-й, OPC UA и т.д.)
- Обеспечение неотказуемости для данных, передаваемых устройством
- Удаленная аттестация устройства
- …

Завтра. Защищенный пакет GOOSE



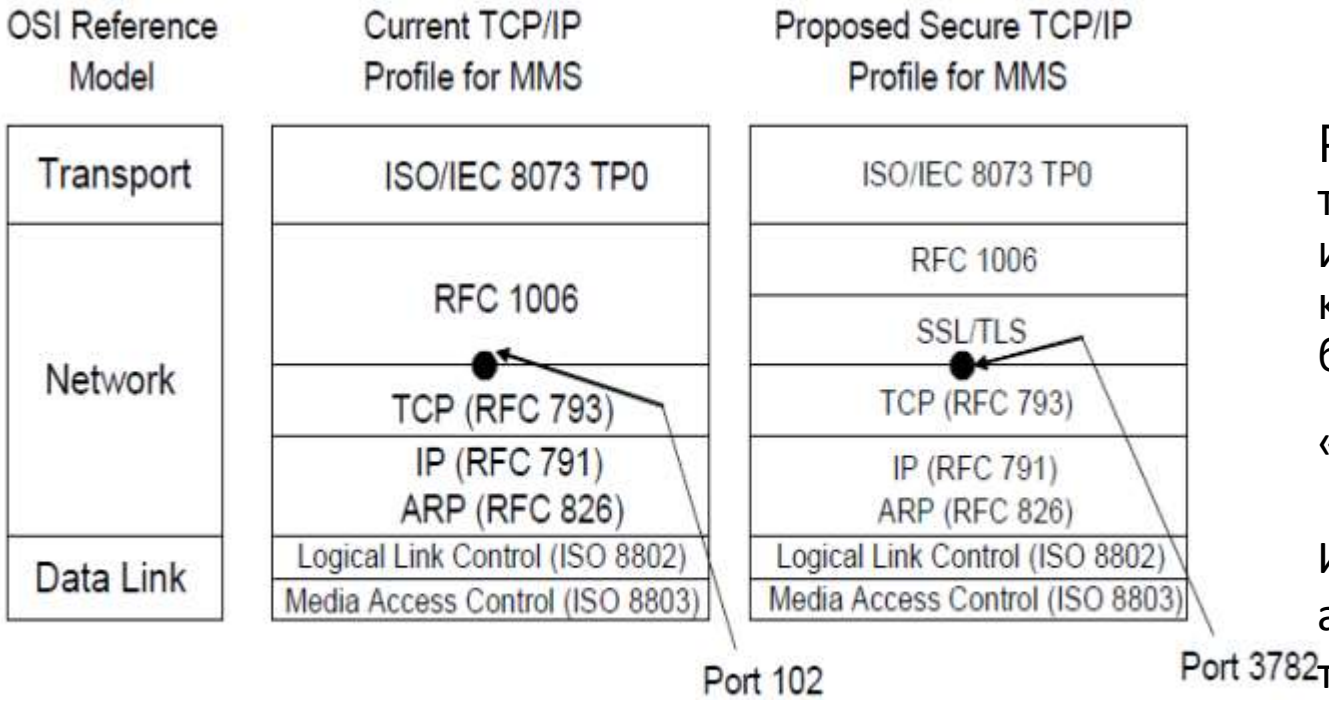


Рекомендации по стандартизации

Использование криптографических алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.10-2012 И ГОСТ Р 34.11-2012

- HMAC_GOSTR3411_2012_256
- HMAC_GOSTR3411_2012_512

Завтра. Защищенный профиль MMS



Рекомендации по стандартизации

P1323565.1.020-2018 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)».

«Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)». На обсуждении.

Криптонабор	Блочный шифр
TLS_GOSTR341112_256_WITH_MAGMA_CTR_OMAC	ГОСТ Р 34.12-2015, "Магма"
TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC	ГОСТ Р 34.12-2015, "Кузнечик"

Реализация защищенных профилей MMS, GOOSE

- Электронная подпись по ГОСТ Р 34.10–2012
- Шифрование по ГОСТ Р 34.12–2015 ,
- Хэширование по ГОСТ Р 34.11–2012.
- Имитовставка (MAC) по ГОСТ 28147-89

Варианты реализации:

- Программная реализация.
- Аппаратная реализация.
- Программно-аппаратная реализация.

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 реализации киберзащищенной цифровой подстанции на основе российских технологий

Владимир Карантаев

к.т.н. MBA

эксперт IEC, IEEE, CIGRE

Автор блога: https://smartgridib.blogspot.com/

Екатеринбург 11 Июля, 2019