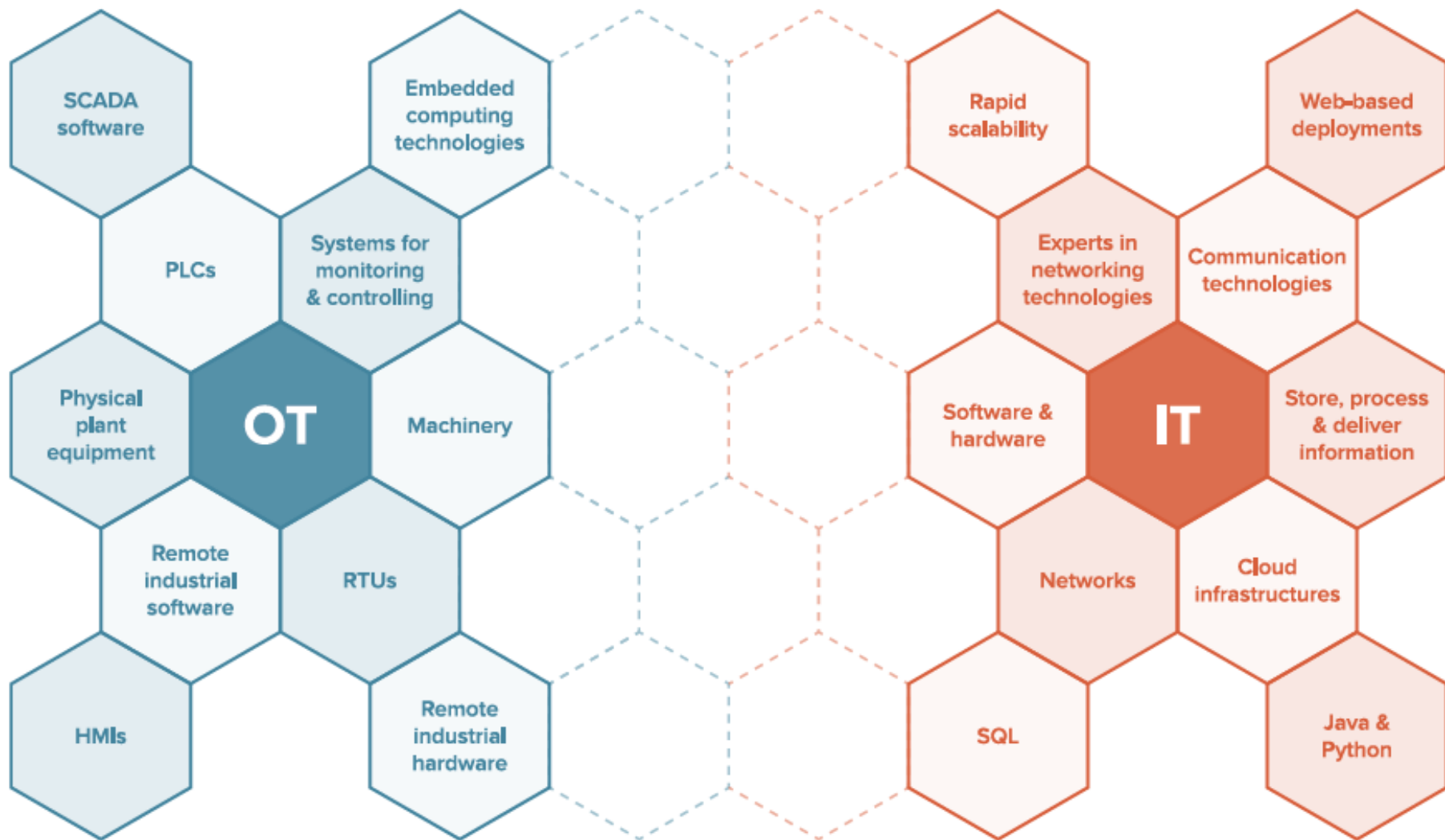


Вопросы обеспечения информационной безопасности (киберзащищенности) цифровой подстанции, как элемента IoT

Владимир Карантаев / к.т.н.
Руководитель РГ4 подкомитета D2 РНК СИГРЭ
Руководитель направления
Vladimir.Karantaev@infotecs.ru

OPERATIONAL TECHNOLOGY + INFORMATION TECHNOLOGY = IIOT

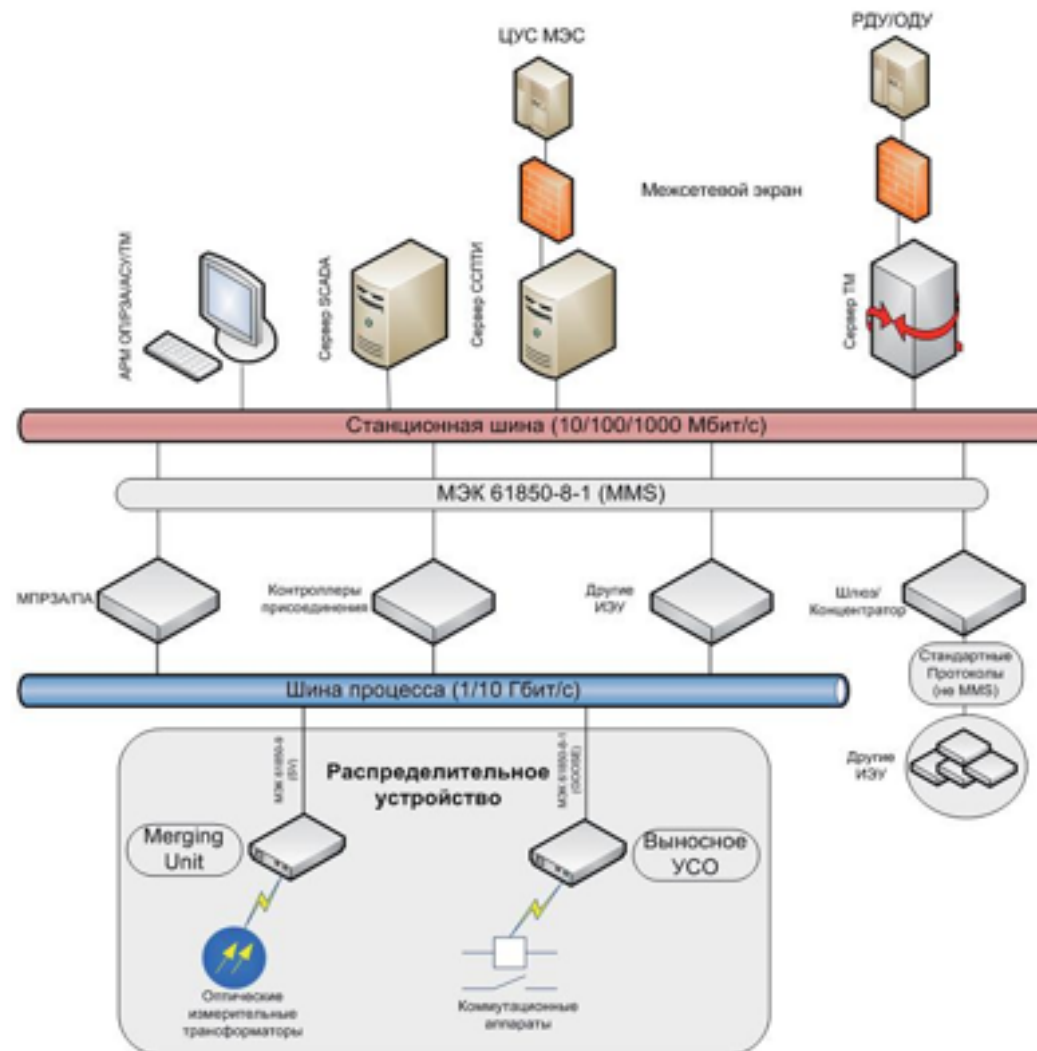


ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ ЕЭС РФ

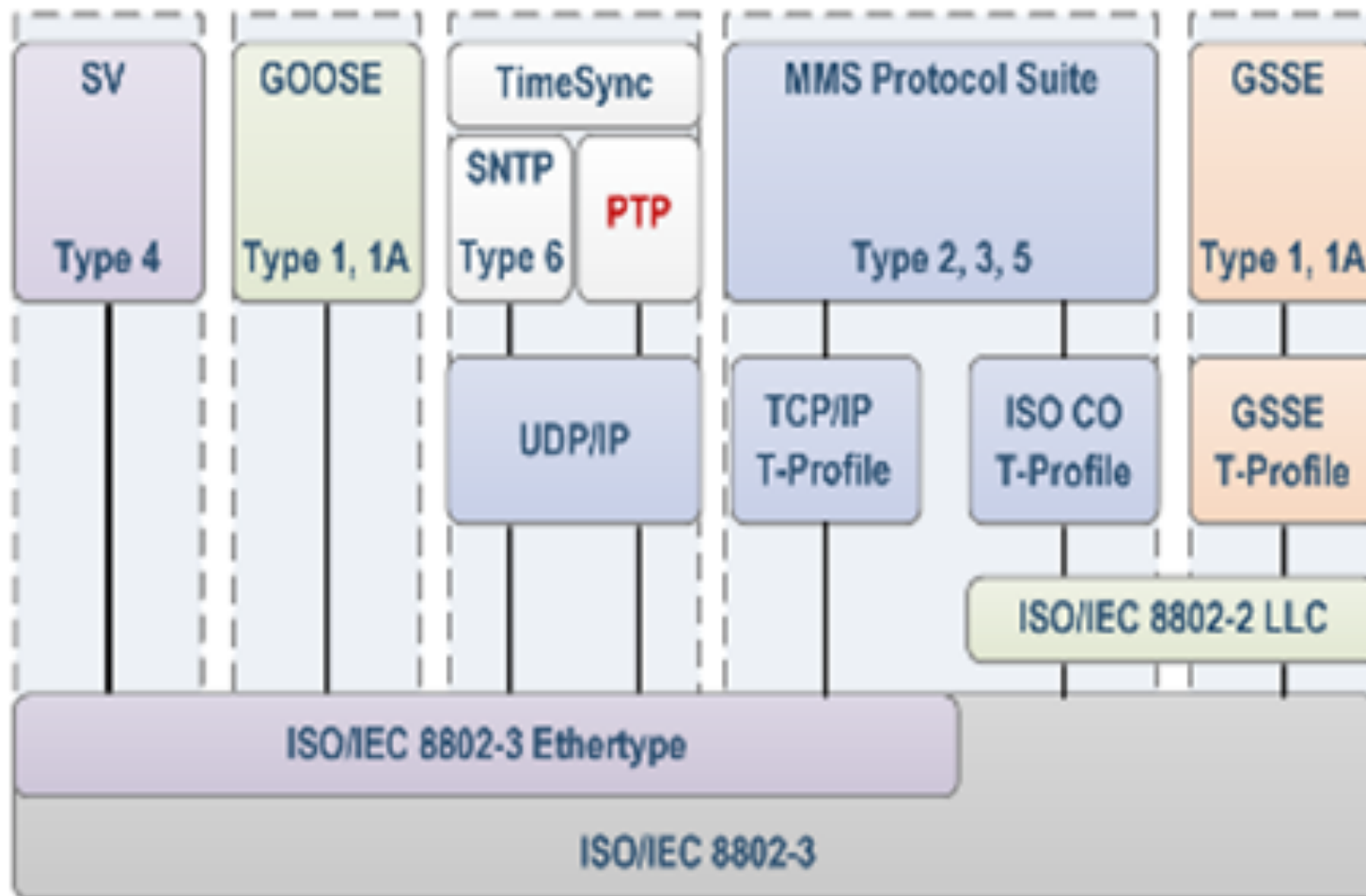
- Внедрение технологий Smart Grid.
- Внедрение технологий Smart metering.
- Внедрение нового управляемого силового оборудования в ААС.
- Внедрение цифровых ПС с учетом развития цифровой обработки.



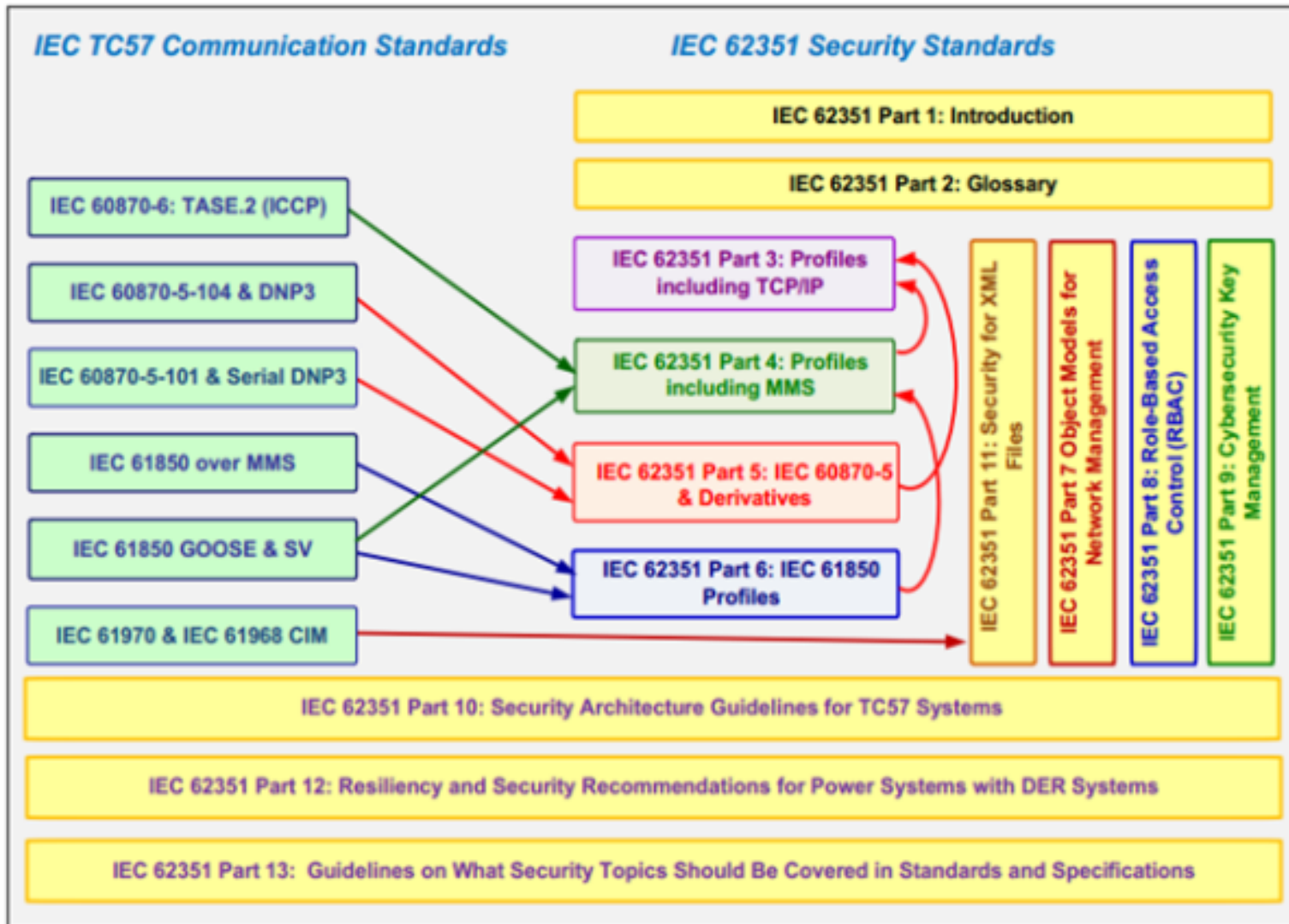
АРХИТЕКТУРА ЦИФРОВОЙ ПОДСТАНЦИИ МЭК 61850



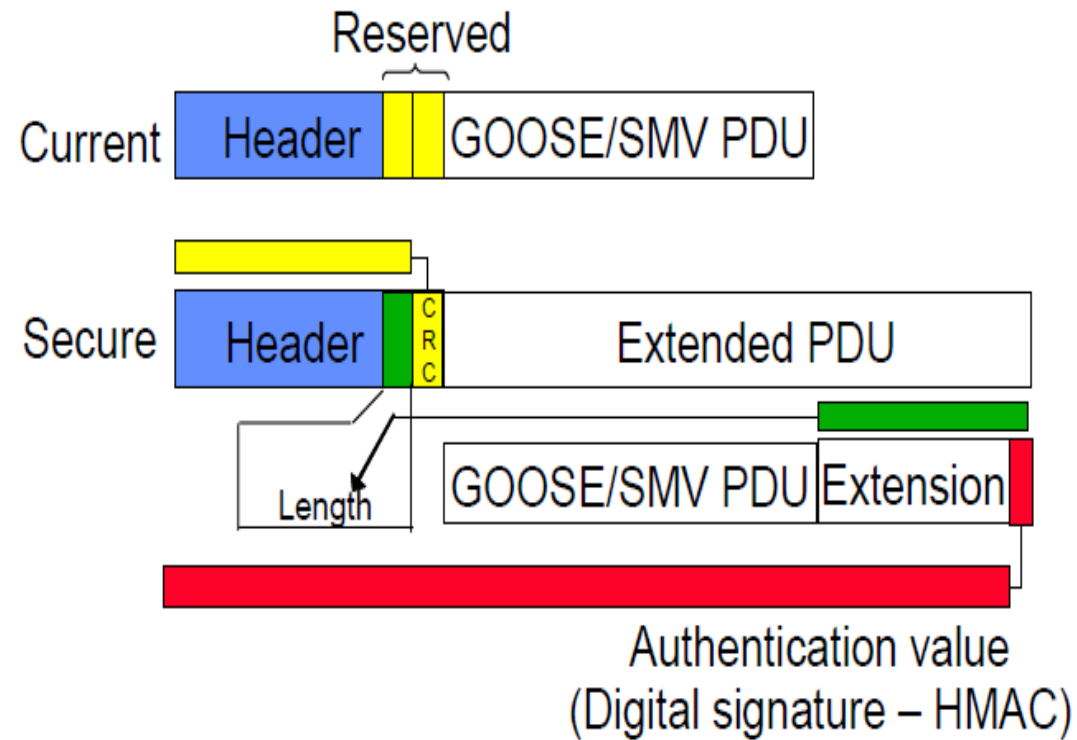
ОБЗОР ФУНКЦИОНАЛЬНОСТИ И ПРОФИЛИ В СООТВЕТСТВИИ С МЭК 61850-8-1



ВЗАИМОСВЯЗЬ СТАНДАРТОВ МЭЖ ТК 57

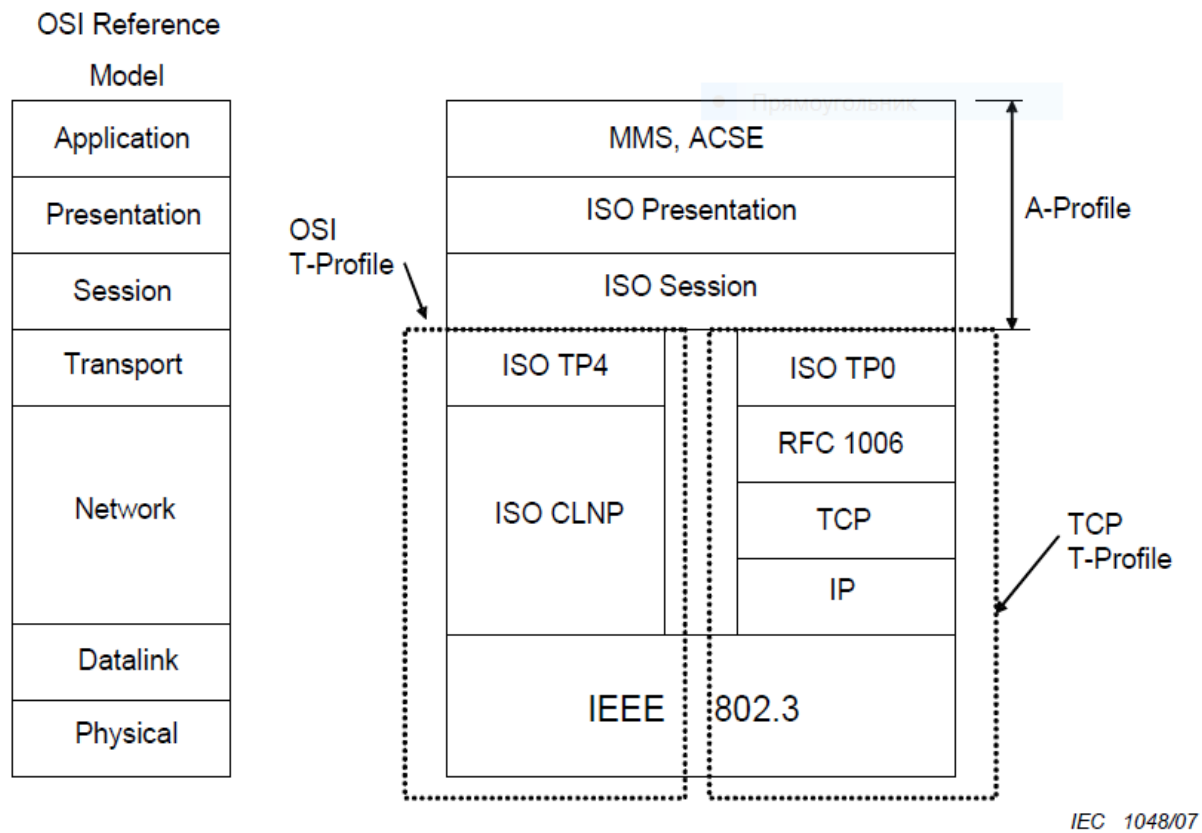


НЕЗАЩИЩЕННЫЙ И ЗАЩИЩЕННЫЙ ПАКЕТ GOOSE/SV

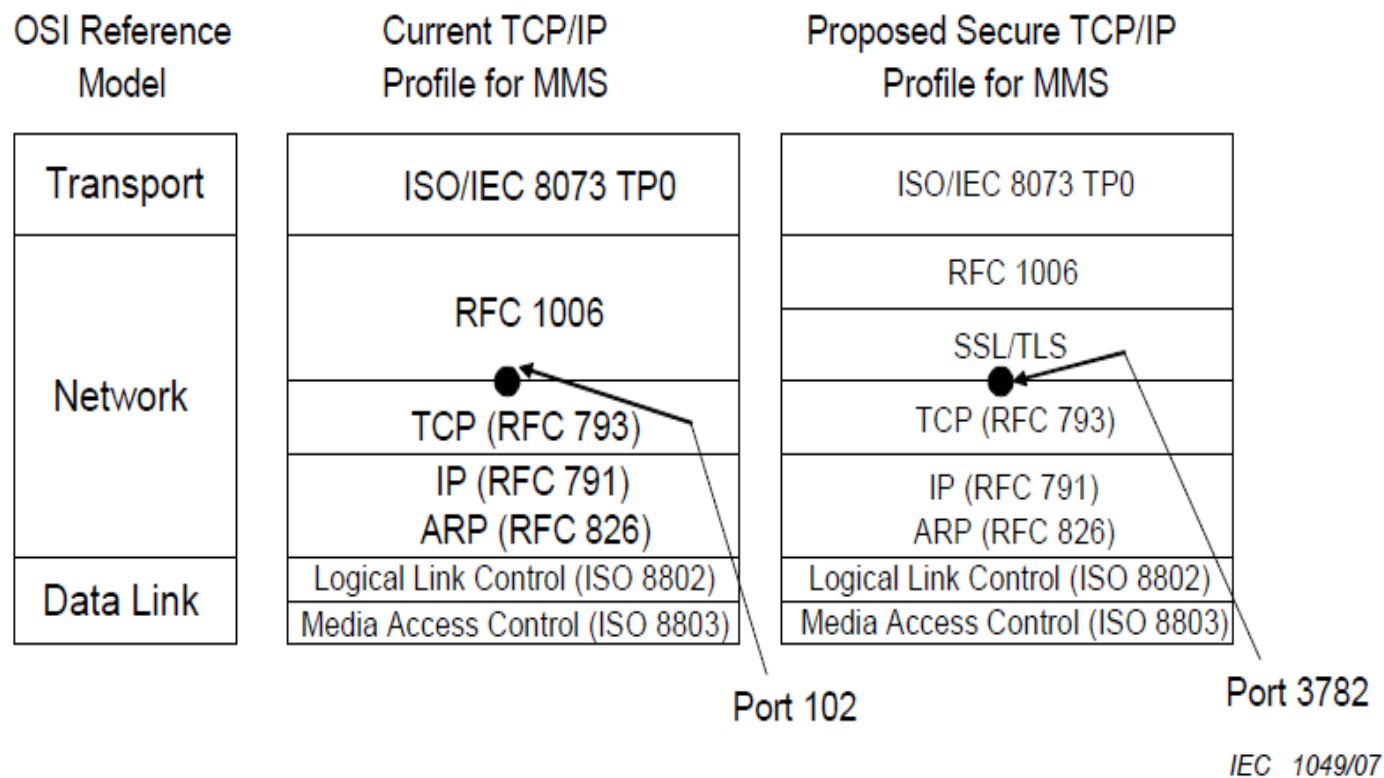


IEC 61707

А и Т ТЕЛЕКОММУНИКАЦИОННЫЕ ПРОФИЛИ MMS



НЕЗАЩИЩЕННЫЙ И ЗАЩИЩЕННЫЙ ПРОФИЛЬ MMS



РЕАЛИЗАЦИЯ ЗАЩИЩЕННЫХ ПРОФИЛЕЙ MMS, GOOSE, SV

- 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:

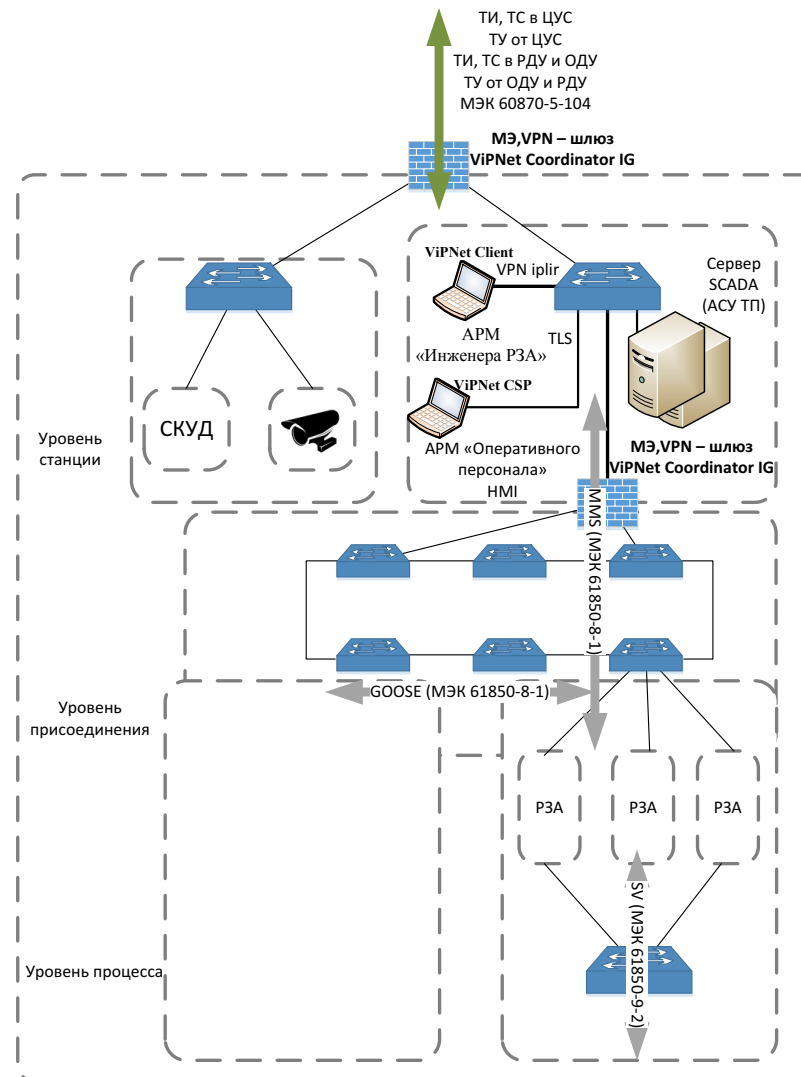
- Программная реализация.
- Аппаратная реализация.
- Программно-аппаратная реализация.

ПРОИЗВОДИТЕЛЬНОСТЬ КРИПТОЯДРА VIPNET НА PKCS#11 ИНТЕРФЕЙСЕ

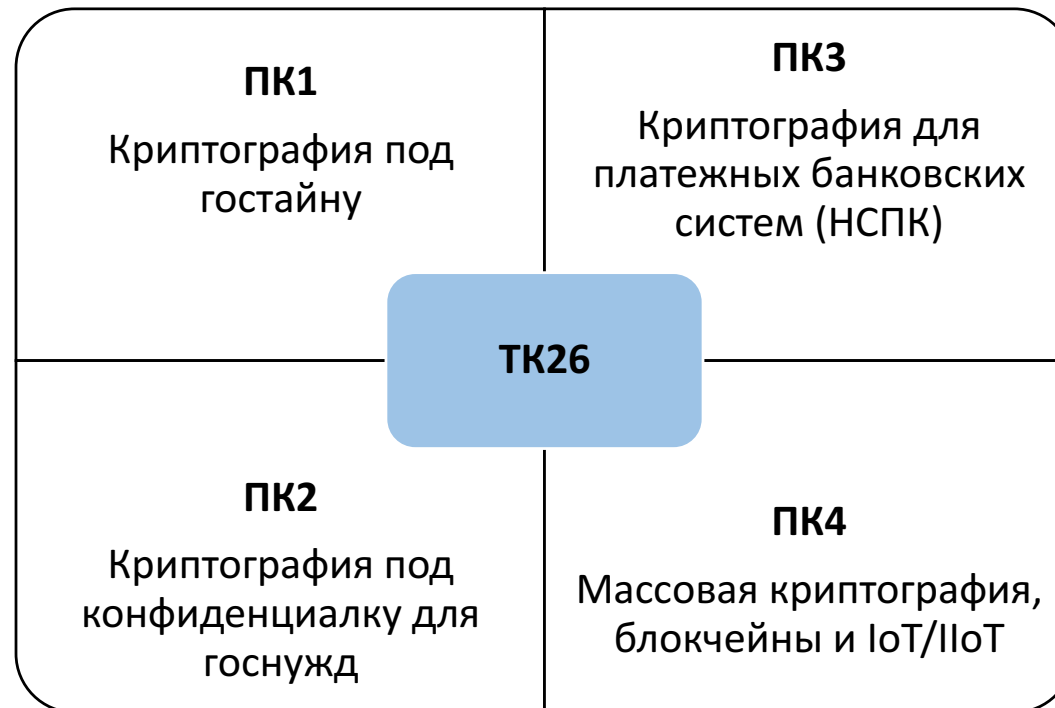
Микропроцессор	Intel		Байкал Т1 (MIPS)		Эльбрус (Е2К)	
Частота, Мгц	2100		1200		800	
Использованный метод	НМАС	МАС	НМАС	МАС	НМАС	МАС
Время обработки блока 64 Байта, мс	0,028	0,024	0,388	0,325	0,881	0,785
Время обработки блока 256 Байта, мс	0,03	0,025	0,38	0,3	0,875	0,843
Время обработки блока 2048 Байта, мс	0,029	0,026	0,55	0,358	0,945	0,775

- Имитовставка (МАС) по ГОСТ 28147-89
- НМАС по ГОСТ Р 34.11-2012

ФУНКЦИОНАЛЬНАЯ СХЕМА ЦПС В КИБЕРЗАЩИЩЕННОМ ВИДЕ



Про ТК26



Криптография
для АСУ ТП



ТЕХНИЧЕСКИЙ КОМИТЕТ ПО СТАНДАРТИЗАЦИИ
«КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ» (ТК 26)



Спасибо за внимание!