



Вопросы кибербезопасности в меняющейся электроэнергетической отрасли.

Владимир Карантаев

к. т. н. MBA

эксперт IEC, IEEE, CIGRE

+ 7 915 221 15 96

Структура доклада:

- Обзор докладов исследовательских комитетов (ИК) по теме «Кибербезопасность».
- Обзор технической выставки на 47 сессии СИГРЭ.
- Глобальные тренды кибербезопасности АСУ ТП.
- Вопросы развития в РФ.

Актуальность

- Принят и работает Федеральный Закон от 26 Июня 2017 № 187 « О безопасности критической информационной инфраструктуры Российской Федерации».
- Утверждена распоряжением Правительства Российской Федерации от 28.07.2017 № 1632р программа «Цифровая экономика Российской Федерации».
- Утверждена 21.12.2018 советом директоров ПАО «Россети» концепция «Цифровая трансформация 2030.
- Общемировая тенденция: реализация концепции «Industry 4.0», развития и внедрения совокупности технологий, называемых Индустриальный интернет вещей (Industrial Internet of Things)».



РОССЕТИ



Развитие ИТД в ПАО «Россети»

2017

Распоряжение ПАО «Россети» от 30.05.2017 № 282р «Об утверждении требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса Группы компаний «Россети».

2019

29 марта 2019 года приказом ПАО «Россети» № 64 утверждены стандарты:

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

СТО 34.01.-21-005-2019 «Цифровая электрическая сеть».





ЛУЧШИЕ МИРОВЫЕ ПРАКТИКИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЭЛЕКТРОСЕТЕВОГО КОМПЛЕКСА ПО СОСТОЯНИЮ НА 2018 ГОД* И МЕСТО КОМПАНИИ «РОССЕТИ»

	TEPCO Япония	Enel Италия	ENEDIS (EDF) Франция	National Grid Велико- британия	KEPCO Корея	Россети
1. Технологии цифровой подстанции (МЭК 61850)						Элементы цифровых подстанций
2. Интеллектуальные системы учета						
3. «Цифровой электромонтер»						Внедрен ГЛОНАСС без аналитического модуля
4. Риск-ориентированная модель управления						В 2018 году внедрен индекс технического состояния оборудования
5. Интеллектуальные системы управления (ADMS)						
6. Автоматизированные системы предиктивного анализа						
7. Кибербезопасность						Антивирусы и отдельные элементы
8. Цифровые системы автоматизированного проектирования (САПР)						Элементы внедрены в ФСК

* Исследования Российского энергетического агентства, аналитические материалы Ernst and Young (2017, 2018)

АРХИТЕКТУРА ЦИФРОВОЙ СЕТИ

Уровень анализа и принятия стратегических решений

Аналитика, оперативно-информационный комплекс (ОИК) в части схемы сети

Уровень ведения хозяйственной деятельности

Данные из технологических систем интегрируются в ERP системы корпоративного уровня ДЗО (система управления производственными активами (СУПА), SAP, 1С и т.д.)

Уровень оперативно-технологического управления

в филиале ДЗО всеми ПС и линиями электропередачи (ЛЭП), размещения всех информационных систем (ADMS, географические информационные системы (ГИС) и т.д.)

Уровень оперативно-технологического управления

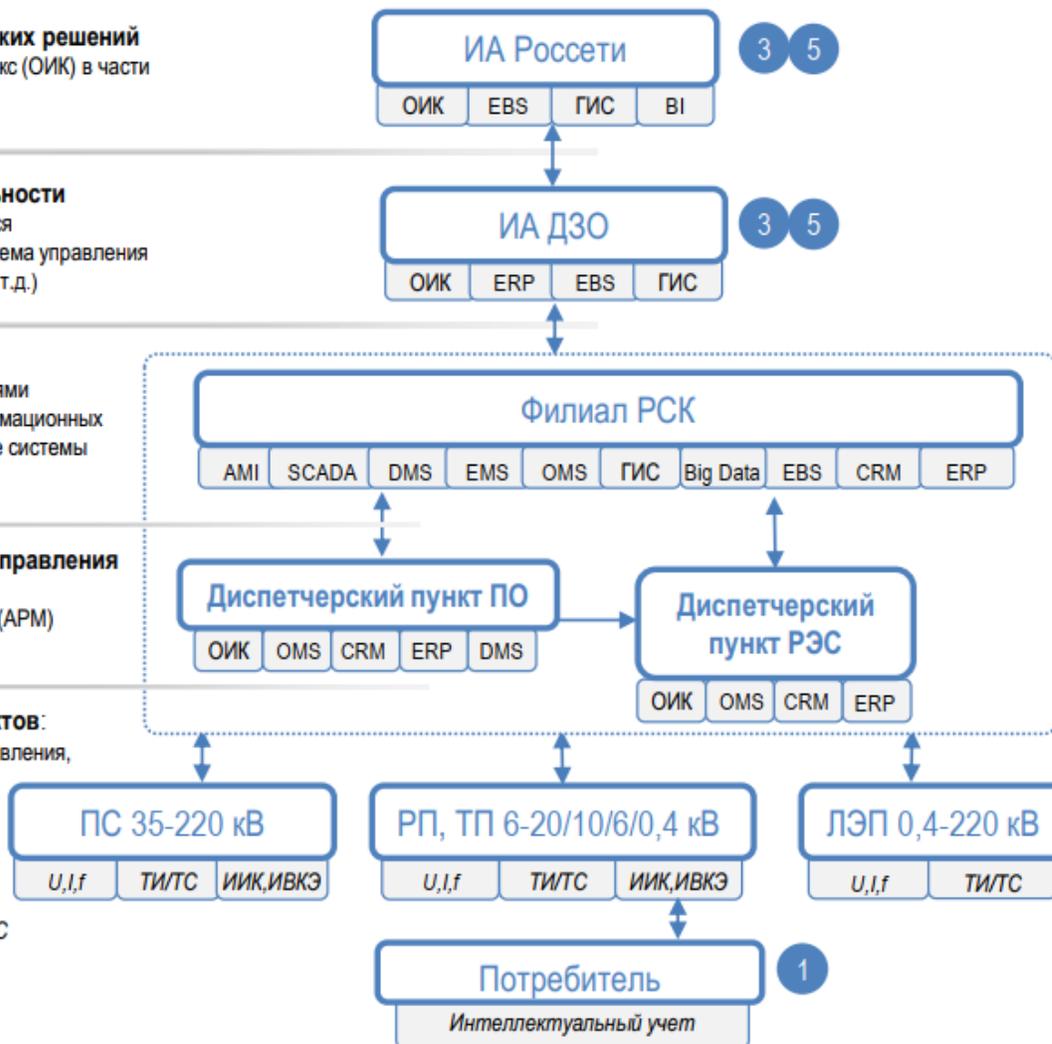
ПО: ПС и ЛЭП 35 кВ; РЭС: 6-20/0,4 кВ
Удаленные автоматизированные рабочие места (АРМ) диспетчеров в рамках зоны обслуживания

Уровень получения информации с объектов:

сбор данных с датчиков: телемеханики, телеуправления, технического и коммерческого учета. Объекты ПС + сеть 0,4-220 кВ

Технологии цифровизации

- 1 - Приборы учета
- 2 - Телемеханизация
- 3 - Системы управления
- 4 - Цифровая ПС
- 5 - Связь



финансово-экономические и обобщенные производственные показатели

3 5

3 5

3 5

1 2

3

4 5

Производственные показатели

Оперативно-технологическая информация



- ИА – исполнительный аппарат
- ДЗО – дочерние и зависимые общества
- РСК – распределительный сетевой комплекс
- ПО – производственное отделение
- РЭС – район электрических сетей
- ОИК – оперативно-измерительный комплекс
- EBS – единая информационная шина
- ГИС – геоинформационная система
- BI – блок аналитики
- ERP – система оптимизации ресурсов предприятия
- AMI – интеллектуальный учёт
- SCADA – система диспетчерского управления и сбора данных
- DMS/ADMS – системы управления распределением
- EMS – система оперативного управления режимами сети
- OMS – управление сетями в аварийном режиме
- Big Data – технология управления большими объемами данных
- CRM – Система управления взаимоотношениями с клиентами
- U, I, f – датчики тока, напряжения и т.д.
- ТИ/ТС – устройство телеизмерения/телесигнализации
- ТУ/ТМ – телеуправление/телемеханизация
- АРМ – автоматизированное рабочее место
- ИИК, ИВКЭ – информационно-измерительный комплекс, информационно-вычислительный комплекс электроустановки
- ТП, РП – трансформаторные и распределительные подстанции

Цифровая система управления «переместила» центр управления с РЭС на уровень филиалов РСК



Обзор докладов исследовательских комитетов (ИК) по теме «Кибербезопасность».

Кибербезопасность один из приоритетных вопросов ИС D2 СИГРЭ

ПТ2 (PS 2): НОВЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В МЕНЯЮЩЕЙСЯ ЭЛЕКТРОЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

- Проблемы кибербезопасности при использовании интернета вещей, больших данных и облачных платформ.
- Проблемы кибербезопасности, связанные с распределенными энергоресурсами и объединением новых провайдеров «гибкости».
- Выявление угроз кибербезопасности с помощью анализа больших данных и машинного обучения.

Перечень представленных докладов по теме «Кибербезопасность»

- **B5-213_2018:** «Design, Concept, Commissioning, Maintenance, Cyber Security of a IEC61850 Process Bus Brown Field Application».
- **D2-306_2018:** «Research and application of deep security protection technology in power industrial control system».
- **D2-309_2018:** «Network and Data Cybersecurity Strategy of the Electrical Power System».
- **D2-201_2018:** «Substation Virtualisation: An Architecture for Information Technology and Operational Technology Convergence for Resilience, Security and Efficiency».
- **B3-305_2018:** «Problems of Information Security in Energy Object Control Systems».
- **D2-301_2018:** «Building a Secure Network Policies, Architecture and Incident Responses CASE CHESF»
- **D2-313_2018:** «Approach to Maintaining Secure Operation of Various Systems in Japanese Electric Companies»

Обучение

Результаты работы WG D2.38 изданная техническая брошюра 698 (ТБ 698).

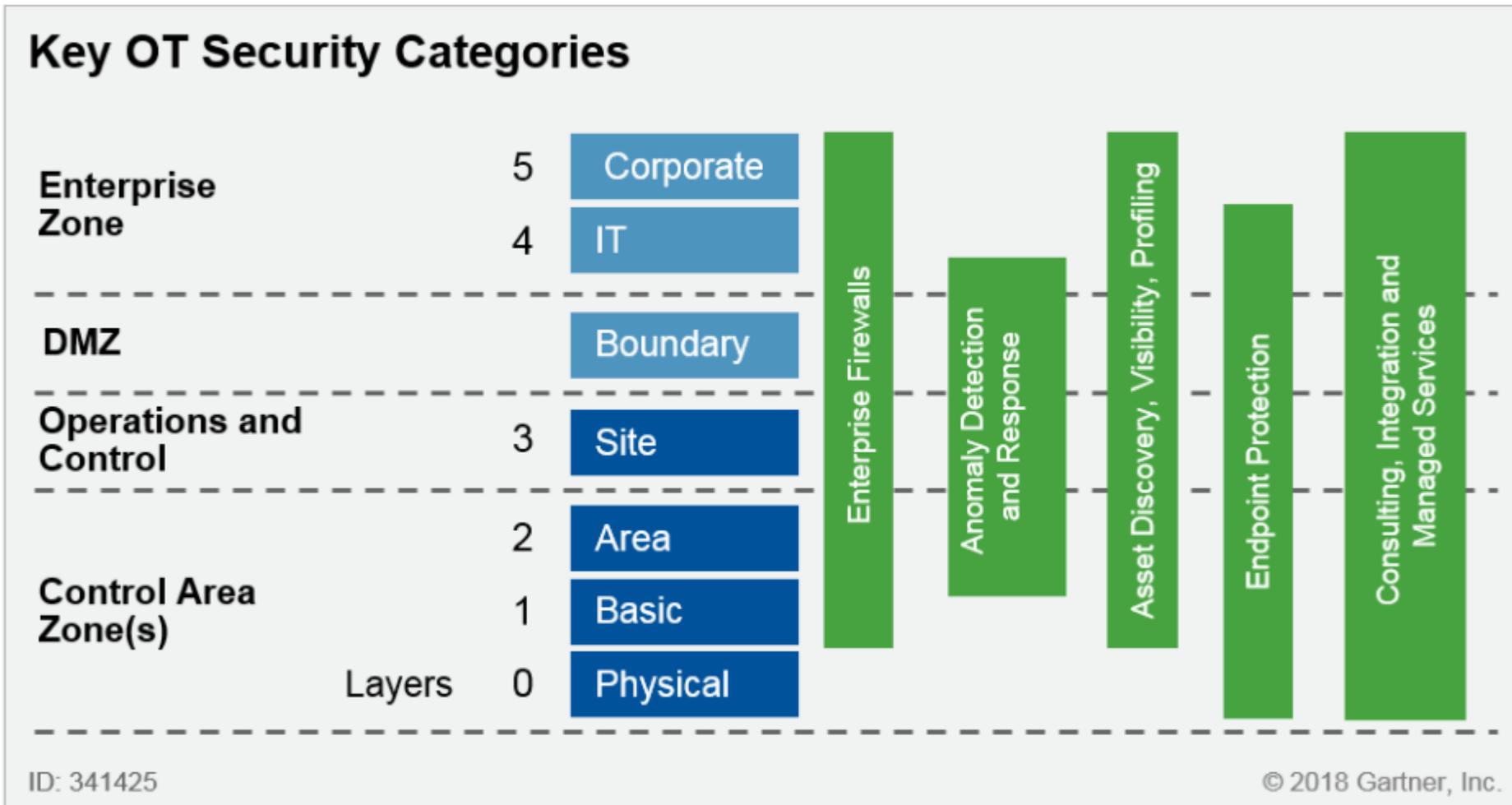
- Title: «**Framework for EPU operators to manage the response to a cyber-initiated threat**»



Обзор технической выставки на 47 сессии СИГРЭ.

Прогноз Gartner на 2018 год

-



Продукты, представленные на выставке: МЭ



Advantech+Stormshield
Next-Gen UTM Firewalls:Stormshield



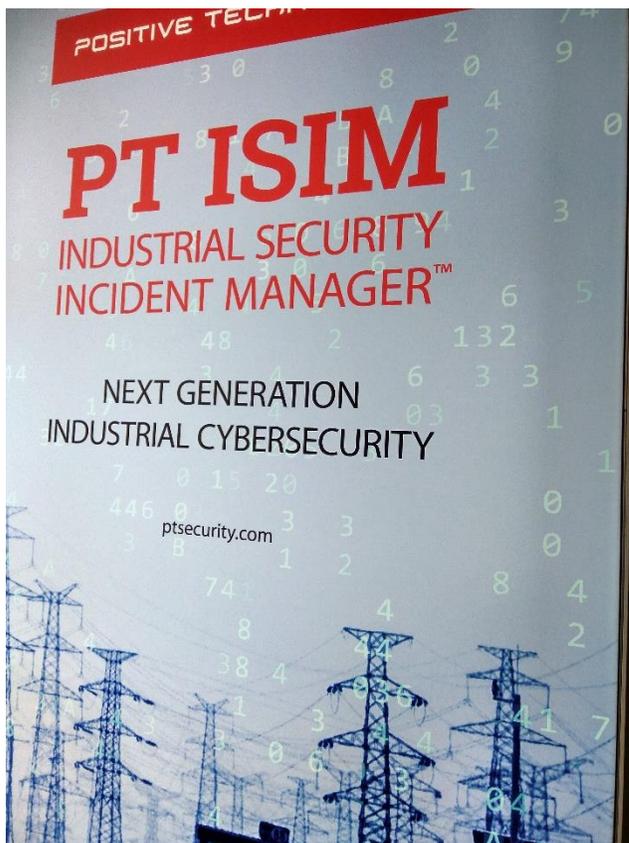
Phoenix Contact
FW:mGuard

Продукты, представленные на выставке: Endpoint Protection



Kaspersky Lab: KICS for Nodes

Продукты, представленные на выставке: Asset Management, Anomaly Detection, Threat Detection



Positive Technology: PT ISIM

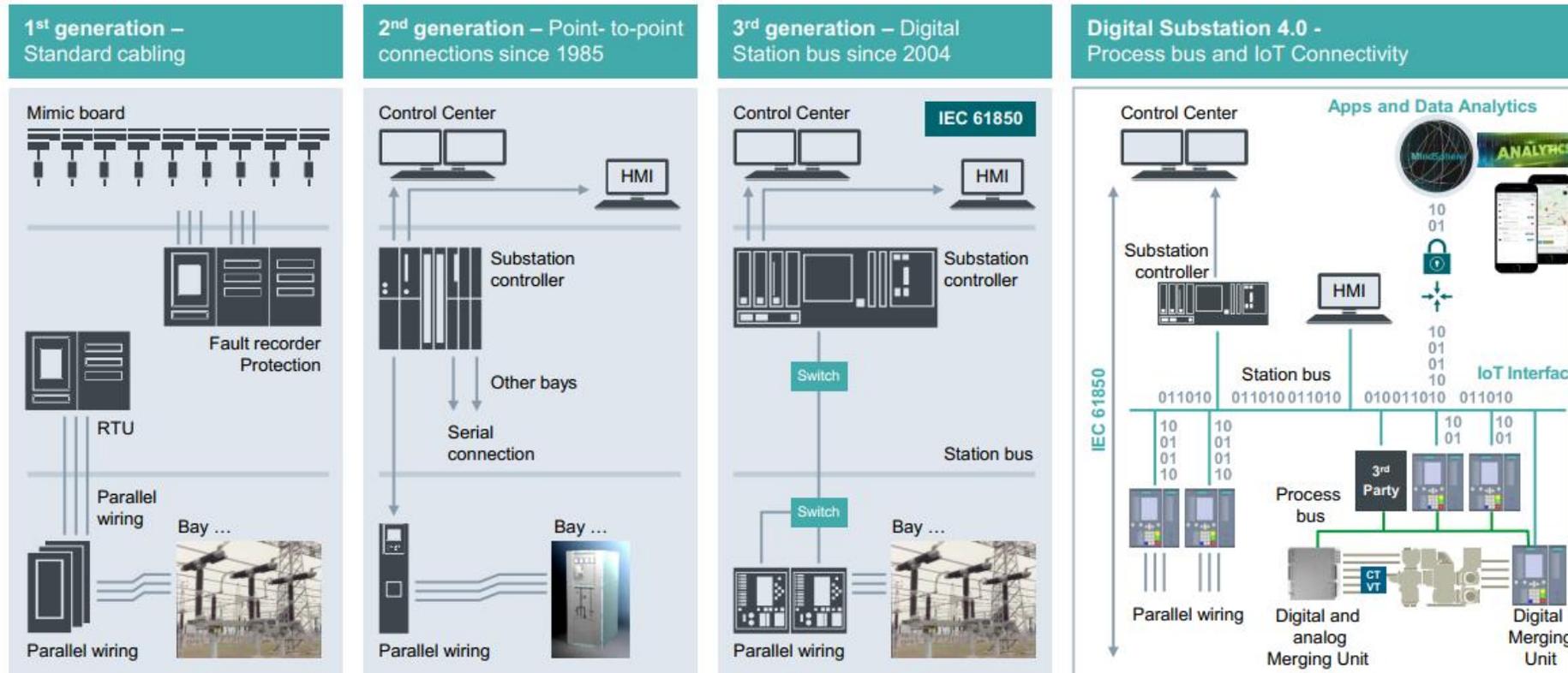


Kaspersky Lab: KICKS for Networks

Cyber Security подход Siemens

Evolution in Substation Automation – SIPROTEC 5 - the core of Digital Substation 4.0

SIEMENS
Ingenuity for life

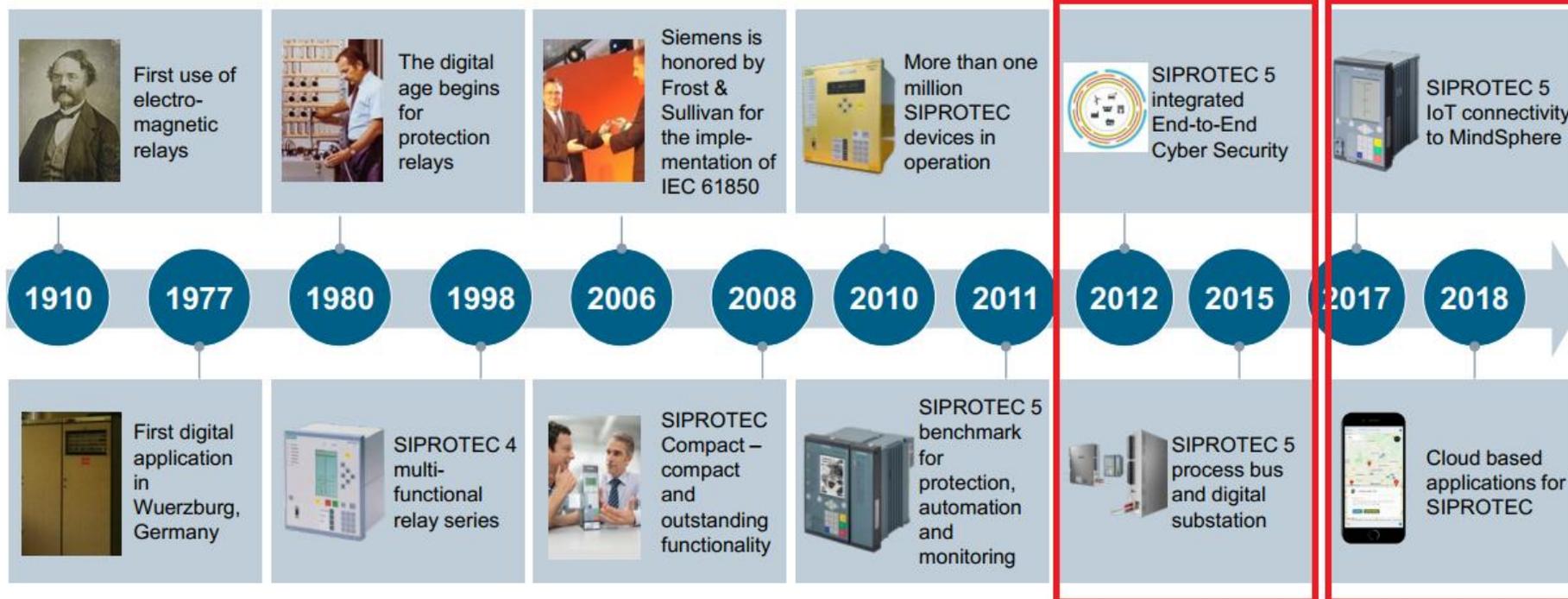


Cyber Security подход Siemens

SIPROTEC –
Synonym for the world’s leading protection technology

SIEMENS
Ingenuity for life

More than 1.6 Mill. devices installed therein >500,000 with IEC 61850



Cyber Security подход Siemens

SIPROTEC 5 – Integrated Cyber Security – Overview



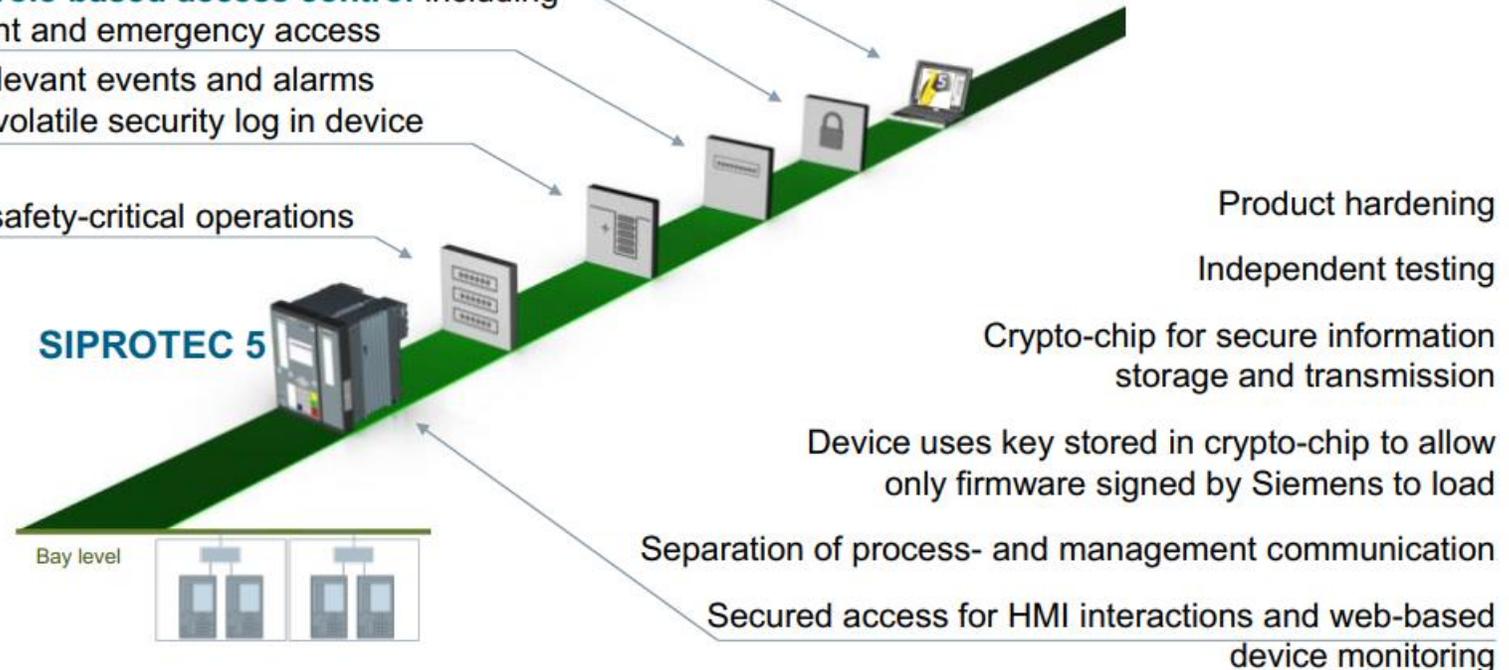
Mutually authenticated and encrypted communication line between DIGSI 5 and the SIPROTEC 5 device

Device-side support for **role-based access control** including central user management and emergency access

Recording of security-relevant events and alarms over Syslog and in non-volatile security log in device

Confirmation codes for safety-critical operations

Secure development
Patch management
Antivirus compatibility



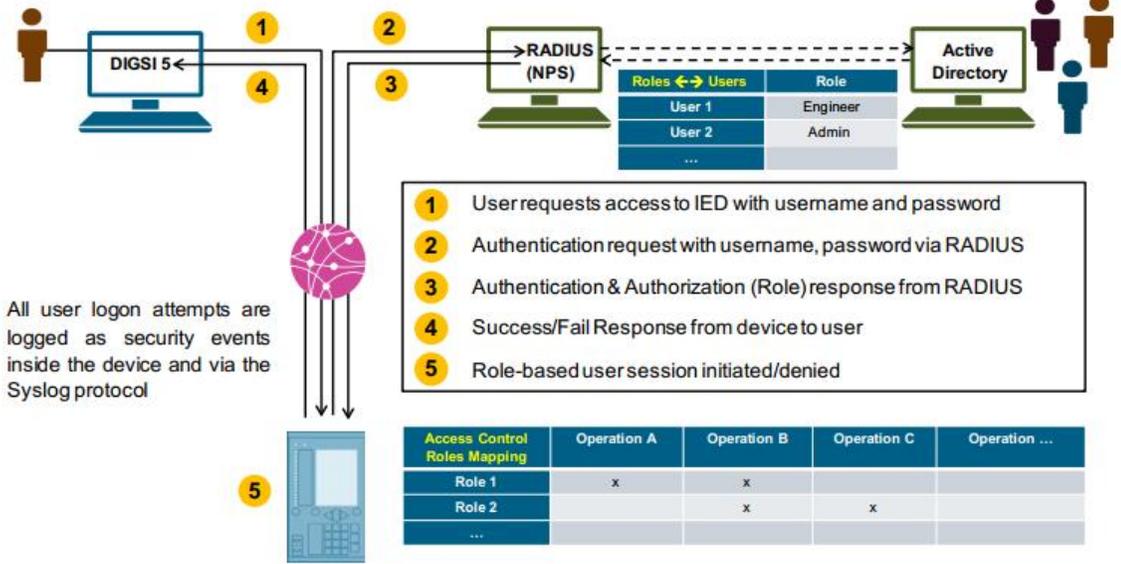
Cyber Security подход Siemens

SIPROTEC 5 – Integrated Cyber Security

NEW V7.8

SIEMENS
Ingenuity for Life

Role-based Access Control (RBAC) with central user management



All user logon attempts are logged as security events inside the device and via the Syslog protocol

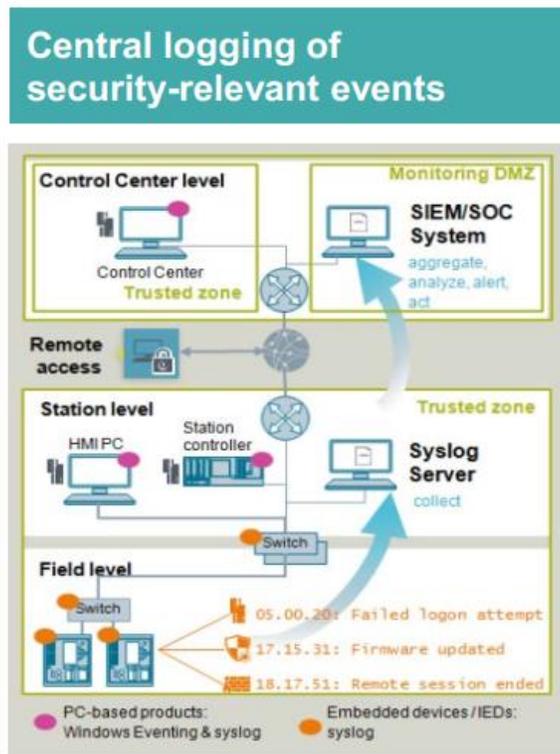
- Use (your existing) centrally managed user accounts and passwords for secured SIPROTEC 5 access
- Works with existing RADIUS servers e.g. Microsoft Active Directory Network Policy Server (NPS)
- Roles and rights adhere to standards and guidelines e.g. IEC 62443, IEC 62351, IEEE 1686, BDEW Whitepaper
- Access control even when RADIUS server connectivity is disrupted
- Feature supported for all forms of interaction: DIGSI 5, Web browser and on-site operation panel
- Audit trail of security-relevant user actions

Cyber Security подход Siemens

SIPROTEC 5 – Integrated Cyber Security

NEW V7.5

SIEMENS
Ingenuity for life



Digitally signed firmware

- Device-firmware is protected against manipulation
- Only firmware digitally signed by Siemens can be loaded and processed
- This is ensured via an integrated crypto-chip with secured key storage and signature technology



Cyber Security подход Siemens

Digitalization of process- and station-level

Where does SICAM GridPass Fit In? Primarily as part of a system project – New/Refurbishment

SIEMENS
Ingenuity for Life

- Designed to work with SIPROTEC and SICAM products
- Designed to work with all products supporting the international security standard for power systems IEC 62351
- Can also be installed at the central (control center) level
- **By the way**
Can also be used standalone as CA!

Unrestricted © Siemens AG 2018
Page 15 July 2018
Energy Management – Digital Grid

Digitalization of process- and station-level

Defense-in-Depth Powered by OT PKI SICAM GridPass is Based on International Standards

SIEMENS
Ingenuity for Life

Manages standard X.509 digital certificates

- Revoke**
Manage and publish a list of revoked certificates
- Renew**
Renew certificates
- Issue**
Sign certificates automatically or manually
- Authenticate**
Check identity and authenticity of automated signing requests

SICAM GridPass
Certificate Manager for Substations

Supports automated CA activities using Est¹ protocol acc. IEC 62351-9

1 EST: Enrollment over Secure Transport protocol, IETF Standard RFC 7030 ([internet link](#))

Unrestricted © Siemens AG 2018
Page 7 July 2018
Energy Management – Digital Grid

Cyber Security подход Siemens

Substation automation
Digitalization of process- and station-level

SIEMENS
Ingenuity for Life

Defense-in-Depth Powered by OT PKI¹ - Usage of Digital Certificates makes Security Controls Manageable

Identity management
Unique IDs for personnel and products for authentication

Access control
Specify role and other constraints for authorization

Secure communication
Agree on cryptographic details for securing network protocols

Malware protection
Validate the source and integrity of OT software and firmware

Data protection
Validate the integrity of process data

Settings protection
Validate the integrity of OT settings

PKI
Digital certificates for your OT Network

1 PKI: Public Key Infrastructure

Unrestricted © Siemens AG 2018
Page 5 July 2018

Energy Management – Digital Grid

...ing new market in cyber security services
Comprehensive portfolio with internal&external resources

SIEMENS
Ingenuity for Life

Assess

Implement

Manage

- Training Cybersecurity**
- Consulting Cybersecurity**
- Penetration Testing**
- Migration to a Cybersecure Substation**
- Patch Management**
- Vulnerability Management**
- Backup and restore**
- OT-Monitoring solution**
- Incident/Event response**

- Training to consider measures for a secure substation framework certified according to IEC 62443-2-4 and -3-3
- Organization and process analysis
- Assessment of installation's vulnerability to cyber threats
- Emulation of a professional human attacker
- Migrate the substation's architecture to a secure state
- Implementation of measures according to IEC 62443-2-4/-3-3
- Information, recommendation, testing and installation
- Continuous detection & protection (antivirus + whitelisting)
- Regular firewall maintenance for hardened substations
- Disaster recovery concept (asset configuration, data, etc.)
- Periodic restoration drills to ensure recoverability
- Security monitoring sensors& solution for real-time OT security
- Centralized collection of security relevant information (SIEM)

Restricted © Siemens AG 2018
Page 5 CIGRE 2018

CIGRE / Digital Grid

Cyber Security подход Schneider Electric



Cyber Security подход ZIV Испания



Кибербезопасность в соответствии с IEC 62351 и IEEE 1686-2013:

- RBAC
- Secure keys
- Physical and logical port disabling
- CyberSecurity event log
- Securing of management protocols

Cyber Security подход Sprecher Automation



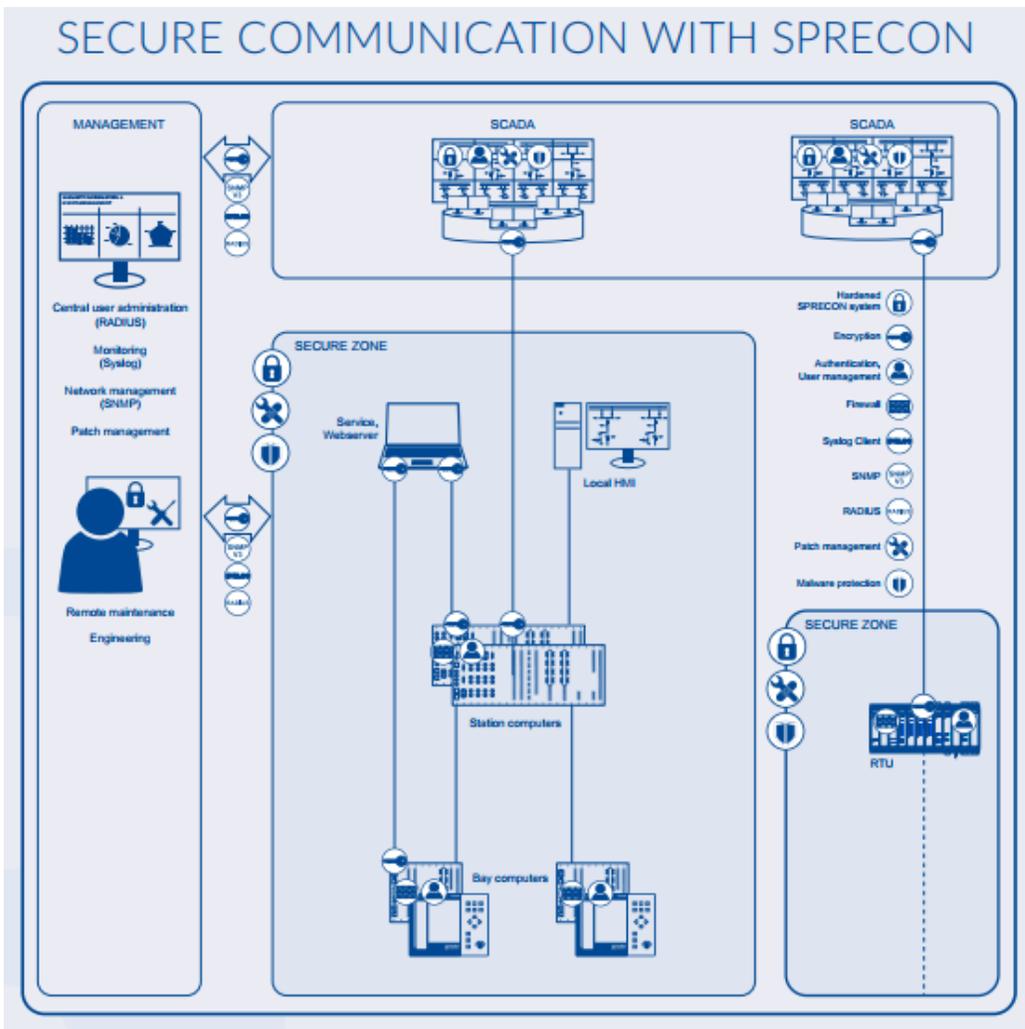
ISO/IEC 27000 series (i. e. ISMS), IEC 62351 and IEC 62443

SPRECON devices support VPN tunnelling for all IPbased services and protocols.

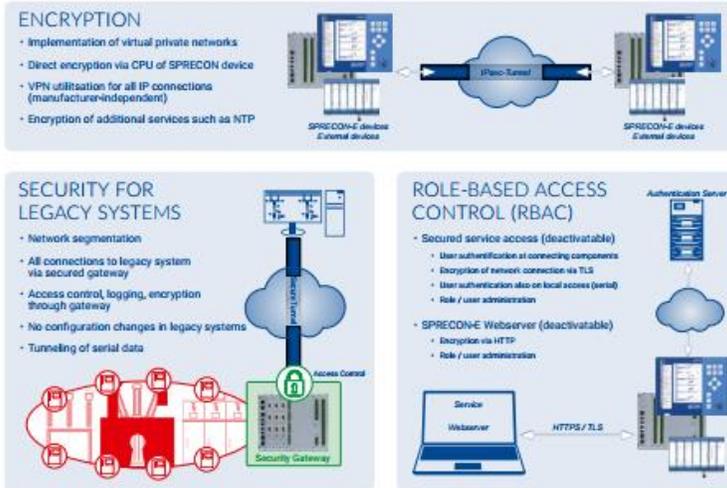
VPN connections – as usual for various projects – can be used for telecontrol or for communication with SCADA systems and may also be applied to secure communication between SPRECON devices.

Full hardening is achieved through encryption of network services such as NTP.

Cyber Security подход Sprecher Automation



IT SECURITY WITH SPRECON

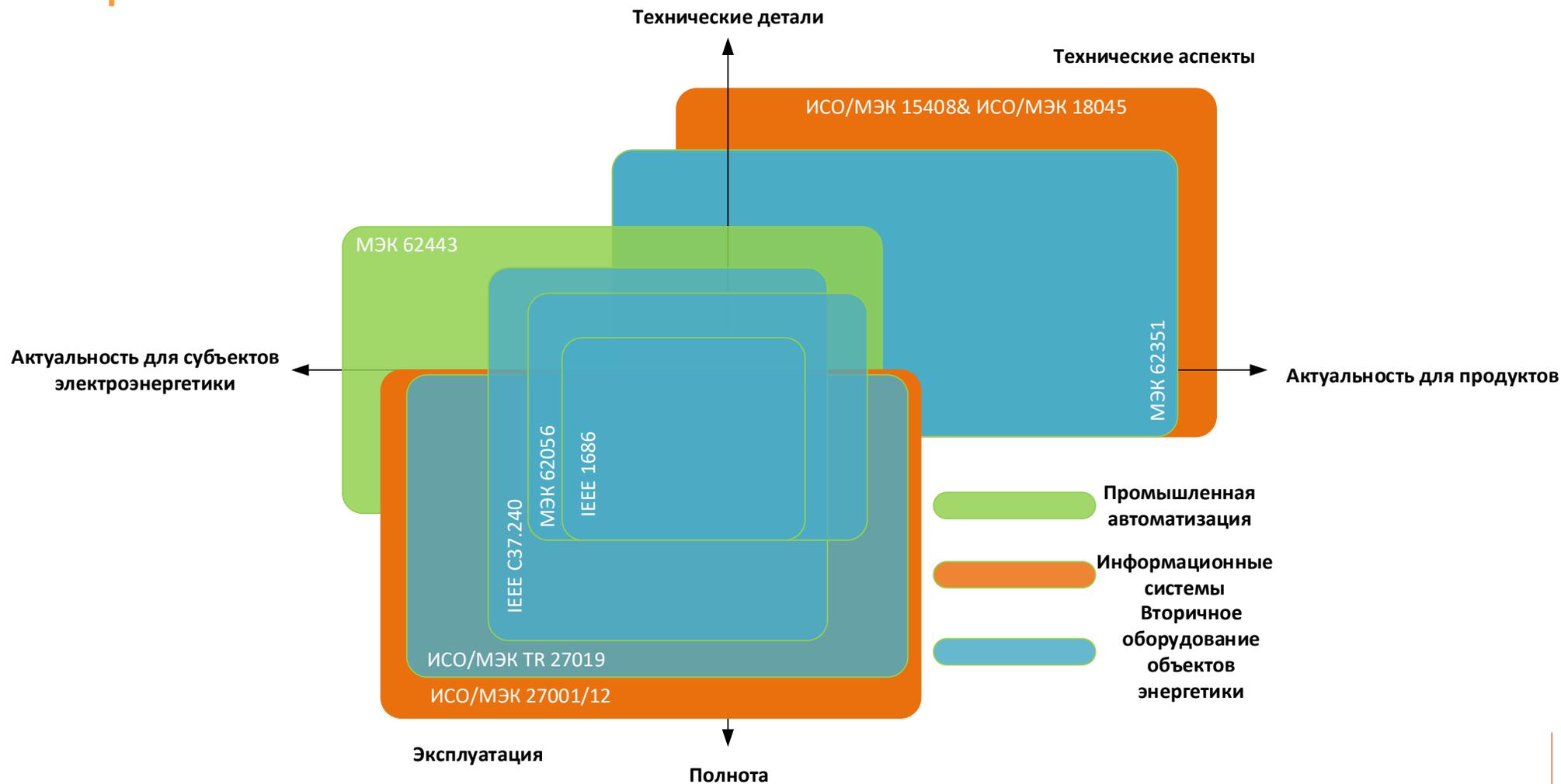


Глобальные тренды кибербезопасности АСУ

ТП

- Следование лучшим практикам или заявление производителей АСУ/АСУ ТП/РЗА о соответствии нормативно-техническим и нормативно-правовым требованиям.
 - NERC CIP и FERC Order No. 693
 - IEC 62351 Security Standards for the Power System Information Infrastructure
 - IEEE 1686-2013 IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities
 - ISO 27001 is a specification for an information security management system (ISMS)
 - IEC 62443 Industrial communication networks - Network and system security. Security for industrial automation and control systems
 - IEC 62541 OPC Unified Architecture standard series
- Разработка и предложение на рынке систем автоматизации, построенных по принципу Secure by Design, **Built-in Security**, Security for safety.
- Со стороны глобальных вендоров систем автоматизации сформировано комплексное предложение для западного и североамериканского рынков по обеспечению кибербезопасности объектов и систем заказчиков: продукты, сервисы.
- Повышение экспертного интереса к SecaaS, Cloud iSOC.

Нормативно техническое регулирование Кибербезопасности АСУ ТП



Вопросы развития

Необходимо

- гармонизировать отраслевые локально-нормативные акты субъектов электроэнергетики с действующими требованиями нормативно-правовых актов
- активнее формировать отраслевые нормативно-технические требования
- рассмотреть задачи по гармонизации в РФ международных стандартов МЭК:
 - МЭК 62351 Управление энергетическими системами и связанный с этим обмен информацией. Безопасность данных и коммуникаций
 - IEC 62443 Network and system security for industrial-process measurement and control
 - IEC 62056 Electricity metering – Data exchange for meter reading, tariff and load control
 - IEC 62541 Унифицированная архитектура OPC



Вопросы кибербезопасности в меняющейся электроэнергетической отрасли.

Владимир Карантаев

к. т. н. MBA

эксперт IEC, IEEE, CIGRE

+ 7 915 221 15 96