Данилин А. В., Генеральный директор ООО "АльтероПауэр", член СИГРЭ

Отчет о работе ИК D2 на 45-ой сессии СИГРЭ, Париж

ИК D2 «Информационные системы и телекоммуникации» на данный момент работает над следующими вопросами:

- Новые приложения для управления энергосистемой
- Приложения интеллектуальных адаптивных сетей для системных операторов и операторов сетей
- Большие данные – приложения и решения
- Объединение функций SCADA, EMS, DMS и рыночных приложений
- Ответственность предприятий электроэнергетики за решение вопросов информационной безопасности
- Цифровые РЗА – вопросы безопасности
- Влияние вопросов информационной безопасности на автоматизацию
- Информационная безопасность в инфраструктуре автоматизации энергосистемы
- Мобильные приложения, системы и инфраструктура
- Беспроводные технологии передачи данных – состав оборудования, приложения, платформы
- Применение общедоступных инфраструктурных решений и частных (закрытых) – за и против

В рамках заседаний членов комитета на 45-ой сессии обсуждались вопросы:

- Подготовка отчета о деятельности комитета
- Роспуск WGD2.32
- Подготовка к выпуску «Зеленой книги» по вопросам информационной безопасности
- Задачи WGD2.39 и назначение нового руководителя, формирование состава членов
- Обсуждение опросника по инициативе WGD2.36 – дискуссия
- Формирование состава WGD2.37
- Обсуждение документа, представленного г-ном Каром «Архитектура SCADA/EMS и интеллектуальные сети»
- Обсуждение программы коллоквиума D2 в 2015 году
- Обсуждение программы следующей сессии в 2016 году

- Актуализация состава всех рабочих групп

Было отмечено:

- Опубликован документ ТВ 588, WGD2.32 «Operations & Maintenance of Telecom Network and Associated Information System in the Electrical Power Utility»
- Опубликован документ ТВ XXX, JWGD2/B5.46 “Application and Management of Cybersecurity Measures for Protection and Control Systems”
- Активное участие членов D2 в разработке концепции «Сети будущего»
- Работа челнов D2 по направлениям обеспечения катастрофоустойчивости ИТ в электроэнергетике, повышению производительности ИТ, обеспечению безопасности ИТ, расширению функциональности и поддержке интеллектуальных сетей, распределенной и возобновляемой генерации

Основная задача D2 на текущий момент – подготовка к публикации «Зеленой книги» по информационной безопасности.

Большое внимание члены D2 уделяют проработке публикаций по развитию SCADA/EMS систем и их интеграции с технологиями SMART GRID.

Были представлены и обсуждены следующие отчеты:

- IEC TC57 “Power System Management and Associated Information Exchange”
- IEEE Power Engineering Society “Power System Communication Committee” (PSCC)
- IETF “Internet Engineering Task Force”
- W3C “World Wide Web Consortium”
- IEEE Power Engineering Society “Substation and PSRC”

Были заслушаны отчеты представителей национальных ИК D2, обсуждены отчеты рабочих групп.

Был поднят вопрос стратегического развития ИТ инфраструктуры для предприятий электроэнергетики – переход на облачные технологии.

Обсуждался план будущих работ и публикаций. Рассмотрен план регулярной встречи и коллоквиума D2 в 2015 году.

Были представлены следующие доклады.

D2-101 «Исследование и применение методов ситуационного анализа кибербезопасности в интеллектуальных сетях»

GAO Kunlun1, WANG Yufei1, XU Ruzhi2
China Electric Power Research Institute
North China Electric Power University

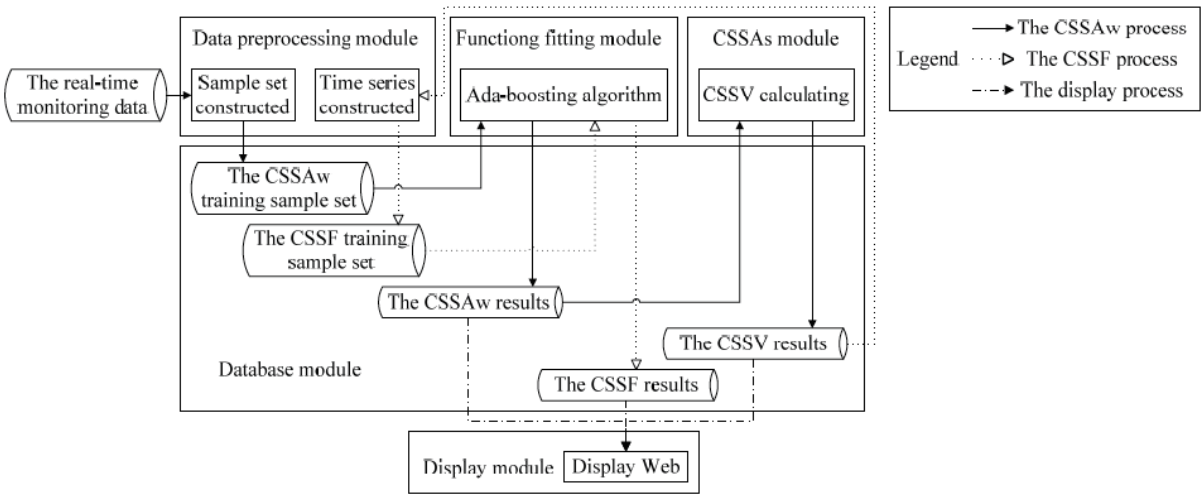
Представлена технология оценки состояния информационной безопасности, наблюдения за ее параметрами и прогнозирования развития опасных ситуаций.

Технология построена на базе алгоритма AdaBoost (алгоритм усиления классификаторов путем объединения их в коммитет). Основной метод – анализ сетевого трафика на предмет идентифиакции различных видов кибератак.

Выделено несколько функциональных подсистем:

- Cybersecurity situation evaluation (CSSE) – оценка (определение) атак.
- Cybersecurity situation awareness (CSSAw) – наблюдение (мониторинг) за трафиком в отельном участке или сегменте сети.
- Cybersecurity situation assessment (CSSAs) – интеграция результатов мониторинга сегментов сети в общую картину безопасности.
- Cybersecurity situation forecast (CSSF) – прогноз развития событий и атак в сети.

Представлены алгоритмы работы CSSE, краткое описание систем визуализации.



Интегрированный фреймворк CSSE модели (cybersecurity situation evaluation)


国家电网 STATE GRID
ISS 信息外网安全监测系统
首页 边界攻击 出口监测 桌面终端 深度分析 统计分析 系统管理 大屏指标 转入网省
出口利用率
利用率15%
今日风险
安全威胁数量：5352
终端告警数量：20177
敏感信息事件：28
病毒木马事件：0
网站攻击事件：130
网络攻击路线图
总部流量
总部流量24 M
监测出口数
100.0%
监测出口数 89
终端用户在线数
100.0%
在线用户数 43286
攻击事件类型
数量(个)
1931261
1655487
1379714
1103941
828168
552395
276622
849
其他 连接状态 连接跟踪 状态跟踪 主动连接 拒绝连接 othe r 欺骗攻击 连接服务 类型
出口应用协议
流量(G)
3442620
2952298
2461981
1971664
1481347
991030
500713
10396
网页 即时通讯 视频 邮件 类别


国家电网 STATE GRID
ISS 信息外网安全监测系统
首页 边界攻击 出口监测 桌面终端 深度分析 统计分析 系统管理 大屏指标 转入网省
边界攻击
实时监测
当日级别最高的五种威胁
序号 威胁名称 威胁类别 级别 数量
1 Web服务... 网络攻击... 5 12
2 HTTP协议... 网络攻击... 5 2
3 网络蠕虫... 网络攻击... 5 1
4 HTTP协议... 网络攻击... 5 1
5 Microsoft ... 网络攻击... 5 1
当日数量最多五种威胁
序号 威胁名称 威胁类别 级别 数量
1 ICMP PIN... 网络攻击... 1 4203473
2 NAT 连接 1 596751
3 SESSION 连接 1 406332
4 AUDIT(1) E... 其他 3 125194
5 NSFocus N... 其他 1 75047
威胁级别分布图（%）
严重威胁0.0%
高度威胁0.1%
中度威胁2.7%
低度威胁0.6%
微度威胁96.7%
日威胁曲线图
数量
3157...
2526...
1894...
1263...
63150
0
15 16 17 18 19 20 21 22 23 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 时间
严重 高 中 低 微

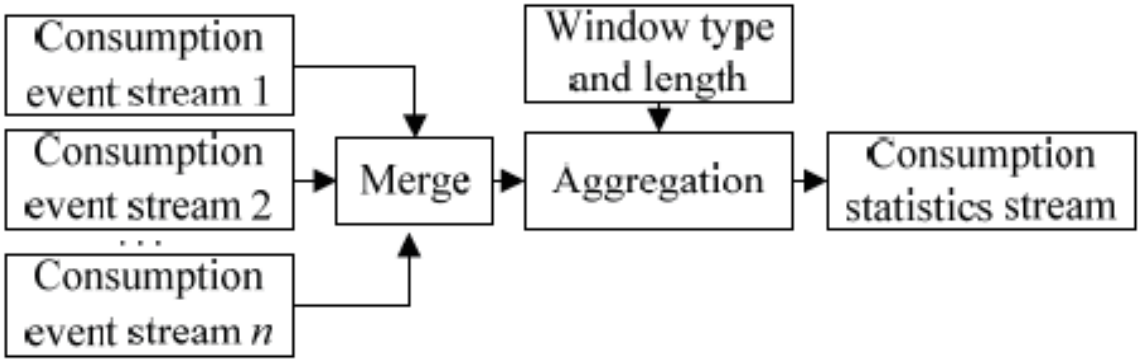
D2-102 «Изучение механизмов точно-в-нужный-момент-времени в системах комплексной обработки событий»

Ji Ye Wang*, Ning Li*, Ying Xin Xie*, Xiao Zhen Li, Da Peng Wang, Feng Yu Wang
Beijing GuoDianTong Network Technology Co., LTD., Nari Group Corporation
China

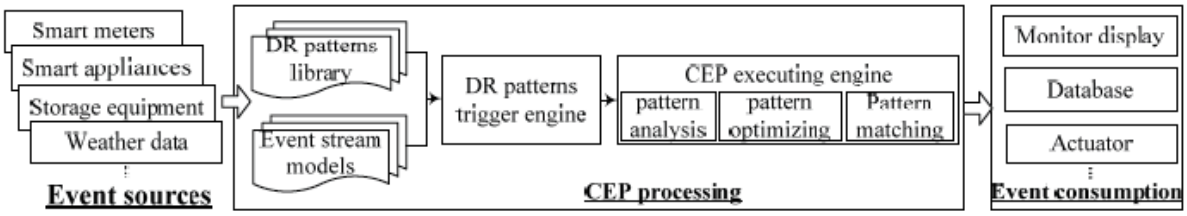
Технология комплексной обработки событий (Complex Event Processing – CEP) оперирует дискретными сигналами (или необработанными событиями) и комплексными (обработанными) событиями, являющимися результатом логической обработки.

Основные операции, выполняемые над дискретными сигналами, это агрегирование, объединение, фильтрация, чтение, запись, модификация и удаление.

Для выполнения анализа текущей ситуации в энергосистеме применяются шаблоны. Например, шаблон «Статистика потребления электроэнергии и мощности».



Для реализации системы помощи в принятии решений в условиях реальной работы энергосистемы реализован фреймворк на базе CEP.



Используется 4 типа источников данных:

- данные реального времени от устройств измерения параметров электрического режима, мониторинга и управления оборудованием;
- ретроспективные данные различных электроэнергетических информационных систем;
- данные не от электроэнергетических информационных систем (метеорологических, полицейских и др.);
- результаты работы экспертных систем.

Система работает как по циклическому принципу, так и по какому-либо заранее настраиваемому событию, отрабатывая те или иные шаблоны.

В докладе представлены примеры практического применения системы в задачах мониторинга потребления и управления генерацией и потреблением в режиме «по запросу» (On Demand Respond).

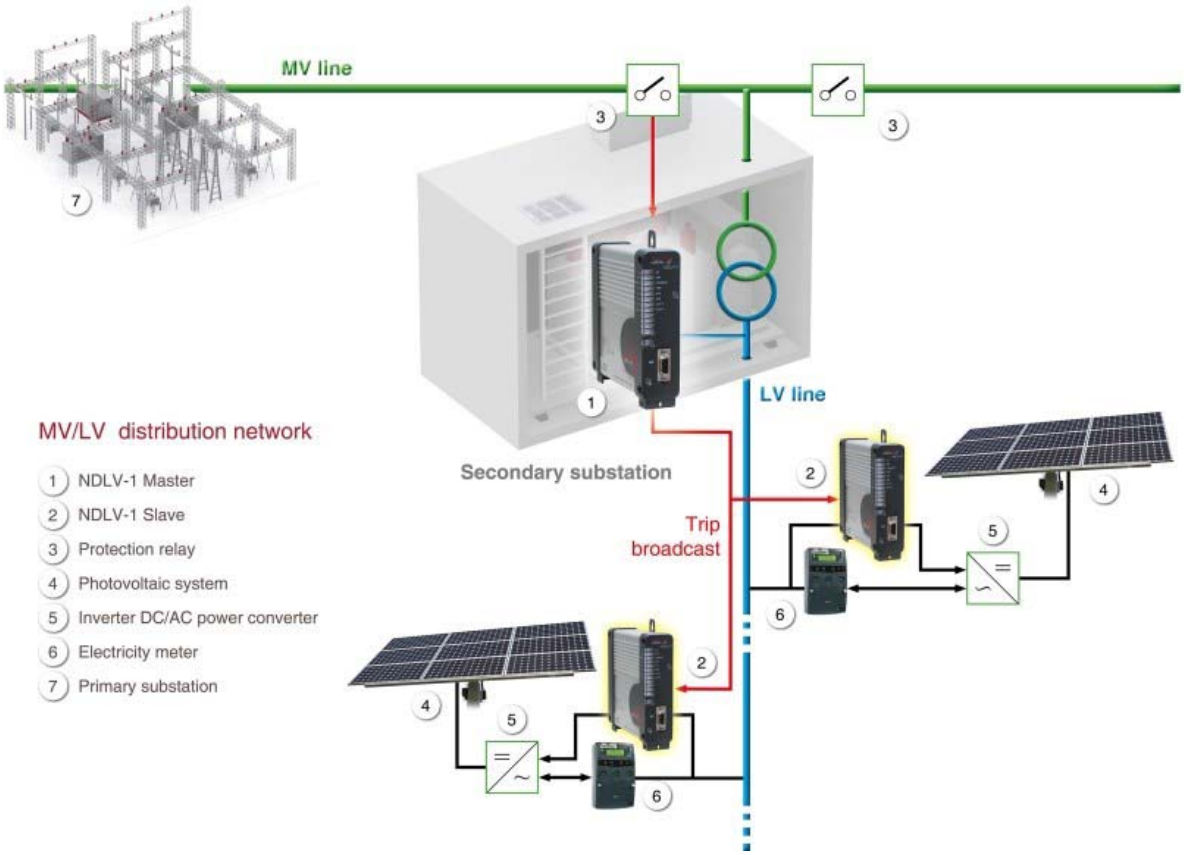
D2-103 «Технологии PLC для интеграции с объектами распределенной генерации»

DAVID GIL (DG), ASIER LLANO (AL), FERNANDO CASTRO (FC), JOSE ANTONIO MORENO (JAM), SONIA MARTÍNEZ (SM), TXETXU ARZUAGA (TA)*
ZIV CG Automation
SPAIN

Доклад посвящен ИТ коммуникациям поверх ЛЭП (Powerline Communications – PLC). Отмечается необходимость в обеспечении постоянной связи с источниками распределенной генерации, которая, как правило, подключена к линиям среднего и низкого классов напряжения. Отмечается важная роль возможности передачи данных и для современных измерительных систем (в том числе, коммерческих).

В современных условиях потребители часто становятся источниками генерации, которые подключены к общим электрическим сетям низкого и среднего напряжений и требуют постоянного мониторинга и управления в реальном времени.

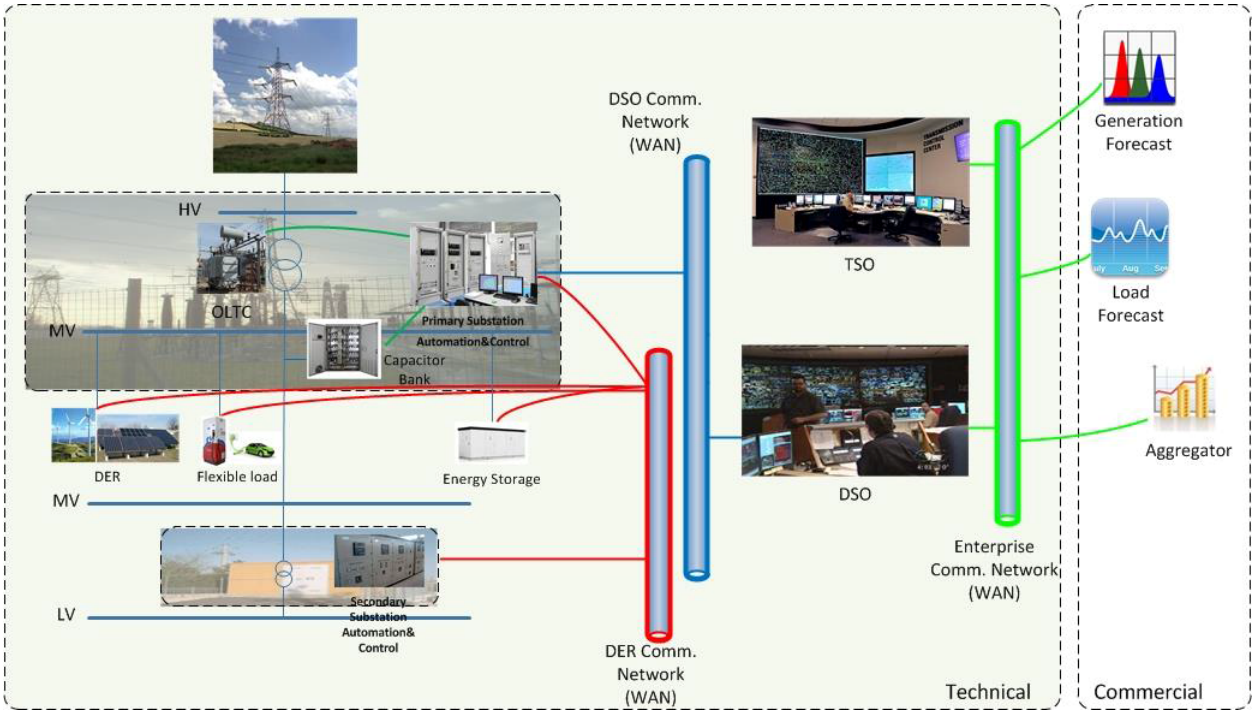
Приводятся основные характеристики ЛЭП низкого класса напряжения как физической среды для телекоммуникаций. Рассматриваются варианты применения ЛЭП как передающей среды для управления средствами релейной защиты, работы контрольно-измерительного оборудования.



D2-104 “Безопасность коммуникаций в задачах контроля напряжений распределенной генерации: анализ воздействия и аномальное поведение”

G. DONDOSSOLA*, R. TERRUGGIA
Ricerca sul Sistema Energetico – RSE spa, Italy

В докладе обсуждаются вопросы архитектуры программно-технических решений для задач контроля уровней напряжений в сетях среднего и низкого напряжения с распределенной генерацией.



Отмечается необходимость информационного обмена между различными субъектами электроэнергетики для реализации задач управления. Учитывая, что субъекты часто принадлежат разным собственникам, отмечается важность управления рисками в области информационной безопасности.

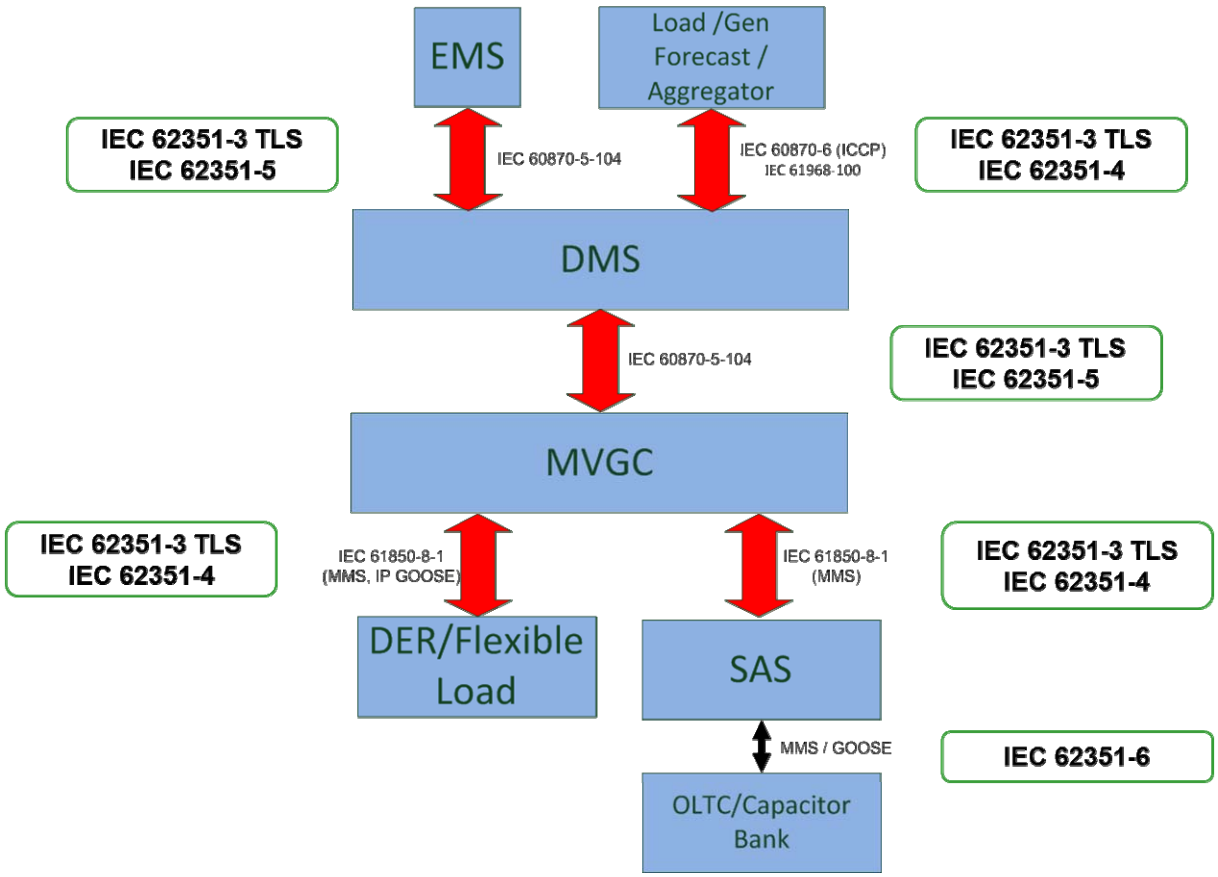
Рассматриваются основные виды атак на технологические сети, их цели и возможные последствия.

Предлагается методика анализа рисков и оценки последствий.

RISK IMPACT LEVELS	Energy supply (Watt)	Energy flow (Watt/hour)	Population	Infrastructures	Data protection	other laws & regulations	HUMAN	REPUTATION	FINANCIAL
HIGHLY CRITICAL	regional grids from 10GW	from 10 GW/h	from 50% population in a country or from 25% in several countries	international critical infrastructures affected	not defined	company closure or collateral disruptions	direct and collateral deaths in several countries	permanent loss of trust affecting all corporation	Thirth party affected
CRITICAL	national grids from 1 GW to 10GW	from 1 GW/h to 10GW/h	from 25% to 50% population size affected	national critical infrastructures affected	not defined	temporary disruption of activities	direct and collateral deaths in a country	permanent loss of trust in a country	>=50% EBITDA
HIGH	city grids from 100MW to 1GW	from 100MW/h to 1GW/h	from 10% to 25% population size affected	essential infrastructures affected	unauthorized disclosure or modification of sensitive data	prison	direct deaths in a country	temporary loss of trust in a country	<50% EBITDA
MEDIUM	neighborhood grids from 10MW to 100MW	from 10MW/h to 100MW/h	from 2% to 10% population size affected	complimentary infrastructures affected	unauthorized disclosure or modification of personal data	fines	seriously injured or discapacity	temporary and local loss or trust	<33% EBITDA
LOW	home or building networks under 10 MW	under 10MW/h	under 2% population size affected in a country	no complimentary infrastructures	no personal nor sensitive data involved	warnings	minor accidents	short time & scope (warnings)	<1% EBITDA
	OPERATIONAL (availability)				LEGAL				

MEASUREMENT CATEGORIES

Приводятся основные стандарты в области информационной безопасности и рекомендации по их применению.



D2-105 “Система мониторинга и управления для оценки эффективности инвертера солнечных источников электроэнергии”

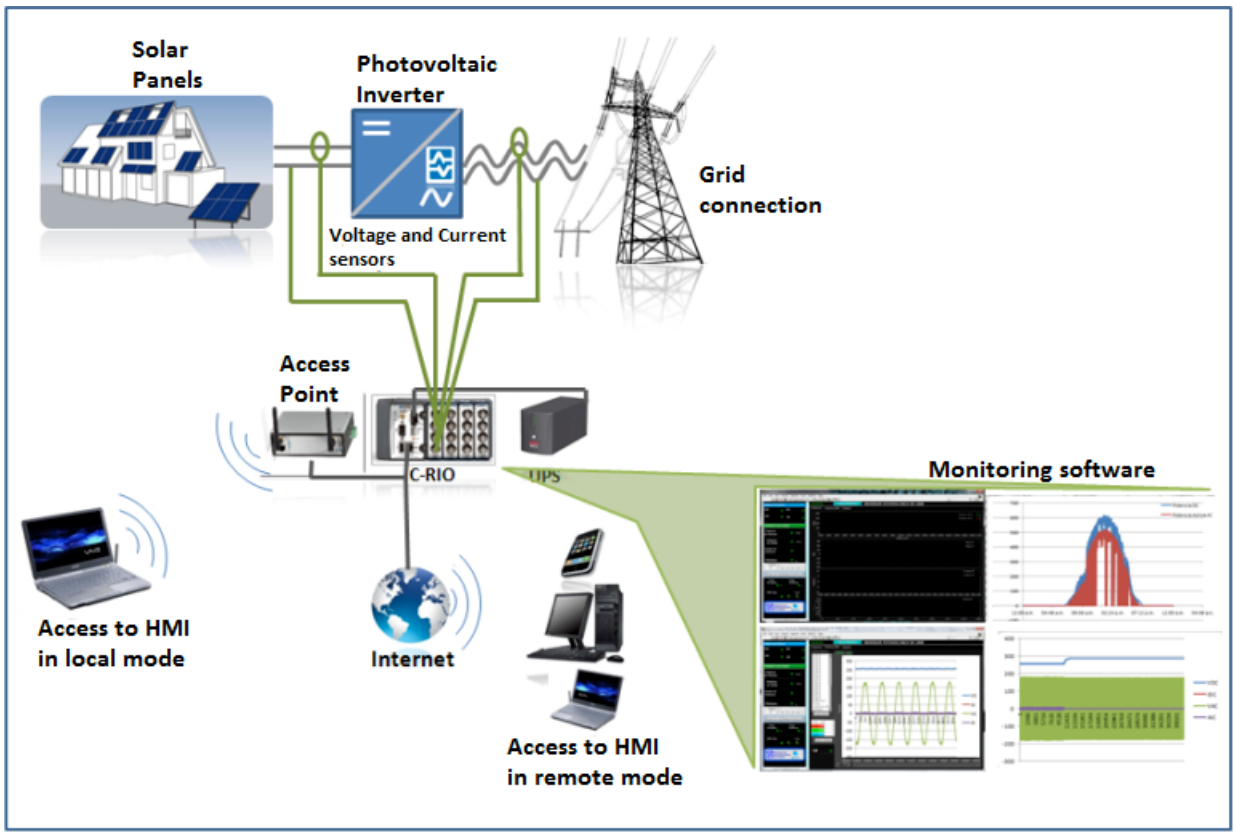
R. GUEVARA*, C. TELLO, J. RODRIGUEZ
Instituto de Investigaciones Eléctricas, Gerencia de Control Electrónica y Comunicaciones
México

В докладе отмечается важная роль инвертора в обеспечении эффективной работы солнечных источников электроэнергии. Соответственно, система управления инвертером оказывает существенное влияние на качество работы всего источника.

Подключенные через инвертер к электрическим сетям солнечные панели требуют точной синхронизации и управления синхронной работой в реальном времени.

В докладе представлены результаты наблюдения за работой инвертеров двух конфигураций, которые позволили существенно повысить эффективность их работы за счет более тонких настроек, которые обеспечивают различные характеристики работы солнечных источников энергии в сети (гармонические составляющие, коэффициент мощности, форма волны тока и напряжения и др.).

Отмечается полезность инструмента в задачах интеграции возобновляемых источников в сети и влияние качественного управления и мониторинга на все аспекты работы солнечной генерации.



D2-106 “Стратегический выбор распределительных электросетевых компаний для организации частных телекоммуникационных сетей”

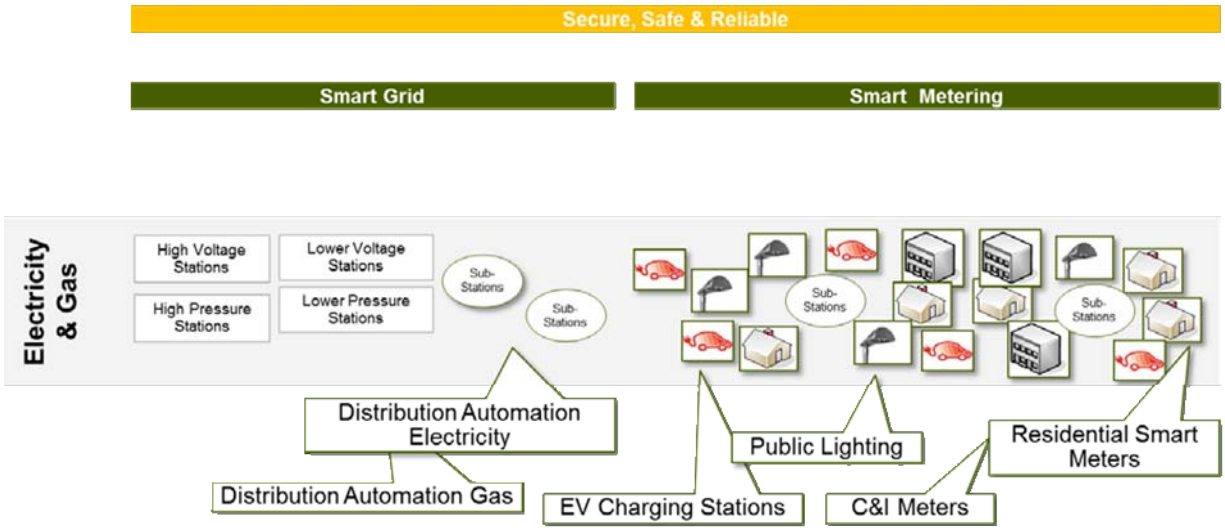
G. ROBICHON, Alliander, Netherlands

В докладе отмечаются серьезные изменения в технической инфраструктуре современной электроэнергетики Европы, которые влекут за собой изменения ИТ-инфраструктуры.

С развитием распределенной генерации, возобновляемых источников электроэнергии, размещением у потребителей интеллектуальных контрольно-измерительных систем зависимость от телекоммуникаций и их безопасности возрастает до критического уровня.

Электросетевая и газоснабжающая распределительная компания Alliander (Нидерланды) осуществляет полномасштабное развертывание SMART GRID и SMART METERING проектов. И телекоммуникации – один из критичных компонентов.

Именно по этой причине Alliander решили создать собственную, третью после электрической и газовой, сеть – телекоммуникационную.



Основные требования к телекоммуникационной сети сформулированы так (в противовес коммерческим сетям):

1. Длительный период эксплуатации. Технологии связи (особенно беспроводной) достаточно динамично сменяют друг друга в последнее время. В таких условиях сложно рассчитывать на длительную эксплуатацию устоявшихся систем связи коммерческими операторами.

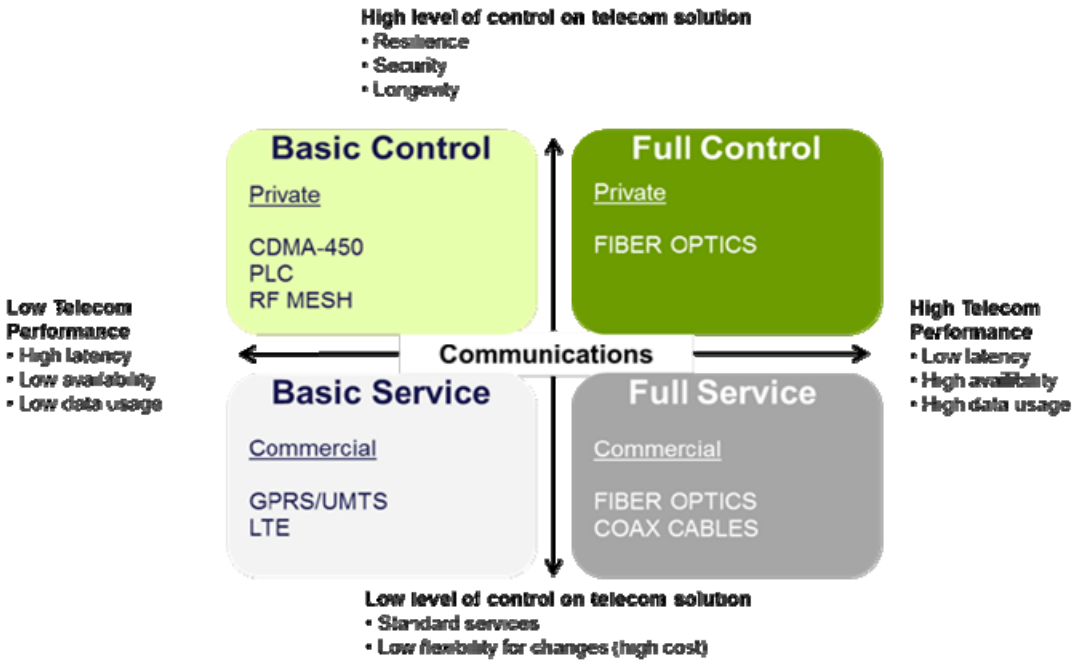
2. Безопасность. Аренда телекоммуникаций у коммерческих операторов не предоставляет необходимых для электро- и газоснабжающих компаний условий информационной безопасности.

3. Большое количество устройств и точек связи. К 2020 году планируется развернуть миллионы интеллектуальных счетчиков на стороне потребителей. Это серьезный вызов коммерческим операторам – смогут ли обеспечить бесперебойную работу таких сетей?

4. Покрытие связью. Локальные сети привязаны к зданиям. Беспроводные ориентируются смартфоны. Электрические подстанции не попадают в эти категории.

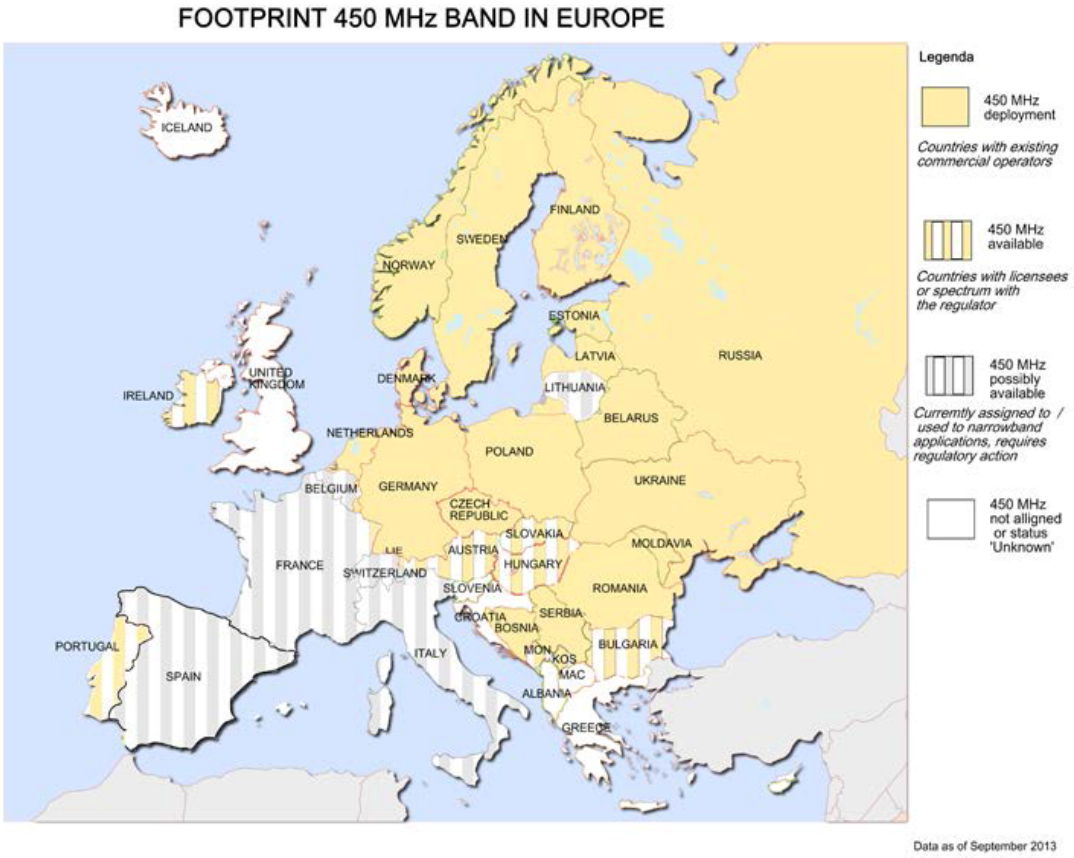
5. Производительность. Коммерческие операторы ориентированы на доставку большого количества данных (мегабайты и даже гигабайты). Это совершенно не является критерием производительности для SMART GRID и SMART METER оборудования.

6. Надежность. Коммерческие сети (их оборудование) часто не обеспечиваются бесперебойными источниками питания и другими средствами обеспечения отказоустойчивости.



С учетом вышесказанного, автор доклада считает наиболее подходящими для создания собственных телекоммуникационных сетей следующий набор технологий:

1. PLC (Power Line Communication) – организация каналов передачи данных по электрическим проводам.
2. RF Mesh сети (радиочастотные).
3. Частные беспроводные сети, построенные на технологиях типа CDMA, работающих в частотном диапазоне 450 МГц.



Автор считает, что наиболее подходящим является третий вариант. В качестве аргумента приводится удачный компромисс между покрытием и ограничениями по пропускной способности этой технологии в Европе.

D2-107 «Будущее интеллектуальных систем измерения и управления их данными»

A.I. BATAINEH, NEPCO, Jordan

В докладе освещается опыт Иорданской распределительной компании NEPCO в создании систем сбора информации от измерительных систем (в основном - счетчиков электроэнергии) AMR/AMI.

Кратко рассматриваются применяемые технологии передачи данных, механизмы организации сбора и обработки данных.

Особо отмечается интеграция проекта с GIS, что существенно помогает персоналу компании в эксплуатации системы и ее компонентов. Подчеркивается роль AMI в развитии систем управления отключениями и других EMS/DMS-приложений.

D2-108 «Применение web-сервисов для обмена данными на европейском рынке электроэнергии»

A. MARTÍN BARBERO E. JIMÉNEZ RAYA J. BEMBIBRE REGUEIRO, RED ELÉCTRICA DE ESPAÑA, S.A.U., SPAIN

В докладе подробно рассматриваются формат сообщений и протоколы информационного взаимодействия между участниками европейского рынка электроэнергии.

Обмен сообщениями организован на базе стандарта МЭК 62325-451-n, который определяет формат сообщений (в виде XSD-схем). Стандарт МЭК 61968-100 определяет структуру сообщения, необходимого для взаимодействия посредством web-сервисов.

До недавнего времени применялись технологии обмена сообщениями в форматах, определенных ENTSO-E, посредством различных транспортных технологий (электронная почта, FTP и др.).

На текущий момент осуществляется переход на обмен сообщениями, сформированными в соответствие с требованиями стандарта МЭК 61968-100, используя в качестве транспортного механизма реализацию требований стандарта МЭУ 62325-451-n. Такой подход существенно снижает затраты времени и финансов на реализацию взаимодействия.

В докладе приводятся технические детали реализации обмена в части описания структуры сообщений, процедур взаимодействия клиент-серверных компонентов между собой.

D2-109 «Опыт использования ВОЛС-ВЛ в Red Electra de Espana»

S. KWIK ALLAN*, J.M. DELGADO ÁLVAREZ, Red Eléctrica de España (REE) - Telecommunications Department, Spain

В докладе освещается опыт специалистов REE в развертывании телекоммуникационных оптоволоконных сетей по воздушным ЛЭП.

Рассматриваются конструктивные особенности кабеля для построения ВОЛС-ВЛ, описываются специфические условия работы кабельной системы на опорах и проводах (или грозотросах) ЛЭП.

Приводятся примеры исследовательских и экспериментальных проектов с описанием технических деталей создания кабельной системы.

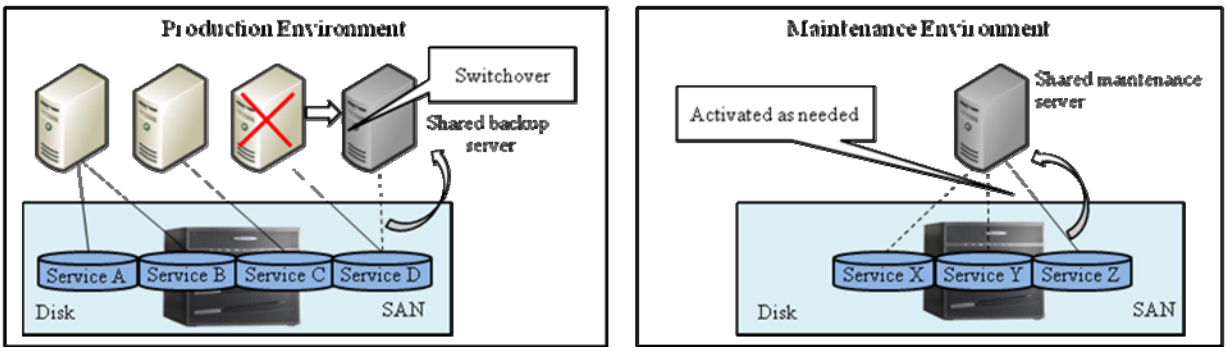
D2-201 «ИТ-платформы японских электроэнергетических компаний»

T. YOSHIDA M. KIKEGAWA Kyushu Electric Power Co., Inc. Tohoku Electric Power Co., Inc., R. HOSHIKAWA M. Okamoto Shikoku Electric Power Co., Inc. Electric Power Development Co., Ltd., N. TAMEHISA T. HANAKITA Cisco Systems GK Fujitsu Ltd., Japan

Японские электроэнергетические компании столкнулись с необходимостью снижения затрат на ИТ одновременно с необходимостью обеспечить катастрофоустойчивость, что стало особенно актуально после последнего крупного землетрясения.

Основной упор в достижении поставленных целей был сделан на технологиях виртуализации и облачных вычислений.

Активно применяется технология SAN Boot.



Создаются дополнительные центры обеспечения связи и телекоммуникаций.

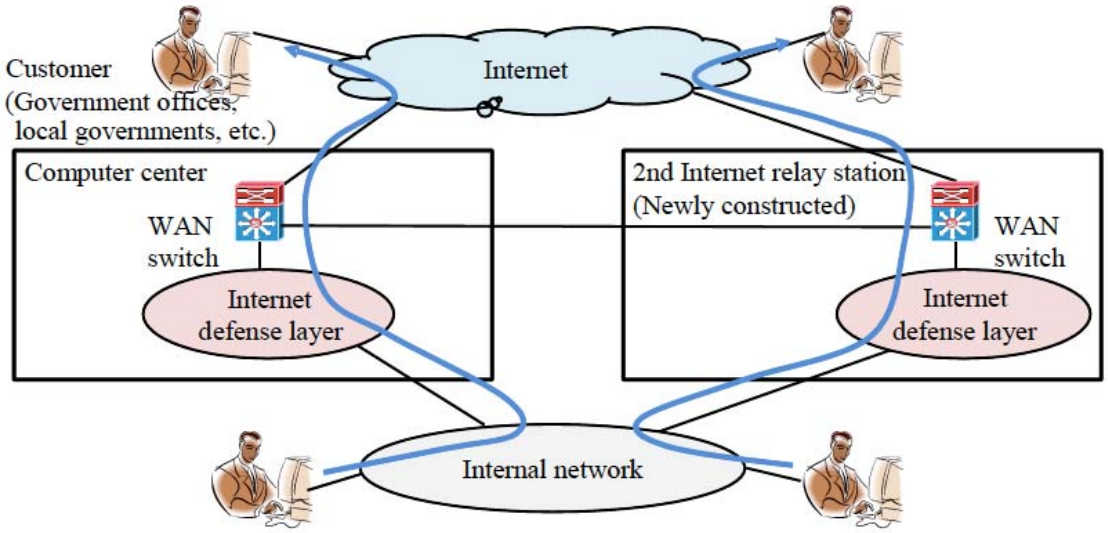
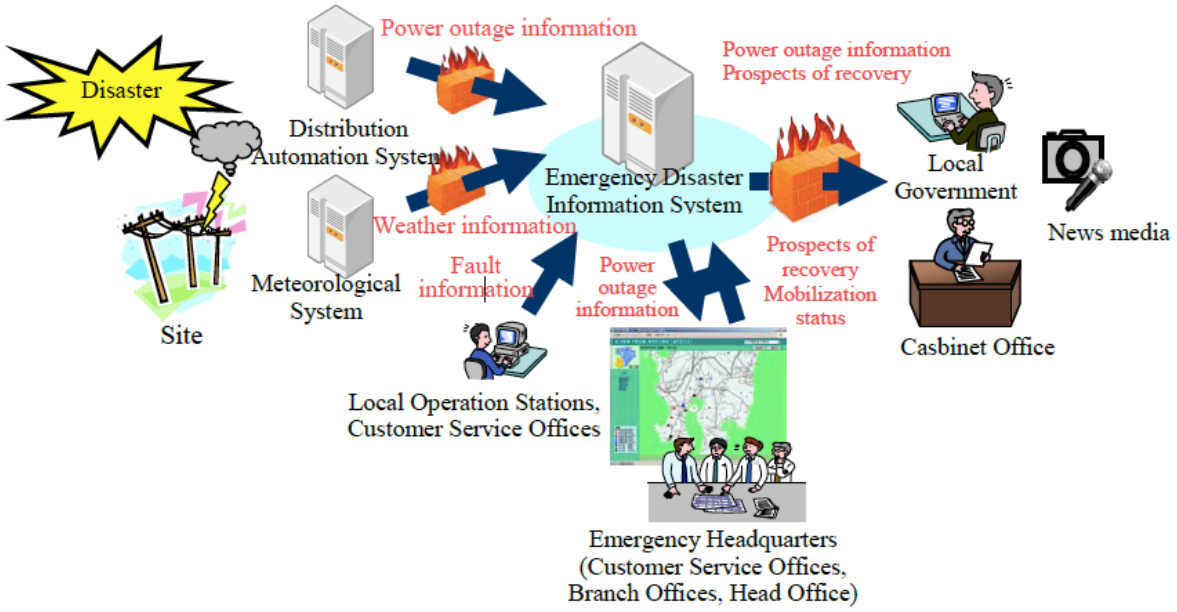


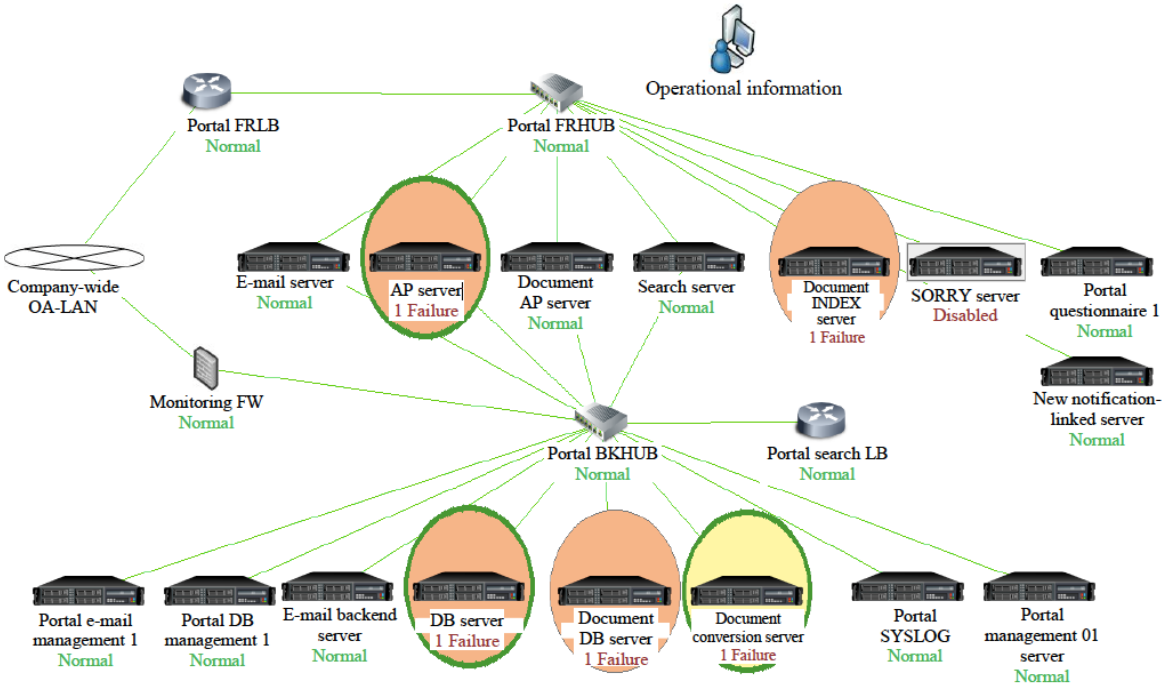
Fig. 2.2-1 Overview of the 2nd Internet Relay Station Configuration

В ЦОДах предполагается устанавливать сейсмоустойчивые полы (компенсирующие вертикальные перемещения).

Для своевременного оповещения, координации действий и информирования создается информационный центр об авариях и бедствиях.



Создаются мощные системы мониторинга за работой оборудования и программными сервисами.



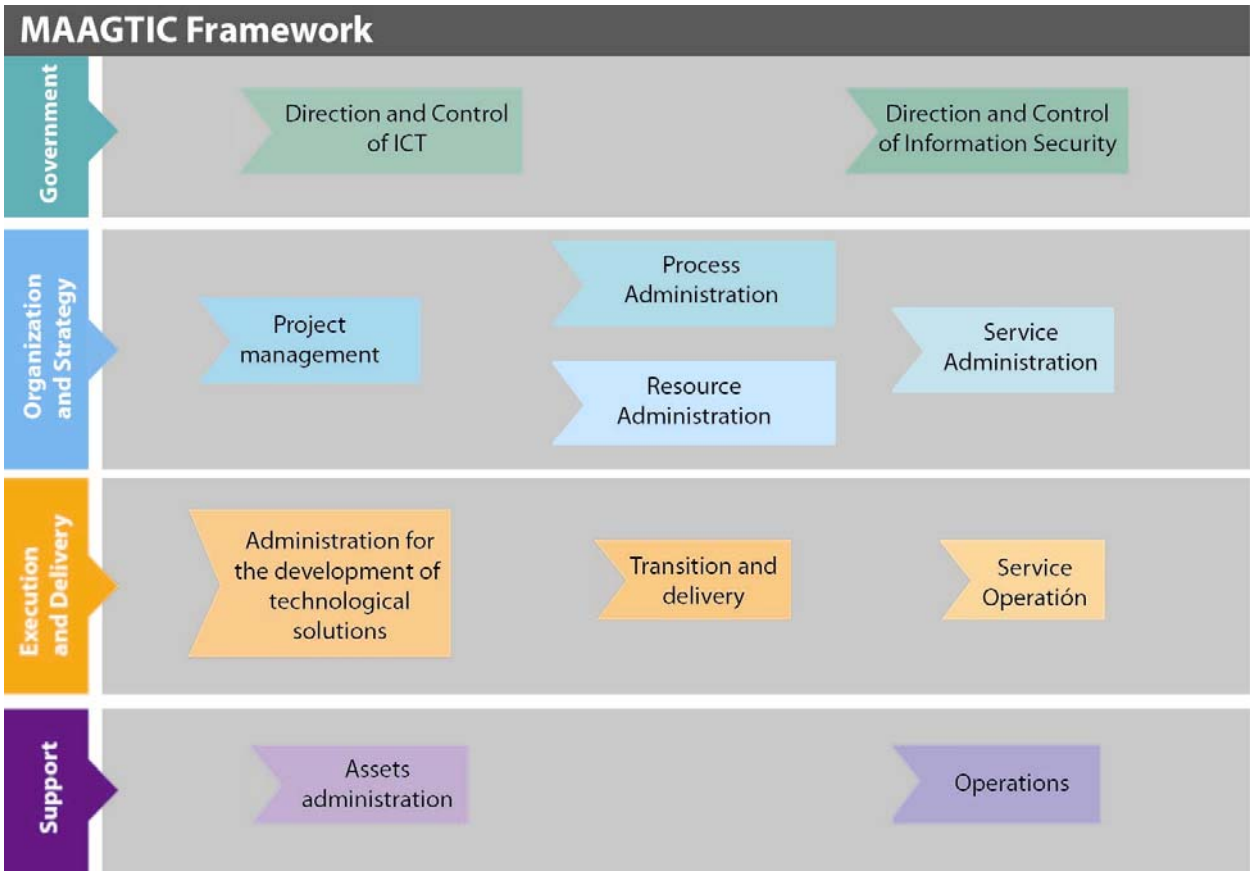
D2-202 «Опыт и практика внедрения управления ИТ в мексиканских электросетевых компаниях»

I. PARRA, G. ARROYO*, A. GARCIA, Instituto de Investigaciones Eléctricas, Comisión Federal de Electricidad, MEXICO

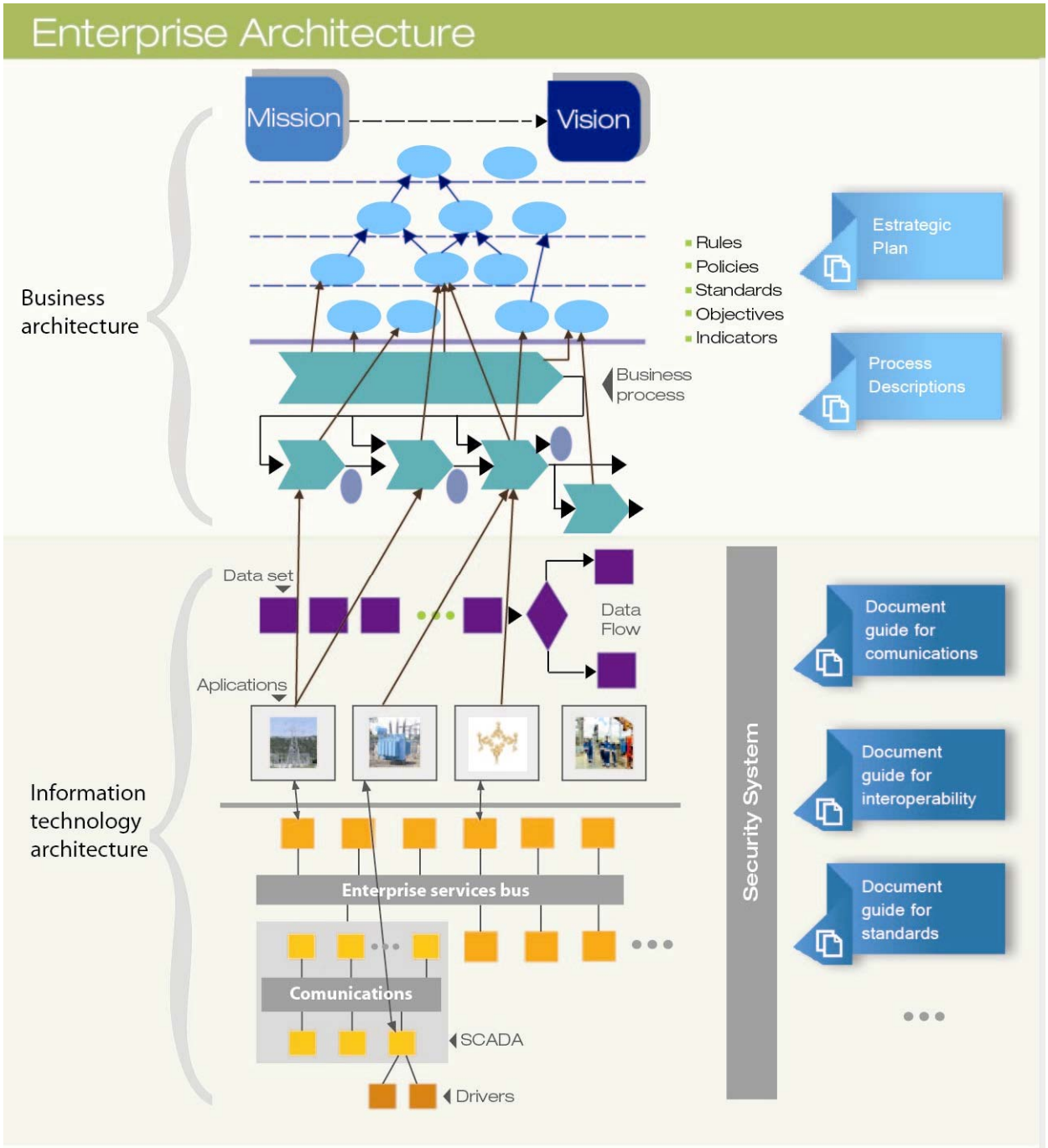
Учитывая нарастающую сложность ИТ-инфраструктуры в связи с развитием технологий SMART GRID, Comision Federal de Electricidad (CFE) приняло решение разработать адаптированный фреймворк на базе ITIL и COBIT, IEC 62351 (безопаснсть), ISO 9001 для управления качеством и PMI для проектного

управления.

Результатом стал MAAGTIC-SI ((In Spanish, Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información) – набор стандартных правил и рекомендаций по внедрению и сопровождению ИТ инфраструктурных и технологических решений.

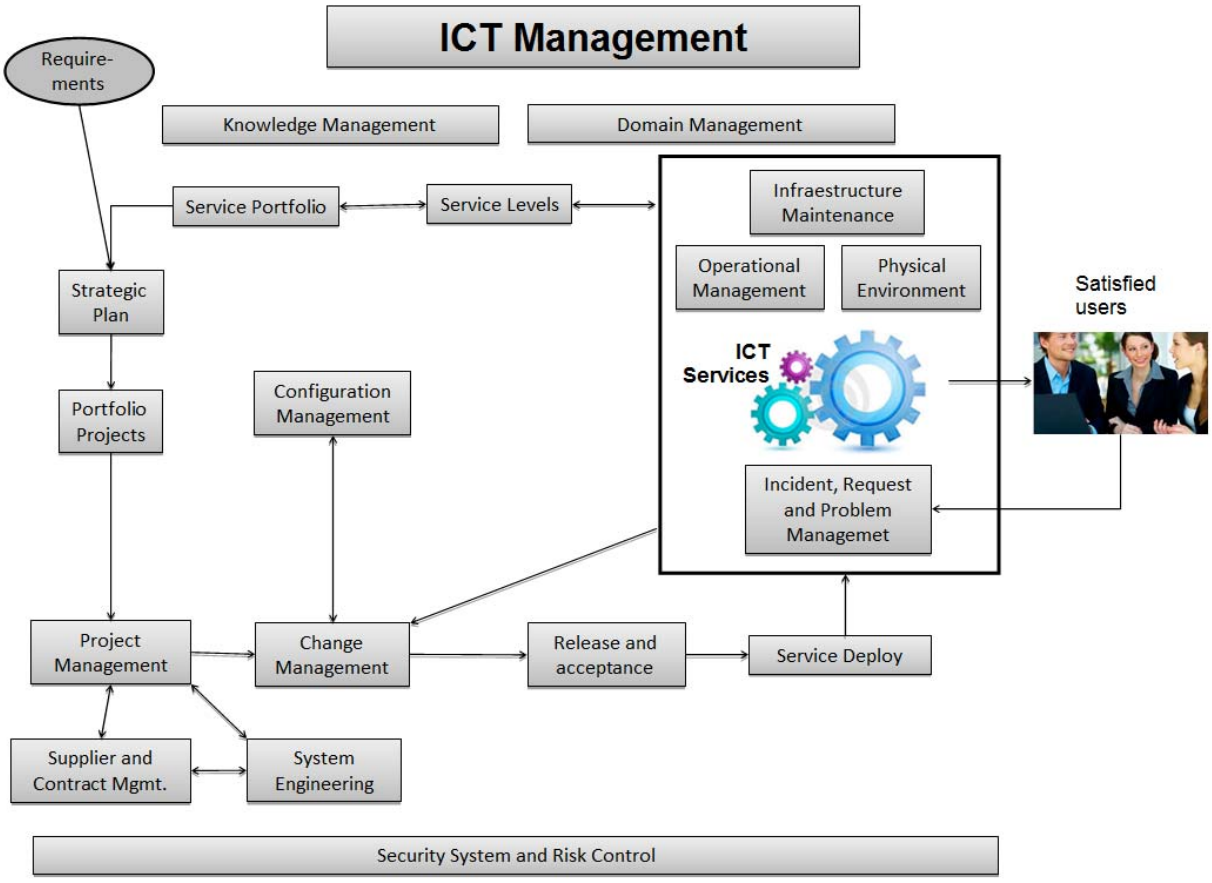


Фреймворк MAAGTIC-SI включает рекомендации по архитектурно-техническим решениям на базе методологии TOGAF. Бизнес-архитектура связывает информационные потоки и процессы.

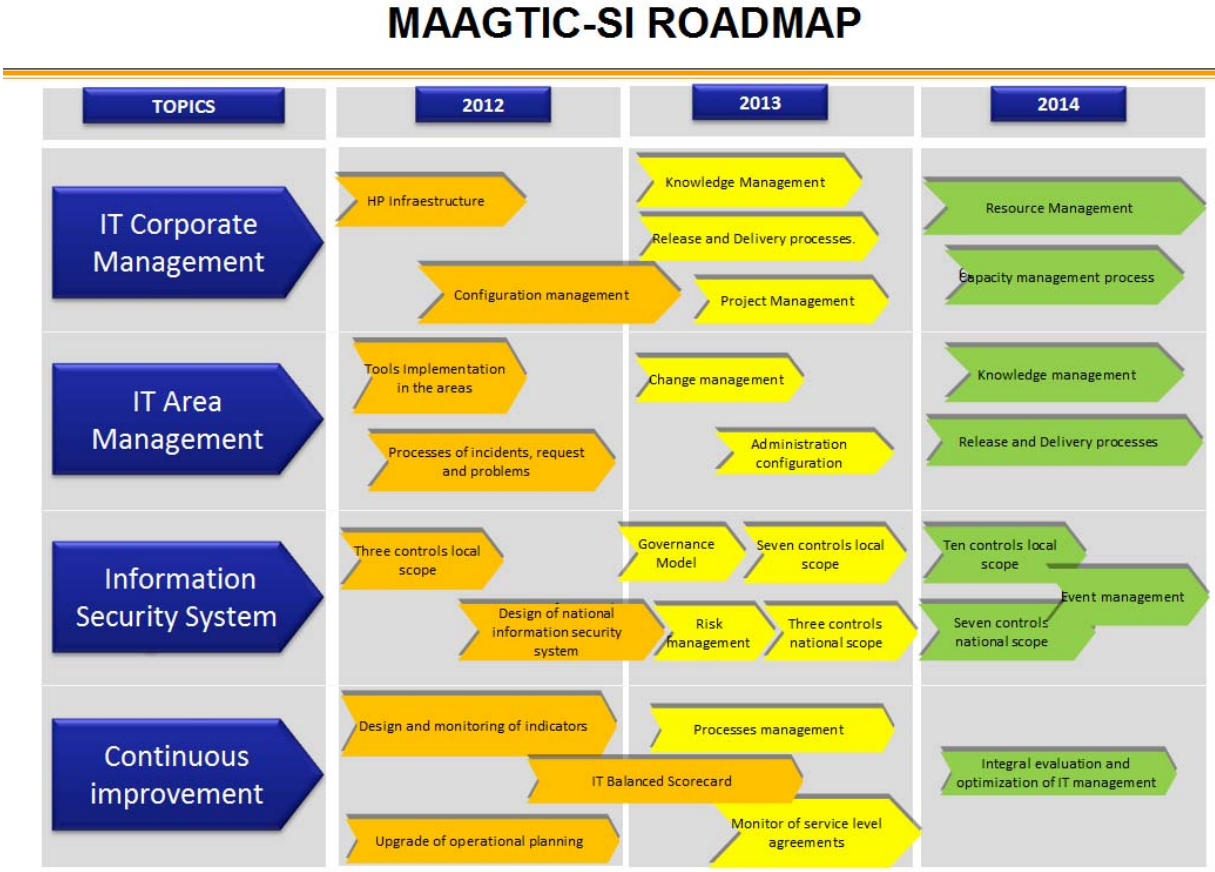


ИТ-инфраструктура CFE состоит из более чем 5000 серверов и порядка 70 000 персональных компьютеров. Осуществляется поддержка более чем 400 информационных технологических и управленческих систем.

В MAAGTIC-SI выделено 29 процессов.



Дорожная карта внедрения всех 29 процессов представлена на схеме:



D2-203 «Безопасность при использовании удаленного доступа в электроэнергетических компаниях»

P. Sitbon*, C. Poirier, J. Zerbst, D.K. Holstein, M. Scherer, R. Evans, Marc Tritschler, Electricité de France, Electricité de France, Vattenfall, OPUS Consulting, Alstom, Snowy Hydro Ltd, PA Consulting, France, France, Sweden, USA, France, Australia, UK

В докладе рассматривается проблематика организации удаленного двустороннего доступа к ИТ-ресурсам электроэнергетических компаний со стороны внешних организаций.

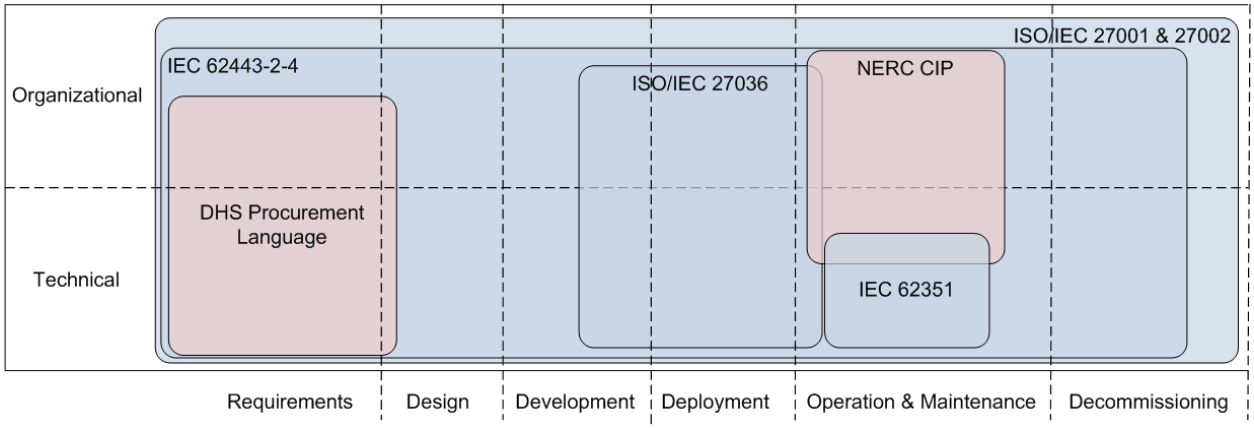
Отмечается производственная необходимость обеспечивать удаленный доступ к ИТ-ресурсам энергокомпаний как сотрудников смежных по производственному процессу организаций (потребителей, диспетчерских центров), так и сопровождающих различное технологическое программное обеспечение.

Отмечаются основные проблемы сопровождения удаленного доступа:

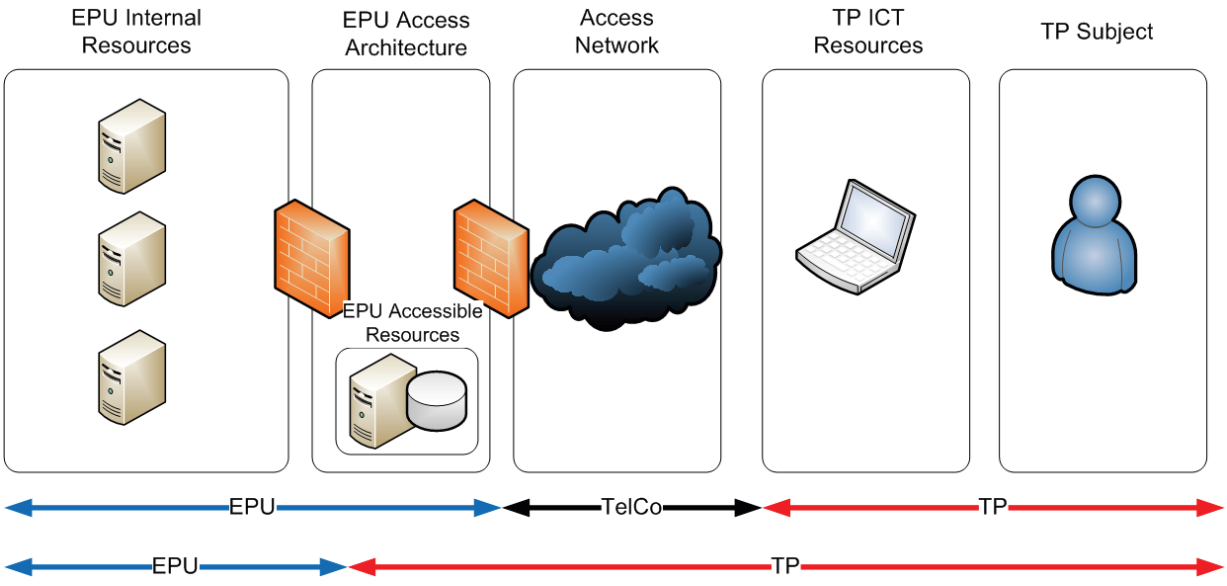
- Постоянное подключение к Интернету или подключение систем разного уровня безопаснсти (например, офисных внутренних сегментов к приложениям и данным Google Docs и т.п.).
- Слабые и легко подбираемые пароли.
- Уязвимости в интерфейсах авторизации и идентификации.

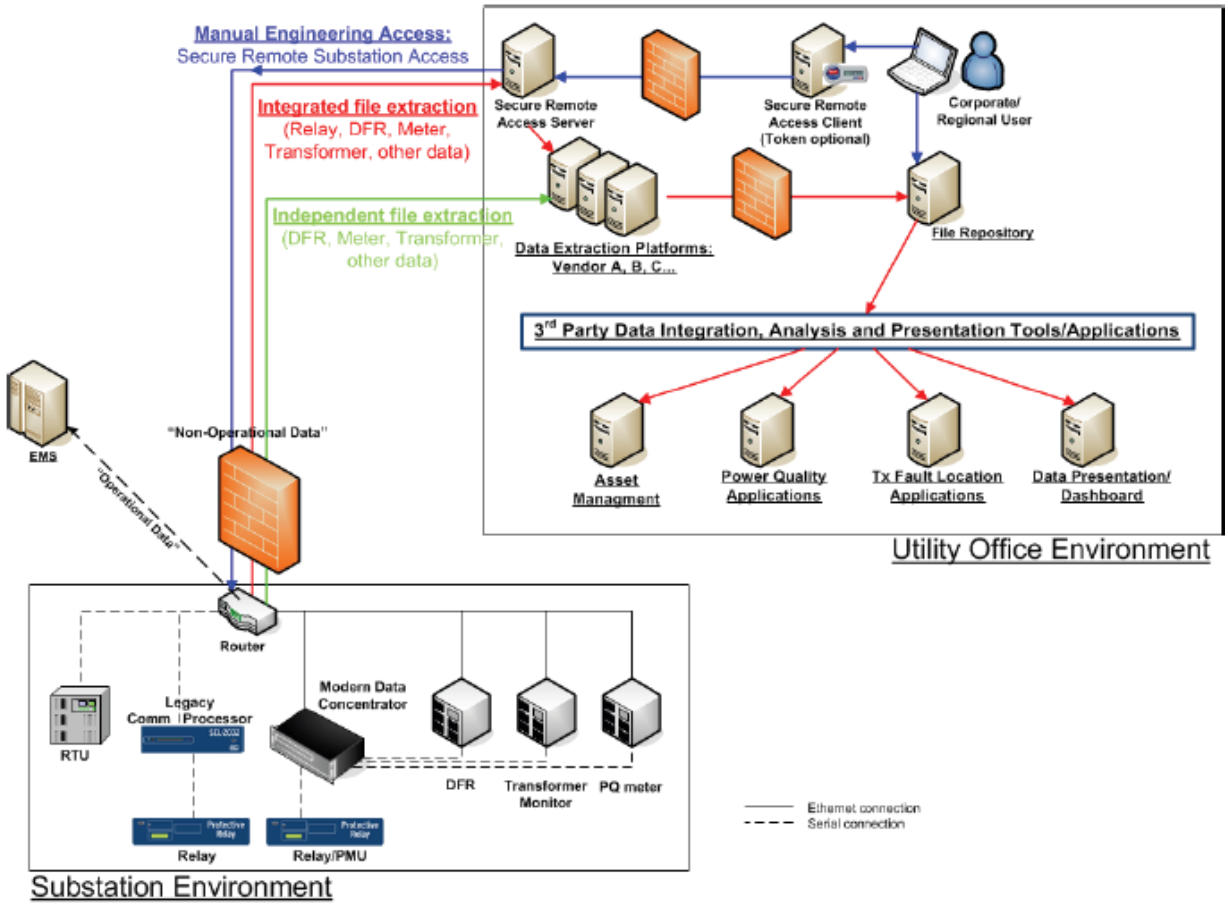
- Не выполнение обновлений операционных систем.
- Отсутствие протоколирование действий пользователей и систем.
- Персонал, осуществляющий удаленный доступ, не обучен и не проинструктирован правилам безопасности.
- Слаборазвитые системы определения атак и вторжений с автоматической сигнализацией.

Приводится анализ стандартов в области обеспечения безопасности и область их применения.



Предлагается типовое архитектурное решения для организации удаленного доступа.

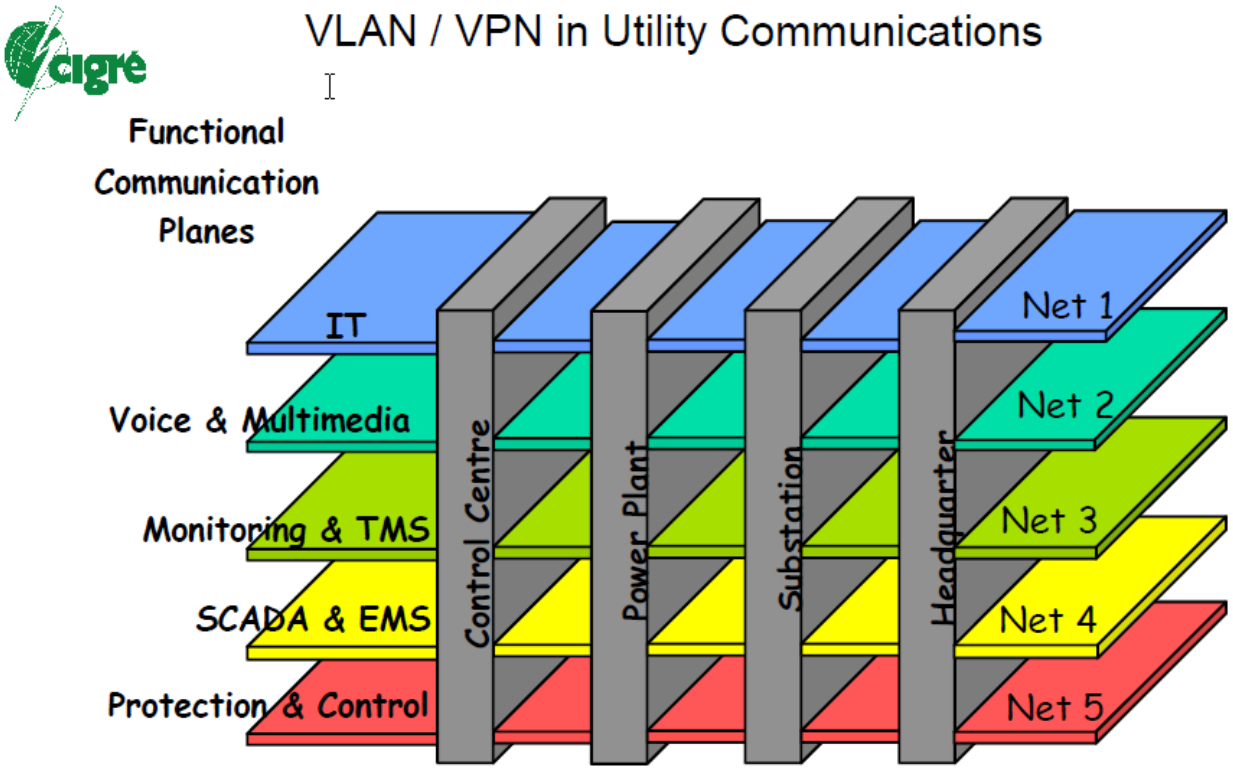




D2-302 «Опыт работы с сетями IP/MPLS»

Thomas Leroy, Elia, Belgium

В докладе идет речь об организации телекоммуникационных сетей на базе парадигмы виртуализации.

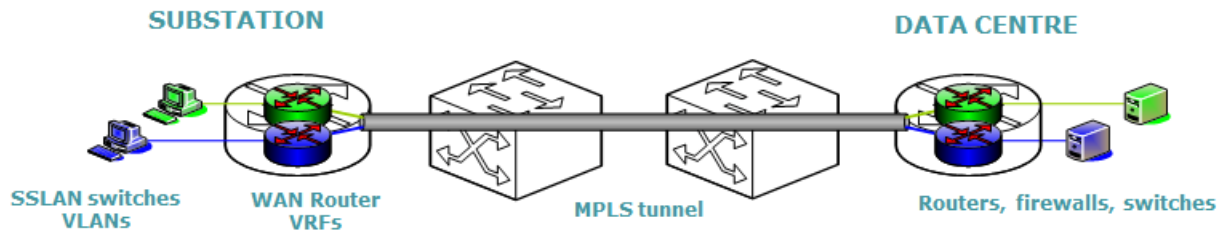


Смещение акцентов в создании сетей от DTM технологии к технологии коммутации пакетов формирует новые требования к сетям:

- Большая пропускная способность (например, на каемры видеонаблюдения не менее 1 Мбит/сек на ону камеру).
- Классификация трафика и управление качеством передачи.
- Интеллектуальное управление трафиком (Traffic Engineering).
- Поддержка VPN.
- Улучшенный сервис поддержки и обслуживания.

Наиболее соответствует этим требованиям технология MPLS и MPLS-TE (Traffic Engineering).

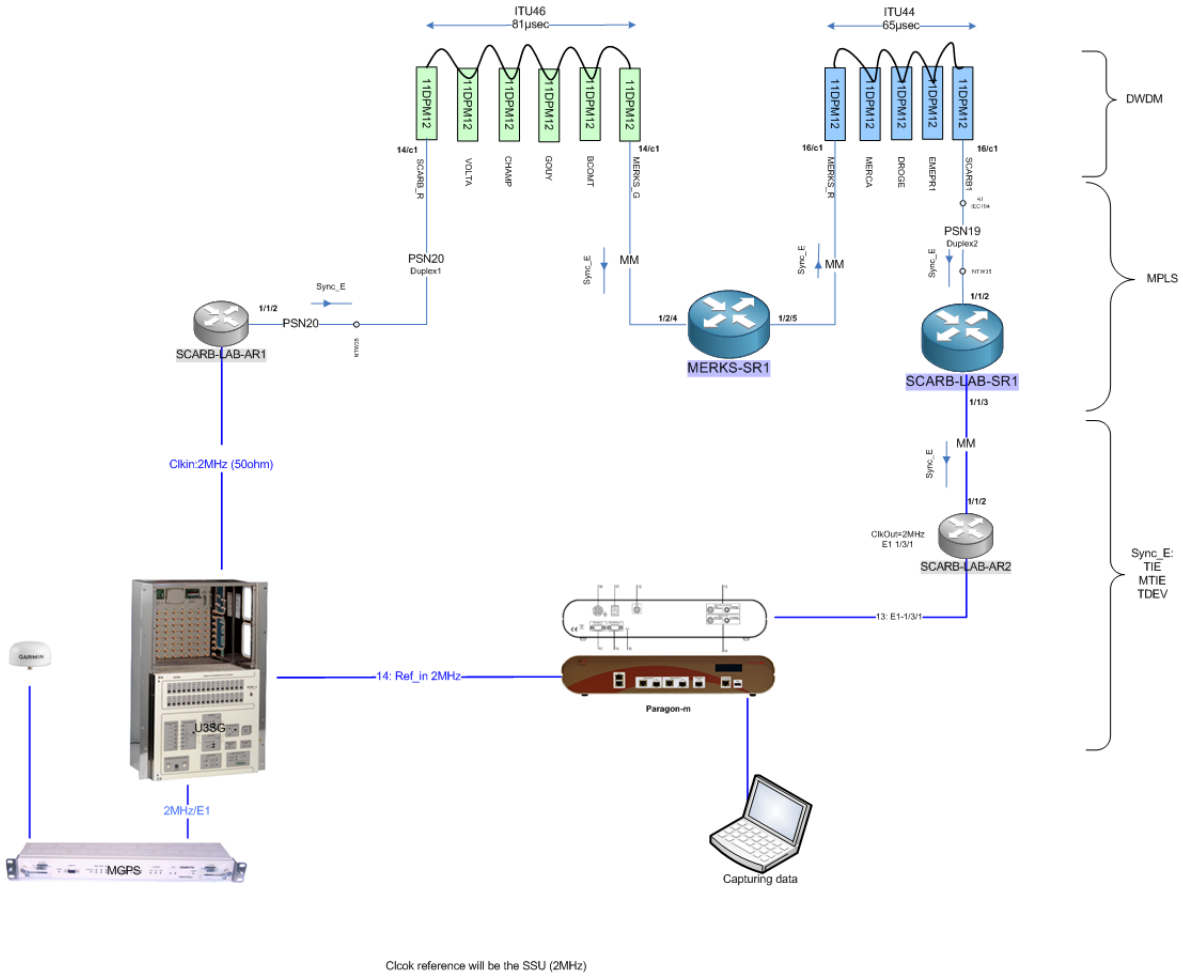
Рекомендуемая схема организации связи, на пример, между подстанцией и диспетчерским центром представлена на рисунке ниже.



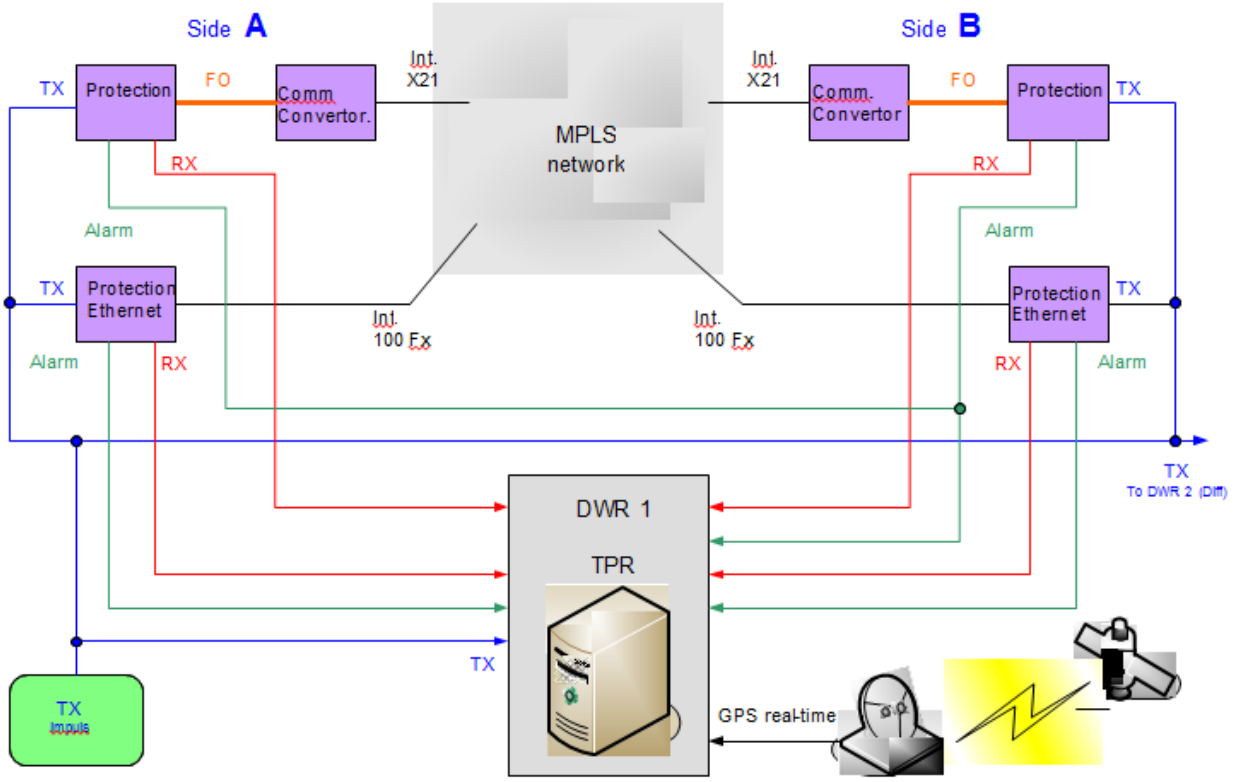
В докладе рассматриваются рекомендуемые схемы подключения различных

информационных сервисов, приведены рекомендации по приоритезации трафика.

Рассматриваются вопросы сетевого синхронизма, задержек по времени.



Представлены схемы организации релейных защит по сетям MPLS и алгоритмы их тестирования.



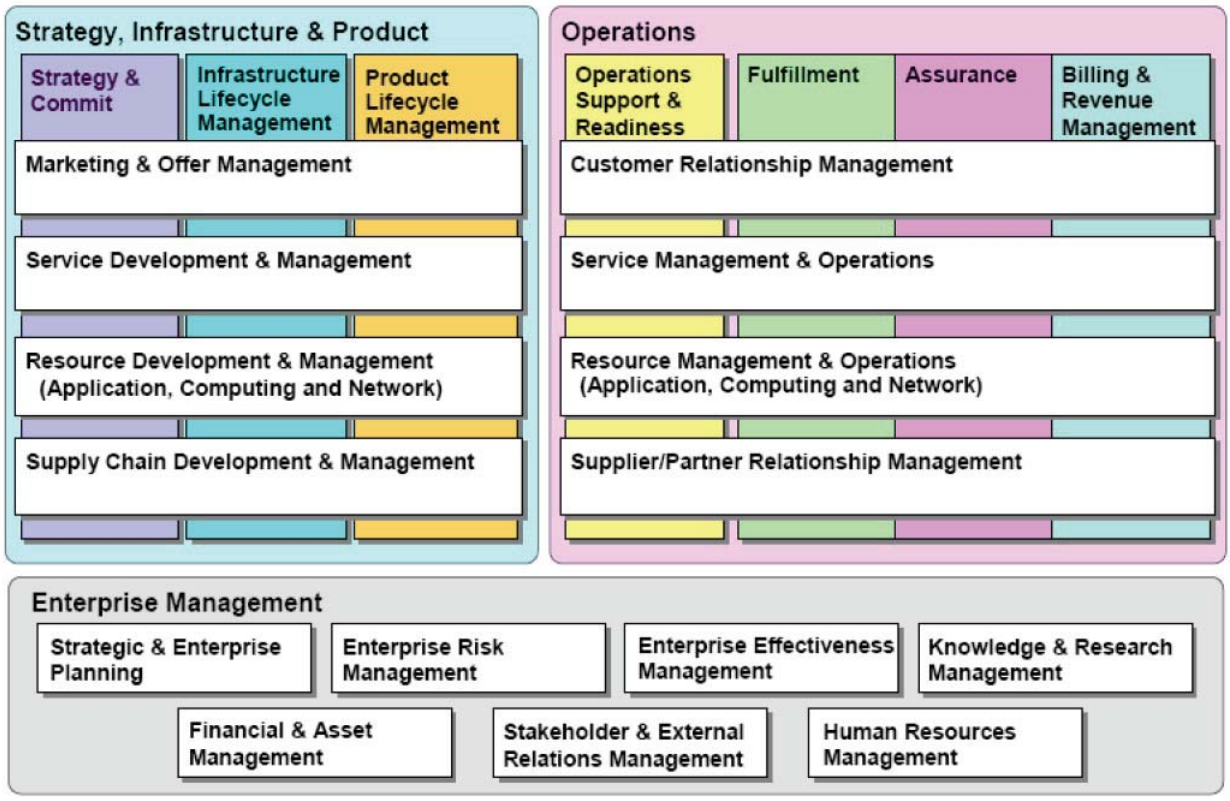
D2-303 «Изменение требований бизнеса Eletrobras Elenorte к телекоммуникациям, управлению и обслуживанию»

MARCELO COSTA DE ARAUJO, MARCOS ALVES RODRIGUES
Eletrobras Eletronorte, Brazil

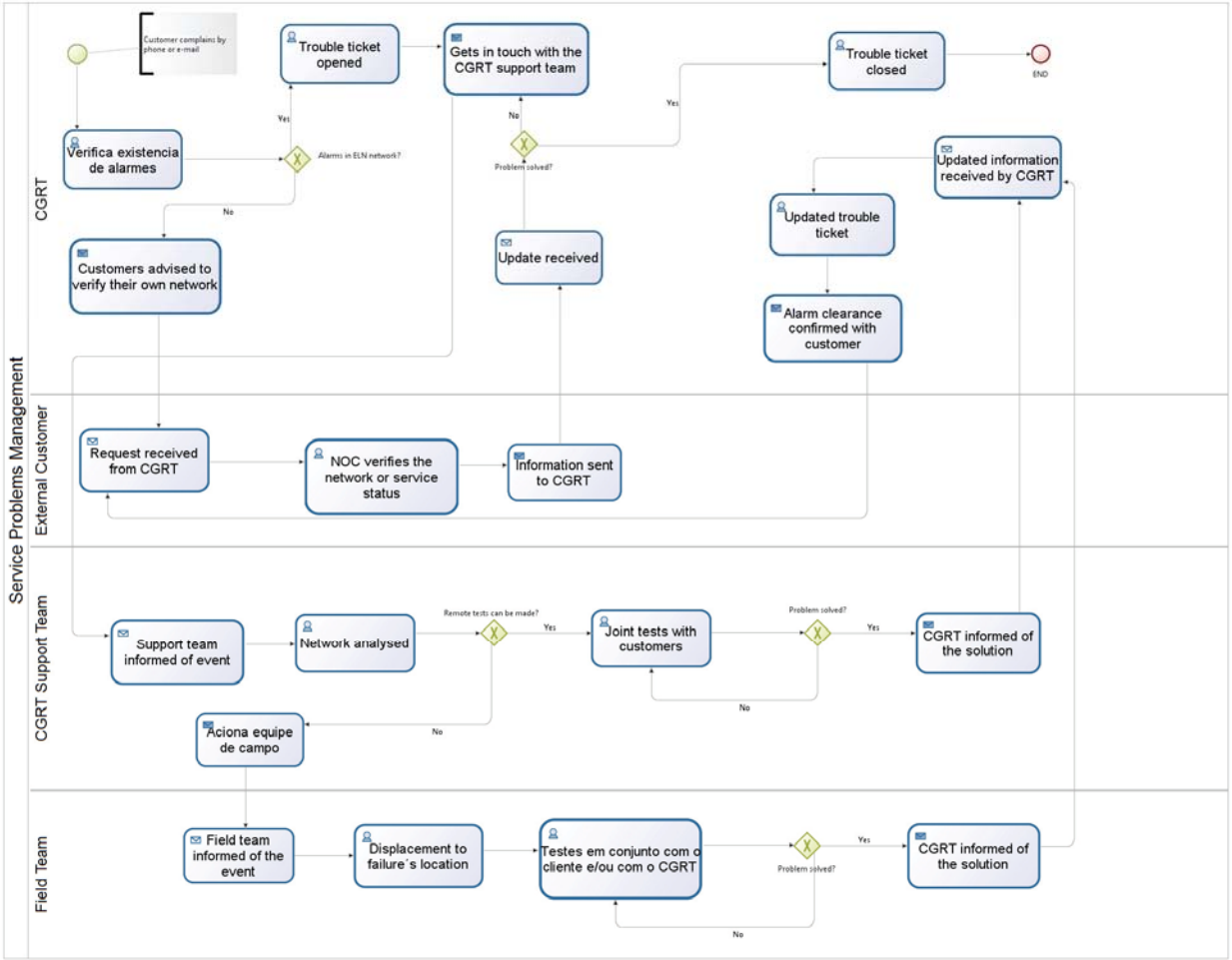
С 2003 года компания Eletrobras Elenorte функционирует в роли телеком-оператора. В докладе рассказывается о пути развития телекоммуникационных сетей и сервисов по мере изменения требований бизнеса к ним.

На текущий момент под управлением компании находятся 80 Гбайт сети DWDM.

В результате обсуждений с бизнес-заказчиком функций и требований по предоставлению телеком сервисов появилась расширенная карта телекомсервисов (eTOM).



Были разработаны диаграммы основных процессов предоставления телеком сервисов.



В докладе отмечается важность применения измеряемых метрик качества оказываемых услуг. Представлены выбранные метрики и дана оценка эффективности их применения.

D2-308 «Телекоммуникационные сети для внедрения Smart Grid»

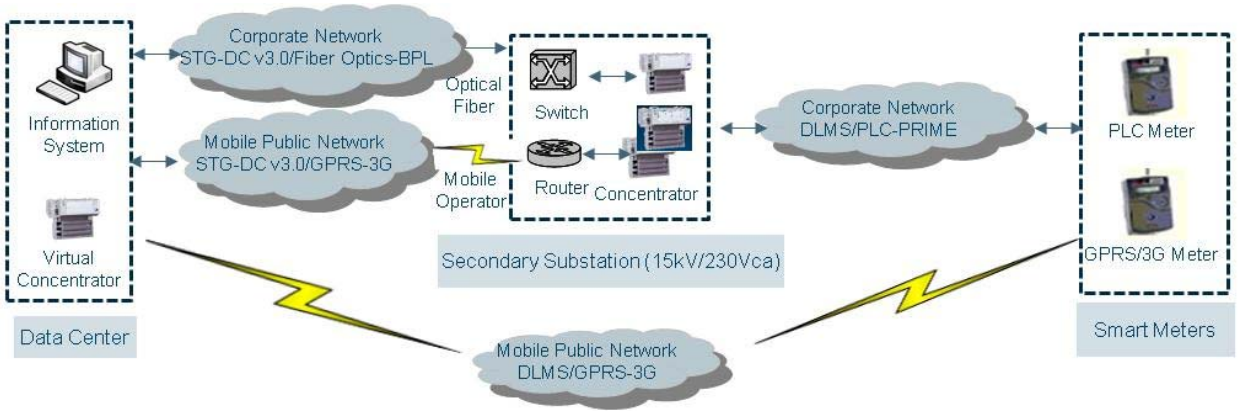
B. PERALTA, Gas Natural Fenosa, Spain

В докладе особая роль отводится стандартизации телекоммуникаций при подготовке к внедрению технологий Smart Grid. Отмечаются усилия, которые Европейская Комиссия затрачивает на стандартизацию.

Предлагается классификация телеком сетей по географическому принципу:

- HAN (Home Area Network): объединяют устройства в рамках одного здания или дома (интеллектуальные счетчики).
- NAN (Neighbourhood Area Network): включают коммуникации между зданиями и сооружениями потребителей и вторичными подстанциями.
- UAN (Utility Area Network): сети, охватывающие подстанции и центр обработки данных электросетевого предприятия.

Для каждого класса сетей предлагается набор стандартов физической и логической связи, рассматривается общая архитектура решения.



Предлагается набор рекомендация по характеристикам сетей для каждого вида сервисов.

Service	Topology	Capacity	Latency	Availabilyty	Integrity
Telecontrol	H&S (1) Symetrical	Very low (<10 kbps)	Medium (<10 s) (2)	High	High
Protection	FM (p2p) Symetrical	High (3) (> 1Mbps)	Very low (< 6 ms)	Very high	Very High (BER<10-6)
Metering	H&S Asymetrical	Medium (< 50 kbps)	Not a constraint	Medium	Low
Distribution Automation	FM Symetrical	High	Very low	Medium	Low
Management	H&S Asymetrical	Medium (<100 kbps)	Not a constraint	High	Low

(1) Substation always, Secondary Substation not always.
(2) Transfer time: T1-T2/2 (IEC 104 timers).
(3) In order to keep delay low when using packet switched networks.
H&S: Hub&Spoke. It's used for centralized architectures.
FM: Full Mess. It's used for distributed architectures.