VICTOR JULIO SOLIS RODRIGUEZ (FIRMA)

Firmado digitalmente por VICTOR JULIO SOLIS RODRIGUEZ (FIRMA)
Fecha: 2022.06.08 19:32:32 -06'00'

Dirección Transformación y Gestión Tecnológica

Unidad Tecnologías de Información y Comunicación

Área Infocomunicaciones

Informe de participación en evento

Distributech Internacional 2022

Realizado por:

MARIO VENEGAS PADILLA (FIRMA)

Firmado digitalmente por MARIO VENEGAS PADILLA (FIRMA)
Nombre de reconocimiento (DN): serialNumber=CPF-01-1070-0392, sn=VENEGAS PADILLA, givenName=MARIO, c=CR, o=PERSONA FISICA, ou=CIUDADANO, cn=MARIO VENEGAS PADILLA (FIRMA)
Fecha: 2022.06.06 15:36:25 -06'00'

Mario Venegas Padilla

Jefe, Área Infocomunicaciones

ROY GERARDO GUZMAN RAMIREZ (FIRMA)

Firmado digitalmente por ROY GERARDO GUZMAN RAMIREZ (FIRMA)
Fecha: 2022.06.07 07:55:44 -06'00'

Visto bueno

Roy Guzmán Ramírez

Director a.i. Transformación y Gestión Tecnológica

6 de junio, 2022

Índice

Distributech Internacional....3
Descripción....3
Objetivos....3
Introducción....3
Desarrollo....3
Charla 1: UU 303 Grid Modernization Communications – Alternatives....4
Charla 2: Keynote Address....10
Charla 3: Next Generation Security for Your OT and DER System....10
Charla 4: Cybercriminals are Looking at IoT Devices: How Can We Negate These Attacks?....12
Charla 5: Gain a Competitive Edge by Selecting and Deploying Antennas for Smart Cities....13
Charla 6: Leveraging Smart Streetlights to Transform Communities into Smart Cities....14
Charla 7: How PG&E Reimagined the Distribution Operations Technology Support Model....15
Charla 8 Customer DER to the Rescue! Responding to Grid Events Through a Modern DRMS....15
Charla 9. Grid Security Visibility, Analytics and Automation....17
Charla 10: How Field Area Network Standards Are Enabling End-to-end Smart Metering....19
Charla 11. LTE for Critical Infrastructure: Standards, Requirements, and Deployments....21
Charla 12: The FLISR Marathon: How a Focus on Incremental Value Can Deliver Key Functionality....23
Charla 13: Building a Sustainable Grid Transformation Strategy and Roadmap....25
Charla 14: Development of a Home Energy Management System Based on WI-SUN/HAN Specification and Open Middleware....27
Charla 15: How to Build Resilience and Adaptability in the Grids – Learnings from Major Utilities Across the Globe....28
Visita al Stand Wi-SUN Alliance....29
Conclusiones....31
Recomendaciones....32
Evaluación del evento....32

Distributech Internacional

Del 22 al 25 de mayo de 2022

Descripción

Es el principal evento anual de transmisión y distribución en los Estados Unidos que aborda las tecnologías utilizadas para mover la electricidad desde la planta de generación a través de los sistemas de transmisión y distribución hasta el medidor y el interior del hogar. Las conferencias y puestos de exhibición ofrecen información, productos y servicios relacionados con los sistemas de control y automatización del suministro de electricidad, eficiencia energética, respuesta a la demanda, integración de energía renovable, medición avanzada, operación y confiabilidad del sistema de transmisión y distribución, tecnologías de comunicación, seguridad cibernética, tecnología de servicios de agua y otros.

Objetivos

- ✓ Investigar sobre las alternativas de comunicación para la modernización de la red de infocomunicaciones.
- ✓ Investigar sobre las tendencias y mejores prácticas desarrolladas para empresas del sector distribución eléctrica en el ámbito de la ciberseguridad.
- ✓ Investigar sobre las tendencias y criterios a aplicar en la planificación del desarrollo de la arquitectura de Infocomunicaciones.
- ✓ Aprovechar el networking profesional para visualizar oportunidades de negocio que den valor agregado a la empresa con uso ampliado de las infocomunicaciones.

Introducción

La finalidad de este documento es informar sobre los conocimientos adquiridos en la visita que se realizó al evento Distributech 2022.

El evento se desarrolló desde el domingo 22 de mayo y hasta el miércoles 25 de mayo de 2022 en la ciudad de Dallas, Texas en USA y contó con la participación de numerosos expositores en el ámbito de la Distribución de Energía Eléctrica, tanto por parte de fabricantes como de empresas de servicios públicos o tipo utilities.

Desarrollo

La asistencia al evento inició el domingo 22 de mayo de 2022 con el proceso de verificación de la inscripción y asistencia al evento.

Luego de ello se inició con la asistencia a las charlas previamente programadas según el horario fijado y que eran de interés para las áreas que se debían cubrir.

A continuación una descripción diaria de las charlas a las que asistí:

Charla 1: UU 303 Grid Modernization Communications – Alternatives

Esta charla fue presentada por Rich Schmidt, quien es consultor ejecutivo de la firma Schmidt Utility Advisors, LLC; y Alice Moy-González quien es vicepresidente de Strategic Development en la compañía Anterix, compañía que se dedica a soluciones de banda ancha para infraestructura crítica.

De acuerdo con lo presentado por los expositores de la Utility University en el evento, existen distintas motivaciones por las cuales las empresas deciden actualizar su plataforma de comunicaciones entre las que se puede indicar:

- Envejecimiento de la infraestructura de comunicaciones existente.
- Nuevos programas de modernización de la red: agregar muchos dispositivos de campo nuevos y que necesitan mejores comunicaciones.
- Comunicaciones de Resiliencia y Confiabilidad: gestión y regulación, mandatos para hacer más confiable la infraestructura de comunicaciones.
- Problemas de seguridad: proliferación de dispositivos de campo conectados y creciente evidencia de ataques que plantean preocupaciones.
- Disponibilidad y expansión de 600 MHz, 700 MHz, 900 MHz y 3,5 GHz de las redes privadas.

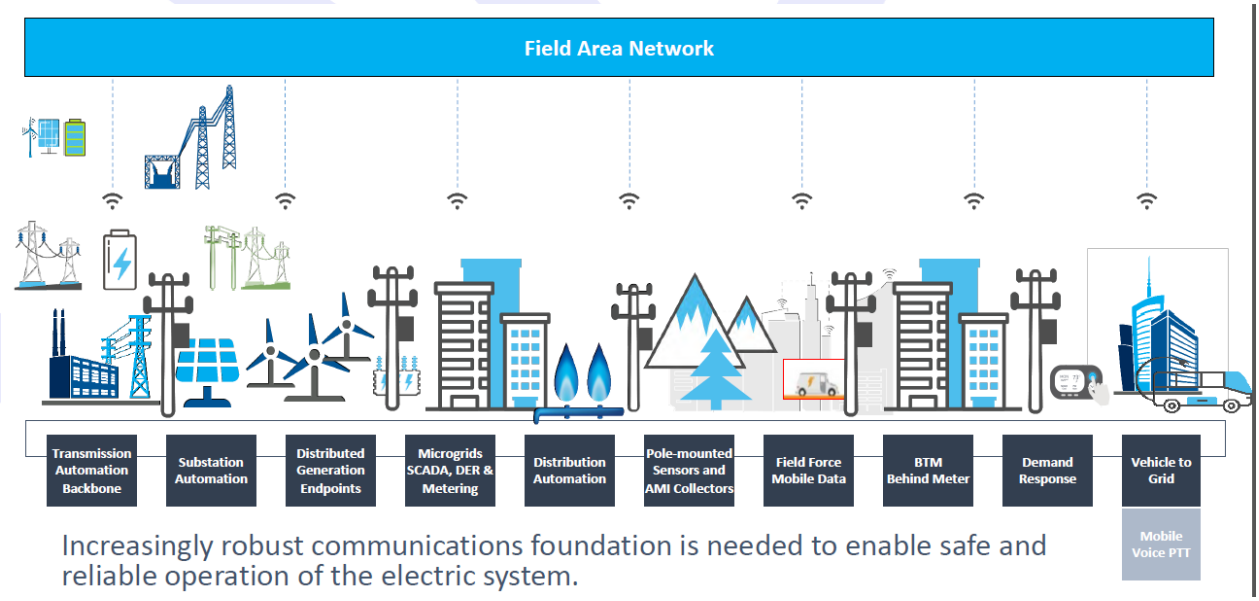
El desarrollo de la industria en general gira en torno a las siguientes tendencias:

- Eventos climáticos extremos, resiliencia, confiabilidad, sostenibilidad, objetivos de descarbonización impulsados por regulaciones, infraestructura envejecida, fuerza laboral envejecida, todos los desafíos e iniciativas en competencia.
- Las empresas de servicios públicos a menudo se mueven rápidamente de la implementación de una nueva plataforma de software a la siguiente y, a menudo, toman atajos en pruebas, capacitación de empleados, ingeniería de reprocesos.
- Las tendencias hacia la nube frente al software local no se están desacelerando.
- Algunas comisiones estatales ahora clasifican la nube o SaaS como un costo de capital cuando varios años de costos de SaaS son facturados por adelantado. Pero muchos estados clasifican a SaaS como un costo operativo.
- Big Data, Data Lakes y SaaS han tenido un gran éxito para almacenar datos y mantenerlos seguros e integrando casos de uso específicos entre varios sistemas, pero a pesar de generar fácilmente informes, exportar análisis o crear canteras para bases de datos, SaaS ha sido principalmente una decepción o infrautilizado.
- Los tres principales desafíos encuestados como principales impulsores de las inversiones en modernización de la distribución (según Black & Veatch Strategic 2021 Directions survey) son: Confiabilidad y resiliencia, Mayor seguimiento de los activos de campo (Administración de Activos) e Infraestructura envejecida.
- Crecimiento de EV (y crecimiento de celdas de combustible de hidrógeno) mucho mayor que el crecimiento fotovoltaico.
- Behind The Meter (BTM) – Mucha necesidad y no muchas soluciones comprobadas de proveedores en norte América.
- Utilities que migran a AMI de tercera generación (los Proveedores de AMI carecen de innovación en esta migración).

En el campo de las Infocomunicaciones se tienen las siguientes tendencias:

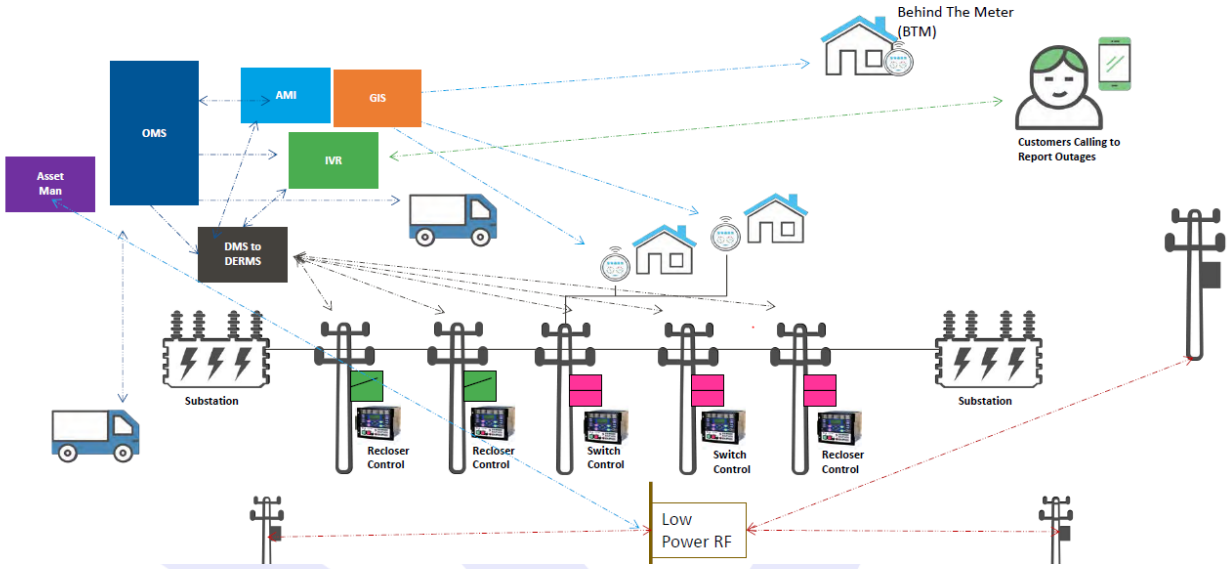
- A medida que las empresas de servicios públicos migran a su AMI de próxima generación, el rendimiento y la fiabilidad del backhaul aumenta.
- Caducidad de 3G celular: nuevas fechas, Verizon 31/12/2022, AT&T 12/2022, TMobile/ Sprint Julio 2022.

- Espectro de compra de servicios públicos: 600 MHz, 900 MHz, 3 GHz.
- Las compras de espectro inalámbrico pueden clasificarse como inversiones de capital.
- Se estima que la mitad de los dueños de infraestructura están estudiando si LTE Privado es apto o no.
- Varios proveedores privados de LTE ingresaron al mercado.
- Los sistemas privados de voz móvil (Land Mobile Radio) mediante radio para camiones no van a desaparecer.
- Crecimiento de servicios pesados: actualización de redes inalámbricas y de fibra con el énfasis en el "endurecimiento", la confiabilidad, la seguridad, y resiliencia. Trabajando para reemplazar la "mezcolanza" de redes de comunicación. 49% de las empresas de servicios públicos utilizan redes privadas para la misión aplicaciones críticas y esto tiene una tendencia más alta cada mes.
- Los servicios públicos continúan migrando de TDM a redes IP.
- Expansión de SCADA a terminales DER (recursos de energía distribuida) con potencia > 1 MW.
- Estudiar el uso de LTE privado en el medidor.
- Arrendamiento de fibra oscura de parte de los dueños de infraestructura (Utilities) a proveedores de banda ancha, empresas de telecomunicaciones, ciudades y escuelas como parte de la tarifa base regulada.



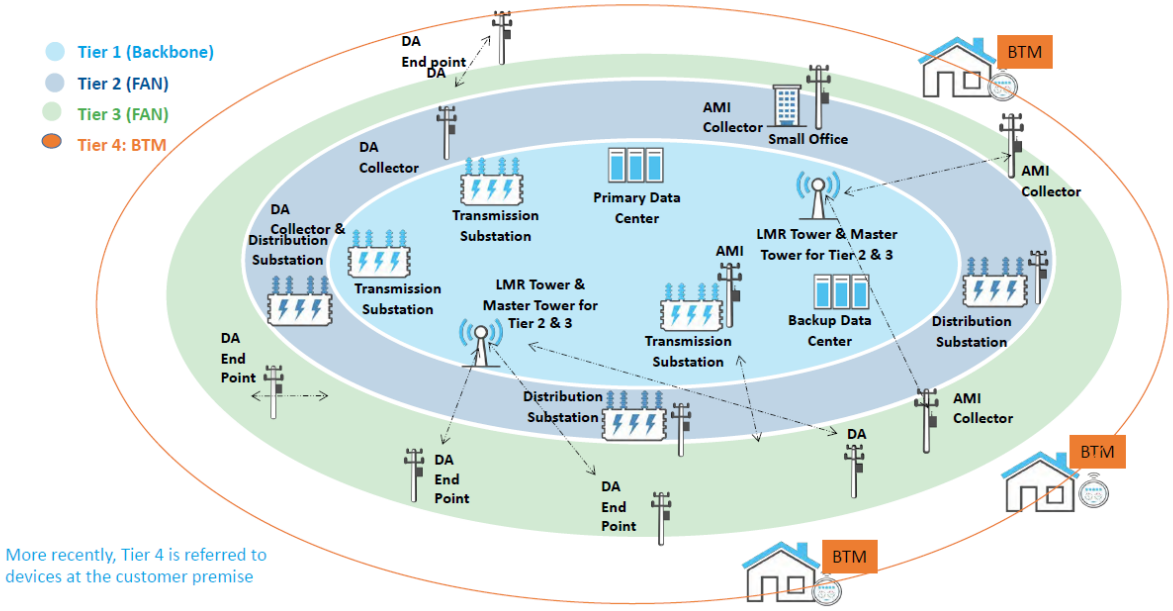
Las redes de trabajo de campo (FAN) deben robustecerse para brindar de manera segura y confiable la operación del sistema eléctrico. Debe considerarse como parte de la FAN todos los elementos y procesos asociados a la gestión de la energía, incluyendo el segmento de automatización (DA), elementos de energía distribuida (DER), medición (AMI), servicios en puntos finales (BTM), respuesta a la demanda, vehículos eléctricos (EV) y demás aplicaciones de la cadena de abastecimiento.

Wholistic Planning- Communications and Automation



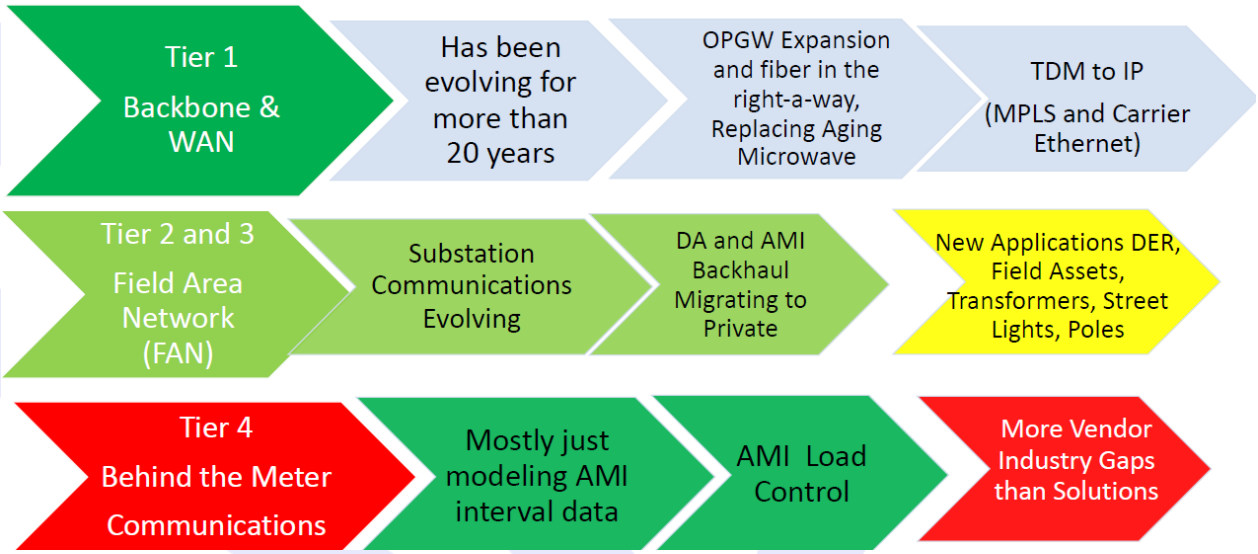
Se requiere una planificación con una visión holística de las comunicaciones y la automatización, teniendo en cuenta los múltiples y variados requerimientos para la adecuada operación de cada uno de los servicios que se soportan y se pueden desplegar como parte del negocio.

Communication Architecture Tiers Definition



Se propone un modelo basado en niveles, donde el nivel 1 hace referencia al Backbone y redes WAN. Los niveles 2 y 3 hacen referencia a la red de trabajo de campo. Por último el nivel 4 define los servicios más allá del punto final de medición.

Utility Communication Architecture Tiers



El nivel 1 es el más evolucionado. Se ha fortalecido de manera constante y se ha potenciado con el uso de la fibra óptica, misma que ha sustituido las microondas en este nivel de manera mayoritaria. Para darle mayor agilidad y valor a las organizaciones se han construido redes orientadas a servicios, basadas principalmente en MPLS.

Los niveles 2 y 3 han evolucionado en tres principales escenarios: comunicaciones en subestaciones, plataforma de comunicaciones AMI como backhaul de la automatización en distribución y nuevas aplicaciones para recursos de energía distribuida, activos de campo, transformadores, lámparas inteligentes y otros.

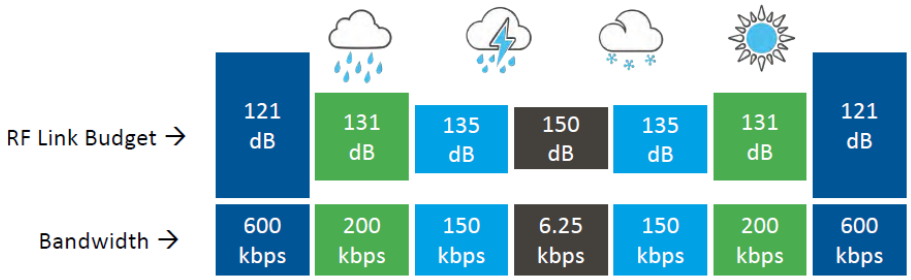
El nivel 4 está más enfocado al control de la carga, sin embargo es donde existen más brechas entre los vendedores de la industria que soluciones comprobadas y concretas.

RF Adaptive Modulation Example

From Microwave to AMI, many products now come with adaptive modulation

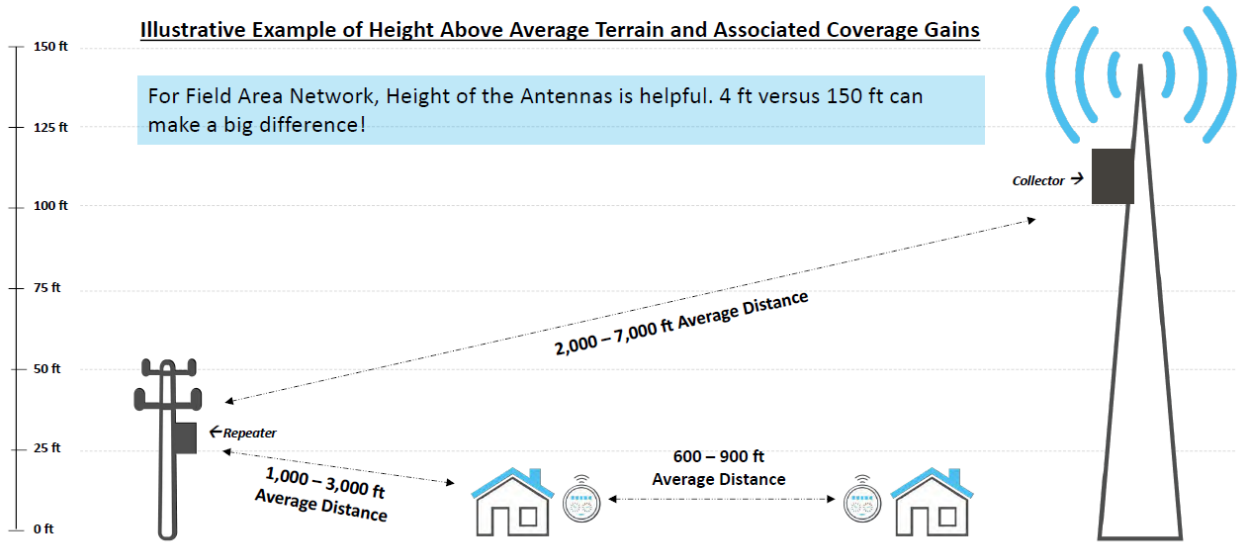
Rainy versus sunny weather reliability target

- ✓ Meter Coverage for worst case weather scenario
- ✓ As weather issues occur, link modulation throttles down (bandwidth) to maintain reliability



Siendo el medio inalámbrico el que permite la mayor cobertura del campo, se ha dado la tendencia en varios fabricantes que habilitan la modulación adaptativa para mantener la confiabilidad de la red cuando se presenten condiciones climáticas adversas. Esto implica menor ancho de banda para mantener la continuidad. Un ejemplo de esta condición es la alternancia entre modulaciones OFDM y FSK.

Extending Coverage – Height Above Average Terrain



Una práctica utilizada en los Estados Unidos para mejorar las condiciones de conectividad en las redes de medidores es dar altura a los colectores.

Factores de éxito en la planificación para el upgrade de las infocomunicaciones

La planificación de la arquitectura de infocomunicaciones debe tener como eje central las necesidades del negocio, las cuales se deben tratar de visualizar en el corto, mediano y largo plazo.
Se puede iniciar planteando las siguientes interrogantes:
¿Qué están utilizando otras utilities para comunicaciones FAN de misión crítica?
¿Tendremos sensores en los postes que van a requerir de comunicaciones?
¿Cuál medio de comunicaciones se debería utilizar para el backhaul de automatización de la distribución?
Si actualmente usamos la plataforma AMI como backhaul para AMI, ¿qué inversiones necesarias se deben realizar en un plazo de 3 a 6 años para fortalecerla?
¿Cuáles son los requerimientos desde el punto de vista de comunicaciones para el futuro?
¿Cuáles alternativas existen para BTM?
Todos estos cuestionamientos se deben realizar teniendo en cuenta la estrategia empresarial, y a partir de este punto inicia el plan para el upgrade de comunicaciones.

Se debe identificar el nivel de criticidad de las aplicaciones, tal como se muestra en la siguiente figura:

Make decisions on what applications are:

	Levels of Criticalness	Typical Reliability Expectations
1	**Critical** - Transmission SCADA, LMR, relay protection	99.99 to 99.999%
2	**Operational** - DA monitoring, AMI, MWM, FDIR, DG	99.9 to 99.99%
3	**Non-Real Time** (Daily, Weekly or Monthly Data Acquisition) - C&I metering, asset management IT/OT, other monitoring or monthly metering	98% to 99%

A nivel de SCADA de subestación se debe cuestionar la periodicidad de captura de datos, la latencia máxima, cantidad de datos y confiabilidad del enlace.
En el caso de AMI, determinar el intervalo de medición, consumo por gestores, reporte de salidas de energía, otros programas, etc.

La confección del plan deberá seguir al menos las siguientes etapas: planeamiento, diseño, validación de tecnologías, construcción de infraestructura habilitadora, diseño detallado e implementación.

En la siguiente imagen se detallan las tareas que implican las etapas anteriormente mencionadas:

Stage 1: Planning	Stage 2: Conceptual Design	Stage 3: Technology Validation	Stage 4: Build-Out Enabling Infrastructure	Stage 5: Detailed Design and Procurement	Stage 6: Deployment PMO
Visioning & Future State Planning	Conceptual Design (Architecture): "Backbone to Last-Mile"	Pilot Procurement (Equip. and Services) for a Lab and Small Pilot	Fiber expansion and network equipment and tower/pole build-out	Procure Equipment, Services and Spectrum	Complete Business Process Mapping for Deployment
Strategic Plan to Grid Modernization Plan to Telecom Master Planning Linkage	Organization, Staffing and Business Model Planning	Define Test Procedures and Performance Targets	Further Spectrum Evaluation and Planning	Complete Last-Mile Detailed Design Migrating from the 25%, 50%, 75% to 100%	Further Application Integration By Use Case
Communications Gap Analysis	Create AMI Migration Plan	Initial Application Integration for Use Cases Planned for Lab	Organization, staffing and pre-deployment planning	Assign resources (internal and external for deployment)	Begin Phased Deployment and Testing Approvals
High-Level Requirements By Application	Determine Procurement Approach: a) turn-key procurement, design & build, b) separate equipment and services, c) Other	Business Process Planning	Expand fiber backbone plan to address last-mile wireless technology selected	Update Organizational Change Management Process Plans	Follow Business Release Deployment Plan (by application)
FAN and AMI Migration Technology Evaluation and Technology Short-Listing	Create Business Case	Lab Testing and then Small Area Field Trial	Asset Management, Software, Tools and Pre-Deployment Planning	Update Business Case and Business Plan	Follow Infrastructure Deployment Plan
Expand Regulatory Planning	Expand Regulatory Plan	Update Business Case	Update Business Case	Update Regulatory Body	Reporting & Tracking Results

Charla 2: Keynote Address

Esta sesión se llevó a cabo en el auditorio del centro de convenciones. El discurso de apertura fue dado por Rick Perry, ex Secretario de Energía de los Estados Unidos y Gobernador de Texas, segundo estado más grande de Estados Unidos. En su discurso, como punto más relevante comentó sobre el gran reto que representa para USA la carbono neutralidad, más conocida en el lugar como **Net0**, pues esto requiere de fuentes de energía estables y de gran capacidad, siendo a criterio del señor Perry que la energía nuclear es la más conveniente para este objetivo. También comentó de la necesidad de reformas legales, que permitan una transición económica sostenida, pues el sector petrolero actual debe sufrir una transformación más que una desaparición.

Charla 3: Next Generation Security for Your OT and DER System

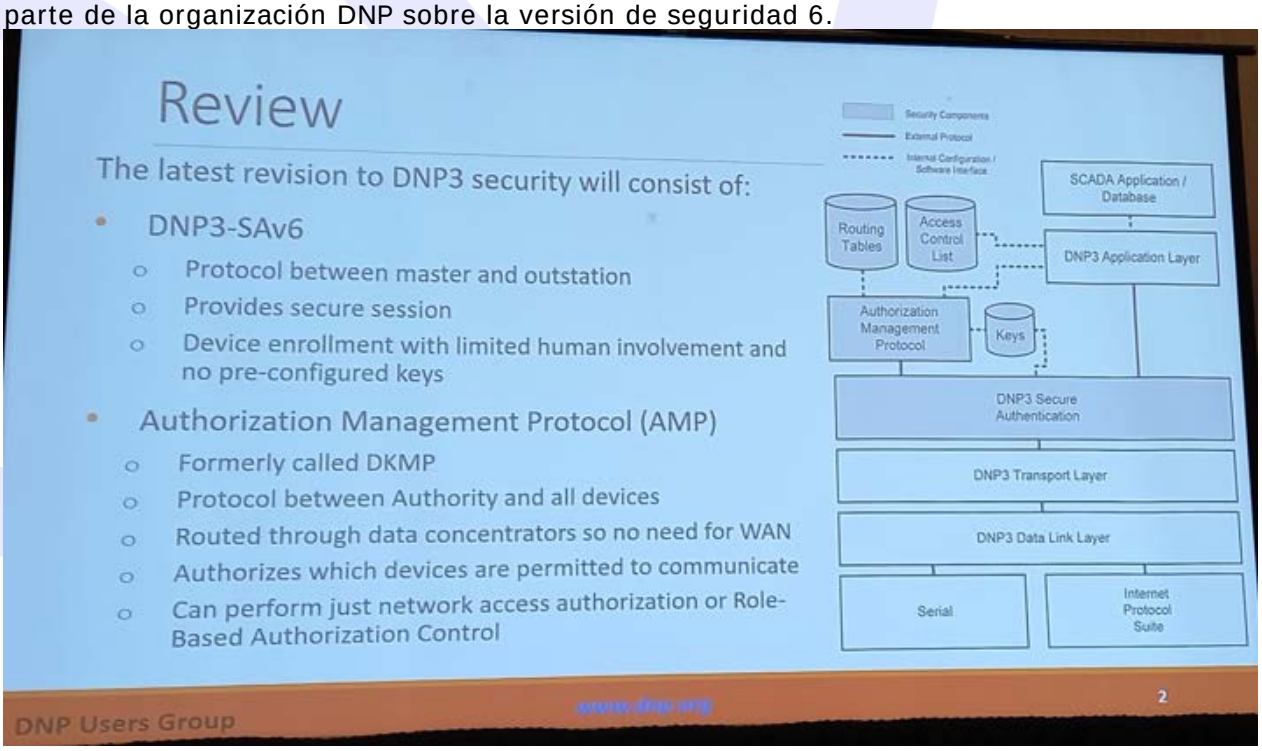
Esta charla fue dada por un panel de expertos compuesto por Ronald Farquharson, presidente de DNP Users Group; Herbert Falk, Director de OTB Consulting Services; Andrew West, Director Regional de SUBNET Solutions; y Scott Farley, Director de Ingeniería de Salt River Project.

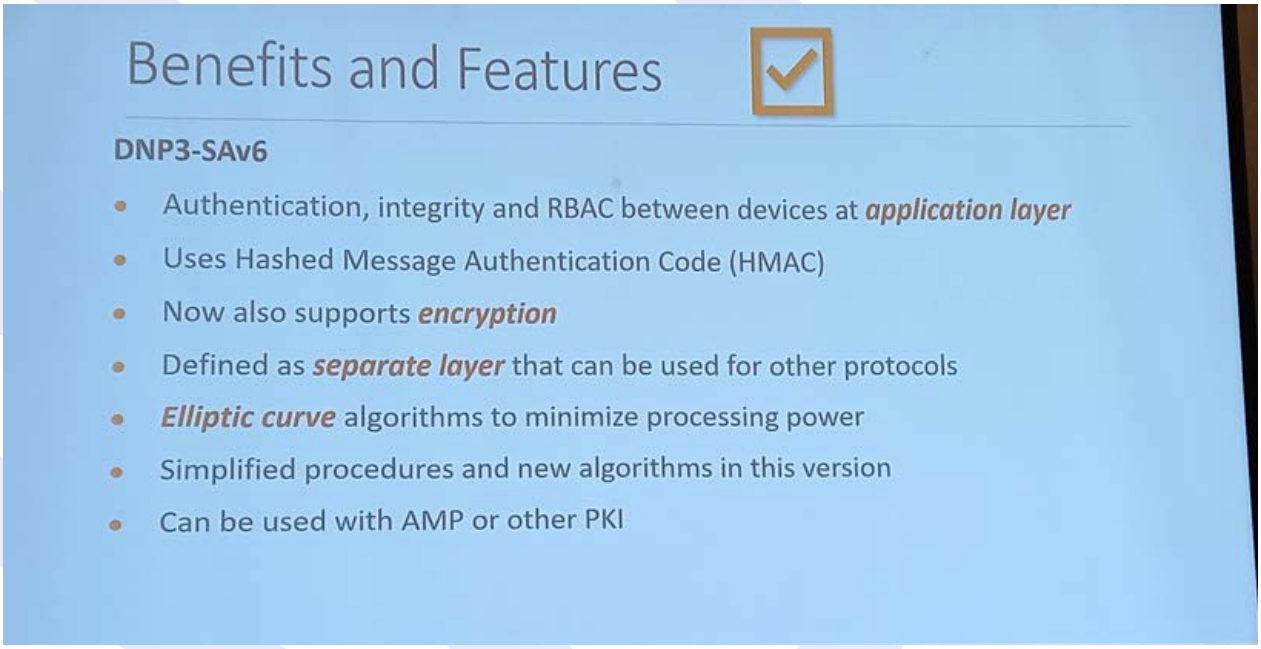
Se mencionó que la industria continúa trabajando diligentemente para abordar las vulnerabilidades cibernéticas para las infraestructuras de TI y OT. Sin embargo, asegurar las infraestructuras OT y especialmente DER presenta desafíos únicos. Los desafíos de ejemplo incluyen proteger los enlaces seriales, administrar las claves de seguridad, abordar la instalación y puesta en marcha práctica en el campo y minimizar los vectores de ataque de empleados no autorizados y actores sofisticados. En respuesta, una empresa de servicios públicos respetada, DNP-UG, EPRI, IEEE e IEC han colaborado para desarrollar protocolos de seguridad de próxima generación que brindan capacidades y beneficios que no se encuentran en ningún otro lugar dentro o fuera de la industria de la energía eléctrica. El trabajo resultante se incluirá en los estándares IEEE nuevos y actualizados.

En el ambiente de las tecnologías operativas para mejorar la seguridad se recomienda verificar la segmentación de la red y las listas de control de acceso al tráfico.

A nivel del protocolo industrial DNP3, el cual es utilizado por las empresas eléctricas, actualmente se está trabajando en la versión 6 del protocolo de seguridad (SAv6). Este protocolo permite sesiones seguras entre el máster y la terminal, autenticación a nivel de la capa de aplicación, encriptación de mensajes, posibilidad de utilizar el protocolo AMP (Authorization Management Protocol) o bien PKI (Public Key Infraestructure) que consiste básicamente en el uso de certificados.
El nuevo Protocolo de gestión de autorizaciones (AMP) incluye: un método para autorizar comunicaciones entre dispositivos conectados en serie e IP, incluidos maestros, Control de acceso basado en roles para cada par de dispositivos, autoridad central recién definida, Orientación sobre la implementación, incluida la integración con SCADA, otros sistemas de seguridad operativa y sistemas de gestión de credenciales de TI.

A continuación se presentan dos imágenes referentes al trabajo que se está realizando por parte de la organización DNP sobre la versión de seguridad 6.



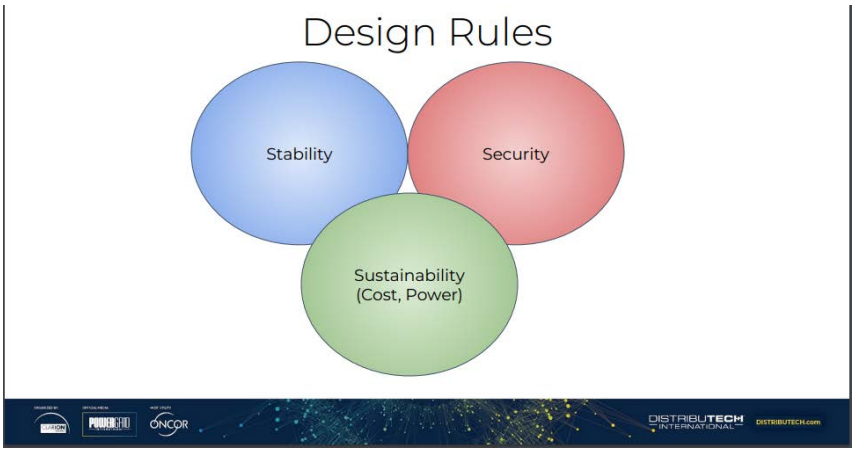


Charla 4: Cybercriminals are Looking at IoT Devices: How Can We Negate These Attacks?

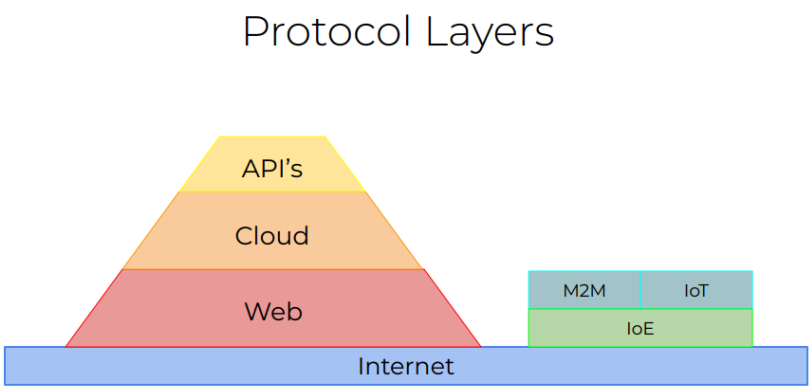
Esta charla fue brindada por Mattias Bergstrom, Arquitecto Líder de Producto de Internet of Everything Corp.

El expositor indica que los despliegues de IoT (Internet de las Cosas) y M2M (Machine to Machine) usando infraestructura TI como nube son una catástrofe esperando por ocurrir. Los ciber terroristas están buscando dispositivos IoT y sus instalaciones como una oportunidad para atacar infraestructura nacional.

Primero se refiere a las reglas de diseño, donde la estabilidad, seguridad y sostenibilidad deben encontrar un balance.



Ubica el Internet de las Cosas en una capa aparte de la Web:



De manera pasiva los riesgos en IoT conllevan problemas de hardware y velocidades en tiempo real, pero de manera activa el malware, inyección de datos y denegación del servicio.

En el mundo web, los vectores de ataque vienen de cualquier sitio que pertenezca a esta zona, la cual es sumamente amplia. El IoT solo necesita un ambiente local. Por lo tanto propone como solución el uso de DataLakes, que gestionan los datos de manera aislada a la web y no se exponen innecesariamente.

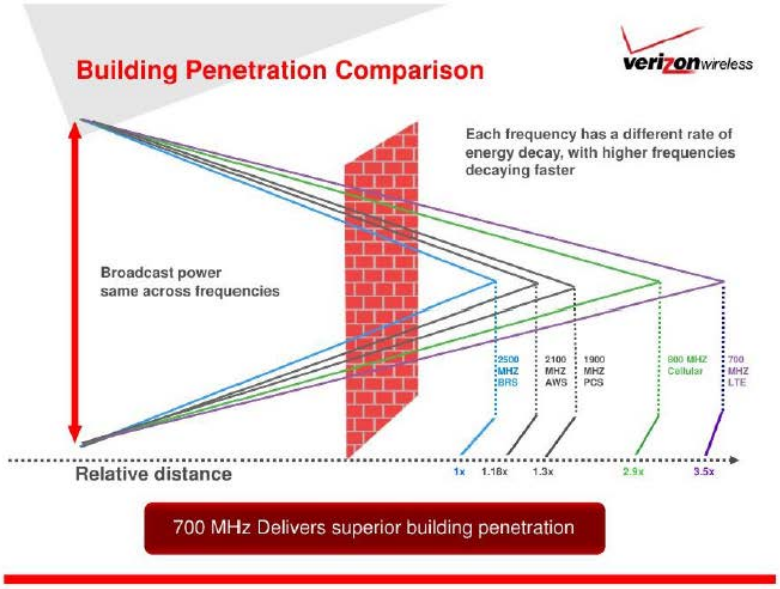
Charla 5: Gain a Competitive Edge by Selecting and Deploying Antennas for Smart Cities

Esta charla fue realizada por Roger Owens, Jefe de Ingenieros en Skywave Antennas Inc.

En muchas ocasiones la antena no es considerada en las etapas tempranas del despliegue de sistemas. Sin embargo, es la pieza que tiene mayor impacto en el rendimiento del sistema de radio.

Inició la charla haciendo un repaso de conceptos relativo a la ganancia de las antenas que se mide en dB y su relación a potencia en dBm, siendo esta una relación logarítmica. Posteriormente se presentaron los patrones de radiación, evidenciando el área de cobertura acorde con el diseño de la antena y con la polarización utilizada.

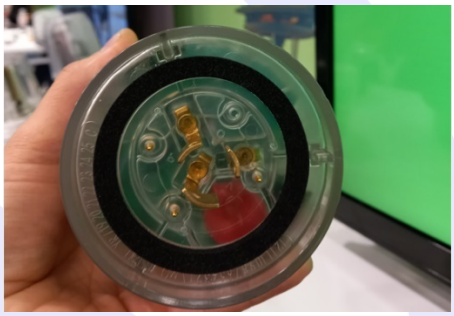
El nivel de penetración de las señales es inversamente proporcional a la frecuencia, tal como se muestra en esta figura:



Como conclusión, se indica que no necesariamente una antena de mayor ganancia es la que se debe utilizar, pues son los niveles de recepción y transmisión específicos de cada red los que determinan esta necesidad. Es decir una antena con mayor ganancia podría percibir mucho ruido, en tanto que una direccional de menor ganancia puede enfocar mejor la señal que se requiere procesar.

Charla 6: Leveraging Smart Streetlights to Transform Communities into Smart Cities

La charla fue impartida por Charlie Nobles, vicepresidente de ventas de Ubicquia.
Se menciona inicialmente que las ciudades y las empresas de servicios públicos de todo el mundo están adoptando soluciones tecnológicas para volverse más inteligentes, seguras y conectadas. Una solución es una plataforma montada en alumbrado público que permite a las ciudades atenuar y programar las luces en función de diferentes requisitos y reducir el consumo de energía del alumbrado público.
En la sesión se concluye que para garantizar una red de energía confiable y resistente, el controlador de la luminaria puede actuar como un medidor de servicios públicos y proporcionar a los clientes informes en tiempo real sobre el consumo de energía y las fallas en el alumbrado público, enviando notificaciones inmediatas si detecta daños por un vehículo o una tormenta.
Como actividad complementaria en el evento se visitó el hub de Landys&Gyr en el cual se logró identificar un controlador de lámpara inteligente compatible con las características de la red de trabajo de campo de la CNFL. Se presenta a continuación dos imágenes del mismo:



Charla 7: How PG&E Reimagined the Distribution Operations Technology Support Model

La charla fue presentada por Elaine Reusing, Directora de la Plataforma de Integración de la Red; Brian Chabot, Administrador del SCADA de Transmisión y Distribución; Danna Zahran, Administradora de Personal y Tony Calabro; Administrador de Energía y Servicios Públicos; todos de P&G.

En el tercer trimestre de 2022, PG&E implementará un Sistema de gestión de distribución avanzada (ADMS) de última generación. Con esta implementación, PG&E reemplazará su sistema SCADA heredado y la aplicación FLISR y sentará las bases para un futuro reemplazo del sistema de gestión de interrupciones y la habilitación de otras aplicaciones avanzadas.

El proyecto tiene por objetivo asegurar las tecnologías de red, transformar la experiencia del usuario ante las salidas del servicio, mejorar las operaciones en el campo, atender las expectativas para el crecimiento de los recursos de energía distribuida (DERs) y consolidar algunos sistemas independientes en una sola plataforma.

Las principales fases del proyecto han consistido en un Proceso de Diseño del Negocio, Entrenamiento y Despliegue y Administración del Cambio. Como puntos clave o lecciones aprendidas se indica: establecer principios de diseño, los procesos futuros deben informar al grupo de diseño de la organización, ser ágiles y diseñar para el cambio, proactivamente diseñar el proceso de transición.

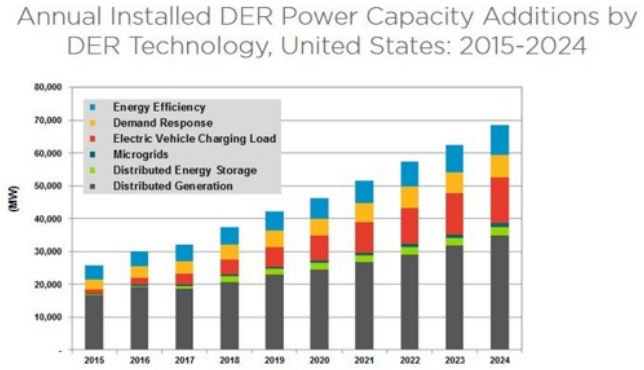
Charla 8 Customer DER to the Rescue! Responding to Grid Events Through a Modern DRMS

La charla fue impartida por Brad Cobb, Gerente de Ernst & Young LLP (EY) y Marlon Argueta, Administrador del Programa de Eficiencia Energética en la empresa Con Edisson.

Se inicia presentando el cambio en el panorama energético para los Estados Unidos considerando como principales variables la energía distribuida, la carga de vehículos eléctricos y respuesta a la demanda en el periodo 2015-2024. A continuación la proyección presentada:

Changing Energy Landscape

- Demand Response is a fast-growing component of increasing distributed energy resource (DER) capacity in the future.
- The future of DER management includes robust Demand Response Management System (DRMS) capabilities.



(Source: Navigant analysis)

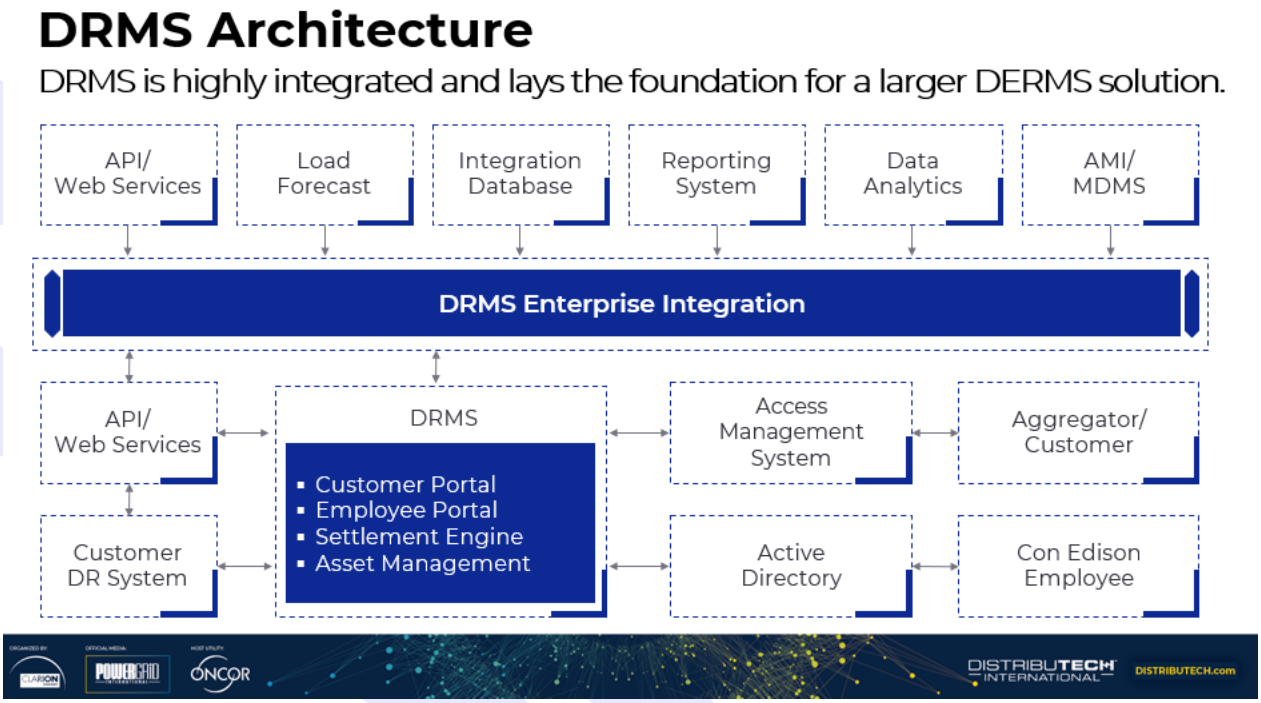
Ante este cambio, surge la necesidad de crear un sistema para administrar estos recursos distribuidos, pero que debe tener como centro la experiencia del cliente. Para ello el sistema se debe basar en cuatro aspectos: investigación e inscripción, notificación de eventos y monitoreo, consciencia de datos y liquidaciones. A continuación se muestra el detalle en cada caso:

Customer Experience in DRMS

Enhanced customer experience is key to customer adoption, which is critical for the success of any Demand Response (DR) program.

El alineamiento entre las capacidades a nivel del dispositivo (DER) y las necesidades de la red incrementan la confiabilidad y eficiencia del sistema.

La siguiente imagen, muestra la forma esquemática en que el sistema de recursos de energía distribuida (DERMS), se integra a la empresa:



Charla 9. Grid Security Visibility, Analytics and Automation

Esta charla fue presentada por Bradley Singletary, Gerente de Deloitte & Touch LLP.

Indica que se consideran factores de amenaza los siguientes:

- La utility está acelerando para defender el valor de la infraestructura existente y el negocio, pero no está segura de sus activos.
- Las innovaciones en tecnología y nuevos negocios incrementan la vulnerabilidad y la convierten en un objetivo.
- La cantidad de intentos de ataques han incrementado significativamente, con objetivos cada vez más específicos.
- Los incidentes son más a menudo vistos por el público, son seguidos por los reguladores y el gobierno.

A nivel de la industria eléctrica la nueva tendencia en materia de seguridad se conoce como Zero Trust, que significa cero confianza. Consiste en que todos los dispositivos conectados no deben ser considerados confiables, independientemente de que estos estén vinculados y verificados desde una red corporativa. Este modelo exige una estricta verificación de autenticidad para cada elemento que intente acceder a recursos de una red privada. Para la verificación de identidad normalmente se hace uso de un certificado digital.

Enfoque de los ataques en Utilities

Indirecto: a través de aplicaciones e infraestructura menos seguras.

- A menudo como daño colateral en torno a otras campañas de amenazas no relacionadas.
- A veces rodean dependencias energéticas estratégicas.

Directo: en el negocio y los clientes.

- Para defraudar fondos de las empresas y sus clientes.
- Para incrementar el debate político alrededor de un negocio.
- Para lograr los intereses de un individuo de la propia utility.
- Para dirigir la inteligencia hacia una infraestructura nacional/regional.
- Por fines políticos.

Previo a la ejecución de un ataque deben darse tres condiciones: un medio de acceso, una oportunidad y un objetivo.

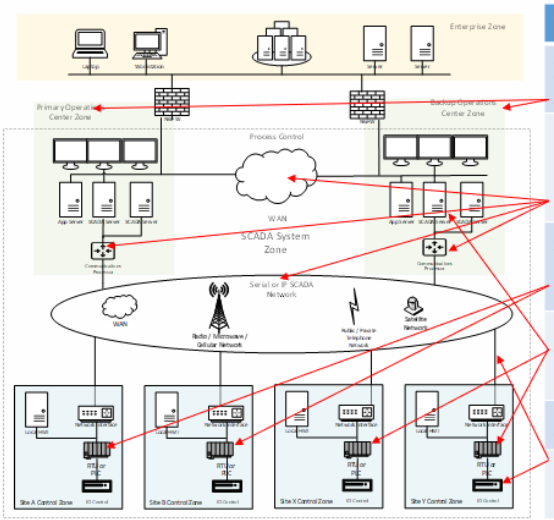
El medio puede obtenerlo el atacante a través de entrenamiento, procedimientos, herramientas, entre otros.

La oportunidad se da cuando el atacante identifica una vulnerabilidad.
Por último acorde con el tipo de amenaza, esta puede dar un motivo u objetivo al atacante.

Las empresas deben enfocarse en el control de las vulnerabilidades, ya que las otras dos están en manos del atacante.

A continuación un ejemplo de lo indicado acá a nivel de un sistema SCADA:

Example Threat Objectives for SCADA



Objective	Potential Threat Behavior
Subvert or Degrade Control and Situation Awareness at Scale	Establish access to control center SCADA and Engineering Access for maximum impact opportunity
Become Man in the Middle	Establish access to wide area SCADA and engineering access protocols and their supporting communications links to inject commands, falsify telemetry, prevent or limit recovery coordination efforts
Subvert or Degrade Targeted Facilities	Establish access at key facilities to target SCADA components and protocols, engineering access components and protocols, and provide access to key physical processes
Expand Targeted Access	Use targeted facility access to potentially threaten adjacent facilities, physical processes, wide area protocols and communications, and the control center
Retain Access and Control	Establish alternate access and retain targeted access to facilities and protocols
Degrade Resiliency	Make process / safety changes, modify or degrade environmental support, limit or damage backups and spares

Como se puede apreciar en la figura anterior, el objetivo del ataque puede ir desde degradar la resiliencia hasta provocar una degradación del servicio a gran escala. El objetivo depende de la profundidad en que el atacante pueda ingresar el sistema, situación que generalmente es gradual y obedece al nivel de vulnerabilidad desde las capas exteriores hasta las capas más internas del sistema.

Key SOC Components of Threat Visibility

SOC Component	Placement	Example Elements
Sensors	• At targets and controls • In the physical process • At/in the Infrastructure • Outside the organization	• Threat Intel and Vulnerability Scans • Network Sensors • System/App Logs • External Reconnaissance
Telemetry / Aggregation	• Across infrastructure • SOC primary/backup • IT/OT primary/backup	• Log aggregators • Security Infrastructure Integrations • Data lake
Event Detection Modeling / Analytics	• SOC primary/backup	• SEIM w/ Business rules • SEIM w/ MITRE ATT&CK • Machine learning / data mining • Risk Dashboards • Search
Event Management	• SOC primary/backup	• Alerts • Case management tools • Ticketing systems

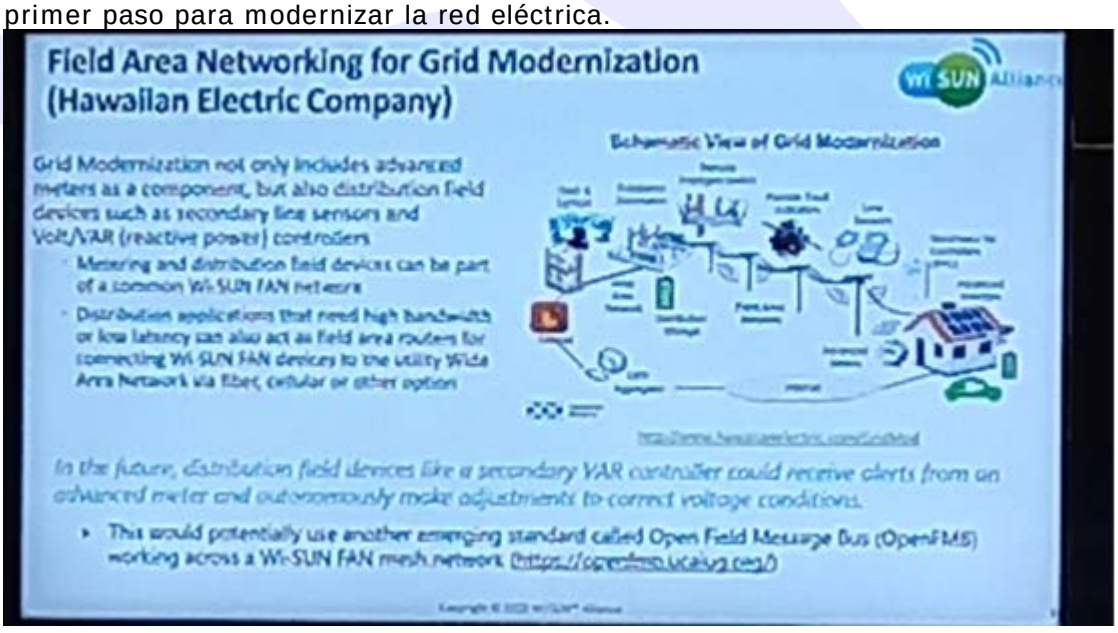
En la figura anterior se muestran componentes clave, que permiten tener visibilidad de la amenaza. El primer componente corresponde a los sensores, que normalmente generan señales que se transmiten a nivel de logs. El segundo componente agrupa estos logs. El tercer componente modela los eventos mediante un sistema de seguridad de información que puede aplicar inteligencia de negocios. El cuarto componente realiza la administración de eventos, generando alertas, herramientas para el manejo de casos y un sistema de tiquetes. El tercer y cuarto componente es posible encontrarlos integrados en soluciones tipo SIEM (Security Information and Event Management). Por lo tanto, para tener visibilidad de las amenazas se requiere de soluciones tipo SIEM, pues a nivel de sensores se tienen grandes cantidades de datos, las cuales es casi imposible analizar, y de las cuales se pierde el enfoque integral del sistema.

Charla 10: How Field Area Network Standards Are Enabling End-to-end Smart Metering

La charla fue impartida por Phil Beecher, Presidente y Director Ejecutivo de Wi-SUN Alliance. Se hizo referencia específica a la adopción del estándar WiSun por diferentes fabricantes como la mejor alternativa para lograr la interoperabilidad en la capa de comunicaciones. Los fabricantes mencionados fueron Cisco, Hexing, Landys & Gyr, Renesas, Silicon Labs, Texas Instruments y Trilliant.

En la imagen anterior se observa que empresas como QualityLogic y Exegin cuentan con herramientas de pruebas para Wi-SUN.

En el caso de Estados Unidos, el expositor hace mención que ya han comenzado algunas empresas con el proceso de adopción de Wi-SUN. Menciona el caso de Hawaiian Electric Company, misma que en conjunto con Landys & Gyr realiza el desarrollo de una red FAN como primer paso para modernizar la red eléctrica.



Otra de las iniciativas mencionadas por el expositor consiste en la estrategia de interoperabilidad para el desarrollo de AMI en los Estados Unidos. Esta estrategia es impulsada por Iberdrola, AvanGrid y EPRI.

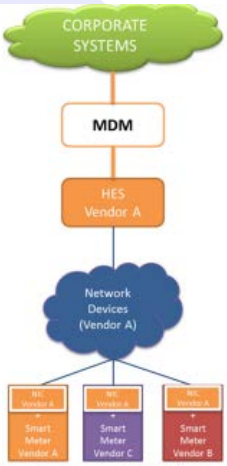


Figure 1. Non-Interoperable AMI Architecture

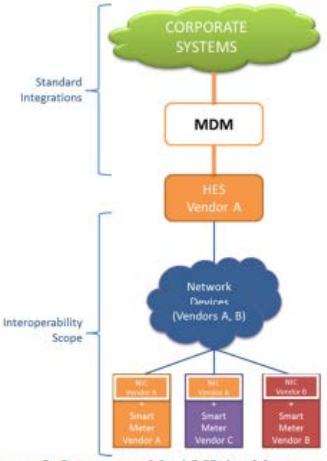


Figure 2. Interoperable AMI Architecture

Las imágenes anteriores son tomadas de dicha estrategia y se puede observar que la interoperabilidad se busca a nivel de la capa de red y los dispositivos que se conectan a la misma. Los objetivos de la estrategia son los siguientes:

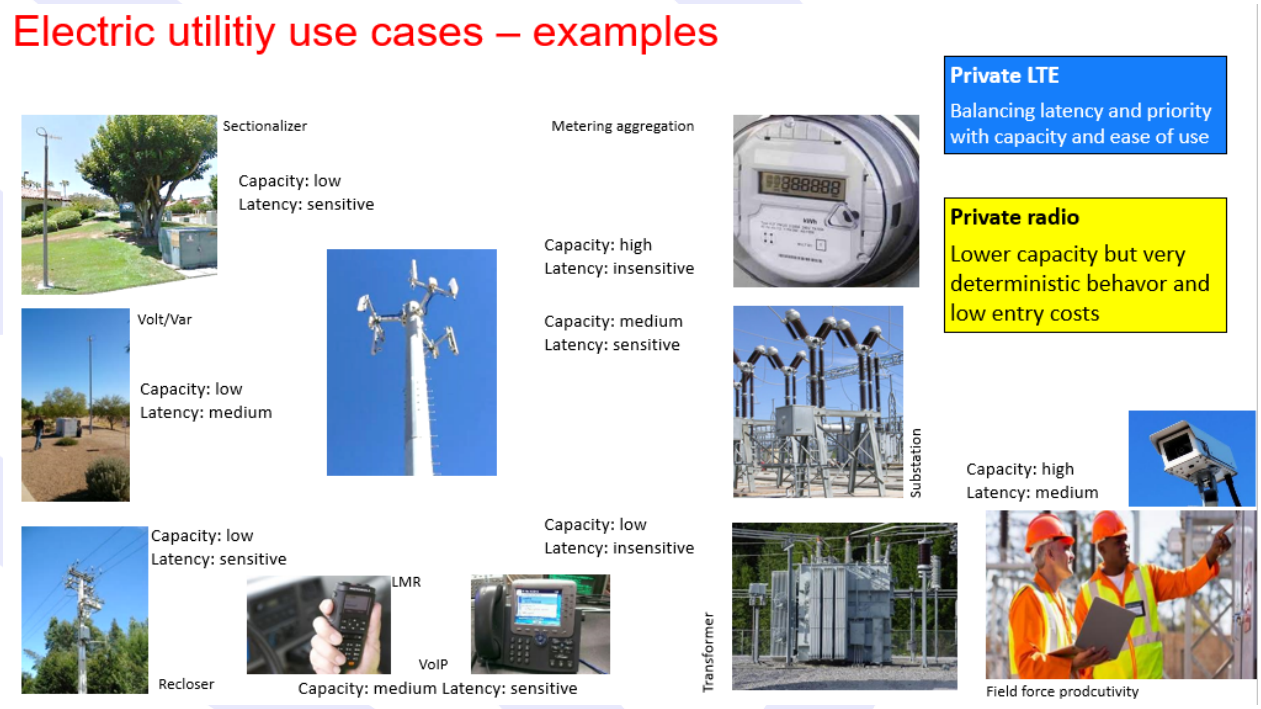
- Menor riesgo de dependencia de un solo proveedor.
- Apalancamiento incremental para negociar mejoras del sistema futuro e influir en la evolución tecnológica.
- Mayor conocimiento y control de la solución, en el ámbito de las telecomunicaciones (Tecnología de radio frecuencia) y en la aplicación (casos de uso de medición y funcionalidad avanzada).
- Aumentar el control de la estrategia de seguridad cibernética.
- Acelerar el desarrollo de nuevos casos de uso y aplicaciones.
- Permitir el uso de plataformas abiertas y flexibles para la operación y mantenimiento de medidores.

Charla 11. LTE for Critical Infrastructure: Standards, Requirements, and Deployments

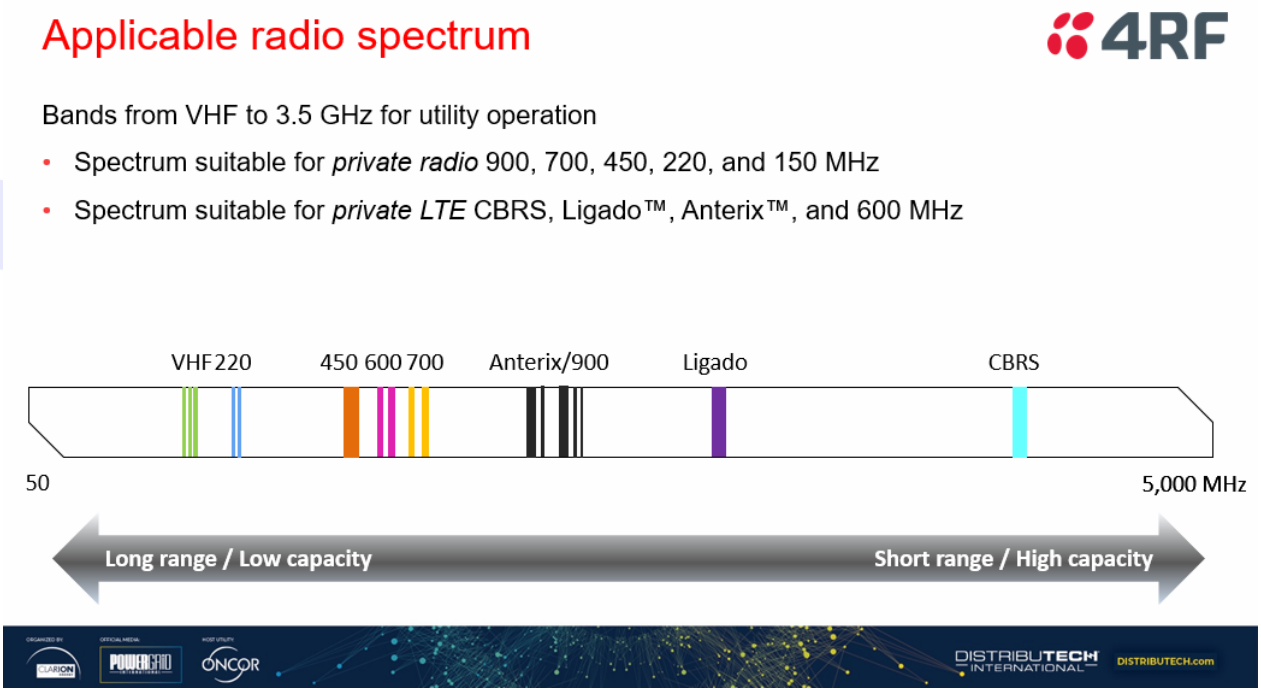
Esta charla fue presentada por John Yaldwyn, Jefe de Tecnologías de la empresa 4RF USA, en Nueva Zelanda.

En el caso de USA con la nueva disponibilidad de espectro privado en las bandas de 600 MHz, 900 MHz y 3.5 GHZ se abre la posibilidad de crear redes privadas LTE para atender necesidades de las utilities.

Los servicios de las utilities se pueden categorizar por capacidad y latencia como se muestra en la siguiente imagen:



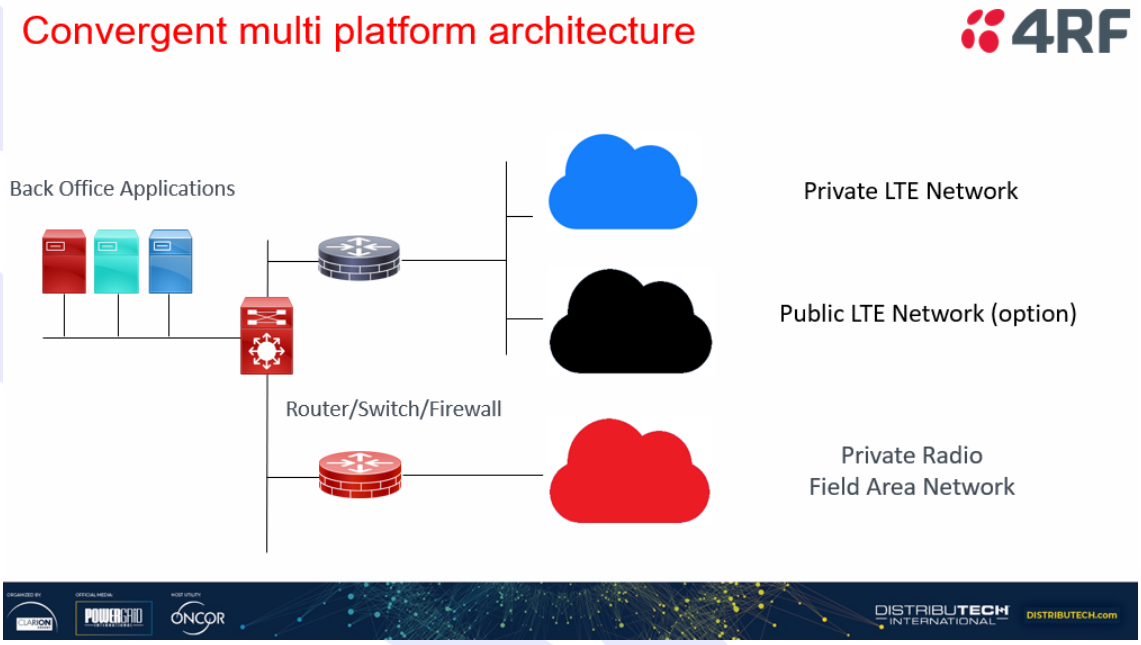
En la siguiente imagen se muestra el espectro aplicable para LTE Privado:



LTE Privado es el habilitador clave para el desarrollo de redes de banda ancha en negocios críticos. LTE no puede ser construido sin espectro y hasta hace poco fue obtenido. Con esta nueva opción, la industria tiene la posibilidad de construir redes con mayor capacidad y conexión para mayor diversidad de dispositivos IoT, pudiendo abastecer las necesidades de mayor capacidad, desafíos sobre las TI y presiones presupuestarias. La fuerza de trabajo móvil

de hoy requiere capacidad de red, la productividad de la fuerza de campo necesita de conectividad en el vehículo o en el sitio.

Se visualiza LTE Privado como un componente más de la arquitectura multiplataforma.



Charla 12: The FLISR Marathon: How a Focus on Incremental Value Can Deliver Key Functionality

La charla fue brindada por Matt Seibert, Líder de Ingeniería en Operaciones de Distribución de Consumers Energy, USA.

Consumers Energy (CE) trabajó con Accenture en un proyecto para entregar una gran implementación de FLISR (ubicación de fallas, aislamiento y restauración del sistema) basada en soluciones DPF (Distribution Power Flow). Consumers Energy ha centrado los esfuerzos de su programa FLISR en los más de 800 circuitos que actualmente tienen DPF convergente en su ADMS (Sistema de gestión de distribución avanzada) de producción.

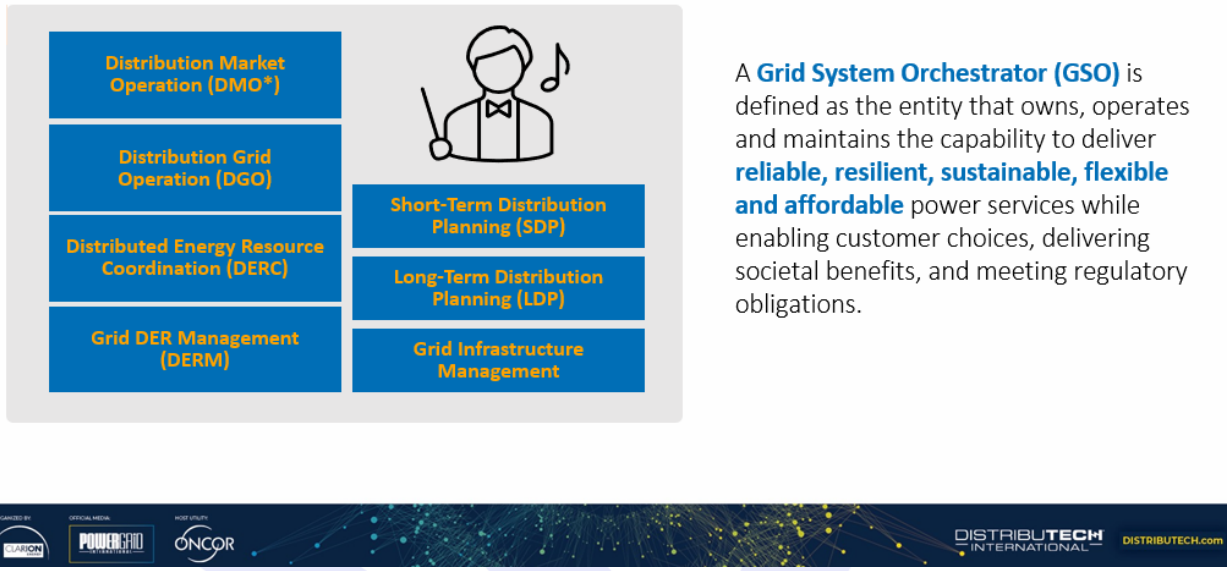
Como parte de la presentación sobresalen las siguientes lecciones aprendidas: la importancia de una solución DPF confiable para generar resultados FLISR consistentes, el papel del hardware, la priorización de casos de uso, la configuración constante del modelo, la necesidad de tener una forma predecible de manejar las violaciones y críticamente, darse cuenta de que, en algunos casos, proporcionar una solución no es tan beneficioso como comprender el problema central. En este aspecto, hicieron uso de un modelo basado en impedancia, de modo que conforme esta cambia se pueden determinar posibles puntos de falla, por ejemplo cuando las líneas de distribución están siendo interferidas por vegetación, lo que a efectos de la solución podría generar resultados no deseados.

Tal como se muestra en la figura anterior, conforme la solución DPF es más confiable, agiliza el análisis de transferencia de carga (resultados FLISR), lo que resulta en minutos adicionales de interrupción del servicio del cliente evitados y tiempos de restauración de interrupción más rápidos para el cliente. Esto ha permitido una mejora significativa del proceso que está ayudando a impulsar el cambio de cultura para respaldar las transferencias de carga como una herramienta de operaciones viable y eficaz.

Charla 13: Building a Sustainable Grid Transformation Strategy and Roadmap

La charla fue impartida por M. Joe Zhou, Director de Black & Veatch Management Consulting, LLC.

En la presentación se habla sobre cómo la empresa Consumers Energy se está preparando para sus metas al año 2040. Dentro de su plan contemplan la modernización de la red para convertirse en un Orquestador del Sistema de Red (GSO) y construir una Plataforma de Servicio de Red (GSP) para permitir las opciones de los clientes y brindar beneficios sociales sin dejar de lado la confiabilidad, así como cumplir con las obligaciones regulatorias.



La plataforma debe incentivar a todas las partes interesadas a conectarse y participar en las transacciones de la red para maximizar la creación de valor para todos. Para lograr el costo total de propiedad más bajo, el GSP debe ser abierto, interoperable, seguro, confiable, flexible y capaz de optimizarse en todos los niveles de participación en la red. La hoja de ruta de modernización de la red establecerá las inversiones necesarias para permitir el viaje de transformación de la red de las aplicaciones dispares y en evolución de hoy a las soluciones integradas y basadas en plataformas del mañana.

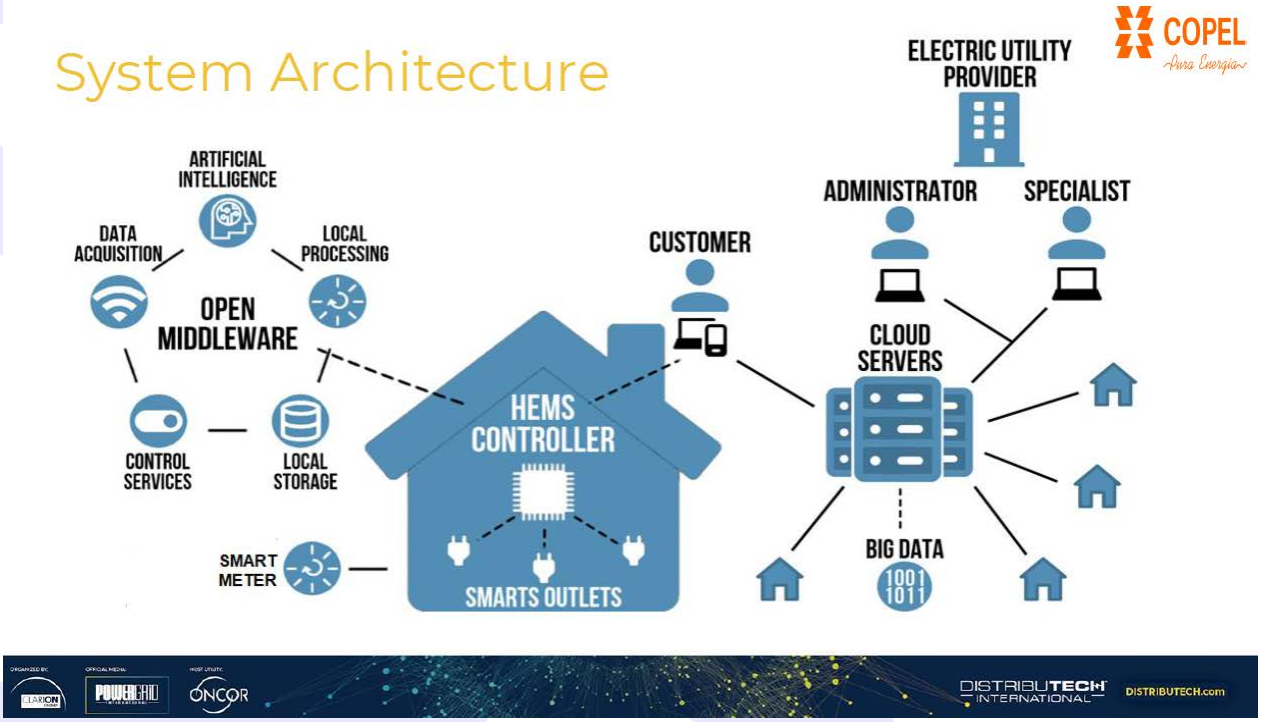
Las razones por las cuales Consumers Energy ha ideado esta postura se basan en:

- Aceleración de la transformación de la red: los objetivos e inversiones en energía limpia cambiarán fundamentalmente la forma en que se genera y distribuye la energía a los clientes, lo que acelerará la transformación de la red rápidamente.
- Desafíos de la red: el rápido aumento de la energía renovable presentará enormes desafíos para la planificación y las operaciones y se complicará aún más por los eventos climáticos extremos y otros problemas de resiliencia.
- Oportunidades: los avances de convergencia tecnológica están aquí para proporcionar nuevas capacidades, por lo que es más crítico alinear una visión de System Orchestrator con un enfoque de plataforma de servicios Grid. Habilitar las capacidades comerciales y técnicas para optimizar y orquestar la red en toda la cadena de valor de entrega de energía es fundamental para cumplir con los planes de energía limpia.
- Transiciones: ¿Cómo hacer la transición con un camino hacia la nueva red altamente automatizada y modular con nuevas tecnologías y configuraciones de sistemas? ¿Cómo probar tanto la tecnología heredada como la nueva y los equipos utilizados al mismo tiempo?

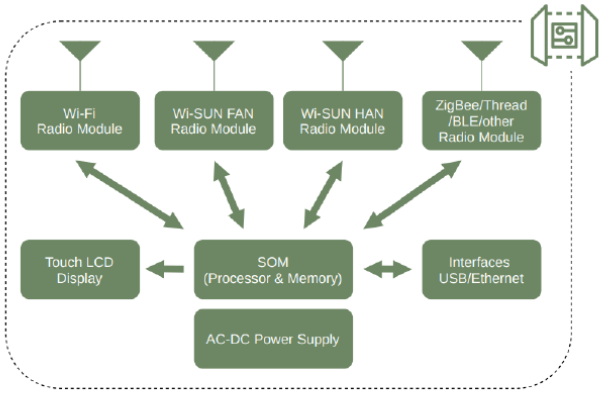
Charla 14: Development of a Home Energy Management System Based on WI-SUN/HAN Specification and Open Middleware

Esta charla fue impartida por Eduardo Lima, Gerente de Investigación y Desarrollo del El Dorado Research Institute.

En la sesión se expuso una solución de un sistema desarrollado para administrar los elementos de energía en el hogar.
Se propuso el siguiente modelo:

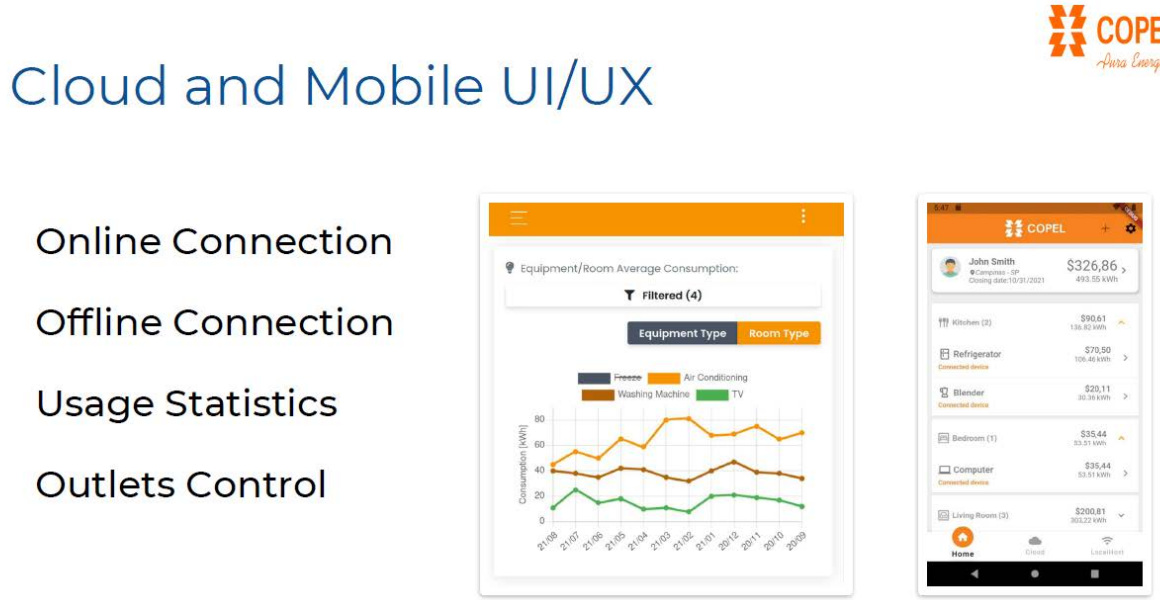


El punto clave para dar vida a este diseño consiste en la programación de un controlador, el cual básicamente es un dispositivo de acceso con interfases a diferentes tecnologías de comunicación, tal como se muestra en la siguiente figura:



HEMS CONTROLLER

Como parte innovadora del desarrollo, se hace una desagregación del consumo dentro del hogar, permitiendo al usuario controlar el gasto por dispositivo, tal como se muestra en la siguiente figura:



DISTRIBUTECH INTERNATIONAL DISTRIBUTECH.com

Según indica el expositor, la solución ha tenido buen recibimiento por parte de los clientes, continúan en el proceso de inteligencia para reconocer dispositivos del hogar de manera automática, y la iniciativa continúa con el objetivo de mejorar la experiencia del cliente y mejorar el ahorro energético, como parte de la responsabilidad social de la empresa con sus clientes y el ambiente. También se espera que el proyecto permita la respuesta a la demanda y la medición en tiempo real en el mediano plazo, una vez que la misma sea desplegada de manera más masiva.

Charla 15: How to Build Resilience and Adaptability in the Grids – Learnings from Major Utilities Across the Globe

La charla fue realizada por Anupam Chakraborty, quien es consultor para empresas de manufatura y de servicios públicos, bajo la firma Tata Consultancy Services en los Estados Unidos.

Se hace énfasis en que para mantener la red en funcionamiento las empresas deben realizar esfuerzos económicos importantes y de manera constante. Esta situación empeora cuando se dan condiciones climáticas severas y la invasión de vegetación en los corredores de conductores. Las condiciones deterioradas de los activos son las principales razones detrás de las fallas y apagones/caídas de tensión.
Las inspecciones proactivas de los activos de campo, la toma rápida de decisiones y la reparación/mantenimiento/reemplazo de estos con regularidad pueden prevenir este tipo de incidentes. Incluso las regulaciones obligan a las empresas de servicios públicos a hacerlo, pero desde la inspección hasta los trabajos de reparación necesarios para la gran cantidad de activos de campo en un tiempo programado es una tarea casi imposible de cumplir para una

empresa de servicios públicos, pues implicaría el gasto de enormes recursos en términos de mano de obra calificada y camiones, además del gasto de Capex en activos.
Las empresas de servicios públicos se enfrentan a la exigente tarea de prepararse para estas interrupciones y desarrollar resiliencia no solo en la infraestructura física sino también en la digital.

Al respecto TCS propone de manera concreta las siguientes acciones:

- Mapear activos
- Crear curvas de vulnerabilidad y mapas de calor de riesgo,
- Modelar escenarios detallados de impacto en la red física y el impacto económico
- Identificar medidas de resiliencia
- Implementar intervenciones de mitigación.

De esta forma indican se hace un uso más equilibrado e inteligente de los recursos, con un mayor nivel de efectividad sobre la resiliencia de la red eléctrica.

Visita al Stand Wi-SUN Alliance

En el stand de Wi-SUN Alliance se pudo observar una prueba de interoperabilidad entre productos de diferentes marcas que han obtenido la certificación WiSun. El laboratorio consiste de una malla donde existe comunicación entre los equipos y se presenta en vivo el flujo de datos a través de la aplicación WireShark. La prueba se encuentra funcionando a modo de laboratorio, en ambiente controlado.

Las marcas vistas en el stand son Renesas, Itron, Landys&Gir, exegin, texas intruments y ROHM Semiconductor.

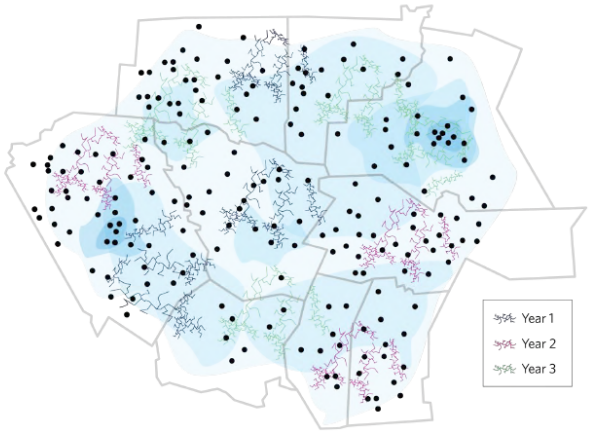
La evidencia de interoperabilidad permite el no depender estrictamente de una sola marca para el desarrollo de soluciones (medición, control, alumbrado), generando mayor competencia, con la posibilidad de mejores soluciones a menor costo.

Por último, se debe hacer un mapeo geográfico de las necesidades y una proyección de desarrollo por etapas en años.

Rollout Deployment by Geography

Understand the DA , DER communications, Next Gen. AMI, BTM Pilots, Substation SCADA, other programs roll-out schedule by geography by feeder by year
The colors represent role-out by year.

Whatever you can do to influence your Engineering Department to deploy by geography by year will generally provides more staff deployment efficiency and opens-up the use of more technology alternatives that require greater density (closeness) of assets by geography.



Conclusiones

La red de trabajo de campo debe adaptarse a los requerimientos técnicos de los servicios de TI y de TO soportados, siendo para ello necesario el uso de distintas tecnologías, aunque esta situación debe minimizarse para evitar una gestión compleja de la red.

Las redes de distribución tienen como tendencia su desarrollo basado en confiabilidad y resiliencia, gestión de los activos de campo y atención de infraestructura envejecida.

En el campo de la ciberseguridad, la nueva tendencia se conoce como Zero Trust, que significa cero confianza. Consiste en que todos los dispositivos conectados no deben ser considerados confiables, independientemente de que estos estén vinculados y verificados desde una red corporativa.

El intercambio de conocimiento con otros profesionales en el evento permitió visualizar desde otra óptica el desarrollo de las comunicaciones en la empresa, incluso poniendo en discusión la conveniencia de gestionar ciertos elementos de la red basado en la conveniencia y eficacia de las herramientas provistas por los fabricantes.

El desarrollo de la arquitectura de comunicaciones requiere de un alineamiento constante con la estrategia empresarial, y debe considerar los requerimientos específicos de las aplicaciones, así como sus planes de implementación en el corto, mediano y largo plazo.

El uso de modulación adaptativa tiene como objetivo la resiliencia cuando las condiciones climáticas no son favorables, sin embargo, debe validarse que esta característica se encuentre

certificada, pues está siendo desarrollada de manera distinta por varios fabricantes, lo que podría generar afectaciones negativas a la calidad de las redes actualmente desplegadas.

Recomendaciones

Basado en la tendencia de Zero Trust, evaluar en la CNFL las condiciones técnicas necesarias para su posible implementación, principalmente en servicios críticos, de modo que se asegure la continuidad y confiabilidad de los servicios.

Realizar de manera periódica un análisis de vulnerabilidades sobre los servicios de TI y de TO, que permitan de manera oportuna tomar acciones preventivas y evitar oportunidades de ataque que puedan ser explotadas en contra de los intereses de la empresa.

Evaluar la capacidad de las herramientas de gestión de la red de trabajo de campo de la CNFL para administrar elementos de forma masiva, considerando la complejidad, el tiempo de aprovisionamiento y el tiempo de recuperación ante fallas.

Realizar una actualización de la estrategia para el desarrollo de la arquitectura de infocomunicaciones, realizando el alineamiento con los nuevos requerimientos de la estrategia empresarial.

Evaluar la instalación de colectores a mayor altura en el área servida de la CNFL, ya que en Estados Unidos ha dado mejores resultados esta práctica.

Evaluación del evento

Distributech Internacional representa una excelente oportunidad para investigar sobre sobre el desarrollo de soluciones en el negocio de distribución eléctrica en un país de primer mundo. Es sumamente valioso conocer las tendencias del mercado en el desarrollo de las tecnologías, siendo esta retroalimentación recibida directamente de los fabricantes y por profesionales altamente competentes. El poder aplicar las mejores opciones para el mercado local, teniendo en consideración las condiciones y limitaciones propias del entorno genera un alto valor agregado. El intercambio de conocimientos con otros profesionales (social networking), permite formar un criterio más amplio ante la adopción e implementación de las tecnologías, discutiendo y argumentando sobre la razón de ser de los productos y sobre la conveniencia, factibilidad y facilidad de gestión de soluciones que los fabricantes ponen a disposición de los clientes. Las conferencias y los hubs donde se desarrolla el evento cuentan con todas las condiciones idóneas para un efectivo proceso de transferencia de conocimientos. Los expositores son profesionales especialistas en cada una de las áreas tecnológicas, con experiencia profesional demostrada en el campo tecnológico que lideran. Tal como queda explícito en el apartado anterior de conclusiones y recomendaciones, la actividad deriva gran valor agregado para el aprovechamiento a nivel de CNFL. En síntesis, el evento es de un alto nivel educativo y contribuye de manera significativa al crecimiento profesional del participante, y por ende beneficia a la empresa para la que trabaja.