2025

Plugfest

Testing Report

UBBA

Utility Broadband Alliance

Table of Contents

Executive Summary

Powering Utility Connectivity for a New Era

The utility industry is undergoing a dramatic transformation — and the 2025 UBBA Summit & Plugfest was where the future of grid communications came to life. Held November 4–6 in Charlotte, North Carolina, the event brought together utility leaders, innovators, and technology providers to test the next generation of utility broadband solutions in real-world conditions.

UBBA is the industry's leading collaboration for advancing private broadband networks, and Plugfest is its proving ground. This is where bold ideas become working systems, where interoperability is proven, and where utilities gain the confidence to deploy technologies that will define grid modernization for decades to come.

In 2025, Plugfest testing was not only technical — it was experiential. Demonstrations included audience participation, making the event both engaging and memorable while reinforcing the practical value of modern utility communications. The five participating teams proved that modern utility communications are no longer optional; rather, they are mission critical.

From smart meters and distributed energy resources to emergency response systems, the testing and demonstrations showed how resilient, high-speed connectivity is essential for the grid of the future.

The Value of Plugfest

UBBA Plugfest uniquely brings together utilities and solution providers to test technologies in realistic, operational environments — not in theory. Lab testing and live demonstrations help utilities understand how new technologies perform in the field, allowing them to make informed decisions on deployment strategies, network architecture, and future investments.

2025 Plugfest

The 2025 Plugfest centered on two strategic utility priorities that reflect the evolving communications needs of the modern grid: Mutual Aid Communications and IoT Innovations for Grid Modernization. Five teams demonstrated how private LTE networks can strengthen utility operations through real-world testing and live demonstrations.

Use Case 1: Mission-Critical Communications for Mutual Aid

These teams focused on ensuring mutual aid crews remain connected during major outages or natural disasters — when communication is most critical. Testing highlighted how eSIM technology enables seamless switching between private and public networks, and how handheld radios and smartphones can stay interoperable across different utility systems.

Key Activities:

- eSIM profile development and multi-network provisioning
- Lab testing and validation of network switching
- Live demonstration of MCPTT and P25-to-P25 interoperability

Use Case 2: Internet of Things (IoT) Innovations

These teams explored how utilities can modernize the grid through advanced IoT connectivity, including AMI 2.0 and next-generation device deployments. Testing focused on LTE-M (Cat-M1) and emerging 5G RedCap/eRedCap technologies, and evaluated how private, public, and hybrid networks can coexist to support large-scale IoT deployments.

Key Activities:

- Coexistence testing of low-power IoT devices and standard LTE users
- Secure, reliable connectivity under heavy network load and outages
- Real-time monitoring of grid equipment and automated response systems

Special thanks to the 2025 UBBA Plugfest Steering Committee:

To guide and support the efforts of the Plugfest teams, UBBA engaged a steering committee for the oversight and to focus on the needs of the utilities. The 2025 Plugfest Steering Committee was an eight-vote committee tasked to help with the decision-making processes of the 2025 Plugfest Report.

- Bobbi Harris, UBBA Executive Director
- Jeff Livingston, Salt River Project
- Dean Newcomb, Xcel Energy
- Tom Bedics, Southern Linc
- Juan Macias, Duke Energy
- Hemat Relan, Nokia
- Kevin Linehan, Ericsson
- Jason McClanahan, Anterix

The Process

At the start of each year, the UBBA Plugfest Task Force initiates the planning and brainstorming phase to define the focus of the Plugfest demonstrations for the annual UBBA Summit & Plugfest conference. Comprising UBBA member utilities and solution providers, the task force collaboratively identifies key use cases to be tested, ensuring that these efforts align with the strategic needs of the utility sector. By focusing on relevant and impactful use cases, the task force ensures that the testing process delivers valuable insights and tangible benefits to utilities, fostering innovation and driving progress in the utility industry.

Given UBBA's emphasis on collaboration, the Plugfest Committee oversaw an extensive review process, considering proposals from many vendor teams, and narrowed the participation down to the 2025 Plugfest teams identified in this paper.

Each team worked together for months developing test plans, defining parameters, and executing tests in various team members' labs. Each team observed and recorded all testing results and lessons learned, which was presented during the 2025 UBBA Summit & Plugfest conference.

The value of Plugfest is the ability of the utility and vendor communities to collaborate and push technology forward to benefit the modernization of the electrical grid. By combining resources, such as lab spaces, utilities can evaluate and gain understanding about various technologies that support their missions. The results in this report are presented in a "raw" state, meaning that the use case teams have compiled these summaries and submitted them to the UBBA leadership to be included in this report. UBBA has only guided the writing of the individual reports. Each team's testing report stands alone with respect to any background materials, perspectives and personal conclusions.

Live testing at the 2025 UBBA Summit & Plugfest in Charlotte allowed attendees to interact with the teams, ask follow-up questions from lab tests, and experience live tests in real time.

2025 UBBA Plugfest Testing Results

This year's effort focused on two use cases: Mission-Critical Communications for Mutual Aid and IoT Innovation. The results of these multi-month efforts are detailed in the following sections.

Use Case 1: Mission-Critical Communications for Mutual Aid

There is a need to improve how mutual aid crews stay connected during major emergencies or crises. This use case encompasses tests that demonstrate how integrating private networks with public networks enables mutual aid crews from different utilities to maintain connectivity and seamless communications during major emergencies, even if infrastructure goes down.

Team: Interoperability Igniters

Verizon, Motorola, L3Harris, Thales, Anterix, Black & Veatch, SDGE, Xcel Energy, Nokia

Overview

This team explored the integration of public and private wireless networks, specifically focusing on how devices handle switching networks during a disaster. The Interoperability Team's tests demonstrate how private LTE can support field operations under realistic conditions.

Overarching Framework

Scenario

The Interoperability Igniter's Plugfest testing fits within a mutual aid scenario of three phases:

- Blue Sky
- Dark Sky
- Private Wireless

The "Blue Sky" phase is when mutual aid crews prepare for the disaster. The crews are not in the disaster area yet, and operating conditions are normal. During the Blue Sky phase, mutual aid crews can connect to a nationwide Public Network with the additional option to utilize Satellite SMS

(the ability for a cellphone to connect directly to a satellite is defined in 3GPP as the NTN specification[1]).

The "Dark Sky" phase is when mutual aid crews are in the disaster area and emergency protocols are in place. During the Dark Sky phase, visiting mutual aid crews can connect to the host utility's Private Network to support mission-critical communications. However, if the host utility's private network were to become unavailable (i.e., fail), mutual aid crews can switch back to using a Public Network connection via priority and preemption cellular services (e.g., Frontline[2], Critical Connect[3]) or deployable Cells on Wheels (CoWs).

The "Private Wireless" phase is when mutual aid crews are working in the disaster area and are connected to the Private Network; mutual aid crews are reliant on the Private Network for mission-critical communications during this phase.

Key Infrastructure

The Interoperability Igniters' Plugfest testing leveraged a combination of commercial devices, private wireless infrastructure, MCX application platforms, and SIM/eSIM profile-management tools to replicate realistic mutual-aid operating conditions.

The following infrastructure elements were used to execute these test cases:

- Nokia Core
- Nokia n48, B106 and n26 radios
- Samsung/Zebra/L3Harris Radios, SAR HMc Devices
- Verizon / P-WLS Network SIM Cards
- Thales SGP.32 SIM OTA Management platform
- Motorola and L3H MCX Clients

Plugfest Testing: Performing MCX on Public Wireless and Private Wireless

"MCX" broadly refers to mission-critical talk, data, and voice services. MCX encompasses mission-critical push-to-talk (MCPTT), mission-critical data (MCData), and mission-critical video (MCVideo).

In the context of the Interoperability Igniter's test cases, "Performing MCX" specifically refers to the following MCX activities/services: onboarding/activation, one-to-one calls, talk groups, videos and texts, priority and preemption (only applicable to Dark Sky conditions/tests), and monitoring/observing MCX users and services via a command center.

[1] https://www.3gpp.org/technologies/ntn-overview
[2] https://www.verizon.com/business/solutions/public-sector/public-safety/
[3] https://www.motorolasolutions.com/en_us/products/command-center-software/broadband-ptt-and-lmr-interoperability/critical-connect.html

Test Case #1: Performing MCX via Motorola's Broadband PTT on Verizon's Public Network During Blue Sky & Dark Sky Conditions

"Broadband Push-to-Talk[4] (PTT)" generally refers to the PTT solution that enables users on a cellular network to exchange instant voice communications over broadband networks using smart devices, rather than traditional radios. Broadband PTT is a 3GPP standard-compliant solution that can run on any carrier's network.

In the context of this test case, "Broadband PTT" specifically refers to Motorola's Broadband PTT solution that runs on Verizon's Public Network. To clarify, only the voice portion of mission-critical services are delivered via Broadband PTT. MCData and MCVideo are delivered using standard broadband data paths (not PTT).

Purpose/Objective

To determine if smartphones connected to Verizon's Public Network can successfully access the MCX system and perform MCX via broadband/Broadband PTT during both Blue Sky (normal) and Dark Sky (disaster) conditions.

NOTE: Priority determines which user traffic "goes first" when the network is busy, while preemption determines which users get "kicked off" first when there isn't enough network capacity. Since priority-based traffic handling cannot be meaningfully evaluated during Blue Sky (normal) conditions, priority and preemption are excluded from Phase 2 of this test case. Priority and preemption are included in Phase 3, as Dark Sky (disaster/emergency) conditions indicate heavy traffic and network congestion.

Test Infrastructure/Environment

- Verizon Public Network
- Smartphones
    - Android Samsung Galaxy S22, S23, S24 Android 14, Band 26)
    - iPhone (IoS, Band 26)
- Verizon Frontline IoT devices
    - Semtech (Sierra Wireless) AirLink XR60/XR90/XR80/RX55
- Motorola's Broadband PTT solution
- MCX user credentials provisioned prior to testing
- Pre-configured priority and preemption policies for MCX users in the MCX system and the public network
- MCX client application
- Laptop for testing

[4] https://www.motorolasolutions.com/en_xa/solutions/what-is-broadband-push-to-talk.html

Demonstration Flow

Phase 1: Initial Configuration

- MCX user accounts are created and configured in the MCX system backend, including:
  - User roles and credentials (including priority and preemption user policies),
  - Authorizing access to MCX services, and
  - Assigning talk groups compatible with Broadband PPT.
- The MCX client application is installed on each test device (smartphone) and configured to operate alongside Motorola's Broadband PTT solution.
- Each smartphone is logged into the MCX client app and is associated with an MCX user account.
- The smartphones are connected to the Verizon Public Network.

Phase 2: Blue Sky

- MCX services are attempted using the MCX client application installed on the smartphones connected to the Verizon Public Network.

Phase 3: Dark Sky

- Dark Sky (disaster/emergency) operating conditions are simulated.
- Priority-enabled MCX users evaluate smartphone connectivity to Verizon's Public Network; maintained connection is confirmed.
- Priority-enabled MCX users evaluate access to the MCX client application and assigned talk groups; maintained access is confirmed.
- An increase in non-priority network traffic is simulated; Verizon's Public Network is congested.
- MCX services are attempted by priority-enabled users via the MCX client application installed on the smartphones connected to Verizon's congested Public Network.
- Priority-enabled MCX users evaluate access to MCX services via the MCX client application; non-priority traffic is preempted as necessary and maintained access is confirmed.

Results

- Initial configurations and MCX onboarding/activation were successful: MCX user accounts were successfully created/configured, the MCX client application was successfully installed on each smartphone, each smartphone successfully logged into a MCX user account, and each smartphone successfully connected to Verizon's Public Network.
- MCX was successfully performed via the MCX client application on the smartphones connected to the Verizon Public Network during Blue Sky and Dark Sky conditions:
  - Participation in talk group calls and one-on-one calls via Broadband PTT was successful.
  - Video sessions and texting between smartphones were successful.
  - MCX service behavior and user presence were successfully observed through the Command Center.

- During Dark Sky conditions, priority and preemption capabilities on Verizon's Public Network were observed through the Command Center; priority and preemption functionality worked as expected.

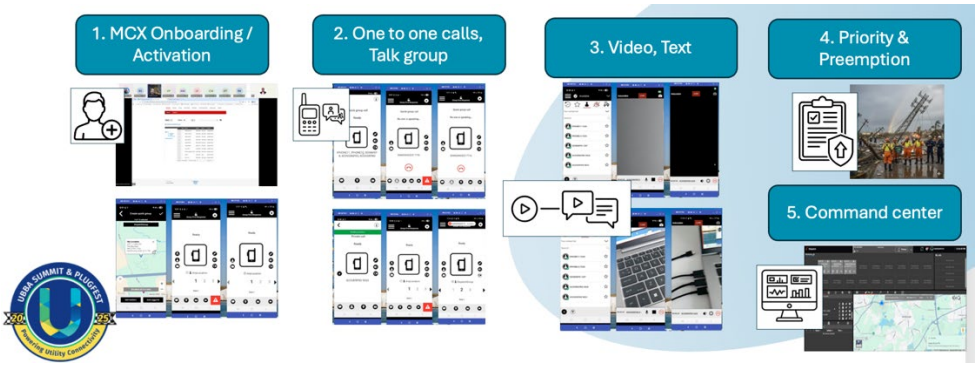

Figure 1 - Performing MCX on Verizon's Public Network During Blue Sky & Dark Sky

Benefits, Lessons, & Takeaways

- Commercially available smartphones can support mission-critical communications during both Blue Sky and Dark Sky conditions. This test case showcases how mutual aid crews can use their own smartphones to perform MCX services via the MCX client application while connected to a Public Network.
- Delivering MCX services via Broadband PTT over a Public Network eliminates the need for traditional LMR radios.
- A comprehensive guide to Motorola's Broadband PTT solution[5] is available online for free.
    - Chapter 15: Quality of Service (QoS), Priority and Preemption (QPP) is suggested as a key area for review and analysis.
- Motorola's Broadband PTT solution provides access to priority and preemption capabilities via feature sets and QPP packages. Feature sets define user abilities (e.g., call types), and QPP packages define user priority levels.
- Figure 2 shows the priority and preemption capabilities of Broadband PTT's three feature sets (Collaboration, Command, MCPTT), and how those capabilities apply across different call types. Column 2 (Default) indicates the baseline priority and preemption capabilities before a feature set is applied, Column 3 (Silver) represents Broadband PTT's Collaboration feature set, Column 4 (Gold) represents the Command feature set, and Column 5 (Platinum) represents the MCPTT feature set.

Call Type	Default	Silver	Gold	Platinum
Private Call - PTT User	Default	Default	Default	Level 1
Talkgroup call	Default	Default	Level 1	Level 2
Broadcast talkgroup call	Default	Level 1	Level 2	Level 3
Emergency call	Level 1	Level 2	Level 3	Level 4
Ambient Listening call	Level 1	Level 2	Level 3	Level 4

Figure 2 - Priority and Preemption Capabilities Across Broadband PTT Feature Sets and Call Types

[5] https://www.verizon.com/content/dam/support/pdf/ptt-plus/Verizon_KODIAK_R12.3_Broadband_PTT_Product_Specification%20VZUG4880424.pdf

- Priority and preemption capabilities ultimately depend on which QoS Class Identifiers (QCIs) are used in LTE/5G networks, as QCIs define how different types of traffic are treated by the network. Figure 3 shows the behavior of each QCI value used in LTE/5G networks. These characteristics determine how the network prioritizes/schedules different types of traffic.

QCI	Resource Type	Priority	Packet Delay Budget	Packet Error Loss Rate	Example Services
1	GBR	2	100ms	10^{-2}	Conversational Voice
2	GBR	4	150ms	10^{-3}	Conversational Video (Live Streaming)
3	GBR	3	50ms	10^{-3}	Real Time Gaming, V2X messages
4	GBR	5	300ms	10^{-6}	Non-Conversational Video (Buffered Streaming)
65	GBR	0.7	75ms	10^{-2}	Mission Critical user plane Push To Talk voice
66	GBR	2	100ms	10^{-2}	Non-Mission-Critical user plane Push To Talk voice
67	GBR	1.5	100ms	10^{-3}	Mission Critical Video user plane
75	GBR	2.5	50ms	10^{-2}	V2X (Vehicle-to-everything) messages
5	non-GBR	1	100ms	10^{-6}	IMS Signalling
6	non-GBR	6	300ms	10^{-6}	Video (Buffered Streaming) TCP-Based (for example, www, email, chat, ftp, p2p ...)
7	non-GBR	7	100ms	10^{-3}	Voice, Video (Live Streaming), Interactive Gaming
8	non-GBR	8	300ms	10^{-6}	Video (Buffered Streaming) TCP-Based (for example, www, email, chat, ftp, p2p...)
9	non-GBR	9	300ms	10^{-6}	Video (Buffered Streaming) TCP-Based (for example, www, email, chat, ftp, p2p and the like). Typically used as default carrier
69	non-GBR	0.5	60ms	10^{-6}	Mission Critical delay sensitive signalling (e.g., MC-PTT signalling)
70	non-GBR	5.5	200ms	10^{-6}	Mission Critical Data (e.g. example services are the same as QCI 6/8/9)

Figure 3 - QCI Characteristics Reference

- Consider the following Key Performance Indicators (KPIs) in Figures 4 and 5 that are essential for evaluating MCX service reliability:

MOS	Characteristics
5	• Excellent • Like face-to-face or radio reception
4	• Good • Imperfections can be perceived, but sound is still clear
3	• Upper range (3.8+) considered acceptable • Mid-to-lower range considered fair-to-annoying with CX risk
2	• Poor, difficult to understand the caller • Annoying, distracting
1	• Bad, very difficult to understand the caller • Difficulty handling the call efficiently or achieving resolution

Expected VoIP Range 3.5-4.2

Figure 4 - Mean Opinion Score (MOS) Ratings for Voice Quality

MCPTT KPIs	Threshold	Likelihood	LTE Packet Delay Budget
MCPTT KPI 1 – Access Time	< 300 ms	95% of all MCPTT requests	< 60 ms
MCPTT KPI 1 – Access Time (Emergency)	< 300 ms	99% of all MCPTT requests	< 60 ms
MCPTT KPI 2 – End-to-End Access Time	< 1000 ms	N/A	< 60 ms
MCPTT KPI 3 – Mouth-to-Ear Latency	< 300 ms	95% of all voice bursts	< 75 ms
MCPTT KPI 4 – Late Call Entry Time (encrypted calls)	< 350 ms	95% of all Late Call entries	< 60 ms
MCPTT PESQ	MOS-LQO ≥ 3.0	N/A	N/A
MCPTT POLQA	MOS-LQO ≥ 3.0	N/A	N/A

Figure 5 - Performance Targets for Reliable MCX Services

- These results establish a baseline for seamless transition from public-network Broadband PTT to private-network MCX services.

Test Case #2: Performing MCX via Motorola's MCX Client Application on Nokia's Private Network During Dark Sky Conditions

SGi and Rx generally refer to network interfaces that connect a cellular network to external applications. In the context of this test case, SGi and Rx are the interfaces connecting Nokia's Private Network to Motorola's MCX client application.

The SGi interface represents the data path that carries Motorola's MCX client application traffic (e.g., voice, messages, and video). The Rx interface represents the "signage" associated with that path, indicating how the traffic should be treated by the network (i.e., priority and preemption).

Purpose/Objective

To determine if Motorola's MCX client application can successfully interoperate with Nokia's Private Wireless (PWLS) Network to perform MCX.

Test Infrastructure/Environment

- Nokia Private Wireless Network
- Utility-style private spectrum configuration (e.g., 3–5 MHz scenarios)
- Motorola's MCX client application
- Rx and SGi interfaces
- Preloaded Nokia Private Network eSIM profile
- Android smartphones
  - Zebra TC58e (Android 14, Band 106)
  - Ecom Smart EX-02 (Android 11, Band 8)
- IoT Devices
  - Sierra Wireless LX60 (Band 8)

Demonstration Flow

Phase 1: Initial Configuration

- Rx and SGi interfaces are enabled to support MCX.
- The Motorola MCX client application is integrated with Nokia's Private Network; connectivity between the Nokia core and Motorola's MCX servers is confirmed via the Rx and SGi interfaces.
- MCX user accounts are created and configured in Motorola's MCX client application system backend, including:
    - User roles and credentials (including priority and preemption user policies),
    - Authorizing access to MCX services, and
    - Assigning talk groups.
- Motorola MCX client application is sideloaded[6] onto test devices (smartphones).
- The smartphones are attached to Nokia's Private Network.
- IP connectivity between smartphones, the Nokia core, and Motorola's MCX client application is confirmed.

Phase 2: Dark Sky

- Dark Sky (disaster/emergency) operating conditions are simulated.
- Priority-enabled MCX users evaluate smartphone connectivity to Nokia's Private Network; maintained connection is confirmed.
- Priority-enabled MCX users evaluate access to Motorola's MCX client application and assigned talk groups; maintained access is confirmed.
- Constrained network conditions are simulated by limiting available bandwidth to 3-5 MHz on Nokia's Private Network.
- MCX services are attempted by priority-enabled users via Motorola's MCX client application installed on the smartphones connected to Nokia's constrained Private Network.
- Priority-enabled MCX users evaluate access to MCX services via Motorola's MCX client application; non-priority traffic is preempted as necessary and maintained access is confirmed.

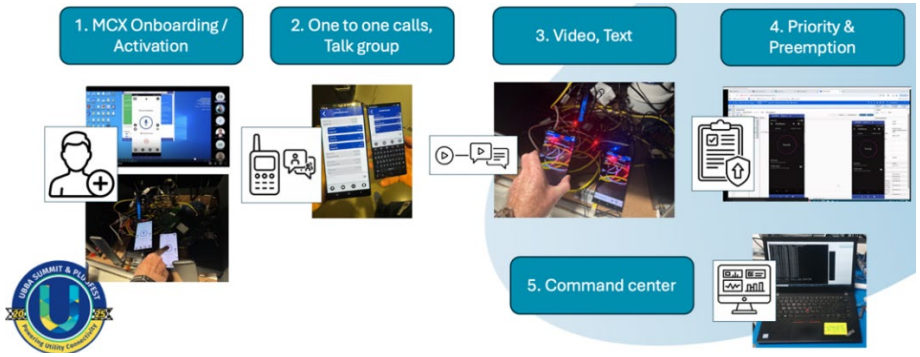

Figure 6 - Performing MCX via Motorola's MCX Client Application on Nokia's Private Network During Dark Sky

[6] https://www.scienceopen.com/document_file/cc3e94ba-632c-49f4-84af-566fa82b28d4/ScienceOpen/027_Goodwin.pdf?utm_source=consensus

Results

- Initial configurations and MCX onboarding/activation were successful: Rx and SGi interfaces were successfully enabled, Motorola's MCX client application was successfully integrated with Nokia's Private Network, MCX user accounts were successfully created/configured in Motorola's MCX system backend, Motorola's MCX client application was successfully sideloaded onto each smartphone, each smartphone successfully connected to Nokia's Private Network, and IP connection between the smartphones, Nokia core, and Motorola's MCX client application was also successful.
- Motorola's MCX client application successfully interoperated with Nokia's Private Network.
- MCX services operated correctly on private wireless. MCX was successfully performed via Motorola's MCX client application on the smartphones connected to Nokia's Private Network during Dark Sky conditions:
    - Participation in talk group calls and one-on-one calls was successful.
    - Video sessions and texting between smartphones were successful.
    - MCX service behavior and user presence were successfully observed through the Command Center.
- Priority and preemption capabilities on Nokia's Private Network were observed through the Command Center; priority and preemption functionality worked as expected.
- Testing showed that MCX services can reliably support voice, video, and data even in constrained spectrum scenarios (e.g., 3–5 MHz), highlighting the feasibility of deploying mission-critical communications on utility-owned spectrum such as 900 MHz.

Benefits, Lessons, & Takeaways

- This test case demonstrates how a mutual aid crew can effectively utilize a private wireless network to perform MCX during an emergency.
- No vendor lock-in issues were observed at the MCX client application level.
- Correct/proper onboarding of MCX users is essential. User provisioning, authentication, and SIM/profile switching must be correctly configured so users can connect to the network with recognized priority.
- While lab/sandbox testing might not reveal any issues, real-world capacity and load patterns differ. Commercial scalability testing is critical.
- Figure 7 provides network capacity estimates under ideal conditions. The 2 columns on the right indicate how many MCX voice or video users can be simultaneously supported per cell at different bandwidths, based on their required bitrates, without degrading performance. 3 and 5 MHz bandwidths are realistic for private networks.
  NOTE: A cell refers to a coverage area of the network; it is the area covered by a single cell tower.

MCX Service	Bitrate per User	3 MHz Network Capacity (number of users/cell)	5 MHz Network Capacity (number of users/cell)
Voice	50 kbps	60-80	100-120
Video	200 kbps	31	54

Figure 7 - Estimated MCX Capacities per Limited Bandwidths

- Utilities can use Table 1 to get an idea of whether additional bandwidth is needed to support their MCX users. However, actual capacity depends on factors such as user distribution, simultaneous use, background traffic, and other loading conditions. Devices closer to the cell's center (i.e., the tower) have a stronger/more reliable connection to the network and use fewer resources, while devices further from the cell's center have a weaker/less reliable network connection and use more resources. Therefore, if most users are at the cell edge, the network can support fewer simultaneous users.

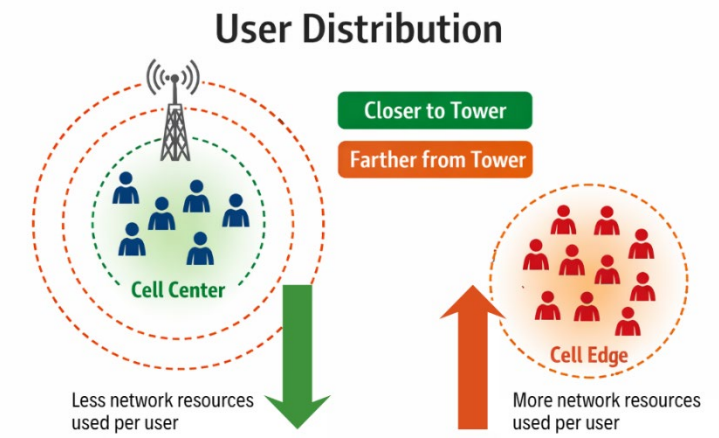

Figure 8 - User Distribution Impact on Network Resources

- Priority and preemption capabilities are critical for ensuring mission-critical users maintain service under constrained conditions.

Test Case #3: Performing MCX via L3Harris's MCX Client Application on Nokia's Private Network During Dark Sky Conditions

L3Harris's MCX client application (Two47) serves as the interoperability bridge between traditional LMR systems and modern devices and enables two-way PTT communications on any Android device.

L3Harris's MCX client application also includes a MCX Dispatch client application that can be installed on any Windows computer and enables Dispatch to communicate with any device via voice calls (both one-to-one calls and calls within assigned talk groups).

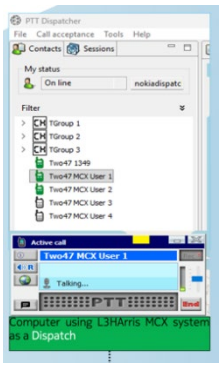

Figure 9 – L3Harris's Windows Dispatch Client

Purpose/Objective

To determine if L3Harris's MCX client application and MCX Dispatch client application can successfully interoperate with a local Wi-Fi network, Verizon's Public Network, and Nokia's Private Wireless (PWLS) Network to perform MCX.

Test Infrastructure/Environment

- Wi-Fi network
- Verizon's Public Network
- Nokia Private Wireless Network
- Rx and Sgi interfaces
- Preloaded Nokia Private Network eSIM profile
- Windows computer
- L3Harris's MCX client applications (i.e., Two47):
    - MCX Smartphone client application (for smartphones)
    - MCX Dispatch client application (for Windows)
- Android smartphones
    - Samsung Galaxy S22 (B26)
    - Zebra TC58e (Android 14, Band 106)
    - Ecom Smart EX-02 (Android 11, Band 8)

Demonstration Flow

Phase 1: Initial Configuration

- Rx and Sgi interfaces are enabled to support MCX.
- The L3Harris MCX client application is integrated with the local Wi-Fi network, Verizon's Public Network, and Nokia's Private Network; integrated connectivity is confirmed via the Rx and Sgi interfaces.
- MCX user accounts are created and configured in the L3Harris's MCX client application system backend, including:
    - User roles and credentials (including priority and preemption user policies),
    - Authorizing access to MCX services, and
    - Assigning talk groups.
- The L3Harris MCX client application is sideloaded onto test devices (smartphones), and L3Harris's MCX Dispatch client application is installed on the Windows computer.

Phase 2: Wi-Fi Network

- The smartphones are connected to the local Wi-Fi network.
- IP connectivity between smartphones, the Wi-Fi network, and L3Harris's MCX client application is confirmed.
- MCX services are attempted using L3Harris's MCX client application installed on the smartphones connected to the local Wi-Fi network.

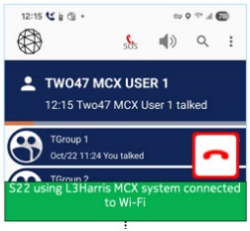

Figure 10 – Using L3Harris's MCX Client Application via Wi-Fi

Phase 3: Public Network

- The smartphones are connected to Verizon's Public Network.
- IP connectivity between smartphones, Verizon's Public Network, and L3Harris's MCX client application is confirmed.
- MCX services are attempted using L3Harris's MCX client application installed on the smartphones connected to Verizon's Public Network.

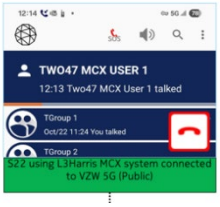

Figure 11 – Using L3Harris's MCX Client Application via Public Network

Phase 4: Private Network

- The smartphones are connected to Nokia's Private Network.
- IP connectivity between smartphones, Nokia's Private Network, and L3Harris's MCX client application is confirmed.
- Dark Sky (disaster/emergency) operating conditions are simulated.
- Priority-enabled MCX users evaluate smartphone connectivity to Nokia's Private Network; maintained connection is confirmed.
- Priority-enabled MCX users evaluate access to L3Harris's MCX client application and assigned talk groups; maintained access is confirmed.
- Constrained network conditions are simulated by limiting available bandwidth to 3-5 MHz on Nokia's Private Network.
- MCX services are attempted by priority-enabled users via L3Harris's MCX client application installed on the smartphones connected to Nokia's constrained Private Network.

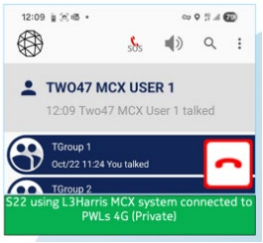

Figure 12 – Using L3Harris's MCX Client Application via Private Network

- Priority-enabled MCX users evaluate access to MCX services via L3Harris's MCX client application; non-priority traffic is preempted as necessary and maintained access is confirmed.

Results

- Initial configurations and MCX onboarding/activation were successful: Rx and Sgi interfaces were successfully enabled; L3Harris's MCX client application was successfully integrated with the local Wi-Fi network, Verizon's Public Network, and Nokia's Private Network; MCX user accounts were successfully created/configured in L3Harris's MCX system backend; L3Harris's MCX client application was successfully sideloaded onto each smartphone; L3Harris's MCX Dispatch client application was successfully installed on the Windows computer.
- Devices successfully connected to the local Wi-Fi network/Verizon's Public Network/Nokia's Private Network; IP connection between the devices, the Wi-Fi network/Verizon's Public Network/Nokia's Private Network, and L3Harris's MCX client application was also successful.
- L3Harris's MCX client application and MCX Dispatch client application successfully interoperated with the local Wi-Fi network, Verizon's Public Network, and Nokia's Private Network.
- MCX was successfully performed via L3Harris's MCX client application and Dispatch client application on the devices connected to the local Wi-Fi network/Verizon's Public Network/Nokia's Private Network:
    - Participation in talk group calls and one-on-one calls was successful.
    - Video sessions and texting between smartphones were successful.
- Priority and preemption capabilities and functionality were successful and worked as expected.

Benefits, Lessons, & Takeaways

- This test case demonstrates how a mutual aid crew can effectively utilize Wi-Fi, public, and private networks to perform MCX during an emergency.
- No vendor lock-in issues were observed at the MCX client application level.

Test Case #4: Public and Private Network Switching with SGP.32

SGP.32[7] refers to the GSMA's latest standard for remotely managing eSIM profiles on IoT devices; the standard introduces built-in triggers and rules that enable devices to automatically deploy new profiles. Under SGP.32, eIM/SM-DP+/DP+ servers and devices with eSIM cards can trigger profile "pull" requests, download and configure new profiles, and switch between active profiles without any manual intervention.

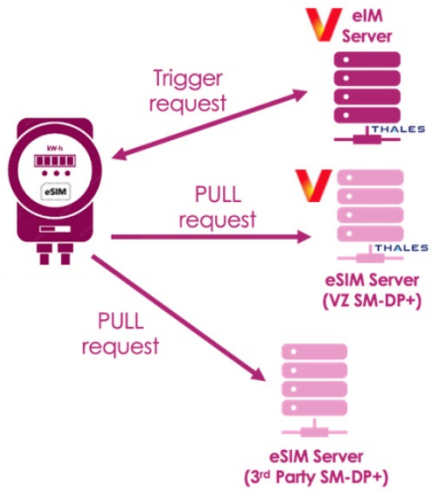

Figure 13 – GSMA SGP.32 Profile Deployment

Purpose/Objective

To determine if a device that is connected to a private network will automatically switch to a public network if the private network goes down, and if the device will successfully switch back to the private network when the private network is restored.

Test Infrastructure/Environment

- SGP.32 SIM OTA platform
- Configured network switching timer (set to 2 minutes)
    - ***NOTE:*** While the timer duration can be altered (e.g., 4 minutes, 10 minutes, 1 hour, 2 hours, 4 hours, etc.), typical industry practice is to wait 2 minutes before switching to another network.
- SM-DP+ / DP+ servers
- Simulated outage
- eUICC configuration:
    - 5G Private Network Nokia Profile preloaded
    - 5G Public Network Verizon Profile preloaded
- Nokia Core and Radio Access Network
- Samsung and Zebra devices with Verizon and Nokia P-WLS SIM cards with profiles

[7] https://www.gsma.com/solutions-and-impact/technologies/esim/gsma_resources/sgp-32-v1-2/

Demonstration Flow

Phase 1: Profile Configuration

- The Utility (Nokia) Private 5G Network is set as the primary/active eSIM profile on the device (as defined in the prioritized Public Land Mobile Network [PLMN] list).
- The Verizon Public 5G Network is set as the secondary/failover eSIM profile on the device (as defined in the prioritized PLMN list).

Phase 2: Outage Simulation

- The device is latched to the Utility (Nokia) Private 5G Network; connectivity is confirmed.

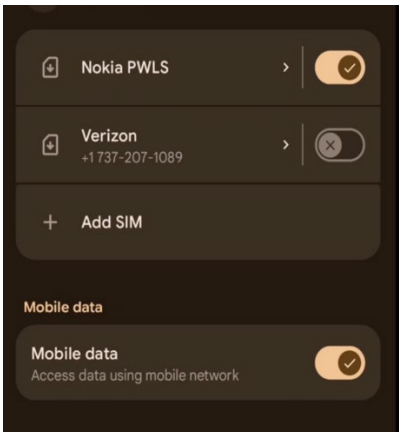

Figure 14 - Device Connected to Private Network

- The Utility (Nokia) Private 5G Network is temporarily disabled and goes “down”; connectivity is lost.

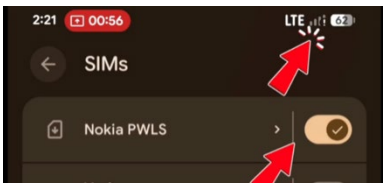

Figure 15 - Lost Connection to Private Network

- A network profile switch is triggered by the lost connection/an event from the card.
- The device automatically switches to the Verizon Public 5G Network profile; connectivity is confirmed.

Figure 16 - Device Connected to Public Network

Phase 3: Restoration Simulation

- The device is still connected to the Verizon Public 5G Network.
- The Utility (Nokia) Private 5G Network is restored and comes back “up”.
- The device reverts its connection to the Utility (Nokia) Private 5G Network from the Verizon Public 5G Network via a pre-defined timer; connectivity is confirmed.

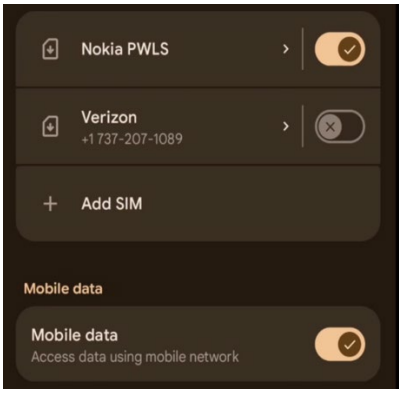

Figure 17 - Device Connection Reverted to Private Network

Results

- When the private Nokia network went down, the device successfully switched over to the public Verizon network via SGP.32.

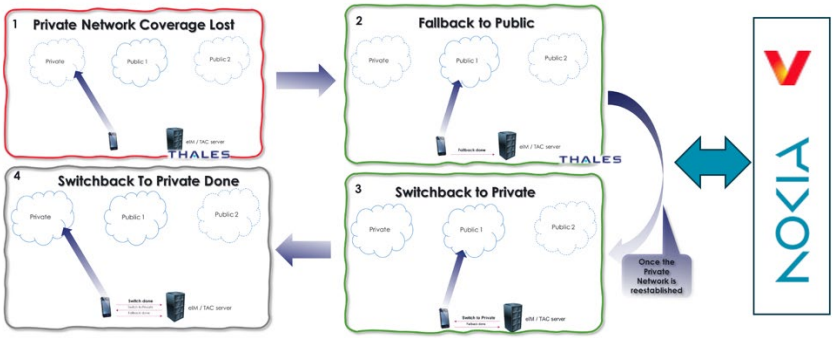

Figure 18 - Network Switching: Private > Public > Private

- When the private Nokia network went down, the device automatically switched to the Verizon Public 5G Network profile within 2 minutes (depending on the device).

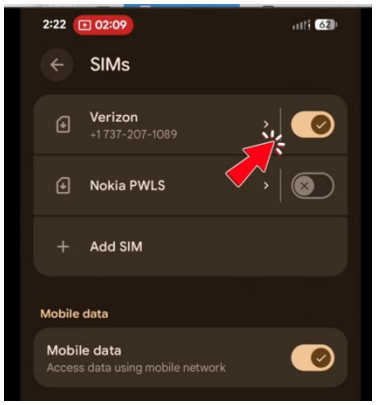

Figure 19 – Connection Time to Public Network

Benefits, Lessons, & Takeaways

- Utilities are seeking a seamless transition from Private to Public 5G networks and vice versa. Automatic failovers promote network resiliency and thus represent a key use case of significant interest to utility providers.
- Using SGP.32 in a SaaS model allows utilities to avoid capital expenditures and reduces the effort required for platform operations and maintenance.
- SGP.32 does not require connectivity to the PWLS network; it only needs the SIM card profile information. This eliminates the need to extend the PWLS network outside the utility datacenter, reducing potential security risks.
- Waiting 2 minutes before switching between networks helps avoid high signaling loads between networks.
- SGP.32 also allows manual network switching.

Overall Lessons & Takeaways

- **Public and private wireless networks are complementary, not competitive.** Plugfest testing confirmed that resilient mission-critical communications for utility mutual aid are best achieved through a layered approach that combines nationwide public wireless coverage with localized private wireless networks. Together, they provide continuity across Blue Sky, Dark Sky, and Private Wireless operating conditions.
- **Standards-based MCX interoperability is production-ready.** Mission-critical voice, data, and video services successfully interoperated across multiple MCX platforms, device types, and network environments. This demonstrates that 3GPP-based MCX solutions can support real-world mutual aid operations without vendor lock-in.
- **Commercial smartphones can support mission-critical operations.** Ruggedized, commercially available Android devices successfully delivered MCX services across public, private, and Wi-Fi networks. This reduces dependence on specialized hardware and enables mutual aid crews to use familiar devices while maintaining mission-critical performance.
- **Priority and preemption are foundational, not optional.** Across both public and private networks, priority and preemption were essential for maintaining MCX service availability under congested and constrained conditions. Proper priority and preemption configuration and validation should be treated as a core design requirement for any utility MCX deployment.
- **Capacity planning must go beyond lab assumptions.** While lab and sandbox testing validates functionality, real-world performance depends on spectrum bandwidth, user density, cell-edge conditions, and background traffic. Utilities must plan for realistic loading scenarios — especially when operating in constrained spectrum environments such as 3–5 MHz.

- **Private wireless can reliably support MCX even with limited spectrum.** Testing demonstrated that utility-owned spectrum (e.g., 900 MHz) can effectively support mission-critical voice, video, and data when properly engineered. This validates private wireless as a viable foundation for emergency operations when public networks degrade or fail.
- **Automated network switching is a key resiliency enabler.** SGP.32-based eSIM profile management enabled seamless, autonomous transitions between private and public networks without user intervention. This capability significantly improves operational resilience and reduces the risk of human error during emergencies.
- **Operational readiness depends on proper onboarding and configuration.** Successful MCX performance relied on correct user provisioning, SIM/eSIM profile configuration, authentication, and policy alignment across networks. These operational processes are as critical as the underlying network infrastructure.
- **Migration from legacy LMR can be evolutionary, not disruptive.** Plugfest results confirm that utilities can adopt broadband MCX while maintaining interoperability with existing LMR systems. This supports phased migration strategies that reduce risk while expanding capabilities beyond traditional voice-only communications.

Team: Gridlock Breakers

OneLayer, Ericsson, L3Harris, Duke Energy, Southern Company, Anterix, Kigen

Overview

This team explored the interoperability of communications systems between visiting mutual aid crews and host utilities, with a specific focus on how visiting crews can retain use of familiar devices while gaining rapid access to host networks and systems.

Overarching Framework

Scenario

The Gridlock Breakers Plugfest testing fits within a general mutual aid scenario:

- An emergency occurs
- Host utility requests help from Mutual Aid crews
- Visitor crew receives the mutual aid request
- Visitor travels to Host's site

The subsequent flow of the scenario varies per test case and is detailed in the Demonstration Flow sections.

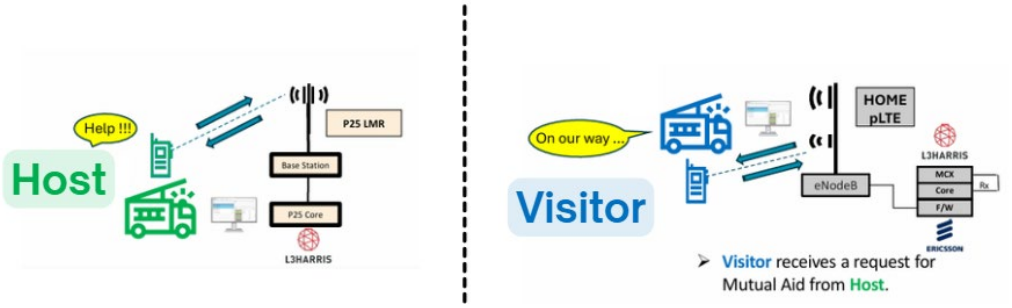

Figure 20 - Testing Scenario

Key Infrastructure

The Gridlock Breaker's Plugfest testing leveraged a combination of public and private wireless networks, LMR systems, MCX platforms, gateways, and eSIM management tools to replicate realistic mutual aid conditions.

The following infrastructure elements were used to execute these test cases:

- P25 LMR networks and radios
- L3Harris Two47 MCX client and dispatch applications
- Public MNO
- Utility private LTE networks
- Wi-Fi hotspot
- LMR–MCX gateway
- Kigen eSIM management platform
- Android smartphones
- Converged LMR/broadband radios

Plugfest Testing: Reducing Mutual Aid MCX Gridlock

"MCX" broadly refers to 3GPP standards-based mission-critical talk, data, and voice services. MCX encompasses mission-critical push-to-talk (MCPTT), mission-critical data (MCData), and mission-critical video (MCVideo).

Test Case #1: Downloading P25 Credentials on Broadband

P25[8], or Project 25, is a set of APCO standards that apply to digital Land Mobile Radio (LMR) systems. P25 standards define how two-way radios talk to each other, so utilities using different equipment can work together during emergencies.

Sideloading often refers to installing an application that came from a third-party source, not an authorized app store. Sideloading can also refer to the act of manually installing an application or manually transferring data onto a device (instead of being automated).

In the context of this test case, Southern Company represents the Visitor, and Duke Energy represents the Host.

Purpose/Objective

To determine if Visitor P25 radios connected to broadband can download and use P25 credentials to operate on the Host's P25 LMR network and access talk groups.

Test Infrastructure/Environment

- P25 radios
- Public broadband connectivity
- Host P25 network
- Two47 MCX-enabled private broadband network
- L3Harris XL Converged radios
- OTA Device Management platform (DM)

[8] https://www.cisa.gov/safecom/project-25

Demonstration Flow

Intended Flow	Actual Flow
• Visitors arrive at the Host site with L3Harris XL-200 Converged (P25 + Broadband) radios. • Visitor connects to broadband and attempts to use the Host's OTA Device Management system to request and download P25 credentials. • P25 credentials are downloaded onto Visitor radios OTA via email and reconfigured to operate on Host's P25 network; Visitor radios are connected to the Host's P25 narrowband network and Two47 MCX-enabled broadband network. • Visitors attempt to access and use P25 mutual aid talk groups.	• Visitors arrive at the Host site with L3Harris XL-200 Converged (P25 + Broadband) radios. • Visitor connects to broadband and attempts to use the Host's OTA Device Management system to request and download P25 credentials. • OTA request and download fails. • P25 credentials are manually sideloaded onto Visitor radios and reconfigured to operate on Host's P25 network; Visitor radios are connected to the Host's P25 narrowband network and Two47 MCX-enabled broadband network. • Visitors attempt to access and use P25 mutual aid talk groups.

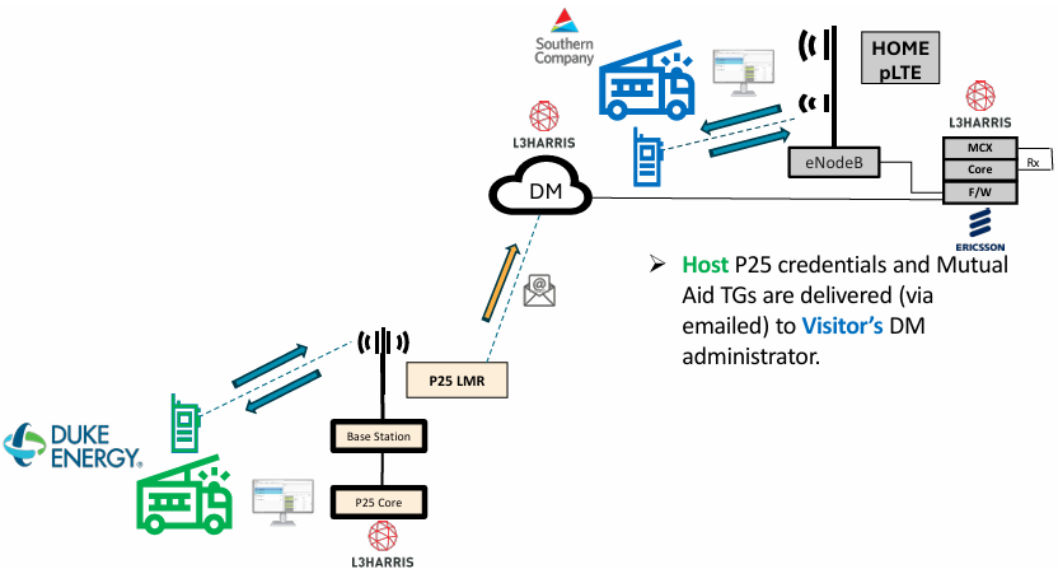

Figure 21 - P25 Credentials Pushed via Email

Results

- The team was unable to provide the OTA (Over the Air) Device Management product to Duke in a timely manner to allow for the download of the P25 credentials.
- P25 credentials were successfully sideloaded.
- L3Harris XL Converged radio successfully connected to both the P25 Narrowband network and the Two47 MCX enabled Broadband network.

Benefits, Lessons, & Takeaways

- To ensure this scenario operates smoothly in a stressful Mutual Aid situation, the visiting utility needs to ensure the OTA Device Management product is operational and that the P25 credentials are available.
    - Manual setup (via sideloading) is time-consuming, but worth considering.
    - Hosts should consider pre-arranging and coordinating the P25 credentials through their OTA Device Management system.
- Enabling visiting utilities to retain use of their existing communications equipment eliminates the need for additional training.

Test Case #2: Downloading Host's MCX Client Application on an MNO

A Mobile Network Operator[9] (MNO) refers to the company/organization that owns and runs a mobile network – public or private. In the context of this test case, MNO refers to/indicates a Public Network.

In this test case, Duke Energy represents the Visitor, and Southern Company represents the Host.

Purpose/Objective

To determine if a Visitor can use their smartphone connected to the Public MNO to download and use the Host MCX application to access talk groups.

Test Infrastructure/Environment

- MNO (Public Network)
- Smartphone
- MCX client application and server

[9] https://www.lenovo.com/us/en/glossary/mobile-network-operator/

Demonstration Flow

Intended Flow	Actual Flow
• Visitor arrives at Host site with a smartphone connected to a Public Network. • Visitor downloads Host's MCX client application from a public app store. • Visitor logs into Host's MCX client application and registers their smartphone in the Host's MCX server; Visitor is provisioned with the Host's talk groups. • Visitor attempts to use the Host's MCX client application installed on their smartphone to access and use talk groups while connected to the Public Network.	• Visitor arrives at Host site with a smartphone connected to a Public Network. • Visitors manually sideload Host's MCX client application onto their smartphone. • Visitor logs into Host's MCX client application and registers their smartphone in the Host's MCX server; Visitor is provisioned with the Host's talk groups. • Visitor attempts to use the Host's MCX client application installed on their smartphone to access and use talk groups while connected to the Public Network.

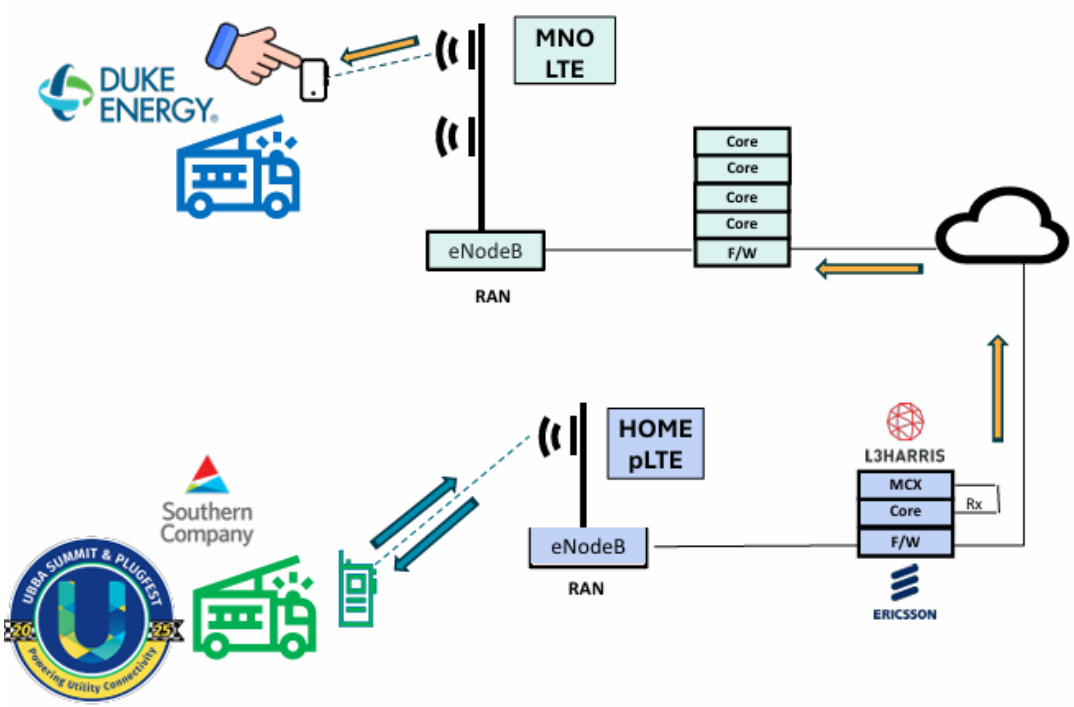

Figure 22 - Visitor Downloads MCX Client App over Public Network

Results

- MCX client application was successfully sideloaded (simulating a PlayStore download) onto Visitor's smartphone.
- Visitor's smartphone successfully connected to and registered in the Host's MCX server and was provisioned with talk groups.
    - Visitor connected to the Host's MCX server and downloaded 7 talk groups in less than 1 minute.
- Visitor successfully used the Host's MCX client application installed on their smartphone to use talk groups while connected to the Public Network.

Benefits, Lessons, & Takeaways

- This test case demonstrates using "over-the-top" MCX services, which means the network does not provide any special "treatment" like priority and preemption. The robustness of the Visitor's MNO connectivity is a key limiting factor, as public networks are often overloaded or unavailable in emergencies.
- Sideloading is time-consuming and prone to human error. To avoid sideloading, the Host must have their MCX smartphone client application enabled for download in their app store.
- Enabling visiting personnel to retain use of their existing communications equipment eliminates the need for additional training.

Test Case #3: eSIM Profile Switching on Wi-Fi

Access Point Names[10] (APNs) are a key part of eSIM profile switching, as they act as a traffic sign to tell devices which network route to use. Once a new eSIM profile is selected, the correct APN must be selected for a device to connect to the Host's network.

In the context of this test case, Southern Company represents the Visitor, and Duke Energy represents the Host.

Purpose/Objective

To determine if a Visitor MCX-capable device can download and activate a Host eSIM profile over Wi-Fi and connect to the Host's network for MCX services.

[10] https://www.samsung.com/uk/support/mobile-devices/how-do-i-check-my-apn-mobile-internet-settings/

Test Infrastructure/Environment

- MCX devices
  - Smartphones
  - MCX-capable radios
- Host network
- Host Wi-Fi hotspot
- Kigen eSIM server
- Visitor eSIM profiles
- Host eSIM profiles
- Host MCX client application
- MCX server

Demonstration Flow

- Visitor arrives at Host site with MCX devices (i.e., MCX-capable radios and smartphones) connected to the Public Network.
- Visitor connects MCX devices to a Wi-Fi hotspot on the Host's network.
- Visitor's MCX devices connect to the Kigen eSIM server via Wi-Fi.
- Host pushes network profiles to the Visitor's MCX devices; profiles are downloaded.

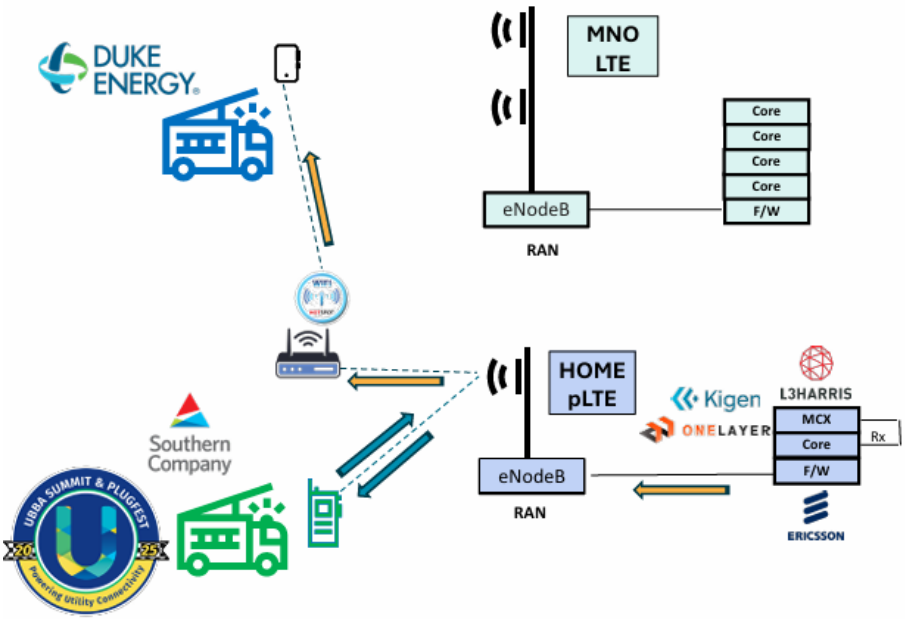

Figure 23 - New eSIM Profiles Pushed to Visitor Device

- MCX devices switch from Visitor eSIM profile to Host eSIM profile.
- Visitor selects the APN and is authenticated on the Host's network profile.
- Visitor downloads and logs into Host's MCX client application; Visitor registers MCX devices in the Host's MCX server.
- Visitor is provisioned with the Host's talk groups.
- Visitor uses the Host's MCX client application to access and use talk groups on the Host's LTE network.

Results

- MCX devices successfully connected to the Wi-Fi hotspot and Kigen eSIM server.
- eSIM profiles were successfully downloaded.
- It took about 60 seconds to connect to the eSIM server and complete the download.
- MCX devices successfully switched from the Visitor eSIM profile to the Host eSIM profile.
- Visitor devices successfully connected to the selected network gate via the APN; Visitor was successfully authenticated on the Host's network.
- Host's MCX client application was previously downloaded; Visitor successfully registered in the Host's MCX server.
- Visitor successfully used the Host's MCX client application to access and use talk groups on the Host's LTE network.
- MCX client download was not tested due to lack of PlayStore access to the MCX client.

Benefits, Lessons, & Takeaways

- Connectivity to the Host network is key for mutual aid crews during emergencies.
- Hosts should consider providing pre-loaded eSIM profiles to enable smoother switching.
- This test case leveraged connectivity to a Host-provided Wi-Fi hotspot; however, Wi-Fi is not ideal in an emergency situation.
- The Host and Visitor need to coordinate ahead of the emergency on how they will use eSIM technology.
- Consider provisioning users in the MCX server prior to the Visitor's arrival to the Host to speed up the onboarding process.
- Enabling visiting personnel to retain use of their existing communications equipment eliminates the need for additional training.

Test Case #4: P25 and MCX System Interoperability via Gateway

A gateway serves as a translator between two different communication technologies (P25, MCX, etc.) that lets them interact without actually merging them. A gateway allows users to gain connectivity to their partner users while continuing to access their own individual MCX users.

In the context of this test case, Southern Company represents the Visitor, and Duke Energy represents the Host. The Host is using a P25 LMR system.

Purpose/Objective

To determine if interoperability can be achieved between the Host P25 LMR network and the Visitor MCX network using a gateway to access talk groups.

Test Infrastructure/Environment

- Host LMR network
- MCX client application
- MCX-LMR gateway
- MCX-capable devices
  - Smartphones
  - P25 radios

Demonstration Flow

- Visitor arrives at the Host's LMR network with MCX-capable devices connected to a Public Network (MNO).
- Host configures an MCX-LMR gateway connected to their LMR network.
- Visitor provides MCX devices or MCX client application to the Host.
- Host connects the Visitor's MCX devices or MCX client application to the MCX-LMR gateway on the Host's LMR network.

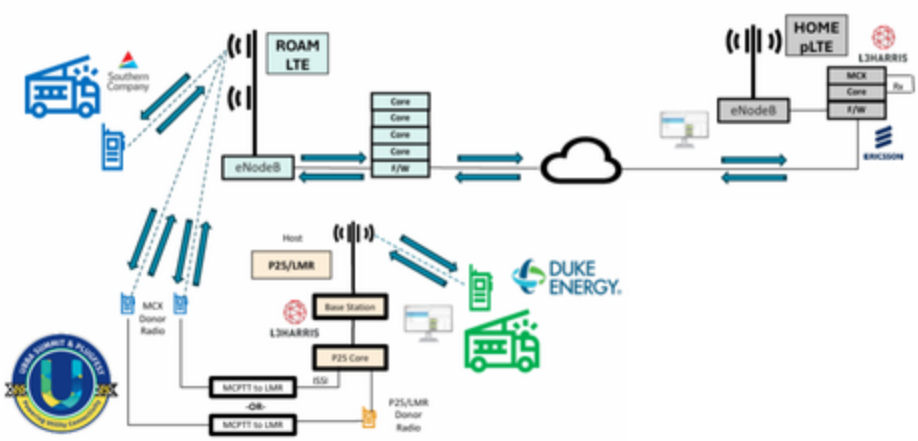

Figure 24 - Host Connects Visitor's MCX Tool to MCX-LMR Gateway

- Talk group between Visitor MCX devices and Host's LMR is attempted.

Results

- The MCX-LMR gateway was successfully configured linking 4 talk groups between the Host P25 network and the Visitor's MCX network over the Visitor's Public Network.
- The gateway was set up using 4 of the Visitor's Two47 MCX radios on one side of the gateway and 4 of the Host's P25 radios on the other side.
- MCX devices and the MCX client application successfully connected to the MCX-LMR gateway.
- Visitor MCX devices successfully connected to LMR talk groups on Host's network via the Host's MCX-LMR gateway.
- Voice latency during testing was minimal and acceptable by both the Host and Visitor (and Plugfest audience).

Benefits, Lessons, & Takeaways

- The LMR-P25 gateway is widely used throughout the P25 space and is the accepted method of interoperability.
- Setting up gateway radios can be a long process due to the physical connections that must be delivered and maintained.
- The lack of connectivity to a Mission Critical LTE network for Visitor personnel represents a potential negative, as public networks may not provide reliable performance during emergency conditions.
- The lack of metadata (i.e., talk group names & radio IDs) during this test case was noticed but acceptable.
- The number of available talk groups is dependent on the number of gateways in place.
- Gateway costs (both hardware and integration efforts) and the associated talk group limitations represent a potential negative.
- The Visitor can maintain use of familiar communication equipment even while connected to a Public Network.
- Enabling visiting personnel to retain use of their existing communications equipment eliminates the need for additional training.

Test Case #5: pLTE-pLTE Local Breakout Roaming

Roaming refers to the general concept of a device operating on a network other than its home network. General roaming may require an IP eXchange[11] (IPX), which refers to the "middleman" network that enables secure interoperability between different networks without a direct connection.

Direct roaming is a specific type of roaming, where two networks directly interconnect without using a third-party roaming provider. Direct local breakout roaming is a sub-type of direct roaming that further defines where user traffic exits the network. Direct roaming/direct local breakout roaming do not require an IPX.

In the context of this test case, Southern Company represents the Visitor, and Duke Energy represents the Host.

Purpose/Objective

To determine if Visitor radios can authenticate through their home pLTE core, roam onto the Host private LTE network using direct local breakout roaming, and access Host MCX Mutual Aid talk groups.

[11] https://www.novell.com/documentation/nw6p/?page=/documentation/nw6p/ipx_enu/data/hjyh8yg8.html

Test Infrastructure/Environment

- XL Converged Radio
- Host network
- Visitor network
- Host MCX server/system

Demonstration Flow

- Visitor arrives at Host site with MCX-capable radios.
- Visitor radios detect Host's network as a valid roaming partner.

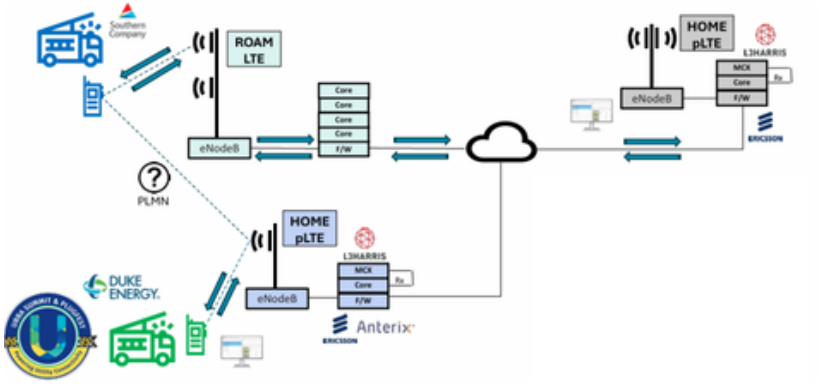

Figure 25 - Visitor Detects Host's Network as Valid Roaming Partner

- Visitor radios attempt to attach to Host's network as roaming users; Host sends authentication request to Visitor's network.
- Visitor radios are authenticated and attach to Host network.
- Visitor registers radios in the Host's MCX server.
- Visitor is provisioned with the Host's talk groups.
- Visitor attempts to use Host's MCX system to access and use talk groups via on Host's network via direct local breakout.

Results

- Host network was successfully configured to route the authentication request for Visitor radios to the Visitor's network.
- Authentication was successfully completed; the latency in the authentication process was not noticeable (as expected).
- Visitor radios successfully attached to Host's network as roaming users.
- Voice calls between talk groups on the Host's MCX server were successful; no voice latency was observed during talk group participation (as expected).
- Interfaces between the networks were challenging, but were overcome.

Benefits, Lessons, & Takeaways

- Direct local breakout requires the coordination of specialized configuration and authentication network resources.
- Since the roaming interconnections (S6a/S8) are directly between the Host and Visitor secure utility core elements, there isn't a need for a 3rd-party IPX provider (which would be more complex, costly, and potentially less secure).

- Direct local breakout eliminates the need to secure agreements and set up connectivity with an outside IPX provider with roaming capabilities.
- Enabling visiting personnel to retain use of their existing communications equipment eliminates the need for additional training.

Test Case #6: Seamless pLTE Interoperable MCX Roaming

Interworking function[12] (IWF) is an emerging network functionality that enables interoperability between different MCX systems and can be used while devices are roaming to enhance the experience. Since IWFs that enable MCX interoperability across different networks are still relatively new, IWF connections are currently limited.

NOTE: An IWF connection was not available for Plugfest 2025; therefore, this test case was not actually executed at Plugfest. Instead, this test case took the form of a conceptual presentation.

Purpose/Objective

To determine if the Visitor can roam onto the Host's network while remaining connected to their MCX system via an Interworking Function (IWF) to access talk groups.

Test Infrastructure/Environment

- MCX devices:
  - XL Converged Radio
  - Smartphone
- Host network
- Visitor MCX system
- IWF connection

Concept Flow

- Visitor arrives at Host site with MCX-capable devices (radios/smartphones) configured to the Visitor's MCX system.
- Visitor devices detect Host's network as a valid roaming partner.
- Visitor devices are authenticated and attach to Host's network as roaming users.

[12] https://www.f5.com/glossary/interworking-function-iwf

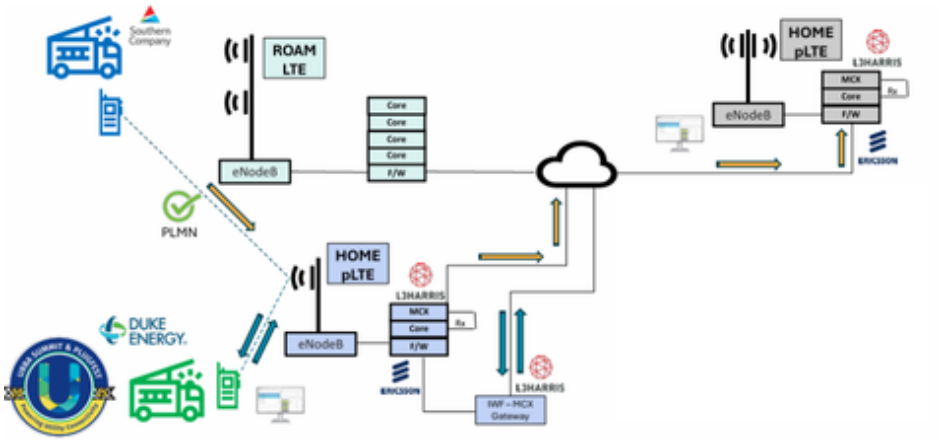

Figure 26 - Visitor Devices are Authenticated and Attach to Host Network as Roaming Users

- Visitor devices maintain registration on Visitor's MCX system while connected to Host's network.
- Visitor attempts to use their MCX system to access and use talk groups via IWF on Host's network.

Benefits, Lessons, & Takeaways

- IWF enables seamless, standards-based interoperability between separate MCX systems, allowing visiting users to roam onto a host network and communicate without manual provisioning, service disruption, or changes to their existing devices or talk groups as well as the visitor's MCX talk groups.
- The seamless connectivity between the Host and Visitor networks represents the future of Mutual Aid communications during emergencies, allowing Visitor personnel to roam on the Host's network while remaining connected to the Visitor's already established MCX configuration, without requiring the Host to configure, provision, or onboard new users.
- Enabling visiting personnel to retain use of their existing communications equipment eliminates the need for additional training.
- IWF connectivity can be established ahead of the Mutual Aid incident and left in place without utilizing IP resources on either network.
- Multiple IWF connections to multiple visitors could be established to further the ability of visitors to operate in during the incident.

Overall Lessons & Takeaways

- **Advance coordination is the single biggest enabler of successful mutual aid communications.** Across every scenario, success depended far more on pre-event coordination than on the specific technology used. Whether dealing with P25 credentials, MCX user provisioning, eSIM profiles, or roaming configurations, utilities that prepare credentials, profiles, and access policies in advance dramatically reduce onboarding time during emergencies. Ad-hoc or manual configuration is possible, but it introduces delay and operational risk in already stressful conditions.
- **Retaining visiting crews' existing devices is critical for safety and speed.** A consistent and significant takeaway is the operational value of allowing visiting crews to keep using familiar radios and smartphones. Every scenario that enabled visitors to retain their own equipment reduced training requirements, minimized user error, and improved confidence during emergency operations. This benefit held true across P25, MCX over public networks, gateways, eSIM switching, and private LTE roaming.
- **Manual workarounds function, but do not scale for real emergencies.** Several scenarios succeeded only through manual intervention (e.g., sideloading credentials, configuring gateways, manual app installs). While these workarounds validate feasibility, they are not sustainable at scale for large mutual aid events. The testing clearly distinguishes between "can be made to work" and "operationally viable under emergency conditions."
- **Public networks can enable interoperability, but are not reliable in crises.** Using MCX over public MNOs proved technically viable and fast to onboard; however, the testing reinforced a critical limitation: public networks are often congested or unavailable during emergencies. Scenarios relying solely on public broadband introduce risk unless paired with mission-critical LTE access, roaming, or fallback options.
- **Mission-critical private LTE provides the most resilient foundation for mutual aid.** Scenarios leveraging host private LTE networks (particularly pLTE-to-pLTE roaming) offered the highest confidence in performance, latency, and service continuity. When visitors could authenticate and operate directly on a host's mission-critical LTE network, the result was predictable behavior and minimal operational compromise.

- **Gateways remain effective but introduce cost, complexity, and limits.** LMR-to-MCX gateways remain a proven and accepted interoperability method, especially within the P25 ecosystem. However, testing highlighted their drawbacks: physical setup time, limited talk group capacity, metadata loss, and cost. Gateways work well as a bridge solution, but they are not a long-term answer for large-scale, dynamic mutual aid events.
- **eSIM technology is promising but requires policy and process maturity.** eSIM profile switching successfully demonstrated rapid network transitions, but also exposed the largest dependency: pre-defined coordination between host and visitor utilities. eSIMs can significantly streamline onboarding if profiles and procedures are defined ahead of time, rather than created during an event.
- **Seamless MCX roaming via IWF represents the long-term end state.** Although not demonstrated live, the discussion around Interworking Functions (IWFs) clarified a shared industry vision: true, standards-based MCX roaming without manual provisioning. This model — where visitors roam onto a host network while remaining connected to their home MCX system — offers the lowest operational friction and represents the future direction for mutual aid communications.
- **Voice Interoperability is achievable today, but not yet frictionless.** Collectively, the Plugfest results show that utilities can achieve meaningful interoperability today using a mix of existing tools and architectures. However, friction still exists in onboarding, configuration, and coordination. Reducing that friction will require continued standards adoption, vendor alignment, and pre-incident planning.

Use Case 2: Internet of Things (IoT) Innovations

For utility companies, understanding and managing the electric, gas, and water grid has historically relied on a mix of manual meter readings, traditional SCADA systems, and limited high-speed monitoring equipment. While these approaches provided essential information, they often lacked real-time detail, granular visibility, and flexibility, especially for remote or hard-to-reach locations. This use case encompasses tests that demonstrate how modern private LTE (PLTE) and IoT technologies can improve device longevity, resiliency, and operational flexibility.

Team: Connectivity Crew

Giesecke+Devrient, Landis+Gyr, Ericsson, Nokia, Anterix, Southern Company

Overview

This team explored how the longevity and functionality of utility IoT devices can be improved, with a specific focus on using SGP.32 eSIM and eSIM IoT Manager (eIM) technology to enable secure, flexible, and fully remote connectivity management for deployed utility IoT devices.

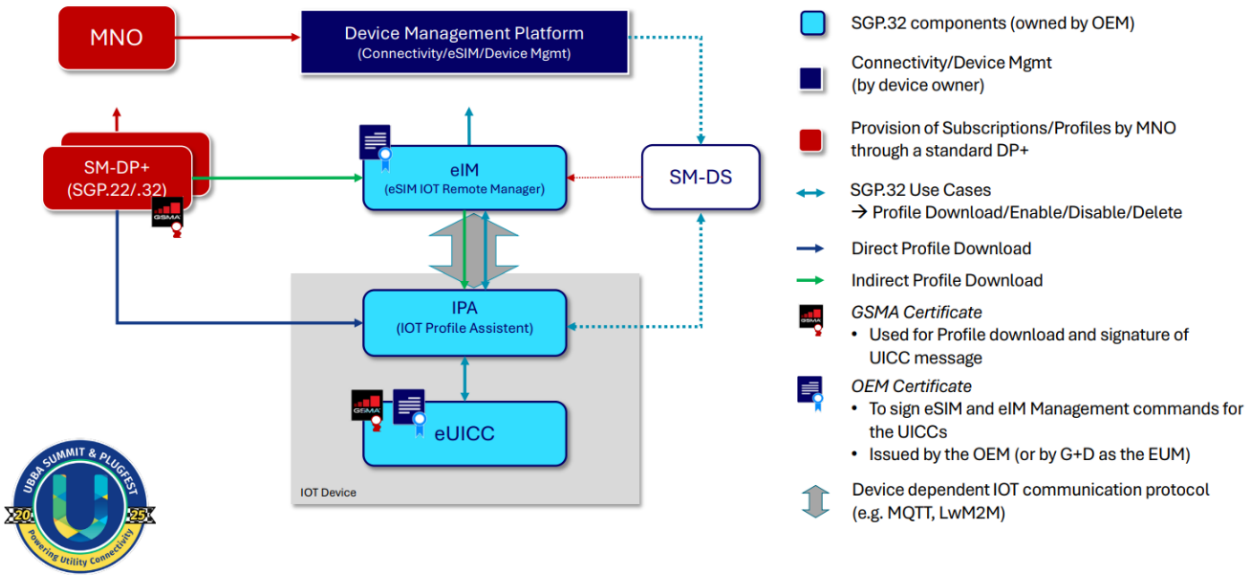

Figure 27 - SGP.32 and IoT Devices

Overarching Framework

Scenario

The Connectivity Crew's Plugfest testing fits within the following general scenario:

- A device is remotely provisioned with an eSIM profile
- The device connects to the primary private network
- An outage occurs
- The device switches to the secondary public network
- Power is restored
- The device reconnects to the primary private network

Key Infrastructure

The Connectivity Crew's Plugfest testing leveraged a combination of IoT devices, private LTE network infrastructure, and SIM/eSIM profile-management tools to replicate practical utility situations.

The following infrastructure elements were used to execute these test cases:

- IoT devices with Embedded Universal Integrated Circuit Cards (eUICCs)
- GE Orbic Router
- LG Revalo Meter
- Preloaded bootstrap eSIM profiles
- eSIM IoT Manager (eIM)
- SM-DP+ server
- Connectivity Management Platform (CMP)
- Private LTE networks
- Ericsson
- Nokia
- Public connectivity via mobile virtual network operator (MVNO)
- Anterix spectrum (Band 8 for private networks)

Plugfest Testing: Performing SGP.32-Based Remote Provisioning and Network Resiliency

SGP.32[13] refers to GSMA's latest standard for remote eSIM management on IoT devices. First published in 2023, SGP.32 introduced triggers and rules that enable devices to automatically deploy new profiles. Under SGP.32, eIM/SM-DP+ servers and devices with eSIM cards can trigger requests to "pull," download, and configure new profiles, and also switch between active profiles without any manual intervention.

[13] https://www.gsma.com/solutions-and-impact/technologies/esim/gsma_resources/sgp-32-v1-2/

Test Case #1: Zero-Touch Provisioning Using SGP.32

A device can be set up and connected to a network for the first time using a preloaded bootstrap profile and the SGP.32 standard. This allows remote configuration of the SIM without needing to physically handle it.

A bootstrap profile[14] refers to a device's preloaded, temporary eSIM profile that provides initial network connectivity. While a bootstrap profile can be designated as the primary profile, in this test case, it's used to securely download the preferred eSIM profile.

A Connectivity Management Platform[15] (CMP) allows all connected devices to be monitored and managed from a single screen. A CPM provides a single dashboard view of each device's eSIM profiles, available networks, connection status (active/inactive), and when it switches or reconnects. This test case uses G+D's CPM platform IoT Suite.[16]

Purpose/Objective

To determine if eSIM profiles can be securely set up and updated remotely, over-the-air (OTA), without anyone needing to physically touch the device.

Test Infrastructure/Environment

- Devices with eUICC containing preloaded bootstrap profile
- Initial network access (via bootstrap profile)
- eSIM management system (eIM)
- SM-DP+ server
- Connectivity Management Platform (CMP)
    - G+D IoT Suite
- Public network
- Private network

Demonstration Flow

- The device is turned on and connects using the bootstrap starter profile.
- The device securely checks in with the eSIM management system to confirm it is authorized.
- The device is directed to the serving network SM-DP+ server to download primary operational eSIM profiles via the management system (eIM).
- The device downloads and saves both its primary/preferred network connection (private LTE) and a secondary/failover option (public network).

[14] https://wirelesslogic.com/iot-glossary/iot-bootstrap-profiling
[15] https://www.gi-de.com/en/digital-security/connectivity-iot/iot-connectivity/iot-connectivity-management-platform
[16] https://www.gi-de.com/corporate/Digital_Security/Connectivity_IoT/IoT-Connectivity/GD_MS_Broschuere_IoT_Suite.pdf

Results

- The device successfully connected to the bootstrap starter profile.
- The device successfully confirmed authorization with the eSIM management system.
- All network profiles were successfully downloaded and saved in less than one minute.
- The device successfully completed the demonstration flow during testing.

Benefits, Lessons, & Takeaways

- eSIM remote provisioning is a valid option for initial field deployment.
- This test was conducted with a single device, but the same process can be scaled to support thousands of devices.
- Connectivity updates and provisioning can be performed in parallel across large fleets, rather than one at a time.
- Operations can be scheduled in batches or triggered automatically via secure APIs from authorized sources (such as utility companies), enabling efficient, large-scale remote management of device connectivity.
- The need to physically handle or replace SIM cards is eliminated.
- Enables faster and simpler device setup.

Test Case #2: Transition from Public to Private Network

This test shows how a device can move from using a public cellular network to a utility's preferred private LTE network after it has been set up.

Purpose/Objective

To determine if devices can automatically use a private network as their primary connection, as managed via the SGP.32 standard.

Test Infrastructure/Environment

- Private LTE networks
  - Ericsson
  - Nokia
- Public cellular connectivity
- eSIM management system
- CPM

Demonstration Flow

- The device connects to a public network.
- The device's private network settings are turned on.
- The device switches to and begins using the private LTE network as its primary connection.

Results

- The device's private network settings were successfully activated.
- The device successfully switched from the public network to the primary/preferred private LTE network and stayed connected without interruption.

Benefits, Lessons, & Takeaways

- Gives utilities greater control over how devices obtain and maintain connectivity.
- Helps lower ongoing connectivity costs.
- Ensures devices use the preferred private network when available.
- Devices can be pre-programmed with preferred network settings so they connect to a private network when available.
- Seamless network switching reduces downtime and helps utilities maintain continuous data collection for operations and billing. It also lowers ongoing costs by eliminating field visits, SIM or device replacements, and by enabling over-the-air updates.
- The pull-based SGP.32 model further reduces costs by removing the need for expensive OTA/SMS platforms, and relying on private networks most of the time can reduce connectivity expenses even more.

Test Case #3: Automatic Failover & Switchback During Network Outage

This test shows how a device stays connected when its main network goes down and automatically returns once service is restored.

Purpose/Objective

To determine if devices can stay connected during network outages and automatically reconnect to their primary/preferred network when it becomes available again.

Test Infrastructure/Environment

- A private LTE network
- Simulated outage
- Public network
- eUICC settings configured to check for network availability about every 2 minutes

Demonstration Flow

- The device is connected to the private LTE network.
- An outage is simulated via disabling the RAN.

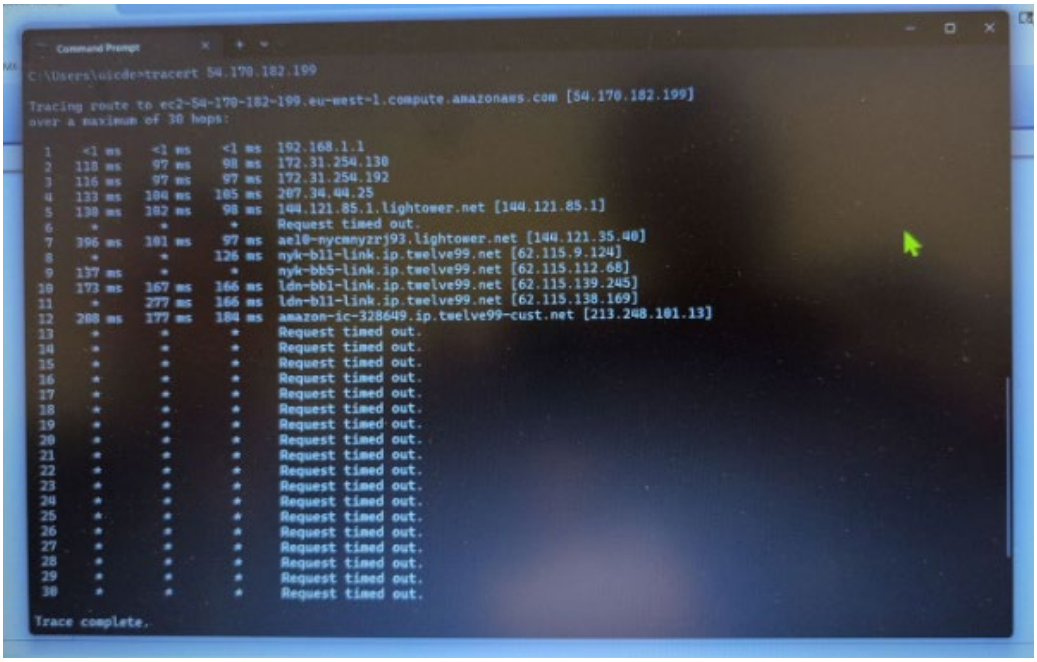

Figure 28 - Network Outage

- The device loses connectivity.
- The device automatically switches to a public network.

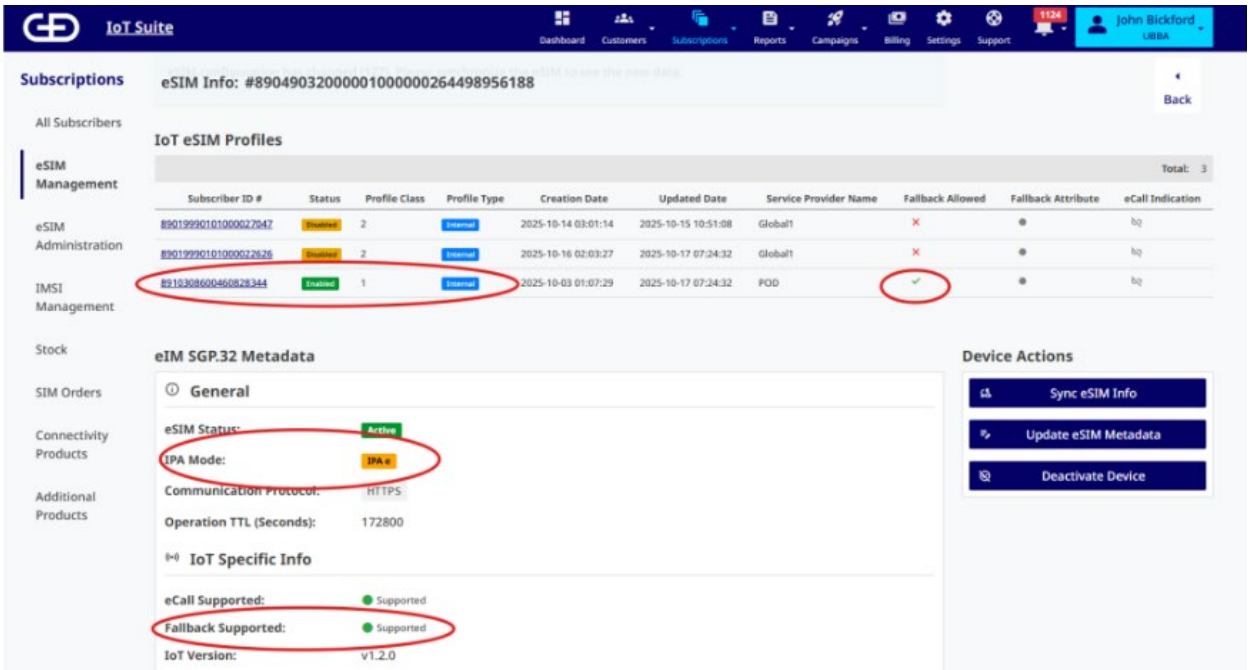

Figure 29 - Automatic Network Switching

- The private network is restored.

- A scheduled eIM check occurs.
- The device recognizes the private network is available and automatically switches back.

Results

- The device operated normally when initially connected to the private LTE network.
- The device successfully switched to the public network during the simulated outage.
- The device successfully reverted its connection to the private LTE network in about two minutes, without needing to be restarted.

Benefits, Lessons, & Takeaways

- The eSIM continuously monitors connectivity. When a device detects a loss of service, it triggers a built-in event that switches the eSIM to a backup network profile. After a set time (determined by the utility), the eSIM automatically checks for the preferred network again and reconnects when it is available.
- To avoid constant switching in areas with unstable coverage, the system waits a set time (as set by the utility) to confirm the outage is real before switching.
- SGP.32 also supports manual network switching.
- Automated failover and recovery logic enables devices to maintain connectivity during outages and return to their preferred network without manual intervention. This reduces downtime, helps utilities maintain service reliability, preserves meter-level data reporting, and strengthens customer trust.
    - This automated process also supports long-term deployment by minimizing the need for field visits and manual network management.

Overall Lessons & Takeaways

- **Centralized visibility during transition periods.** Managing devices through a single connectivity management platform (CMP) made it easier to monitor both SGP.32 devices and those using legacy SIM standards. Utilities transitioning to SGP.32 over time may benefit from investing in a centralized dashboard to manage mixed device fleets, simplifying operations and improving visibility during the transition.
- **eSIM remote provisioning works.** Connectivity works at initial field deployment and remains through ongoing operation and network disruptions. These capabilities enable continual monitoring and remote management of eSIM profiles and connectivity throughout the life of the device in the field.
- **Align eSIM management to device capabilities.** Testing showed that the best eSIM management approach depends on device characteristics such as processing power and battery life. Utilities should evaluate device classes in advance and select the appropriate management model for each deployment scenario to ensure reliable performance.

- **G+D's SGP.32-certified eSIM IoT Manager (eIM) and eSIM solution (i.e., IoT Suite) directly addresses device-to-network connectivity challenges utilities face in the real world.** By allowing connectivity to be managed remotely without dispatching crews or physically replacing SIM cards, this approach has the potential to simplify day-to-day operations, lower costs, and improve long-term reliability for large fleets of utility IoT devices.
- **Validate switching behavior through targeted pilots.** Network switching works reliably across frequencies as long as the device modem supports the bands. Large volumes of devices and data can move between public and private networks without issue, provided the network can support the load. To confirm real-world performance, utilities should begin with a robust pilot that mirrors these scenarios and expands into field environments before scaling.
- **Real-world applications.** A device can be securely provisioned remotely, connect to a utility's private network, automatically switch to an alternate public network during an outage, and seamlessly return to its preferred private network once service is restored. This scenario reflects real-world utility environments where reliable connectivity, minimal manual intervention, and fast recovery from network issues are essential.
- **Confirm resilience benefits through controlled testing.** The Plugfest demonstrated that SGP.32 devices can maintain connectivity and automatically recover from simulated network outages. Rapid switching is possible (under a minute or two), but utilities should configure a delay to ensure stability before returning to the preferred network. This delay is customizable through the GSMA-based eUICC application (IPAe). Additional testing is recommended to quantify resilience, maintenance reduction, and operational benefits compared with existing connectivity models.

Team: LTE Lap Leaders

Ericsson, Southern Linc, Itron, Kigen, BEC Technologies, Anterix, Hitachi Energy, Black & Veatch, Duquesne Light, Palo Alto Networks

Overview

This team explored how LTE and private LTE networks can support utility-grade IoT deployments across the full device lifecycle, specifically how LTE, Cat-M1, and NB-IoT coexist in shared spectrum and how to configure them efficiently for utility use cases.

Overarching Framework

Scenario

Utilities are increasingly adopting smart devices for electricity, gas, and water management. The LTE Lap Leaders' Plugfest testing fits within a scenario that simulates a typical utility environment:

- Private LTE network carrying multiple types of IoT devices.
- Devices include constantly powered electricity meters, battery-powered gas/water meters, and high-speed grid monitors.
- Networks tested for spectrum efficiency, battery optimization, traffic prioritization, and data integrity under different load conditions.

Key Infrastructure

The LTE Lap Leaders' Plugfest testing leveraged a combination of IoT devices, private LTE network infrastructure, network management systems, eSIM profile-management tools, and data visualization tools to replicate realistic operating conditions.

The following infrastructure elements were used to execute these test cases:

- Private LTE Networks: Live pLTE networks on Band 106 and Band 26 with 3–7 MHz bandwidths
- eSIM Platforms: Kigen SAS-accredited eUICCs
- Ping Things PredictiveGrid™ platform
- IoT Devices:
  - Constantly powered (electric meters) – BEC MX-220-UT-5G[17]
  - Battery-powered (gas/water meters) – BEC M120N-CM1[18]

[17] https://bectechnologies.net/devices/mx-220-ut-5g/

[18] https://irp.cdn-website.com/cd85d6ad/files/uploaded/Billion-M120N-Datasheet_v20230104-EP06E.pdf

Plugfest Testing: Scalable, Resilient, and Mission-Critical IoT on LTE

Massive IoT[19] refers to connecting a huge number of low-power, low-cost devices like smart meters and sensors. These devices don't need high-speed or frequent communication but must operate reliably for years, often in challenging locations like basements or far from cell towers.

Two LTE-based technologies dominate this space:

- **NB-IoT (Narrowband IoT):** Extremely low-power, ideal for simple devices in tough radio conditions. Low data rate (~250 kbps).
- **Cat-M1:** Slightly more complex, higher data rates (up to 1 Mbps), lower latency, still energy efficient.

Both support sleep modes (PSM and eDRX) to conserve battery and can extend network coverage beyond normal LTE signals.

NOTE: The LTE Lap Leaders' test cases were conducted prior to Plugfest; the demonstration flows are thus written in the past tense.

Test Case #1: Massive IoT Deployment (Cat-M & NB-IoT)

Guard bands[20] refer to small, unused portions of the spectrum between adjacent channels that act like buffers. Guard bands "separate" frequencies to reduce the likelihood of interference.

Purpose/Objective

To determine if large numbers of smart devices, such as meters and sensors, can be deployed on LTE networks without interfering with other critical communications, while efficiently using available spectrum.

Test Infrastructure/Environment

- Cat-M1 devices
- NB-IoT devices
- LTE network

[19] https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/massive-iot/
[20] https://uweb.engr.arizona.edu/~krunz/TR/guardband_aware_Feb2011.pdf

Demonstration Flow

- Cat-M1 devices were added inside LTE carriers with bandwidths of 3, 5, and 7 MHz.
- NB-IoT devices were deployed either inside LTE carriers, in guard bands, or on separate small carriers.
- Measurements were taken to confirm that each type of device and carrier was transmitting correctly.
- A video was streamed on LTE while Cat-M devices send data to see how the network handles congestion.

Results

- Both Cat-M and NB-IoT devices worked alongside LTE without issues
- LTE traffic was successfully prioritized.
- Critical applications (like video or SCADA systems) stayed smooth even when Cat-M devices were sending data.
- NB-IoT devices achieved longer coverage distances.

Benefits, Lessons, & Takeaways

- Utilities can deploy large numbers of IoT devices alongside LTE traffic without interference.
- Cat-M and NB-IoT complement each other, offering flexibility for both higher-data and low-power, deep-coverage devices.
- The higher power and special design of NB-IoT devices enable longer coverage distances.

	NB-IoT	CAT-M1	LTE
Uplink Peak Throughput/ UE	~151 kbps 1)	~1,119 Mbps 2)	5 Mbps
Downlink Peak Throughput/ UE	~118 kbps 1)	~500 kbps 2)	10 Mbps
Bearer	FDD	FDD	FDD & TDD
Cell Range	Up to 120 km	Up to 100 km	10s of km up to 200km
Coverage extensions	CE Level 0,1,2	CE Mode A	
Battery Life	Up to 10 Years	Up to 10 years	Use case dependent
UE Energy Efficiency	PSM, eDRX, RAI	PSM, eDRX, cDRX, RAI	Power Saving Mode, extended DRX
Mobility	Connected & Idle Mode Mobility	Connected & Idle Mode mobility	Connected & Idle Mode mobility
Voice	Not supported	VoLTE	VoLTE

Figure 30 - Theoretical Capabilities

Test Case #2: Battery-Powered Devices – Extended Battery Life (Cat-M1 & NB IoT)

Power Saving Mode (PSM)[21] and Extended Discontinuous Reception[22] (eDRX) refer to power consumption settings that help extend the life of IoT devices.

PSM allows devices to "sleep" in a low-power state between scheduled transmissions. eDRX supports more fine-tuned consumption, with more precisely scheduled intervals.

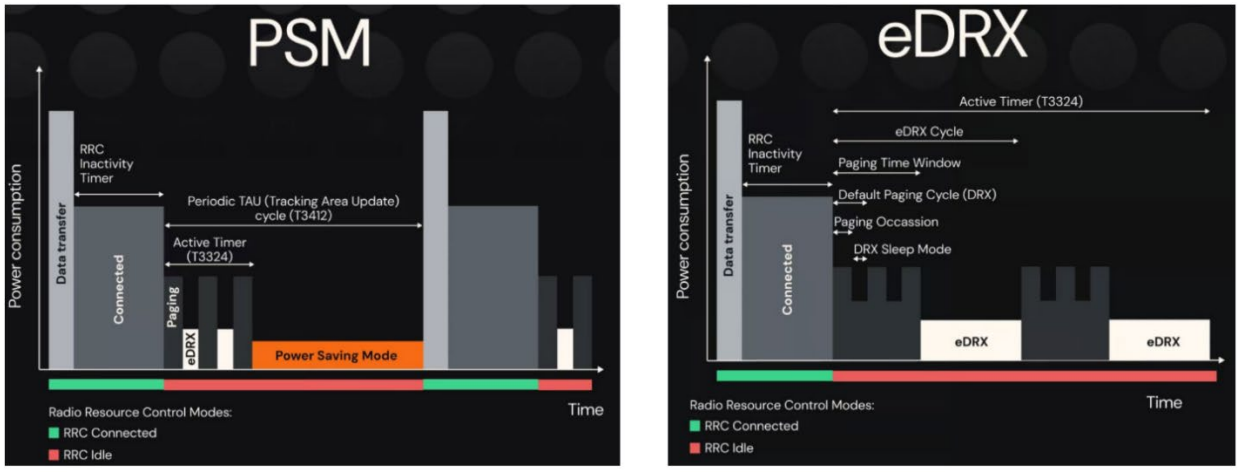

Figure 31 - PSM & eDRX Comparison

Purpose/Objective

To determine if Cat-M1 or NB-IoT devices in gas and water meters provide better battery performance, and to identify the settings that best maximize battery life while still quickly responding to network requests like gas shutoffs or reconnects.

Test Infrastructure/Environment

- Gas and water meters
- IoT devices
    - Cat-M1
    - NB-IoT2

Demonstration Flow

- Gas and water meters with D-cell batteries were set up (12 AH allocated for communications).
- Devices were configured in two power-saving modes: PSM and eDRX.
- PSM implementation: 3 transmissions per day were scheduled.
- eDRX implementation: 10-minute cycle with scheduled listening periods for messages was set up.

[21] https://kigen.com/glossary/power-saving-mode-psm/
[22] https://kigen.com/glossary/#:~:text=eDRX%20(Discontinuous%20Reception)

- Each transmission sent a 512-byte data packet.
- Daily energy use was measured and compared for Cat-M1 and NB-IoT2.

Results

- Cat-M1 consumed less power than NB-IoT2 due to shorter transmission times and smaller "listening windows."
- PSM and eDRX led to similar battery life overall, but eDRX allowed the network to reach devices faster.

Benefits, Lessons, & Takeaways

- Cat-M1 is more energy-efficient than NB-IoT, making it ideal for long-life battery-powered meters.
    - Cat-M1 is more likely to achieve the "10+ year battery life" target under real-world usage.
- eDRX allows devices to respond quickly to network commands while still conserving power.

Test Case #3: Offline eSIM Profile Download & Switching (SGP.32)

Requiring a continuous cellular connection to update an eSIM increases the risk of failed updates, drains battery life, and can leave devices stranded if connectivity drops mid-process. Enabling secure, incremental profile downloads that can pause and resume makes large-scale IoT deployments more resilient.

Purpose/Objective

To determine if updating eSIMs on battery-powered devices (without needing a full online connection) improves battery life and reliability during updates or profile changes.

Test Infrastructure/Environment

- Battery-powered devices
- Private LTE network
- Network manager tool

Demonstration Flow

- Devices started with a private LTE profile.
- An offline profile was sent using a local radio connection (not cellular) in small pieces.
- The download was intentionally interrupted mid-way.
- The device automatically resumed downloading from where it stopped.
- Once complete, the device loaded the new profile into the eSIM.
- The device switched to the new profile and confirmed connectivity.
- The network manager updated its record of which profiles were active.

Results

- The download successfully resumed after interruptions.
- Battery life was successfully conserved.
- eSIM profiles were loaded and switched without error.

Benefits, Lessons, & Takeaways

- All demonstration steps were protected with highly secure, accredited systems, including encrypted key exchange.
- Offline, incremental eSIM downloads reliably resume after interruptions, thus saving battery and reducing update failures.
- This approach lets utilities securely provision devices without continuous internet access. It also makes it easier to manage large-scale deployments over the full device lifecycle — which is critical when devices are expected to operate unattended for 10+ years.

Test Case #4: Time-Series & Mission-Critical IoT Applications on Private LTE

Phasor Measurement Units (PMUs) produce Synchrophasor, measurements of electrical conditions on the grid. PMUs are often used in tandem with Power Quality (PQ) meters, which measure voltage, current, and power.[23]

Point-on-Wave monitors actively monitor and capture precise waveform measurements of electricity at very high sampling rates, while advanced substation monitors passively monitor and capture data.

Purpose/Objective

To determine if private LTE networks can handle high-speed, time-synchronized data from many devices to support advanced grid monitoring and analytics that were previously only possible with wired networks.

Test Infrastructure/Environment

- Private LTE network (3 MHz x 3 MHz)
- PQ meters
- Distribution PMUs
- Transmission Synchrophasor
- Advanced Substation Monitors
- Point-on-Wave monitors

[23] https://www.electroind.com/synchrophasors-explained/

Demonstration Flow

- A private LTE network covering a substation was set up.
- Multiple types of devices were connected to the network.
- A power flow simulator was used to simulate real-world data.
- Data was transmitted through the LTE network to a dashboard for visualization:
    - PQ Meters: 1–10,000 samples/sec
    - Distribution PMUs: 1–200 samples/sec
    - Transmission Synchrophasor: 20–40 samples/sec
    - Advanced Substation Monitors: 500 samples/sec
    - Point-on-Wave Monitors: 3,000 samples/sec
- Multiple tests were run to assess performance as the number of samples and devices increased.

Device	# of Devices	# of Streams per Device	Point Per Sec
meter - PQ	1	16000	1
meter - PQ	1	1	1
meter - PQ	1	10	1
meter - PQ	1	100	1
meter - PQ	1	1000	1
meter - PQ	1	2000	1
meter - PQ	1	3000	1
meter - PQ	1	3500	1
meter - PQ	1	4000	1
meter - PQ	1	4500	1
meter - PQ	1	5000	1
meter - PQ	1	5500	1
meter - PQ	1	6000	1
meter - PQ	1	7000	1
meter - PQ	1	8000	1
meter - PQ	1	10000	1
meter - PQ	1	12000	1
meter - PQ	1	14000	1
meter - PQ	1	16000	1
meter - PQ	1	18000	1

Device	# of Devices	# of Streams per Device	Point Per Sec
DPMU	1	1	30
DPMU	1	5	30
DPMU	1	10	30
DPMU	1	20	30
DPMU	1	40	30
DPMU	1	100	30
DPMU	1	150	30
DPMU	1	200	30
DPMU	2	10	30
DPMU	2	20	30
DPMU	2	40	30
DPMU	2	100	30
DPMU	2	150	30
DPMU	2	200	30
DPMU	3	20	30
DPMU	3	40	30
DPMU	5	20	30
DPMU	5	40	30
DPMU	6	20	30
DPMU	6	40	30
DPMU	7	40	30

Device	# of Devices	# of Streams per Device	Point Per Sec
Tsynch	1	20	60
Tsynch	1	40	60
Tsynch	2	20	60
Tsynch	2	40	60
Tsynch	3	20	60
Tsynch	3	40	60
Tsynch	4	20	60
Tsynch	4	40	60
Tsynch	5	20	60
Tsynch	5	40	60

Device	# of Devices	# of Streams per Device	Point Per Sec
POW	1	1	3000
POW	1	2	3000
POW	1	3	3000
POW	1	4	3000
POW	1	5	3000

Device	# of Devices	# of Streams per Device	Point Per Sec
Sub Mon	1	1	500
Sub Mon	3	1	500
Sub Mon	6	1	500
Sub Mon	9	1	500
Sub Mon	12	1	500
Sub Mon	12	1	500
Sub Mon	12	1	500
Sub Mon	15	1	500
Sub Mon	18	1	500
Sub Mon	18	1	500
Sub Mon	15	1	500

Figure 32 - Performed Test Runs

Results

- The LTE network successfully and reliably transmitted all high-speed, time-synchronized data.
- Capacity analysis showed the network could support many more devices in the future.

Benefits, Lessons, & Takeaways

- GPS-based synchronization enables precise voltage and current measurements.
- Private LTE networks can handle high-speed, time-synchronized data from multiple devices, supporting advanced grid monitoring.
- A capacity analysis showed the network also has ample capacity for future device growth, enabling scalable, mission-critical IoT applications (see Figure 33).

Device	Units/Substation	Growth Potential
PQ Meters	40 units/substation	150×
PMUs	24 units/substation	85×
Transmission Synchrophasor	6 units/substation	16×
Advanced Substation Monitors	2 units/substation	20×
Point-on-Wave Monitors	1 unit/substation	7×

Figure 33 - Capacity Analysis

Overall Lessons & Takeaways

- **Massive IoT deployment is feasible alongside LTE traffic.** Cat-M and NB-IoT devices can coexist with LTE networks without interference, allowing utilities to scale IoT deployments efficiently.
- **Cat-M is generally more energy-efficient than NB-IoT for battery-powered devices**. Longer battery life can be achieved while still enabling network-initiated actions with eDRX.
- **Dynamic network scheduling protects critical communications.** LTE traffic can be prioritized over IoT devices when networks are congested, ensuring reliable operation for mission-critical applications.
- **Offline eSIM provisioning improves reliability and flexibility.** Incremental downloads can resume after interruptions, conserving battery and enabling secure device updates in the field or in factory settings
- **Private LTE networks can support high-speed, time-synchronized data.** Advanced applications like PMUs, substation monitors, and point-on-wave monitoring can be deployed wirelessly with high fidelity.
- **Future scalability is strong.** The tested networks have sufficient capacity to handle many more devices per substation than currently deployed, supporting long-term growth.
- **High-quality data enables improved operational insights.** Time-synchronized, high-resolution measurements allow utilities to detect grid issues in real time and support predictive analytics, enhancing grid resilience and efficiency.

	Bandwidth	Coverage Range	Battery life	UL/DL Peak Throughput	Mobility	Security
Cat-M1	3 - 20 MHz	154dB 100km	10 years +	1.1/0.5 Mbps	Supported	Full e2e 3GPP
NB-IoT	min 400 kHz	164dB 120km	10 years +	150/120 kbps	Limited	Full e2e 3GPP
LTE Cat1bis	1.4-20 MHz	144dB 200km	Days/month	5/10 Mbps	Supported	Full e2e 3GPP

Figure 34 – Connectivity Comparison

Team: IoT Turbo Chargers

Xcel Energy, Southern California Edison (SCE), Exelon Energy, Anterix, Black & Veatch, Nokia, Ubiik, Kigen, Itron, BEC Technologies, Verizon, One Layer

Overview

This team explored how today's utility communication technologies can support AMI 2.0, grid modernization, and future operational needs, while remaining flexible enough to evolve over time. The testing emphasized practical, real-world scenarios rather than theoretical performance.

The IoT Turbo Chargers' goal was not to promote a single network model, but to demonstrate how different technologies can coexist and complement one another in utility environments.

Overarching Framework

Scenario

The IoT Turbo Chargers' Plugfest testing focused on scenarios that utilities are actively dealing with today or expect to face in the near future:

- Higher data volumes from next-generation meters
- Real-time or near-real-time customer energy information
- Integration of solar, batteries, and other distributed energy resources
- Increased need for network resiliency during outages
- Long device lifecycles that must span multiple technology generations

Key Infrastructure

The IoT Turbo Chargers' Plugfest testing leveraged a combination of IoT devices, LTE-M technology, private network infrastructure, and eSIM technology to realistically replicate how utilities deploy and operate networks in the field.

The following infrastructure elements were used to execute these test cases:

- Private cellular networks operated by utilities
- Public cellular networks for backup and extended coverage
- Smart meters and grid-connected devices
- Central network monitoring tools to observe performance
- Embedded SIMs (eSIMs) that allow devices to switch networks remotely
- Security and asset visibility tools to monitor connected devices

Plugfest Testing: Connectivity for a Modern Utility Grid

Utilities face a rapidly evolving communications landscape, with growing demands for secure, reliable, and flexible networks to support smart meters, IoT devices, and advanced grid operations.

LTE-M (Cat-M1) offers reliable coverage, power-saving features, and dynamic network resource management, making it well-suited for today's smart grid applications, while emerging 5G RedCap/eRedCap[24] provides higher data capacity, network slicing, and support for advanced applications like AI and energy sharing.

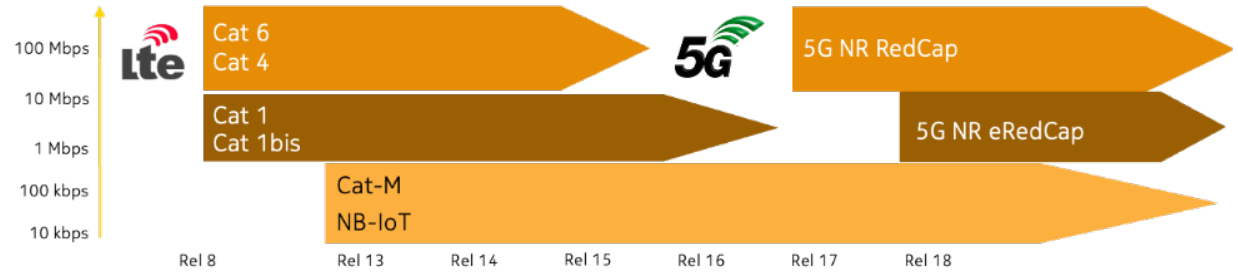

Figure 35: 5G RedCap and eRedCap

	RedCap (Rel 17-20)	eRedCap (Rel 18-20)	Cat-M (Rel 14)	NB-IoT (Rel 14)
Max bandwidth	3-20MHz	3-20MHz	1.4MHz	200kHz
Peak uplink rate	120Mbps	10Mbps	1.1Mbps	160kbps
Peak downlink rate	220Mbps	10Mbps	0.59Mbps	120kbps
Duplex mode	TDD/FD-FDD	TDD/FD-/HD-FDD	HD-FDD	HD-FDD
Availability	Nationwide by 2027	Nationwide by 2029	VZ, AT&T, T-Mo	VZ, T-Mo
Module cost	500% => 250-300%	120-175%	100% (reference)	60-100%

*Figure 36: 5G RedCap and eRedCap Capabilities**

***NOTE**: Cat-M module cost is used as the baseline (100%). All other module costs are expressed relative to this baseline. RedCap module cost is currently estimated at ~500% (5×) of Cat-M and is expected to decrease over time to ~250-300% (2.5-3×).

[24] https://www.ericsson.com/en/reports-and-papers/white-papers/redcap-expanding-the-5g-device-ecosystem-for-consumers-and-industries

Test Cases #1 & #2: Sharing Wireless Capacity Across Multiple Uses

These tests examine how multiple types of utility traffic (such as smart meter data and operational communications) can safely and efficiently share the same wireless network, instead of requiring separate networks or fixed capacity assignments.

Test Case #1 focuses on technology coexistence, specifically how LTE, Cat-M1, and NB-IoT can operate side-by-side in the same licensed spectrum bands.

Test Case #2 focuses on dynamic spectrum resource allocation, which is how the network automatically shifts capacity between applications as demand changes.

Figure 37: Dynamic Spectrum Resource Allocation

Purpose/Objective

To determine if network congestion during peak meter activity can be prevented, and to determine if it's possible to avoid reserving capacity that sits unused most of the time.

Test Infrastructure/Environment

- LTE network
- Cat-M1
- NB-IoT
- Smart meters
- Network monitoring tool

Demonstration Flow

- A shared wireless network is established using LTE (the same cellular technology used in commercial mobile networks)
- Multiple technologies are enabled on the same network:
  - LTE for operational traffic
  - Cat-M1 for smart meters
  - NB-IoT for very low-data devices
- LTE traffic is introduced and a baseline is established
- Smart meter devices are connected:
  - First with no data
  - Then with light data
  - Then with heavy, peak-style data
- Network monitoring tools are used to track:
  - How much capacity was assigned to each application
  - Whether performance changed as traffic increased

LTE UL Load (%)*	Available PRBs for LTE UL Data	PRBs used for Cat-M1 UL Traffic	% Available PRBs Utilized for LTE traffic	Cat-M Load
94%	13	NA	100%	No Cat-M UE connected
99%	13	0	100%	Cat-M UEs connected but no traffic
75%	12	1	100%	<10% Cat-M load
65%	11	2	100%	<20% Cat-M load
76%	10	3	84%	>50% Cat-M load
0%	8	4	0%	100% Cat-M Load

Figure 38 - Observed Network Behavior

Results

- The network successfully redistributed capacity in real time without congestion. Resource allocation behaved as designed, with capacity assigned dynamically based on demand.
- At the tested load levels (which were representative of real-world utility use rather than full network saturation) LTE uplink latency and throughput showed no measurable degradation, even when Cat-M1 traffic was active.
- Meter traffic successfully only used bandwidth when needed.
- Idle meter capacity was automatically returned to operations: In the 3 MHz carrier (15 total PRBs, with 2 reserved for control), dynamic spectrum sharing allowed LTE operational traffic to use up to 13 PRBs when Cat-M1 demand was low or idle — providing up to ~45% more uplink capacity compared to a statically partitioned network.
- Meter traffic was correctly prioritized.

Benefits, Lessons, & Takeaways

- Utilities can safely run meter traffic and operational applications on a single private LTE network (even during peak meter activity) while maintaining predictable performance.
- Under higher Cat-M1 load, the eNB scheduler applied the configured QoS settings to allocate PRBs on demand, ensuring meter traffic met its performance requirements. When meter traffic subsided, resources were quickly released back to LTE, with no observable impact on operational applications.
- Dynamic spectrum sharing ensures meter traffic gets priority when needed, operational traffic reclaims unused capacity when meters are idle, and overall network efficiency improves without overbuilding infrastructure.

- Cat-M1 traffic was modeled using a UE/traffic emulator and consumed up to 6 physical resource blocks (PRBs) within a 3 MHz carrier when active. Performance remained consistent, with average uplink throughput of ~570 kbps and uplink round-trip time of ~75 ms, aligning with typical AMI and meter backhaul requirements.

Test Case #3: Improving Network Efficiency by Releasing Connections Faster

A Release Assistance Indicator[25] (RAI) refers to the setting that tells a network device to disconnect quickly after sending data, freeing capacity for other devices. RAI allows network resources to be released faster (within 1 second of inactivity) rather than waiting for the normal 5-second timeout. This efficiency is critical for private networks with only a single Cat-M1 channel, where directly connected meters could otherwise exceed network capacity.

Releasing unused connections more quickly frees up network space for other devices.

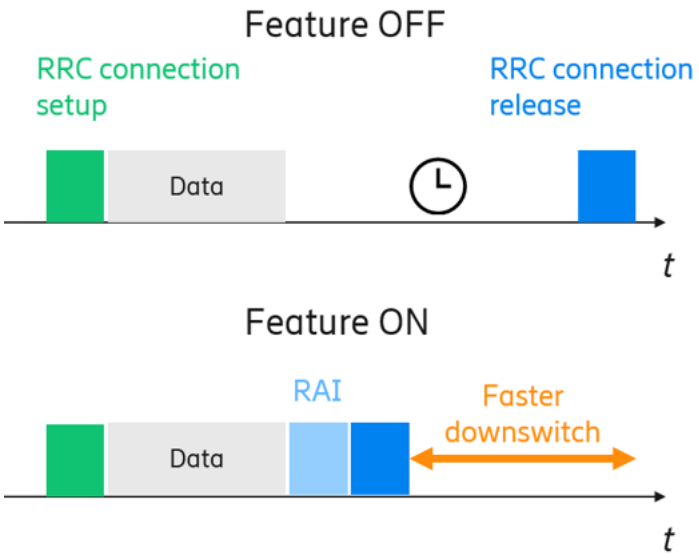

Figure 39: RRC vs RAI

Purpose/Objective

To determine if the RAI feature is ready for real-world deployment in private cellular networks supporting AMI 2.0 meters by assessing the number of devices a network can support and improving efficiency on private networks.

[25] https://docs.nordicsemi.com/bundle/ncs-3.2.0-preview3/page/nrfxlib/nrf_modem/doc/sockets/rai.html

Test Infrastructure/Environment

- Cat-M1 modules
  - Nordic
  - Sequans
  - Sierra Wireless
- Private network
- Frequency bands (Band 8 and Band 26)

Demonstration Flow

- Three different Cat-M1 devices from separate manufacturers are set up to test the RAI feature.
- Each device is configured according to its method — some using AT commands, others using timer settings.
- The devices are connected to the private Cat-M1 network, simulating typical AMI 2.0 meter traffic.
- The meters operate normally, and periods of inactivity are introduced to trigger the RAI mechanism.
- Inactivity shorter than 1 second is tested to confirm that sessions would disconnect and automatically reconnect as designed.

Results

- RAI worked consistently across all tested Cat-M1 devices with no device-specific issues.
- When a device stopped sending data for 1 second, the network safely released its session resources without any unexpected disconnects or slow reconnections.
- The captured logs verified that the UE (User Equipment) Context Release Request was sent correctly 1 second after the last ping.
- Device performance was consistent across frequency bands.
- Network capacity was used more efficiently.

Benefits, Lessons, & Takeaways

- Cat-M1 meters can safely “let go” of the network when they are done transmitting, without causing connection problems.
- Using a 1-second idle timeout strikes a practical balance by keeping connections stable while freeing up space for more meters, enabling utilities to support more devices on the same network without congestion or added infrastructure.
- Shorter timeouts can cause unnecessary reconnects. When a much shorter timeout (200 milliseconds) was tested, connections were repeatedly closed and reopened between packets. While this was technically expected, it created avoidable overhead and was not suitable for meter traffic, so the 1-second setting was chosen instead.
- While full network loading was not simulated, this approach is expected to increase overall capacity by roughly 30–50% compared to older settings.

Test Case #4: Delivering Near Real-Time Meter Data Over Private Wireless

Extended Transfer Block Size[26] (TBS) enables the network to send larger amounts of data at once, instead of sending it in several smaller amounts.

16QAM modulation[27] enhances spectrum efficiency and data transmissions.

Purpose/Objective

To determine if a private Cat-M1 network can:

- Handle high-frequency meter data streams (1-second power updates and 5-second energy data)
- Support a realistic adoption rate (10–25% customer uptake)
- Maintain network performance and reliability that's comparable to or better than Wi-Fi
- Evaluate the effect of Extended Transfer Block Size (TBS) and 16QAM modulation on throughput and sector capacity.

Test Infrastructure/Environment

- Private LTE network
- Itron test meter
- Load device
- Itron data hub

Demonstration Flow

- A test meter is connected to a controllable load device (heater) to simulate real-time power changes.
- The meter streams high-frequency power measurements over a private Cat-M1 LTE network to the Itron data hub, allowing operators to view near real-time data on a portal.
- Network parameters are adjusted to maximize throughput:
    - Extended TBS enables larger data blocks per transmission.
    - Modulation changes from QPSK to 16QAM in strong network conditions to increase data rates.
- The meter is configured to send 1-second data every 2 seconds, simulating a high-frequency load scenario.
- Performance is tested across the cell coverage area, including strong-signal conditions and the outer edge of the cell.
- Additional simulations explore optimization options, including sending data every 5 seconds and adjusting HTTP timers, to estimate scalability for multiple subscribers.

[26] https://wraycastle.com/blogs/knowledge-base/transport-block-size
[27] https://16qam-system.readthedocs.io/en/latest/

Results

- Sending data every 2 seconds allowed about 100 meters to report at once.
- Using the improved network settings, data speed reached up to 600 kbps in strong signal areas.
- At the far edges of coverage, speed was slower, around 180 kbps.
- Changing the update interval to every 5 seconds allowed about 1,000 meters to report at once.
- Data sent over the private Cat-M1 network arrived quickly with no noticeable delays.
- NB-IoT network showed occasional interruptions or glitches.
- Real-time display of meter loads worked smoothly.

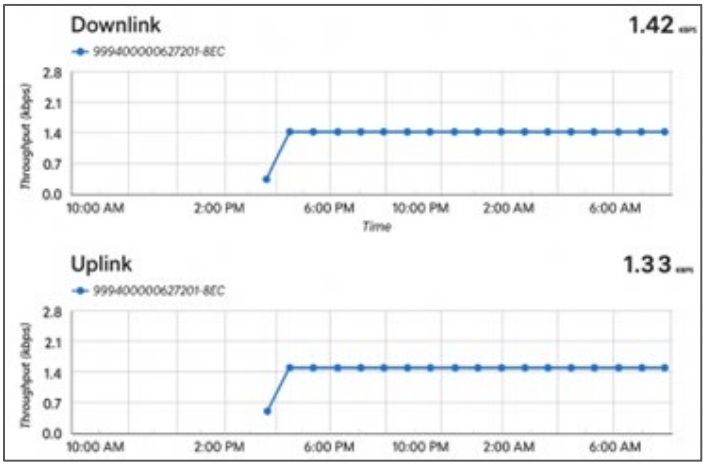

Figure 40: Customer Engagement Streaming Agent Network Trace

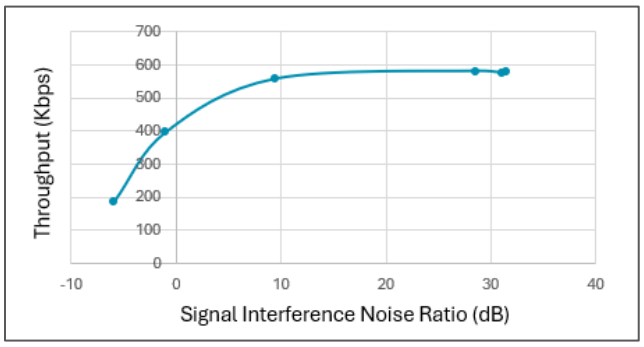

Figure 41: Throughput (kbps) vs. Signal Interference Noise Ratio (dB) with Extended TBS Enabled

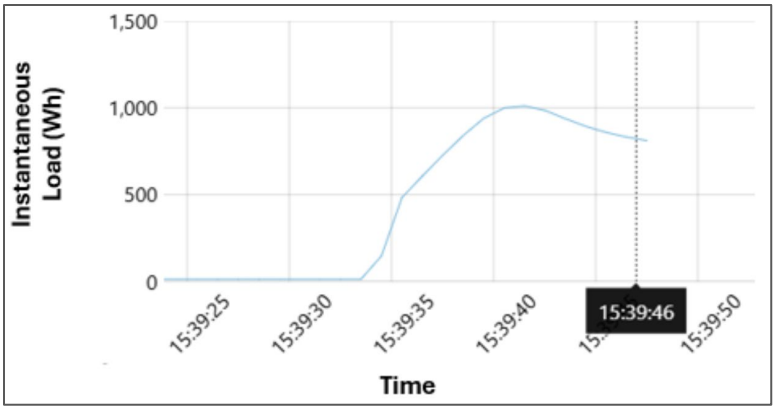

Figure 42: Instantaneous Load (Wh) on meter with Cat-M

Benefits, Lessons, & Takeaways

- Private LTE Cat-M1 networks are a viable alternative to Wi-Fi for delivering high-frequency AMI 2.0 data, providing better reliability, scalability, and operational efficiency while supporting enhanced customer engagement.

Test Case #5: Supporting Advanced Grid Monitoring Over Wireless

Traditionally, high-speed grid monitoring data requires fiber. But with STTP, fiber is an option, not a requirement. The Streaming Telemetry Transport Protocol[28] (STTP) refers to an industry standard for transporting high-volume, continuous streams of data. STTP protocol is agnostic to the data transmission method, so long as it's IP-based.

A Power Flow Simulator (also known as a Power Flow Data Generator) helps mimic real-world power conditions and electrical behavior in the field by generating representative grid data, including voltage, current, phase angles, frequency, and power.

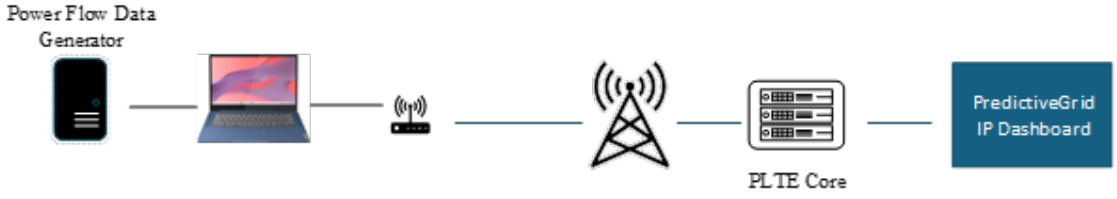

Figure 43: Power Flow Data Generator

[28] https://sttp.info/

Purpose/Objective

To determine if private LTE/5G networks can reliably maintain data integrity while transmitting GPS-synchronized, high-frequency time-series data from utility equipment to support real-time grid monitoring and mission-critical applications such as power quality analysis, fault detection, and renewable energy integration.

Test Infrastructure/Environment

- Power Flow Simulator
- Private LTE network
- Gateway device
- PredictiveGrid dashboard
- PQ meter
- PMU
- Synchrophasor
- Advanced Substation Monitor
- Point-on-Wave Monitor

NOTE: Network speed and delay were not the focus of this testing. The goal was to evaluate how the applications behaved, not to measure network performance. As a result, the test environment was not tuned to capture latency or packet loss. Some test conditions were intentionally unrealistic — for example, placing thousands of devices on a single tower — which would never happen in a real utility deployment, where only one or two such devices are typically present per site. Because of this, any network timing results from this test should not be viewed as representative of real-world performance.

Demonstration Flow

- A Power Flow Simulator generates representative grid data.
- Data points are streamed through the STTP protocol over a private LTE network using a 3 MHz × 3 MHz channel, which supports continuous high-speed data.
- The data passes through a gateway device and is displayed on a PredictiveGrid dashboard, allowing operators to visualize the high-frequency measurements in real time.
- The sampling frequency is adjusted to simulate different real-world use cases:
    - PQ Meter: 1 sample/sec
    - Distribution PMU: 30 samples/sec
    - Transmission Synchrophasor: 60 samples/sec
    - Advanced Substation Monitor: 500 samples/sec (future use)
    - Point-on-Wave Monitor: 3000 samples/sec (future use)
- Each test point sends 25 bytes of data per sample, representing detailed electrical measurements from multiple phases and meters.

Results

- Private LTE successfully transmitted high-frequency, time-synchronized data without noticeable delay or data loss.
- GPS synchronization allowed alignment of measurements across multiple locations, critical for wide-area situational awareness.
- The network supported multiple devices per tower, with capacity for additional growth.

Device	Units/Substation	Growth Potential
PQ Meters	40 units/substation	150×
PMUs	24 units/substation	85×
Transmission Synchrophasor	6 units/substation	16×
Advanced Substation Monitors	2 units/substation	20×
Point-on-Wave Monitors	1 unit/substation	7×

Figure 44 - Capacity Growth Potentials

- Wireless performance met monitoring requirements.

Benefits, Lessons, & Takeaways

- The dashboard allowed testing of real-time signal quality, latency, and synchronization across multiple devices and locations, demonstrating how the system could handle high-speed, continuous data.
- High-fidelity data enables real-time detection of voltage fluctuations, oscillations, and potential grid instabilities that traditional SCADA systems cannot capture.
- Private LTE/5G networks can complement or replace fiber in many grid-monitoring scenarios, giving utilities the precision, visibility, and control needed for modern grid operations and future advanced applications.

Test Case #6: Network Resiliency Through Remote SIM Provisioning (SGP.32)

Utilities need resilient communications that can adapt over time and ensure devices stay connected even when a network goes down. SGP.32 enables remote eSIM profile management for IoT devices, adapted from consumer eSIM specifications.

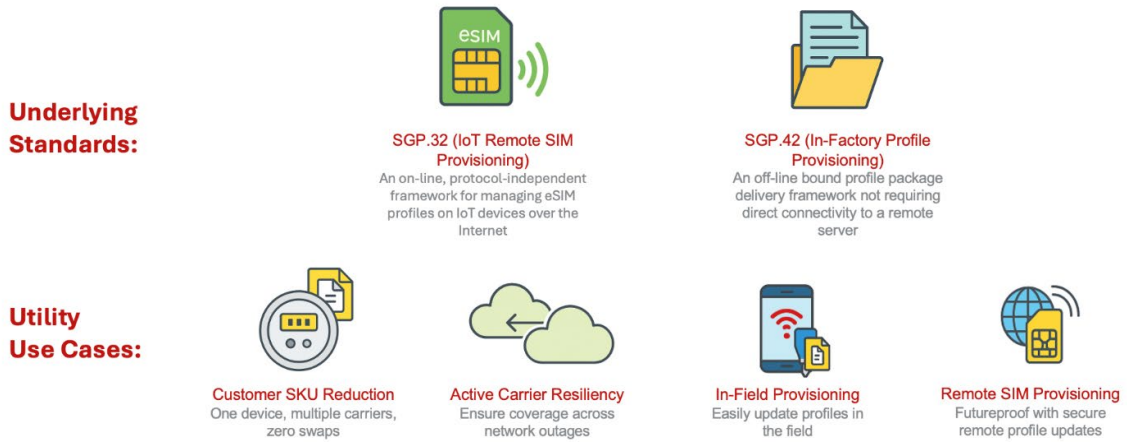

Figure 45: SGP.32

Purpose/Objective

To determine if automatic switching between networks without manual intervention is possible using the SGP.32 remote SIM provisioning standard. Specifically, this test case focused on several real-world utility needs:

- Starting devices on public cellular and later transitioning to private cellular once a private network is built
- Adding a backup carrier for redundancy or improved coverage
- Automatically switching to a backup network during outages
- Returning devices to the primary network once service is restored
- Managing all of this remotely, without truck rolls

Test Infrastructure/Environment

- Private LTE network
- Public Verizon profile
- eIM system
- IoT devices
- Simulated network outage

Demonstration Flow

- A utility device is initially connected to a private LTE network using an eSIM.
- A new public cellular profile (Verizon) is prepared for download using an eSIM IoT Manager (eIM) system.
- The network operator enters an activation code into the SIM management platform, which creates a secure job to download the new profile to the device.
- The device checks in with the eIM and downloads the new cellular profile over a standard secure internet connection.
- The new profile is installed.
- The private LTE network is intentionally shut down to simulate a network outage.
- The eSIM detects the loss of coverage and, after a short timer expires, automatically switches to the backup public cellular profile.
- The private LTE network is restored.
- A command is sent from the eIM to switch the device back to its original private network profile.
- The device automatically reconnects to the private LTE network.

Results

- Devices were successfully initially deployed on the public cellular network.
- Cellular profiles were successfully downloaded and installed, typically in about one minute for small profiles.
- Devices successfully switched to a backup network when the primary network went offline.
- Devices successfully reconnected to the primary network after restoration without manual intervention.
- Backup carriers for redundancy or improved coverage were successfully added.

Benefits, Lessons, & Takeaways

- Remote SIM provisioning using SGP.32 is a practical utility-ready solution for building resilient, flexible communication networks that can adapt over the life of the grid.
- Active carrier switching works reliably using SGP.32.
- An eIM can serve as a single central hub, simplifying secure connectivity to multiple carriers.
- Being able to manage the entire process remotely reduces costly or time-consuming truck rolls.

Test Case #7: Security and Visibility for Private Wireless Networks

With the rapid increase in connected grid assets, utilities require stronger protections against external threats and faster detection of abnormal activity.

Purpose/Objective

To determine if advanced security and asset management tools can identify all connected devices, reduce cybersecurity risk, and improve situational awareness across private cellular networks.

Test Infrastructure/Environment

- Private network
- IoT devices:
  - BEC
  - Nokia SAR-Hmc
  - Nordic nRF9160
  - Sequans GM02S
  - Sierra Wireless HL-7810
- OneLayer Bridge™[29]
- Nokia Core Enterprise Solutions (NetGuard security suite)
- Zero-trust security capabilities, including asset discovery, micro-segmentation, geofencing, anomaly detection, and orchestrated mitigation

Demonstration Flow

NOTE: The NetGuard–OneLayer integration was not demonstrated at Plugfest.

- All devices connecting to the private 5G/LTE network are automatically discovered and fingerprinted, including operational technology (OT) devices connected behind cellular routers.
  - OneLayer Bridge™ is used to identify and protect all devices connected to the private 5G/LTE network, including utility endpoints and field assets, which provides clear visibility into previously hidden equipment.

[29] https://onelayer.com/introducing-onelayer-bridge-a-private-cellular-security-solution/

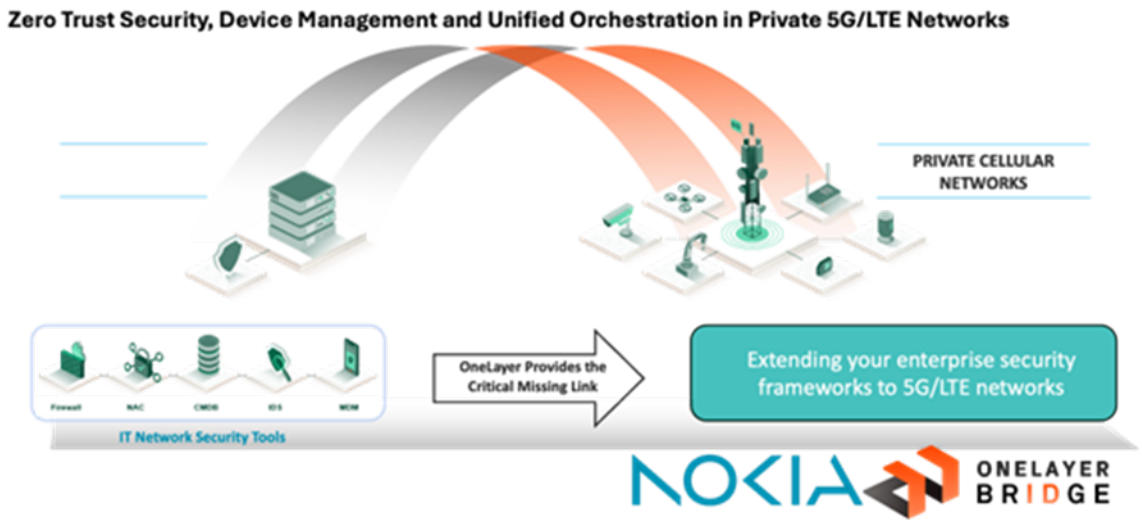

Figure 46: Nokia OneLayer Bridge

- Nokia Core Enterprise Solutions, combined with OneLayer, secures the network and device identities while giving the team a complete view of connected devices and their activity across the private wireless environment.

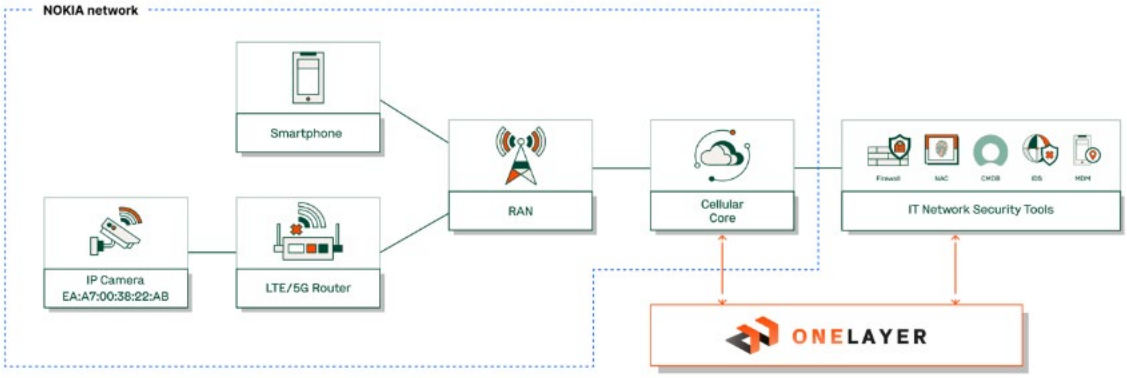

Figure 47: Nokia One Layer Bridge

- Zero-trust security is validated with real device events. Multiple devices are monitored, and simulated incidents — such as SIM swaps, unauthorized manufacturer devices, and device changes behind routers — trigger alerts in the system monitoring view.

Results

- Full visibility of all devices connected to the private wireless network, including previously hidden or unmanaged assets, was achieved.

Benefits, Lessons, & Takeaways

- Faster detection of abnormal or unexpected network activity
- As private wireless networks scale, clear visibility and strong security controls become essential.

- Utilities can securely deploy and manage private 5G/LTE networks while maintaining awareness of every connected device.
- By applying zero-trust principles and continuous monitoring, utilities can better isolate and respond to potential security incidents before they impact operations. Utilities are enabled to reduce cyber risk, accelerate incident response, and protect critical grid operations as device counts continue to grow.
- OneLayer Bridge™ benefits private 5G/LTE security and OT asset management by extending protection to utility endpoints and field assets.

Test Case #8: Managing Distributed Energy Resources Over Wireless

As utilities integrate more distributed energy resources (DERs) such as rooftop solar and community-scale generation, they must:

- Maintain safe voltage levels on distribution circuits
- Prevent unintentional islanding (when generation continues feeding a circuit during an outage)
- Respond rapidly to fault conditions
- Coordinate monitoring and control across field devices and control centers

Direct Transfer Trip (DTT) refers to a method to quickly disconnect energy devices during a fault to protect the grid.

Purpose/Objective

To determine if private wireless networks can reliably support DER monitoring, control, and protection functions while responding quickly during fault conditions.

Test Infrastructure/Environment

- Solar inverter
- DERMS
- Voltage sensor
- Inverter
- Feeder
- Simulated fault conditions
- Private wireless network
- NB-IoT
- LTE/Cat-M1
- 5G RedCap

Demonstration Flow

- A solar inverter is connected to the grid and placed under the control of the utility's Distributed Energy Resources Management System (DERMS), located at the utility data center.
- A voltage sensor on the distribution feeder continuously measures voltage and sends readings to the DERMS over a private wireless network.
- During normal operation, the DERMS analyzes the voltage data and sends control commands to the inverter to adjust output and keep voltage within safe limits.
- Fault conditions on the feeder are simulated using protection relays.
- When a fault is detected, a Direct Transfer Trip (DTT) signal is triggered over the low-latency private wireless network.
- The inverter is automatically disconnected from the feeder to prevent overvoltage or unintentional islanding.
- Different wireless technologies (NB-IoT, LTE/Cat-M1, and 5G RedCap) are evaluated to confirm they can support monitoring, control, and protection requirements.

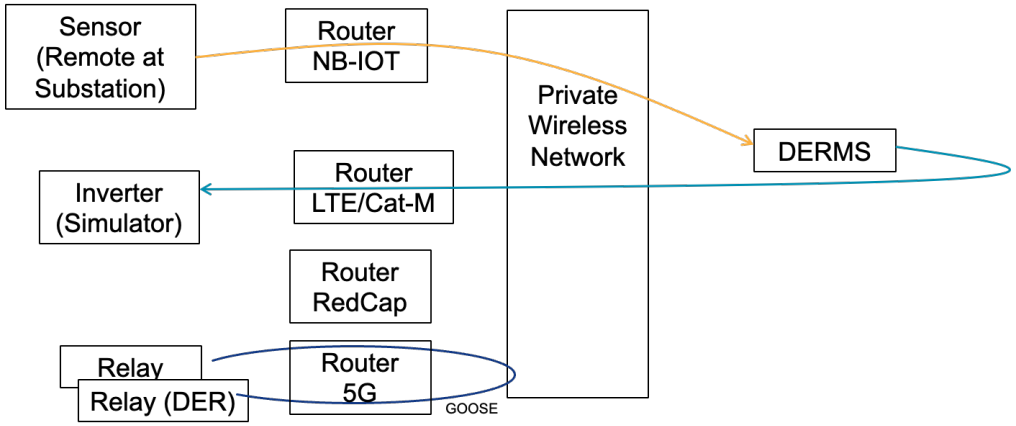

Figure 48: DERMS Data Flow

Results

- Voltage successfully stayed within limits.
- Control actions occurred as expected.
- The network enabled a fast response that safely disconnected the solar system to prevent damage or unsafe conditions when a problem was simulated on the line.

Benefits, Lessons, & Takeaways

- Private wireless networks can effectively support how utilities monitor and manage distributed energy resources like solar.
- The system keeps voltage levels within safe limits during normal conditions by sharing measurements and adjusting equipment automatically.
- Reliable wireless communication helps utilities safely integrate more renewable energy while keeping the grid stable.

Test Case #9: Low-Power Connectivity for Simple Utility Devices

NB-IoT[30], a low-power wireless technology, can support simple utility devices that send small amounts of data and are expected to operate for long periods without frequent battery replacement. These types of devices are often used for basic monitoring where speed is less critical.

Purpose/Objective

To determine if NB-IoT can provide reliable coverage while maximizing battery life for large numbers of low-power sensors deployed across wide service areas.

NOTE: The testing focused on how well the network performed for basic data reporting rather than fast or time-critical communications.

Test Infrastructure/Environment

- NB-IoT
- Band 103
- Aclara Meter
- Nokia EPC

Demonstration Flow

- Devices are connected using NB-IoT.

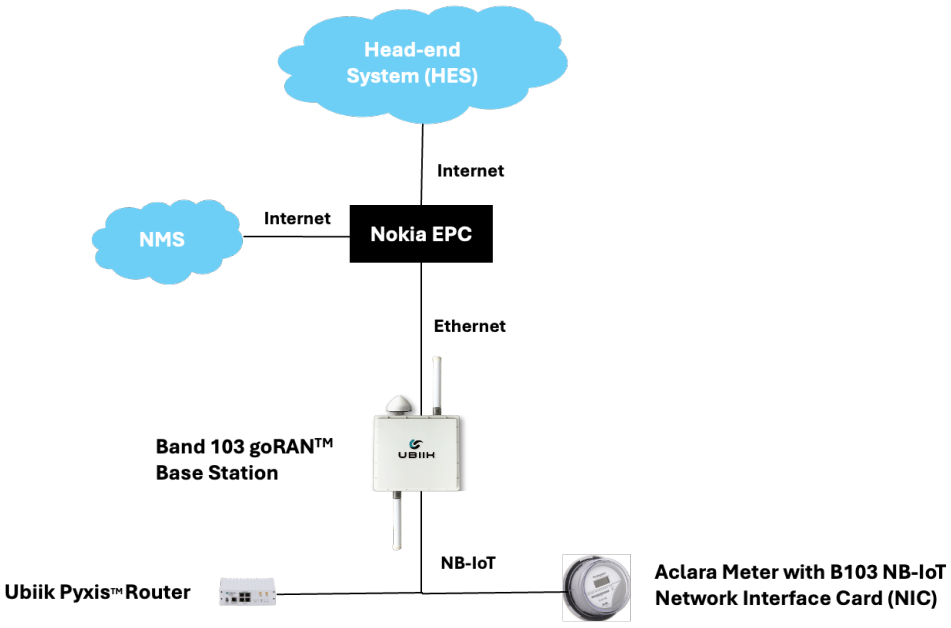

Figure 49: B103 NM-IoT

- Devices are tested for coverage, reliability, and power consumption.

[30] https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/narrow-band-internet-of-things-nb-iot/

Results

- Coverage, power use, and reliability were successfully evaluated and showed strong coverage and very low power usage, allowing devices to operate for extended periods on a single battery.

Benefits, Lessons, & Takeaways

- NB-IoT is a good fit for simple, non-critical utility applications such as basic sensors and status monitoring.
    - Since NB-IoT is designed for small data transmissions, it is not well-suited for applications that require quick responses, frequent updates, or large data transfers.
- With its wide-area coverage and ability to support large numbers of devices, NB-IoT offers utilities a cost-effective option for long-lasting, low-maintenance deployments — especially when used alongside other wireless technologies that handle more demanding use cases.

Overall Lessons & Takeaways

- **No single network fits every use case.** Utilities benefit from flexible designs that allow private and public networks to work together.
- **Today's technologies are ready now.** Existing cellular and wireless solutions can reliably support AMI 2.0 and core grid applications.
- **Plan for evolution, not replacement.** Devices and networks should be chosen with future standards and growth in mind.
- **Network capacity can be shared efficiently.** Dynamic use of network resources supports more devices without overbuilding infrastructure.
- **Small adjustments make a big difference.** Minor configuration changes can significantly improve performance and scalability.
- **Private wireless is operationally ready.** Private networks can support mission-critical utility applications at scale.
- **Automatic network switching improves resiliency.** Devices that can move between networks reduce outages and field intervention.
- **Visibility and security are essential.** Knowing what devices are connected and how they behave is foundational to secure operations.
- **Wireless can replace fiber in some cases.** Modern wireless networks can support advanced, time-sensitive grid applications.
- **Operational simplicity matters.** Solutions that are easier to manage are more likely to succeed in real-world utility environments.

Cumulative Glossary

Acronym / Term	Definition
Advanced Substation Monitors	Devices that monitor substations for high-resolution electrical data.
AMI / Advanced Metering Infrastructure	Systems for remotely reading meters without manual visits. Automated data transfer between meter endpoints and utilities.
AMI 2.0 / Advanced Metering Infrastructure 2.0	Modern smart meters and systems that send energy usage data frequently and automatically, helping utilities monitor and manage the grid.
AMR / Automated Meter Reading	Technology that automatically collects meter data when in physical proximity.
APN / Access Point Name	A gateway setting that allows devices to connect to a mobile operator's data network and access external networks like the internet.
Band 106 / Band 26	Specific frequency ranges used for LTE networks. [B106 = 900MHz, B26 = 850MHz]
Cat-M1 / Category M1 (also called LTE-M)	A low-power LTE standard for IoT devices with moderate data speeds (~1 Mbps) and low energy use, suitable for battery-powered meters and sensors.
CMP / Connectivity Management Platform	A centralized control of eSIM connectivity, managing networks, profiles, and devices from one unified interface.
CPD / Constantly Powered Device	IoT device that is always connected to a power source, like an electricity meter.
CoWs / Cells on Wheels	Portable cellular base stations mounted on trailers or trucks that can be rapidly deployed to restore or enhance wireless coverage during emergencies or special events.
DERMS / Distributed Energy Resources Management System	A system that monitors and controls distributed energy resources (like solar panels, batteries, or small generators) so the grid stays stable, voltage stays safe, and power is balanced.
DP+ server / Data Preparation Plus server	A GSMA-defined server that prepares, encrypts, and delivers eSIM profiles to devices during remote SIM provisioning and profile switching.

DTT / Direct Transfer Trip	A method to quickly disconnect energy devices, like a solar inverter, during a fault to protect the grid.
Dynamic Traffic Prioritization	Network capability to give priority to critical communications over less urgent IoT data during congestion.
eDRX / Extended Discontinuous Reception	Power-saving mode for IoT devices that allows them to “sleep” but still listen for network messages at set intervals.
eIM / eSIM IoT Manager	A GSMA-defined management system introduced with SGP.32 that coordinates remote eSIM profile lifecycle management, including downloading, activating, and switching profiles.
eSIM / embedded Subscriber Identity Module	A digital SIM embedded in a device that enables remote provisioning, activation, and switching of mobile network profiles without requiring a physical SIM card.
eSIM server / embedded Subscriber Identity Module server	A backend system that supports the provisioning, management, and lifecycle control of eSIM profiles, typically implemented through SM-DP+/DP+ and eIM functions.
eUICC / Embedded Universal Integrated Circuit Card	The secure hardware component within a device that stores and manages one or more eSIM profiles and enforces profile switching and security policies.
Extended TBS / Extended Transfer Block Size	A setting that allows devices to send larger chunks of data at once, improving throughput on wireless networks.
GSMA / Global System for Mobile Communications Association	The group that sets standards and guidelines to make mobile networks, devices, and services work together.
Guard Bands	Frequency ranges between LTE carriers used to minimize interference and sometimes host NB-IoT devices.
High-Fidelity Data	Detailed, precise data with minimal loss, used here for real-time grid monitoring.
Incremental Download	Process of sending data (like an eSIM profile) in small pieces, allowing interrupted downloads to resume.
IoT / Internet of Things	A network of physical objects (i.e., devices, appliances, and sensors) that are equipped with software and internet connectivity. This allows them to collect, share, and act on data, creating “smart”

	environments that can monitor conditions, automate tasks, and improve efficiency without direct human control.
IPX / IP eXchange	A “middleman” network that enables secure communication and interoperability between different mobile networks without requiring a direct connection.
IWF / Interworking Function	A network component that translates or bridges different communication protocols so that devices on different networks can communicate seamlessly.
LMR / Land Mobile Radio	A wireless communication system used by public safety, utilities, and other organizations for voice and data communication over a dedicated radio network.
LTE / Long-Term Evolution	Standard for mobile broadband networks.
Massive IoT	Large-scale deployment of low-power IoT devices like smart meters and sensors that operate reliably over long periods.
MC / Mission-critical	Refers to the systems/functions essential to the success and safety of an operation during emergency situations.
MCPTT / Mission-critical push-to-talk	A 3GPP-standardized service that provides instant, secure, group-based voice communications with priority and preemption over LTE and 5G networks.
MCX / Mission-critical talk, data, and voice	MCX encompasses mission-critical push-to-talk (MCPTT), mission-critical data (MCData), and mission-critical video (MCVideo).
MNO / Mobile Network Operator	A company that provides wireless communication services to customers and owns the physical network infrastructure.
MVNO / Mobile Virtual Network Operator	A company that provides wireless communication services to customers, but does not own the infrastructure. Instead, MVNOs lease network access from an MNO and then resell it under their own brand.
NB-IoT / Narrowband IoT	A low-power cellular technology for IoT devices, offering long battery life, deep coverage, and cost efficiency.
Network Management Tool	Software used to monitor, configure, and control devices and network operations.

NOC / Network Operation Center	A centralized facility where network performance, availability, security, and incidents are monitored and managed.
NTN / Non-Terrestrial Network	A 3GPP-defined network architecture that provides connectivity via satellites or other non-ground-based platforms to extend coverage beyond terrestrial networks.
Over-the-top MCX services	The network does not provide any special “treatment,” such as priority or preemption.
P25 / Project 25	A suite of standards for digital two-way radio communications used by public safety agencies to ensure interoperability between different vendors’ systems.
PLMN / Public Land Mobile Network	A mobile network (public or private).
pLTE / Private LTE	LTE network deployed and operated privately by utilities for dedicated, secure communication.
Private LTE Profile	LTE network configuration stored on an eSIM or device, allowing it to connect to a specific private LTE network.
PMU / Phasor Measurement Unit	Device that measures voltage and current phasors in real time, providing GPS-synchronized data for grid monitoring.
Point-on-Wave Monitors	Devices that capture precise waveform measurements of electricity at very high sampling rates.
Power Flow Simulator	Software used to mimic real-world electricity flow and test devices under realistic conditions.
PQ Meters / Power Quality Meters	Devices that measure voltage, current, and other quality metrics of electricity at high sample rates.
PSM / Power Saving Mode	LTE IoT device power-saving mode where the device sleeps between scheduled transmissions to conserve energy.
PWLS / Private Wireless Network	A utility- or enterprise-owned cellular network that provides localized, secure, and controlled wireless connectivity independent of public carrier infrastructure.
RAN / Radio Access Network	The portion of a cellular network that connects end-user devices to the core network via radio technologies such as LTE or 5G.
RAI / Release Assistance Indicator	A setting that tells a network device to disconnect quickly after sending data, freeing capacity for other devices.

RedCap/eRedCap / Reduced Capability 5G	A 5G technology for IoT devices that need higher (85-150Mbps) data rates or lower latency than LTE-M, while still being energy-efficient.
Sample Rate	Samples/second. How many measurements a device takes per second. Higher rates give more detailed data.
SAS / Security Accreditation Scheme	Ensures that devices, eSIMs, and profiles are installed and updated securely, following industry security standards.
SCADA / Supervisory Control and Data Acquisition	System used by utilities to monitor and control the grid.
SGP.32	A GSMA standard that defines remote eSIM provisioning and management of IoT devices.
SGP.42	A GSMA standard that enables eSIM profile provisioning during factory production.
SIM OTA / SIM Over-the-Air	A method for remotely updating, managing, and provisioning SIM or eSIM profiles without physical access to the device.
SM-DP+ server / Subscriber Manager Data Preparation+ server	A GSMA-defined server responsible for securely preparing, encrypting, and delivering eSIM profiles to devices during remote provisioning.
Transmission Synchrophasor	High-speed phasor measurement devices at the transmission level for time-synchronized monitoring.
Utility Network Efficiency	How effectively a utility's network handles multiple devices, data types, and communications without delays or interference.
3GPP / Third Generation Partnership Project	3GPP is the international standards organization that defines how mission-critical services should work.

Conclusion

The 2025 UBBA Summit & Plugfest was a standout success, reinforcing UBBA's position as the leading catalyst for utility broadband innovation. The event demonstrated that utility communications are entering a new era: One where private broadband networks, combined with public and hybrid connectivity, deliver the speed, reliability, and resilience required for modern grid operations.

The UBBA Plugfest 2025 proved that utilities are not simply evaluating new technologies — they are actively deploying them, testing them, and integrating them into real-world operations. The event's live demonstrations and collaborative testing validated that modern communications architectures can support the scale, security, and performance demands of the grid today and into the future.

For utility leaders, the message is clear: modern utility communications are not optional upgrades — they are strategic business imperatives. The success of the 2025 UBBA Plugfest also showed that collaboration between utilities, solution providers, and ecosystem partners is accelerating the pace of innovation across the industry.

UBBA Plugfest remains the premier platform for collaboration, innovation, and real-world testing, helping utilities make confident decisions, reduce deployment risk, and drive the future of critical infrastructure connectivity. As the industry continues to evolve, UBBA and its Plugfest process will remain the place where utilities can see tomorrow's communications capabilities in action today.

Contributing UBBA Members

- Anterix
- Ericsson
- Nokia

- Duke Energy
- Duquesne Light
- Exelon
- San Diego Gas & Electric
- Salt River Project
- Southern California Edison
- Southern Company
- Xcel Energy

- BEC Technologies
- Black & Veatch
- Giesecke + Devrient
- Hitachi Energy
- Itron
- Kigen
- L3Harris
- Landis + Gyr
- Motorola
- One Layer Verizon
- Palo Alto Networks
- Thales
- Ubiik

UBBA
Utility Broadband Alliance