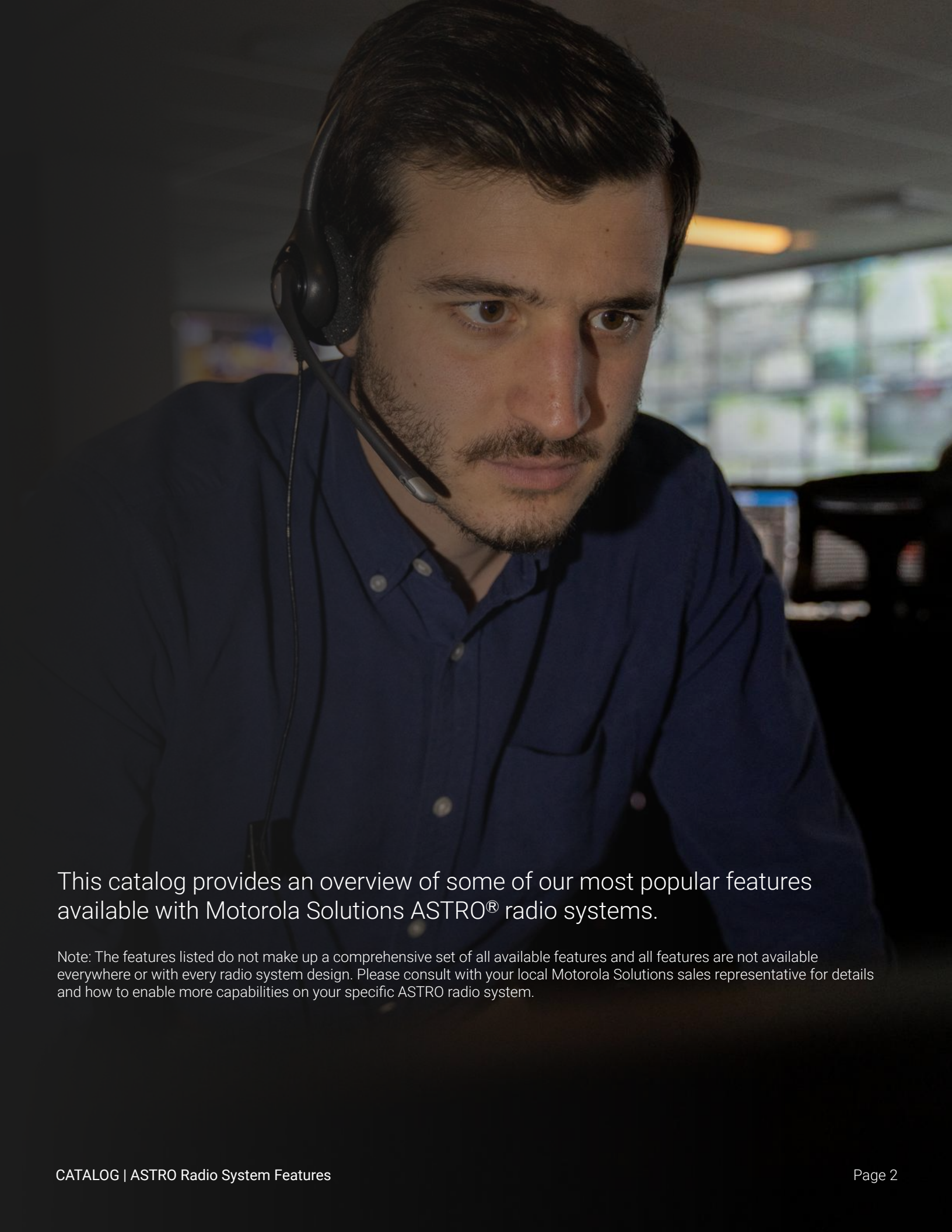
ASTRO Radio Systems Feature Catalog

MOTOROLA SOLUTIONS



This catalog provides an overview of some of our most popular features available with Motorola Solutions ASTRO® radio systems.

Note: The features listed do not make up a comprehensive set of all available features and all features are not available everywhere or with every radio system design. Please consult with your local Motorola Solutions sales representative for details and how to enable more capabilities on your specific ASTRO radio system.

Table of Contents

Operational Modes

Enable the call types that can improve the efficiency and operations of your fleet and visitors.

Operational Modes

P25 FDMA Trunking Operation

P25 Phase 1 FDMA (Frequency Division Multiple Access) is the original modulation scheme defined in the P25 standard for digital voice communication. The narrowband channel is defined in the standard as 12.5 kHz wide.

P25 Digital Conventional Operation

This feature adds support for P25 standards-compliant conventional channels onto ASTRO trunking systems.

Adding conventional channels to ASTRO trunking systems allows dispatchers to communicate with both P25 trunking and P25 conventional radio users. Dispatchers can also patch audio between conventional and trunking users to enable communication between groups that normally do not need to interact.

P25 Phase 2 TDMA Trunking

TDMA (Time Division Multiple Access), as defined by the P25 standards in Phase 2, enables two concurrent voice calls in the same 12.5 kHz channel of an FDMA voice call. FDMA operation supports one call per 12.5kHz channel. Compared to FDMA, TDMA increases the voice capacity of the radio system.

ASTRO radio systems with TDMA compatible equipment can add TDMA operation to expand voice capacity without adding base stations and associated equipment and without the need to acquire additional frequencies.

Operational Modes

Dynamic Transcoding

Dynamic Transcoding translates between FDMA and TDMA audio formats for sites in the same system or different systems. This enables radio users of different modes to communicate without downgrading everyone on the call to FDMA, thereby preserving the capacity benefits of TDMA on those sites with all TDMA capable radios.

Radio users from FDMA-only and TDMA-only sites are able to join a Dynamic Talkgroup without changing the modulation at either site.

Dynamic Dual Mode

Dynamic Dual Mode automatically switches call assignments between FDMA and TDMA, with no user intervention, based on subscriber radio and site capabilities. Dynamic Dual Mode consists of two software features that when used together, enables seamless operation of between FDMA and TDMA call services. This may be particularly useful in systems with subscriber radios or site equipment which are only capable of FDMA.

Dynamic Talkgroup Assignment automatically switches configured talkgroups between FDMA and TDMA modes based on the mix of radios participating in the call. When all radios in the call are TDMA capable, the call talkgroup will be assigned as a TDMA call. If any radio is only capable of FDMA-only, the call will be processed as FDMA.

NOTE: Talkgroups can be configured as Dynamic, TDMA-only or FDMA only.

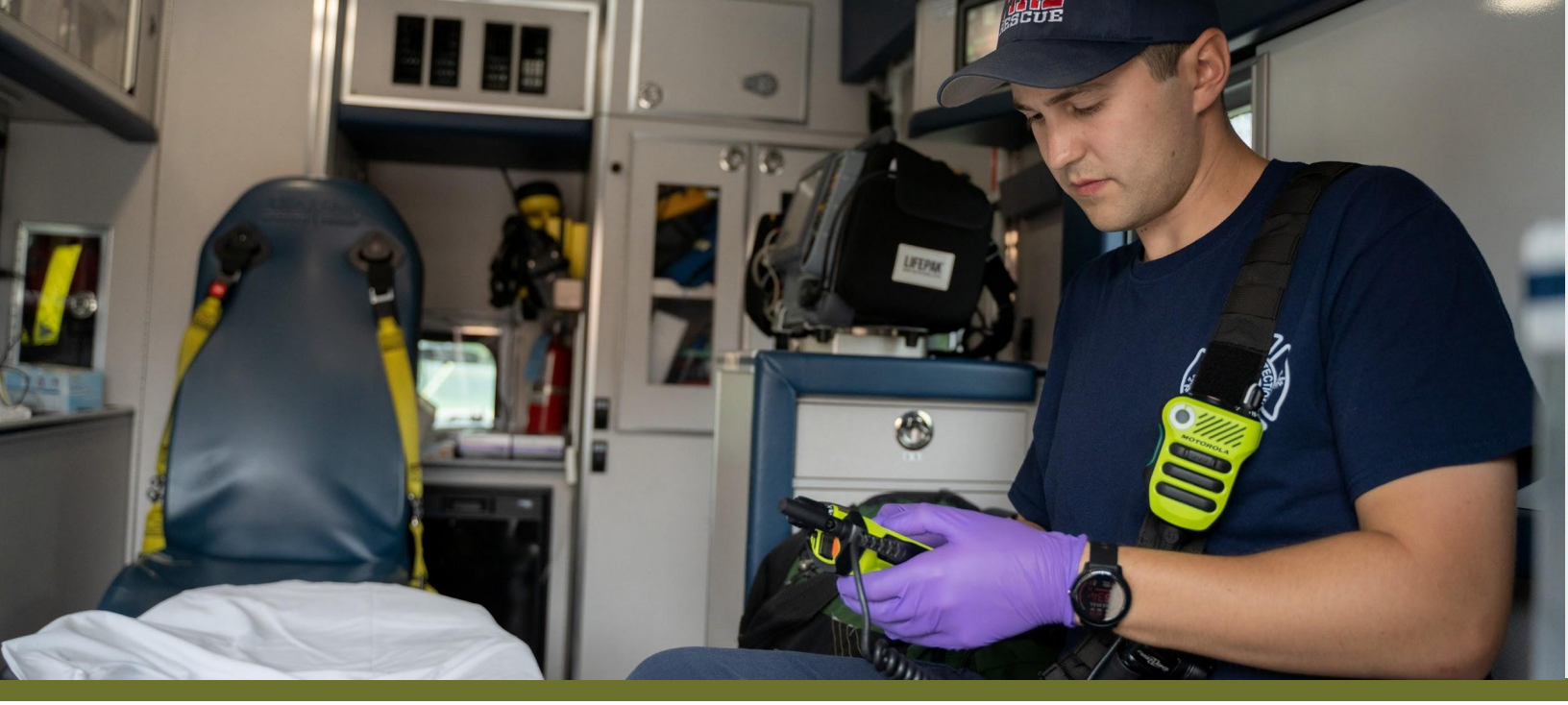
Dynamic Channel Assignment automatically switched the base station between FDMA and TDMA based on the call type.

NOTES:

- ASTRO base stations can be configured as Dynamic, TDMA-only or FDMA-only.

Reliability and Resiliency

Maximize uptime and ensure continuity of operations



Reliability and Resiliency

Dynamic System Resilience (DSR)

Dynamic System Resilience (DSR) adds a geographically separate ASTRO core to protect against a catastrophic failure. DSR includes redundancy for voice, network management, data and information assurance services. In the event that the remote sites cannot connect with their currently active core, the sites will switch to their alternative core.

DSR provides continuity of operations in case of disaster, thus ensuring end user communications are maintained in the event that the primary Master Site experiences a catastrophic event.

Software Redundancy

ASTRO Software Redundancy installs another copy of the ASTRO software within virtual machines onto the ASTRO zone core equipment. In the event of a catastrophic software corruption or failure, the backup software can take over services and quickly restore normal service.

CirrusCentral Core - Resilience Package

CirrusCentral Core is a secondary core for ASTRO systems. It resides in a secure cloud environment, geographically separated from events that may occur locally. It can can take over key ASTRO core functions in the event of a catastrophic loss of the primary ASTRO core site.

The cloud-core runs software that is designed for a cloud environment and is always up to date with new features as they become available. Networking equipment connects the sites and consoles to the cloud-core. The cloud-core cannot be used with systems that already use DSR.

Learn more on our CirrusCentral Core web page.

SmartConnect

When P25 service is unavailable, SmartConnect automatically reroutes P25 voice and data packets over available broadband networks and then back again when back in P25 coverage. P25 voice information is unchanged, so radio functionality and voice quality are maintained.

APX and APX NEXT radios can use SmartConnect based on their equipage and access to broadband connections such as LTE, Wi-Fi and satellite.

Learn more on our SmartConnect webpage.

Reliability and Resiliency

Geo-Redundant Prime Site

Geo-Redundant Prime site maintains wide-area simulcast subsystem operation in the event of a catastrophic loss of a simulcast prime site.

Edge Availability with Wireline Consoles

Edge Availability introduces a fallback option for a trunking subsystem, such as simulcast, in the event that the subsystem loses communication with Master Site. During a fallback condition, Edge Availability passes call control outward to the system edges, allowing the subsystem to maintain services normally provided by the core.

This can be particularly useful in statewide systems to help maintain operations in high-valued regions when communication lines to the core are cut.

Regional areas utilizing Edge Availability benefit from:

- Multi-site voice operation across local RF and dispatch sites
- Talkgroup roaming across local RF sites
- Wireline dispatch capability providing emergency alarm with aliases, console priority and access to all talkgroups without using control stations
- Same talkgroup/user access control for site registrations as in normal wide-area mode

Distributed Conventional Architecture (CSUB)

Distributed Conventional is a an architecture designed for resilient backup conventional operation. The architecture organizes consoles, comparators and conventional channels into a collection known as a Conventional Subsystem (CSUB).

The CSUB can operate independently and continue to process conventional audio during a failure or loss of connectivity to the zone core, or zone cores as in a Dynamic System Resilience (DSR) system. Extensive interconnectivity within the CSUB allows multiple network paths between locations, further increasing resiliency within the CSUB.

High Availability Data

High Availability Data eliminates all single points of failure for P25 data services by providing redundant gateways, software and links that support data traffic. This increases reliability for location and other critical data services.

High Availability Air Traffic Router (ATR)

High Availability ATR provides redundancy with automatic failover for critical ATR applications used to monitor system performance and radio control services.

Data

Enhance your mission-critical voice communications for a safer, quicker and more effective response

Data

Integrated Voice and Data

Integrated Voice and Data provides P25 compliant voice and data communication on the same RF equipment - eliminating the need to dedicate channels for voice or data.

Each channel can be configured to support voice-only, data-only or voice and data traffic. The site will select the channel based on the call type, channel availability and channel capability.

Enhanced Data

Enhanced Data increases data efficiency by up to 12X over standard P25 data inbound data services such as location updates.

- Supports upto 150 data users per channel at a 30 second cadence, with a message size of 24-36 bytes
- Option to protect data channel pre-emption from voice at a site/system
- Independent agencies operating on the same ASTRO network can share Enhanced Data channels

Advanced Messaging Solution

Advanced Messaging enables text-based messaging on ASTRO radio systems. Users can send and receive text messages to individuals and talkgroups directly from their data enabled radio. Command staff can send BOLO alerts and data query information to front-line staff. And when integrated with CAD systems, personnel can automatically receive dispatch information and remotely update their status.

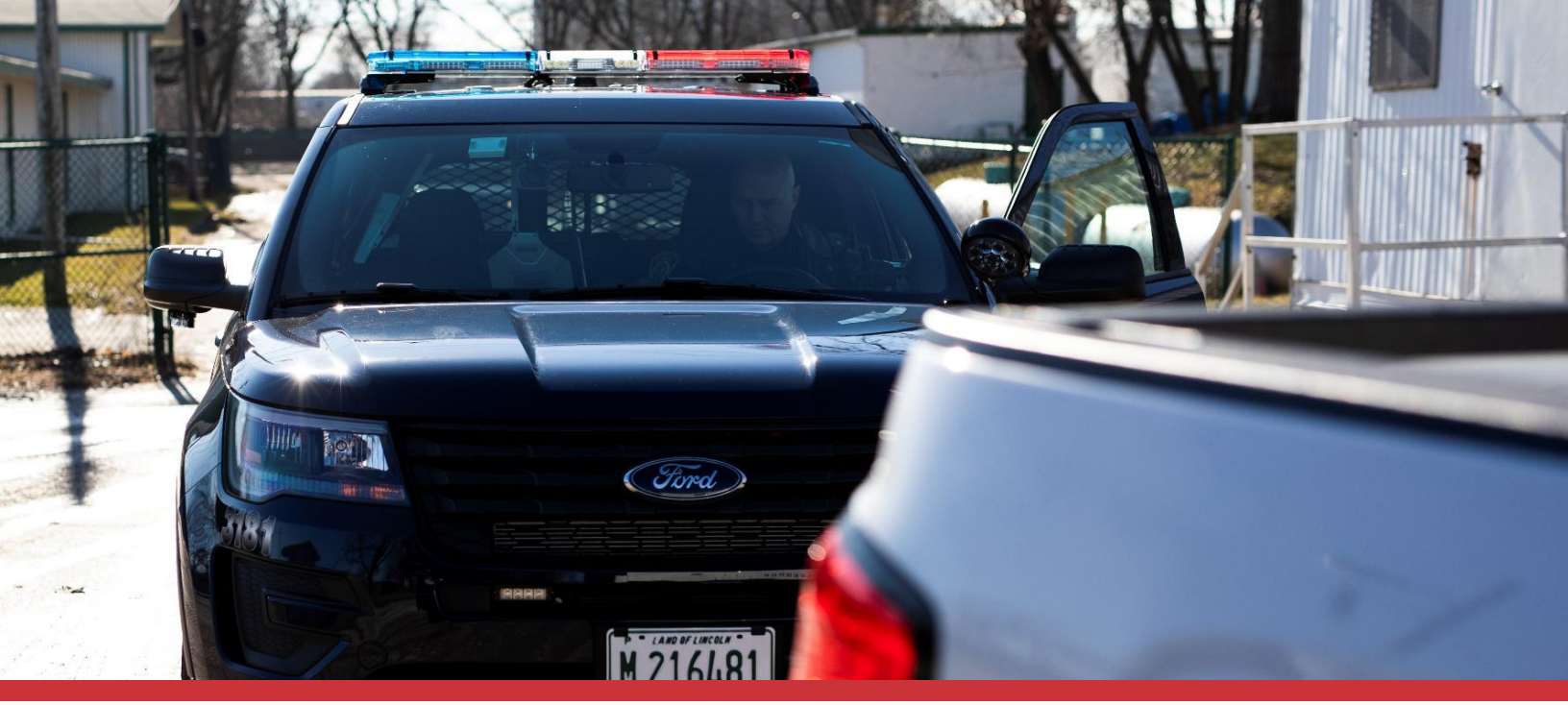
Advanced Messaging Solutions frees up air time for critical voice communications and helps first responders to stay better informed to keep them safer and more able to serve the community.

Learn more on our Advanced Messaging Solution webpage.

Site Selectable Trunking Alerts

Site Selectable Alerts for Trunking introduces the ability to generate pre-configured pre-recorded voice announcement or tone alerts for affiliated ASTRO two-way radios at selected site(s). If equipped, the two-way radio will display the type of alert.

These alerts can help system users be informed of impending critical activities and events that could present life safety risks.



Data

Group Services

Group Services delivers data over a broadcast channel such as a talkgroup. This is an efficient way to disseminate the same data to many radios at once. Unlike a standard talkgroup, the radio receives broadcast data, but cannot send broadcast data. Normal voice traffic has priority, so Group Services pauses whenever there is a voice transmission.

Alias Group Download is a group service that enables the ability to send an updated PTT ID from the Provisioning Manager to multiple radios. When the user of the updated ID presses the PTT button, the alias is updated in the receiving radios' local contact list. This saves time by eliminating the need to manually update radio codeplugs every time a user changes his/her radio.

Watch our Alias Group Download video.

User Login Alias Update is a group service that ensures a radio user's alias is updated on all radios and dispatch consoles with the simple action of a user logging into the radio.

This is useful for agencies that regularly share radios between users and want others to see who is talking. Logging into the radio identifies the user alias and Alias Group Download pushes the alias updates to all radios within the talkgroup.

Talkgroup Text Messaging

This group service enables dispatchers to quickly send a text message to a specific voice talkgroup, reaching every APX radio simultaneously. It is ideal for broadcasting high priority text information - BOLOs, AMBER Alerts, APBs, Weather Alerts and more.

Watch our Talkgroup Text Messaging video.

Over-the-Air Software Updates

This group service distributes radio software to a group of radios over the P25 network as a background service. The process is managed by the Radio Management application. During idle periods, radios will receive a firmware file over a broadcast channel designated for programming. The broadcast will repeat, allowing all radios to receive the updates on during their idle time. Even if it takes days for every radio to receive the full file, this can be faster than bringing each radio into a shop for a manual upgrade.

Flashcode and codeplug files are unique to each radio and are a much smaller file size. These files are delivered during idle periods over an OTAP data channel. When a radio has all 3 files, it will ask the user to accept the upgrade.

- Update an entire fleet without pulling radios and personnel out of the field and into the shop.
- Save time and effort to keep radio software current.
- See the download progress of each radio and each file.

Watch our Over-the-Air Software Update video video.

Data

Location

The ability for radios to send their satellite-based location data to map-based applications is often considered a safety requirement. ASTRO radio systems support APX radio location information over IV&D and Enhanced data channels or a voice channel depending on the type of trigger:

- Periodic / regular cadence
- Distance traveled
- Request
- Power on / off
- Emergency
- PTT / receive

Location on Voice (PTT or Receive) - When location on voice is enabled, APX radios can send location data while on a voice call without leaving the call. On every PTT, APX radios can continuously send location updates over FDMA and TDMA voice channels. While receiving a voice transmission, APX radios can send their location data over inbound TDMA slots or in hangtime without pressing PTT.

Over-the-Air Programming (OTAP)

OTAP, sometimes referred to as Programming Over P25 (POP25), allows a user to configure a radio remotely over a P25 data channel by sending a sequence of commands over-the-air to read and write radio codeplug information.

Mission Critical GeoSelect

Mission Critical GeoSelect allows mapping applications to push new geofences to APX radios, enabling automated radio actions when the radio crosses a boundary. The radio will use its GPS location to determine when a boundary is crossed and then take the prescribed action defined with the fence..

Radio actions can include: change talkgroup/channel, report location, send status update, play audible voice announcement or tone, change radio transmit power level and more.

With Mission Critical GeoSelect, dispatchers can dynamically set a fence around an active incident area. Upon entering the geofence, the radio can play a voice announcement warning of the incident, change the radio to the incident channel and reduce the radio's transmit power. When the radio exits the geofence, it returns to normal operation.

Personnel Accountability

The Personnel Accountability application provides visibility of status of on-scene personnel to the Incident Commander. This NIMS-compliant application provides automatic user/company registration with PTT ID and alias, emergency alarm indication, channel-left indication, low battery indication, power down indication, roll call, evacuation tones, manual and automatic polling.

Learn more on our Personnel Accountability webpage.

Interoperability

Enable seamless communications across agencies, networks and technologies.

Interoperability

Critical Connect

Critical Connect enables interoperable voice and data communication between multiple systems and technologies.

A single P25 standards-compliant ISSI link from the ASTRO radio system to Critical Connect can provide interoperability with other radio systems including ASTRO, MOTOTRBO, 3rd-party P25 systems, public LTE and private broadband networks.

Critical Connect allows frontline personnel to seamlessly collaborate with responders from other agencies, critical infrastructure providers and government officials. Whether in response to an incident or coordinating a community festival, Radio Managers can easily and remotely turn on interoperable talkgroups in just a few clicks. And when the event is over, it can be just as easily turned off.

Learn more on our Critical Connect webpage.

WAVE PTX

WAVE PTX is a carrier-independent broadband Push-to-Talk (PTT) service that provides push-to-any multimedia communications. WAVE connects teams across different devices, networks and locations. WAVE works with ASTRO radio systems via Critical Connect to provide seamless PTT communication between P25 radio and broadband PTT users.

WAVE PTX Mobile App turns a smartphone into a PTT handset. Multimedia messaging support enables group sharing of text, photo, video and file attachments. Location and mapping enables the ability to see a team on a map and set a meeting place.

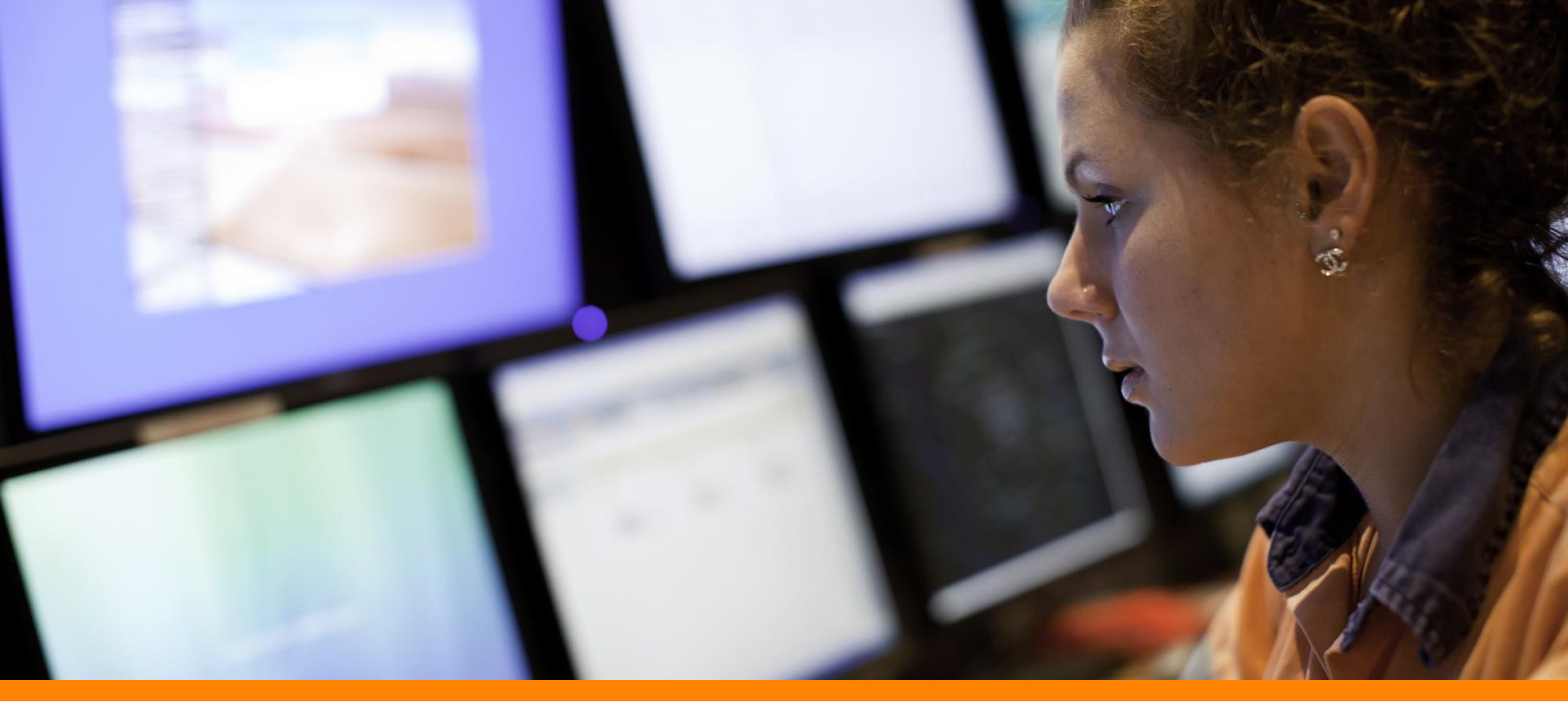
WAVE PTX Dispatch app puts dispatch functions on a standard web browser. Multimedia capabilities enable the ability to send/receive text, photo, video and file attachments while mapping function shows the location of teams on a map.

Whether an incident response or a planned event, group communication between ASTRO and WAVE users delivers better outcomes through increased collaboration across disparate teams.

Learn more on our WAVE PTX webpage.

Network Operations and Management

Maximize network operations and maintenance with better system visibility and control of critical assets



Network Operations and Management

Provisioning Manager (PM)

The Provisioning Manager is a system application that enables centralized provisioning of an ASTRO system with various system-level, user-level, and device-level configuration required for proper system operation. Specifically, the application allows you to configure subscriber radios, consoles, system infrastructure, and radio traffic applications.

With the Provisioning Manager, you can perform the following tasks:

- Configure system-level parameters for Trunked Radio System (Voice and Data Systems), Console System, Conventional System, and Foreign System.
- Configure subscriber information, such as radios, talkgroups, multigroups, agency groups, foreign groups, and Broadcast Data Agencies.
- Configure conventional system infrastructure at the zone that includes conventional sites and channels.
- Configure Console infrastructure that includes console sites, dispatch consoles and its peripherals and AIS consoles.
- Configure Auxiliary I/O (inputs/outputs) that allow a console operator to both control external devices (to perform tasks such as turning on lights, closing doors, or overriding channels) and monitor inputs (to enable detection of door-open alarms, and so on).
- Configure security policies to control access to data and capabilities for the users on the system.

Unified Network Configurator (UNC)

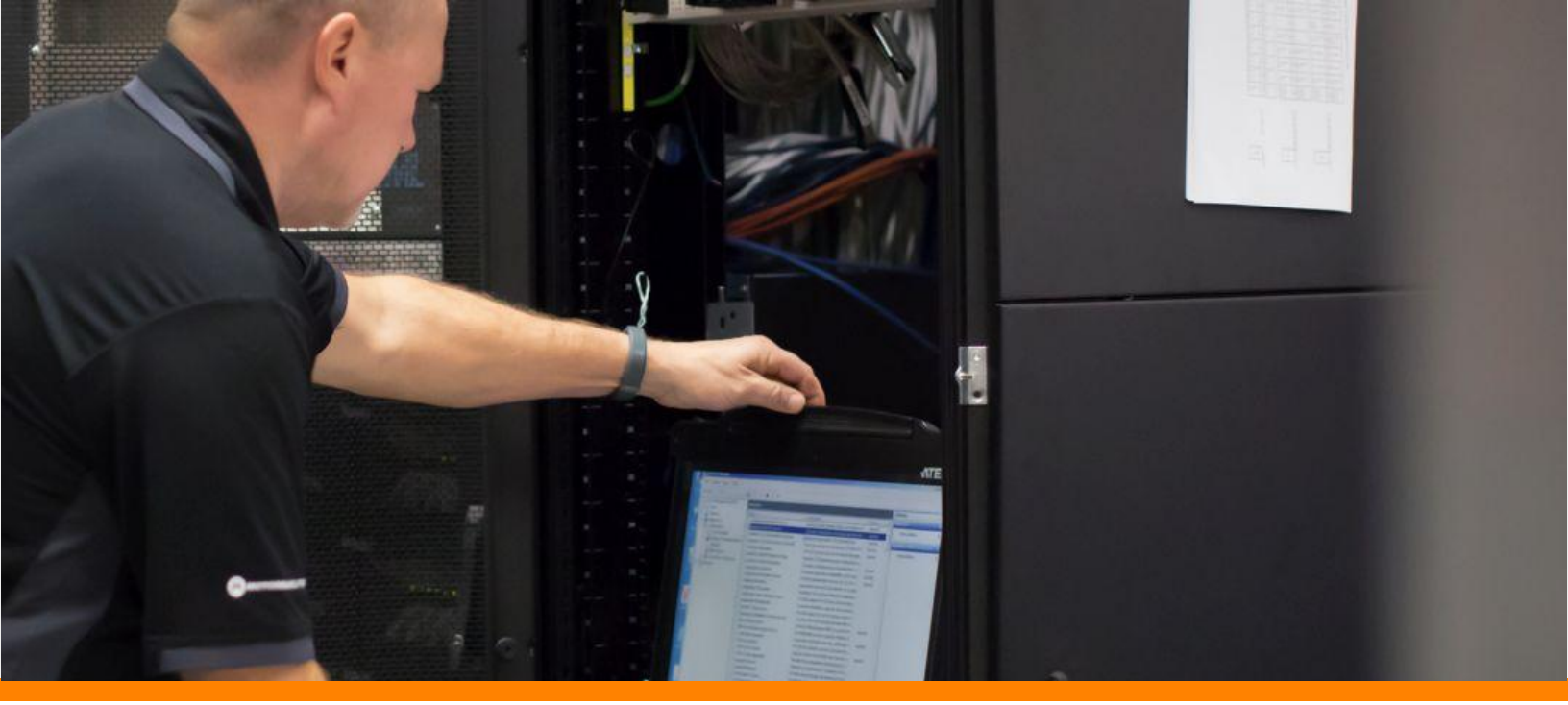
The UNC is a central network configuration solutions that provides controlled and validated configuration management of system devices.

With the UNC you can provide the following tasks:

- Secure interface for configuration management
- Distribution management for mapping updates
- Bulk transfer mechanism for certain devices in the system
- System level view of all configuration data

Provisioning Manager Interface (PMI)

The PMI is a Application Programming Interface (API) for external applications to provision data for the ASTRO radio system in the Provisioning Manager.



Network Operations and Management

Channel Partitioning

Channel Partitioning feature allows the user to configure the system such that agencies, or a subset of agencies, have exclusive use of specific RF channels.

Security Partitioning

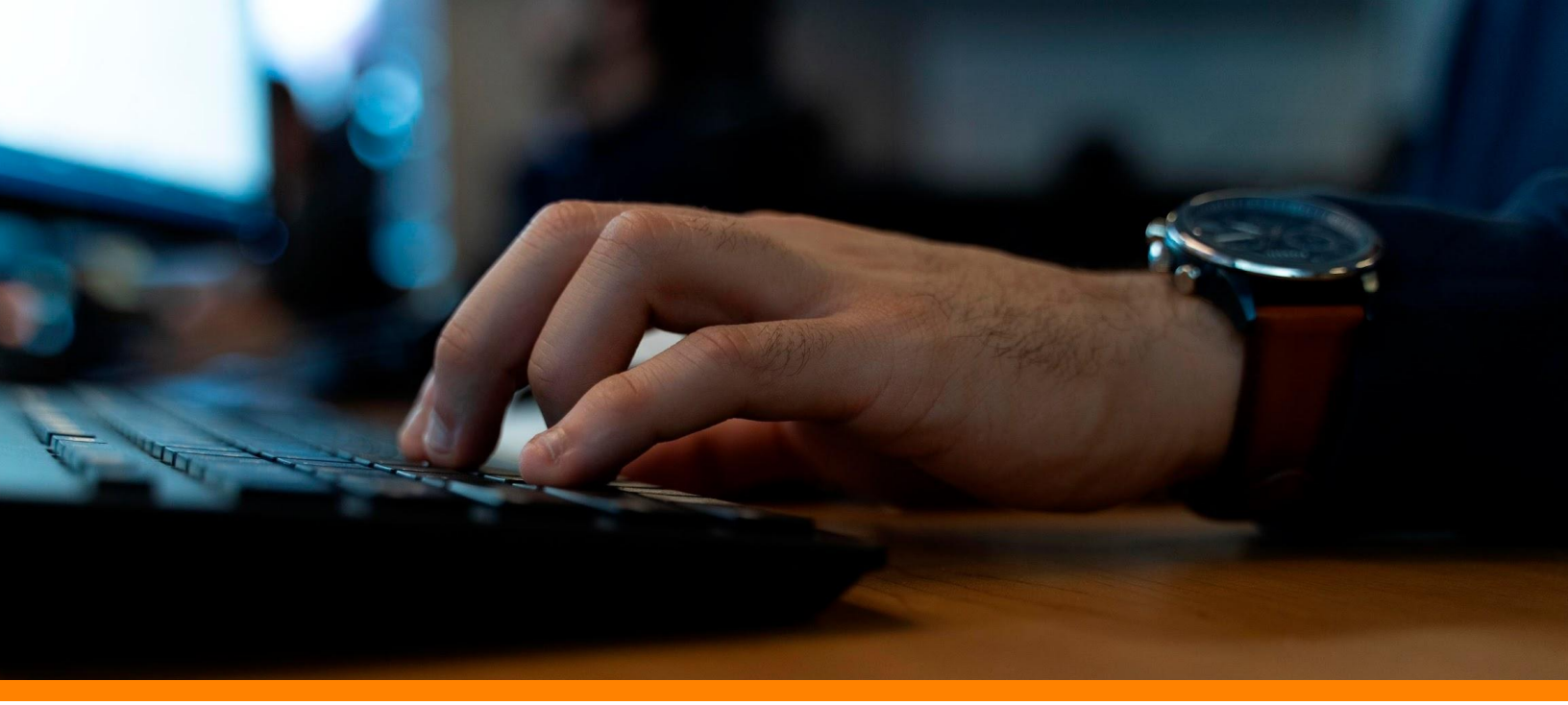
Security Partitioning allows configurable items to be assigned to security groups in order to give control over these items to different manager-users or agency. Each user is given access only to information based on security group. A super manager can partition access to information in a centralized database according to a number of different user categories. A super manager can also grant or restrict access to multiple zones for a manager user.

Dynamic Frequency Blocking

Dynamic Frequency Blocking provides a coordination of channel usage between known interfering channels at adjacent sites. Dynamic Frequency Blocking prevents the simultaneous assignment of known interfering channels.

Dynamic Shared Services

Dynamic Shared Services supplements the Telephone Interconnect Service by dynamically controlling the sharing of voice channels between Dispatch and Interconnect Service. It controls both the maximum number of simultaneous interconnect calls as well as the maximum length of interconnect calls to ensure adequate resources to voice channels for dispatch service. The periodic adjustment of channels available for interconnect is based on traffic loading and the entered target levels of service.



Network Operations and Management

Unified Event Manager (UEM)

UEM is an application that provides reliable fault management services for ASTRO radio systems.

The main functions are:

- Device discovery
- Fault management
- Supervision
- Synchronization

The UEM client includes a navigation tree to quickly select different fault management views. Maps provide a graphical representation of managed resources at the zone or system level.

Fault management includes processing a presentation of events sent by a network element in the form of a Simple Network Management Protocol (SNMP) trap or inform, or a Simple Object Access Protocol (SOAP) message.

A UEM Lite version is available for standalone Conventional system configurations.

UEM SNMP Element Management Toolkit

The UEM Simple Network Management Toolkit (SNMP) enables the ability to define SNMP messages between third-party devices and the UEM. This allows system operators to monitor faults on critical third-party devices directly from the UEM.

UEM Enhanced Navigation

With UEM Enhanced Navigation a user can navigate through zone and system health information using drill-down navigation, traversing through additional views visualizing data related to infrastructure health.

The enhanced navigation offers the following features:

- System map, Site View and Network Element View
- Visualization of RTU I/O information
- Drill-down navigation

Microwave Map View

Microwave view allows the ability to view the status of all microwave radios in a zone on a single map screen. Microwave radios and their relation to each other are represented on a map.

Email Notification

Email notification is designed to send SMTP messages to a destination app outside the RNI firewall. Rules allow notifications based on device type, severity and more.

Northbound Interface (NBI)

The NBI allows fault information to be forwarded to a higher level manager-of-managers from the Unified Event Manager (UEM).

Network Operations and Management

ZoneWatch Grid and Control

Zone Watch is a performance management tool to monitor radio call traffic for an individual zone in real time. This application uses different Watch Windows that allow you to display only the information you want to see.

Examples of trunking activity and radio call traffic displayed in the Watch Windows include the following:

- Radio IDs
- Talkgroup IDs
- Aliases
- Specific call information
- Channel and talkpath assignments (FDMA & TDMA)

Affiliation Display is an application that displays the association of a radio with a talkgroup and a site, and information about conventional channels, console sites, and consoles. It enables you to monitor how radio users travel between different sites in a zone and how they communicate with other members of their assigned talkgroup and those outside of their talkgroup.

Radio Control Manager (RCM)

The Radio Control Manager is used primarily by dispatchers to monitor and manage radio events, issue and monitor commands and make informational queries of the system database.

RCM can perform the following actions:

- Send commands to radios over the air and monitor their status.
- Check the status of a radio.
- Monitor events sent from radio users in near real time as the information becomes available in the system.
- Create, view, schedule, and export standard reports on RCM activity on the system.

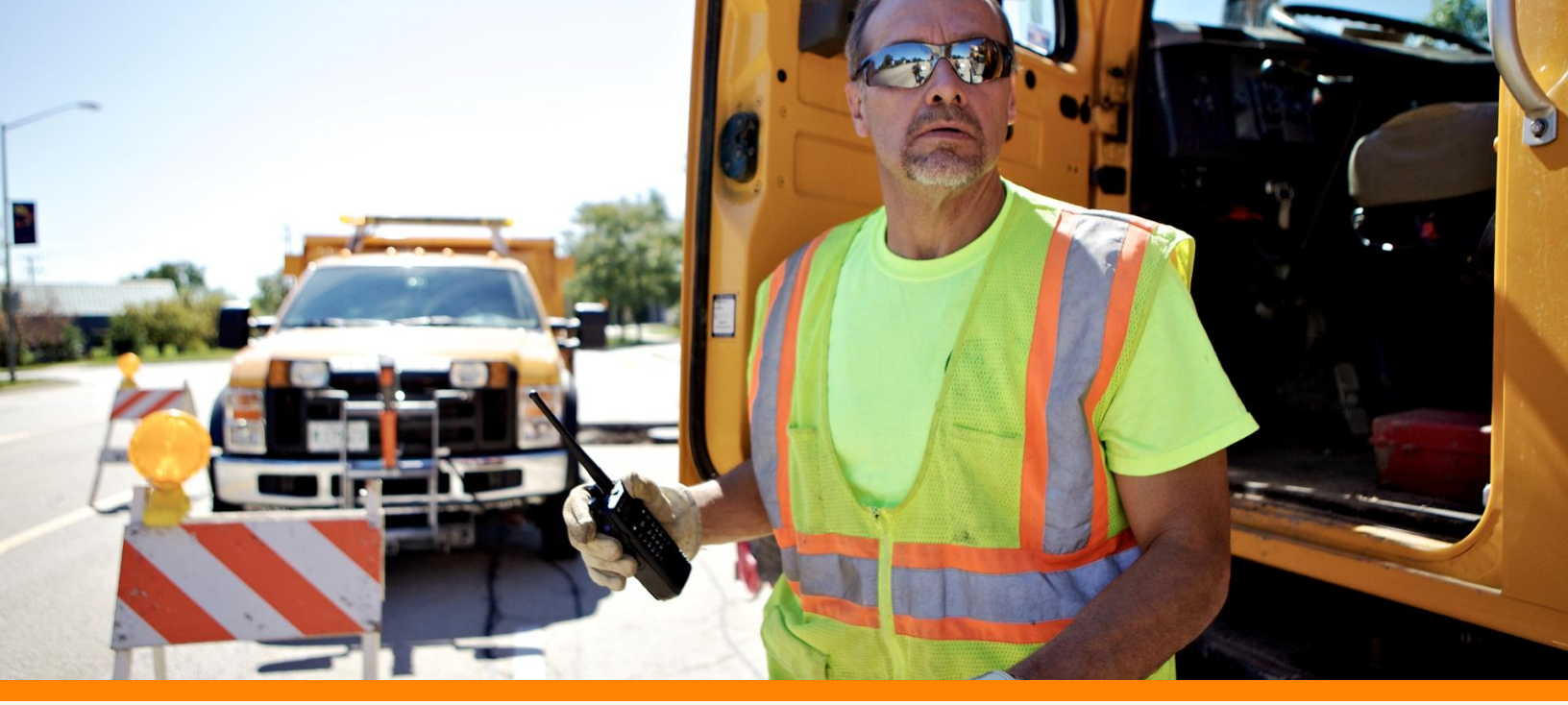
Key radio commands and operations:

Regroup assigns an affiliated radio to a new talkgroup.

Selector Lock disables the talkgroup selector switch on the radio so the radio users cannot switch to another talkgroup.

Selective Inhibit functionally disables an affiliated radio(s). All buttons, selector switches and menu operations are disabled and no voice communications are possible.

A Storm Plan is a set of predefined commands for use during an emergency or planned activity. Activating a storm plan would dynamically regroup preselected radios into a designated talkgroup without the need to regroup them individually.



Network Operations and Management

CAD Interface (CADI)

The Computer Aided Dispatch Interface (CADI) API is an application programming interface for use by third-party Computer Aided Dispatch (CAD) applications. CADI provides a high-level, function-based programming interface for performing dispatch actions within a radio system from a custom software application. The CADI API enables third party suppliers to write software application programs, called CADI clients, which monitor radio systems for dispatch purposes.

The API gives the CADI client application direct access to the commands and events used by the radio system and its network management applications.

Flexible Air Traffic Information Access (ATIA)

ATIA is an Application Programming Interface (API) that provides a continuous near real-time stream of call data for third-party applications. Non-call activities such as subscriber rejects, affiliations and radio commands are issued in unique data formats.

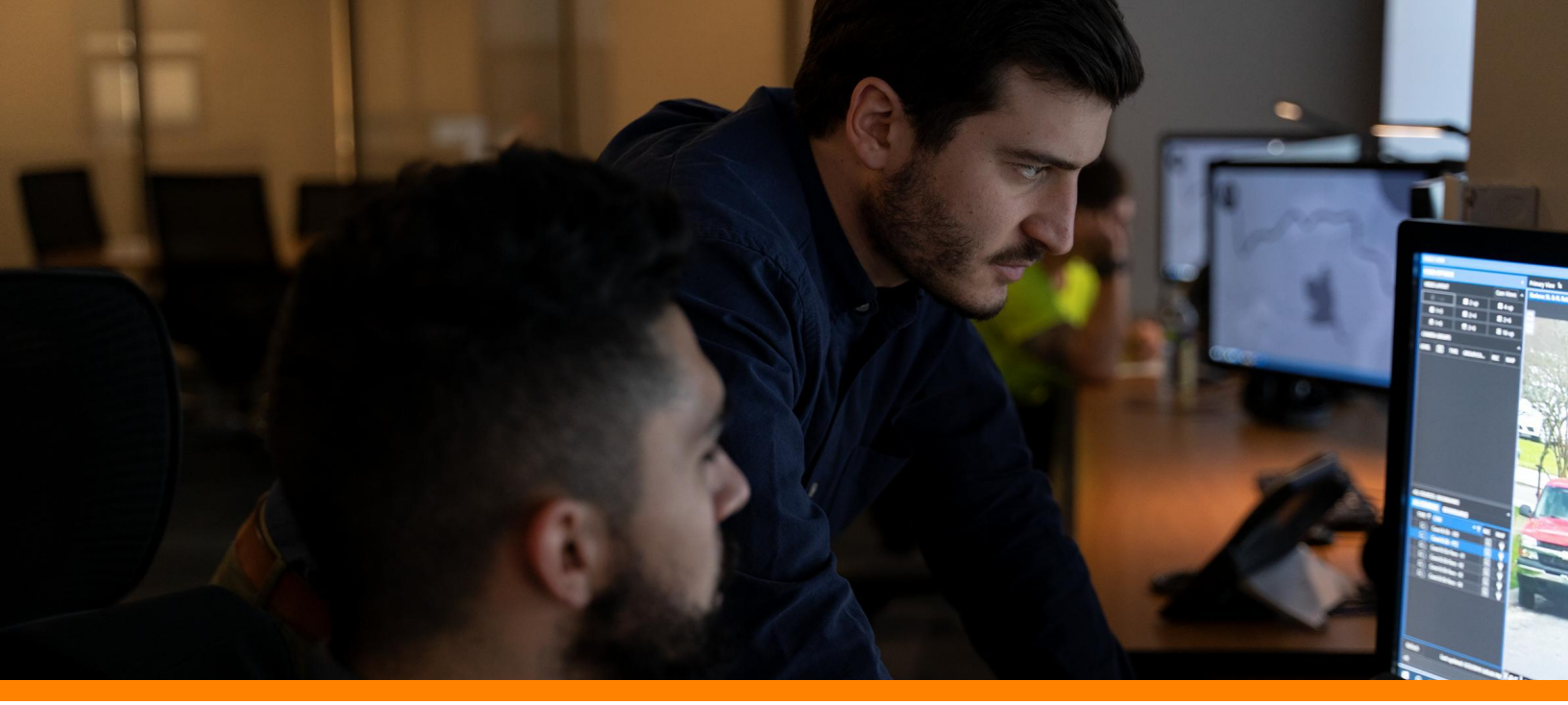
ATIA information can be used to generate detailed billing or management reports from the data provided by the ATIA interface in conjunction with third-party products and apps.

Dynamic Reports

Dynamic Reports provides near real-time call data collection (e.g., average sites per call) and displays usage trends and patterns of activity for effective monitoring and reporting. Predefined parameters and template formats display the value of multiple statistics for one or more system elements (e.g., Channels). Once a report is activated, a Dynamic Report displays data plotted according to the system element and the time interval selected.

Historical Reports

Historical Reports generate reports on system-wide activity and individual zone activity. The reports contain statistical data that is gathered at specific, predefined time intervals. Historical Reports monitors and analyzes information about zones, sites, channels, talkgroups, and users to understand how the system is performing and utilized. Users can utilize the Report Scheduler window to schedule zone-wide and system-wide reports to occur automatically at specified times with an output to a printer or data file.



Network Operations and Management

CirrusCentral Management

CirrusCentral Management is an optional cloud-based system management application built for ASTRO trunked radio systems. A dashboard view provides system health at a glance, while advanced tools and an intuitive interface makes it easy to gain better insights into the radio system's performance. Alarm aggregation and topology views ease troubleshooting and event resolution.

CirrusCentral resides in our secure cloud and always runs the most up-to-date software. A standard web browser on any device is all that is needed to securely manage the ASTRO system from anywhere. CirrusCentral Management is complementary to the existing on-premise based Private Radio Network Management suite (PRNM).

Alarm and Event Aggregation reduces alarm flooding by grouping related events. Use predefined groups or create your own. Efficient sorting through alarms and events cuts through the clutter to quickly get to root causes.

Call Monitoring enables a real-time view of call activity, trunking status, channel utilization and affiliations on an easy to view graphical representation of the ASTRO radio system.

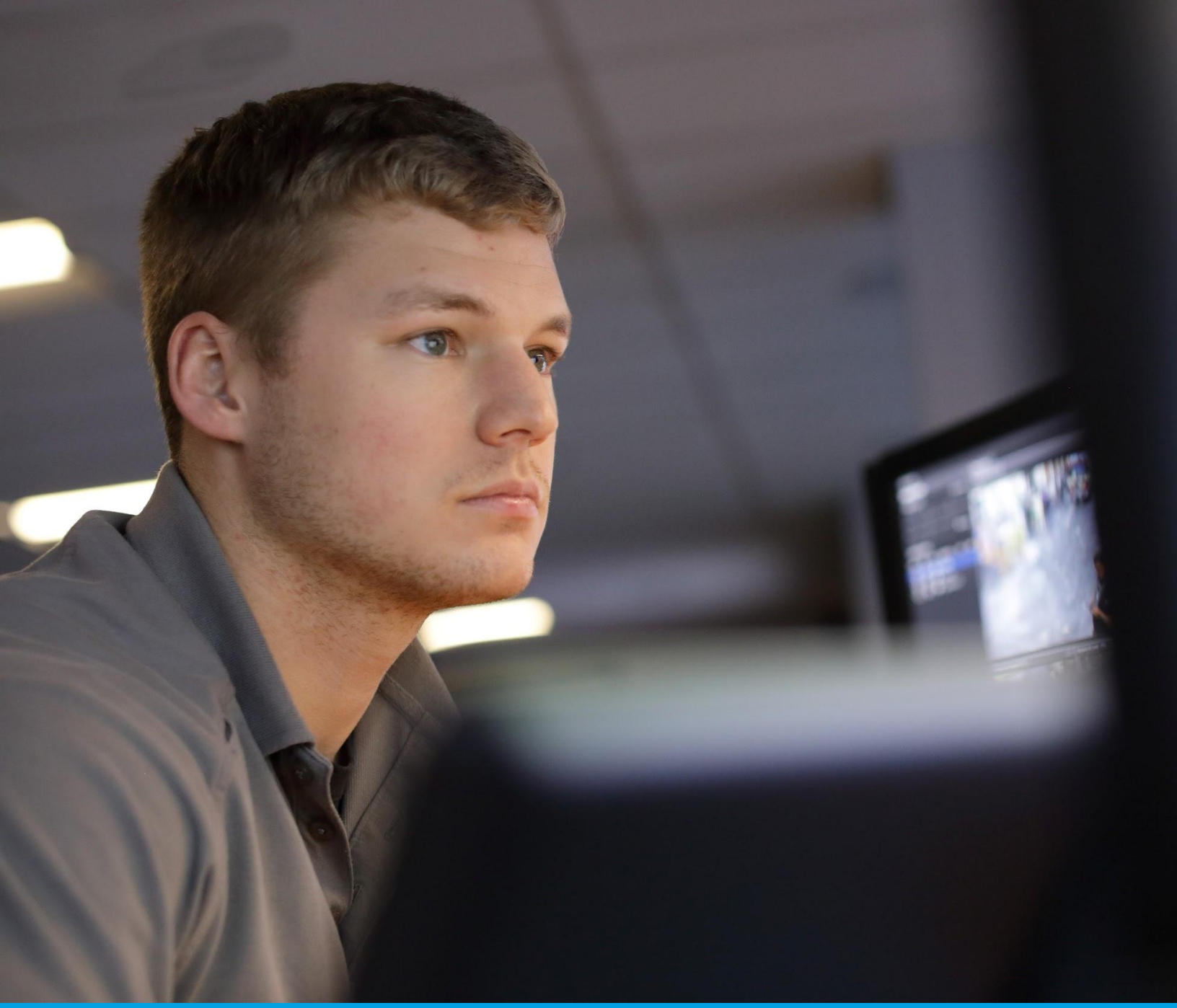
Email Fault Notification informs you of alarms while away from the screen. Individual site and severity preferences allow each user set which alert types to receive notifications.

Site Load View

Provides a real-time graphic representation of ASTRO site load and capacity. Radio and talkgroup affiliations show how the fleet is distributed across the sites. Trends help distinguish between momentary peaks in demand and a growing concern.

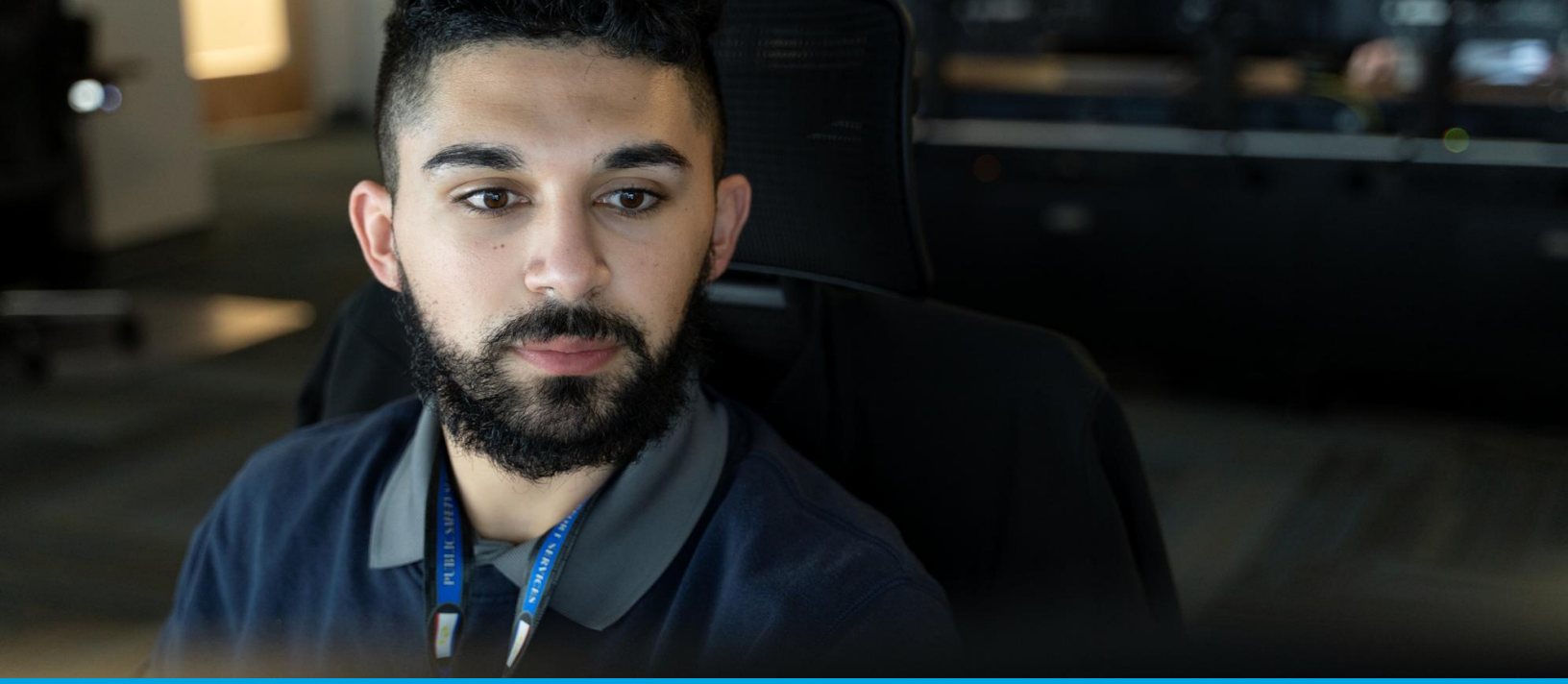
Reporting provides the insights to quickly triage call failures, inspect individual radio activity and access security risks related to lost radios.

Learn more on our CirrusCentral Management webpage.



Security

Protect your mission-critical radio system from unauthorized access or malicious disruption



Security

Radio Authentication

Radio authentication prevents illegitimate radios from gaining access to the radio network. It enhances security by authenticating radios before allowing registration to the system. The Authentication Center is a central database that stores the authentication keys for all P25 radios in the system. This feature uses the P25 link layer authentication standard.

Host-based CSMS

Host-based Core Security Management Server improves security at the network, endpoint and application levels for certified Windows products used throughout the ASTRO system by enabling product specific firewalls to ensure that traffic flowing through the system is only what is required.

Real-time Intrusion Detection System (IDS)

IDS monitors ASTRO network traffic for potential security threats using signature-based detection and anomaly-based detection. In signature-based detection, the IDS uses its attack-signature database to match the traffic with the predefined attack patterns called signatures. For anomaly-based detections, IDS looks for any irregularities in the protocol used for transferring the data.

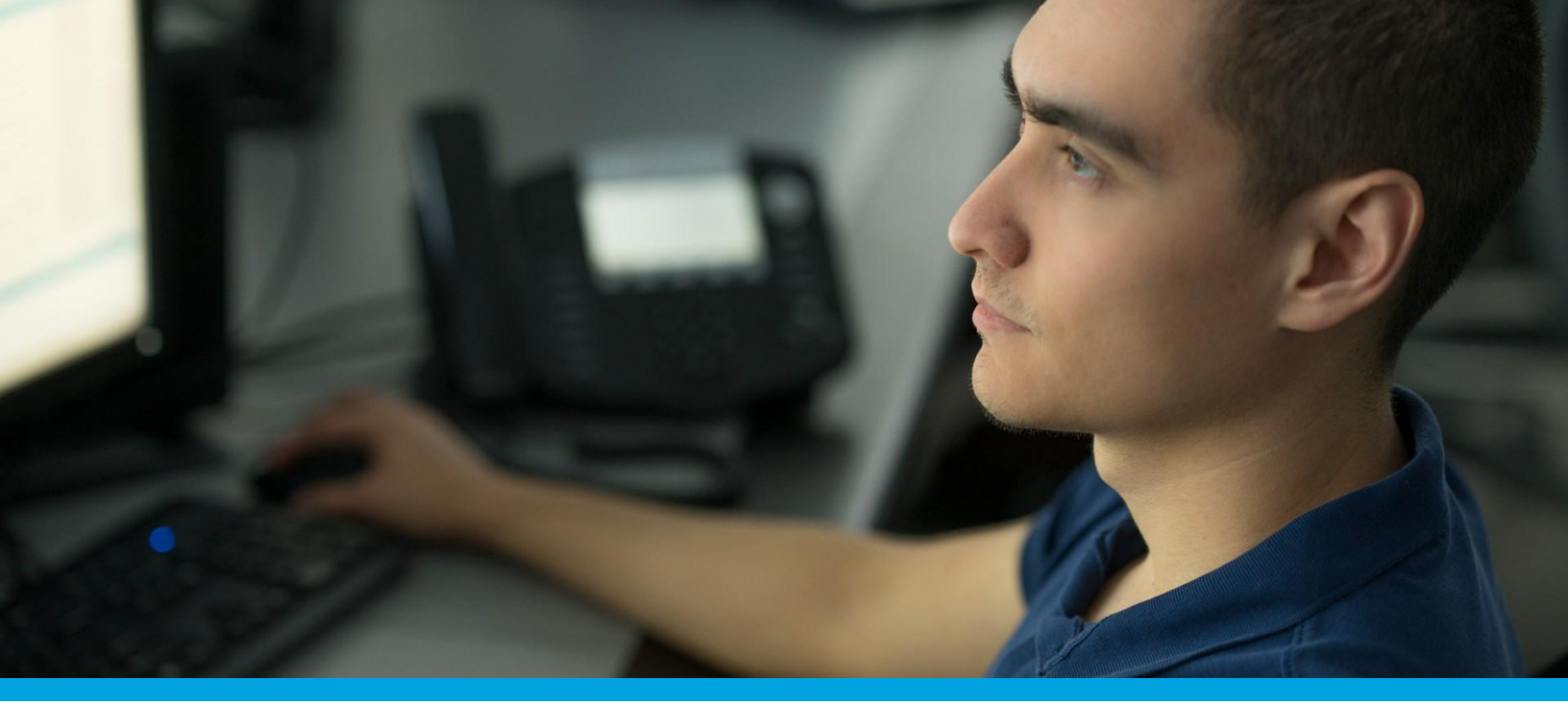
IDS can inspect non-encrypted traffic in an IP-IP tunnel; inspection of encrypted traffic is not supported. If suspicious activity is detected, the IDS will send alerts to the Unified Event Manager (UEM), and syslog to the Centralized Event Logging Server (if present in the system).

Link Encryption and Authentication / Router Encryption

Router Encryption enables encrypted links between network transport devices that transverse the following untrusted zones:

- The Wide Area Network (WAN) link located outside the Local Area Network (LAN) of the Radio Network Infrastructure (RNI)
- The DeMilitarized (DMZ) zone between the RNI and the Customer Enterprise Network (CEN)

Devices supporting encrypted links include: Site Router, Subsite Router, Edge Router, Border Router or Gateway, RNI-DMZ Firewall



Security

Two-Factor Authentication (2FA)

Two-factor authentication requires a second form of identity verification before a user is able to log into the ASTRO network remotely or log in locally within the network on the devices at operating system level.

This adds an extra layer of security, making it harder for attackers to gain access.

Smart Card Multi-Factor Authentication

Smart card multi-factor authentication and provides reliable identification, secure authentication and access for privileged and non-privileged accounts. It combines username-password input with verification of smart cards, such as CAC or PIV, allowing only authorized personnel to access the network. This meets the US federal compliance mandate HSPD#12.

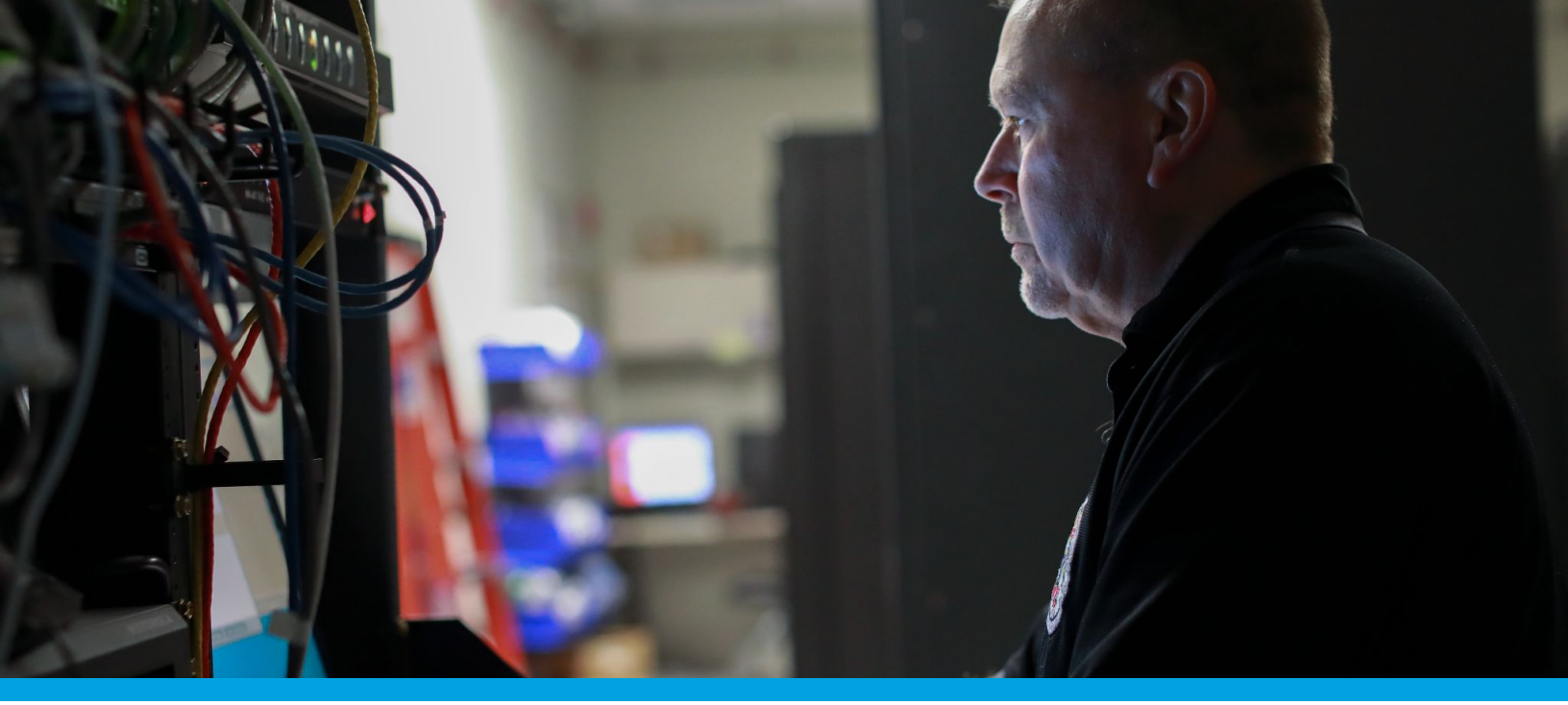
Backup and Recovery (BAR)

Backup and Recovery is a centralized backup and restore function of critical and non-critical system data. It supports multiple instances of backed up data with the ability to create media for off-site storage. Two levels of BAR are available based on the clients that need to be backed up.

NOTE: Devices outside the Radio Network Interface (RNI), such as in the Customer Enterprise Network (CEN) cannot be backed up by the Backup and Restore Server.

Service Access Architecture

Service Access Architecture provides secure remote access via WAN, VPN, dial-up or a remotely located LAN switch for system managers as well as contracted Motorola Solutions service personnel. For security purposes, authenticated access can be provided via FortiToken MFA solution that allows user to use either hard or soft token as a second factor.



Security

Router Encryption

Connecting dispersed sites across the ASTRO radio system can require sensitive information to transverse networks outside the radio network infrastructure. Router Encryption enables encrypted links between network transport devices that transverse untrusted zones including the Wide Area Network (WAN) link located outside the customer enterprise network (CEN) and the DeMilitarized Zone (DMZ) between the radio network interface and the CEN.

OSPF/BGP Router Authentication

The various sites and components of ASTRO radio systems are connected via an IP network constructed of routers. OSPF and BGP router authentication uses shared keys between peer routers to verify the authenticity of packets sent between sites and components within an ASTRO system.

Ethernet Switch Port Security

The aim of Ethernet Switch Port Security is to prevent unauthorized access to the system via ports on a network switch. Two methods are available to secure system ports, MAC port lockdown and 802.1X for service ports.

MAC Port Lockdown is the permanent assignment of a given MAC address to a specific port on the switch. It ensures traffic intended for a specific MAC address can only go through the assigned port. This is useful to prevent an intruder from hijacking a MAC address from a known user in order to steal data.

IEEE 802.1X defines port-based, network access control that is used to provide authenticated network access. With port-based network access control, a network device cannot send any frames on the network until permission is granted through an authentication process.

Mission-Critical Hardening

The hardening of ASTRO radio systems ensure the devices are configured to the currently available recommendations, typically defined by the latest DISA Security Technical Implementation Guides (STIG). Hardening applies configuration settings that help enforce STIG compliance and applies organization specific login banners on devices.

Security

Voice Encryption

Encryption allows digitally encrypted communications between radios and dispatch consoles. Once encryption is in place, voice transmission is sent as an encrypted, digital signal. Endpoints must be programmed with a matching encryption key to decode the digital signal.

This protects against scanners and other users of the frequency from eavesdropping on sensitive radio transmissions.

Supported encryption algorithms includes:

- TDMA: AES, ADP, DES-OFB
- FDMA: AES, ADP, DES-OFB, DVI-XL, DVP-XL and DES-XL

Encrypted Integrated Data

ASTRO Integrated Data can use AES or DES-OFB encryption for conventional systems to protect inbound and outbound data traffic. Conventional systems use a CAI Data Encryption Module (CDEM) to encrypt and decrypt data messages between the Packet Data Gateway (PDG) and the subscriber unit.

Encryption key provisioning and key loading is done through the Key Variable Loader (KVL) and central management of encryption

Over-the-Air Rekeying (OTAR)

OTAR allows users to remotely change encryption keys of portable and mobile radios over the RF channel. The Key Management Facility (KMF) is the key manager of the system and formulates and originates the OTAR messages.

By reducing the time and effort to re-key, OTAR can enhance the security of radio systems by encouraging more frequent encryption keys changes

Learn more on our OTAR webpage.

Key Management Facility (KMF)

The KMF provides a robust and feature rich platform for effectively managing secure interoperable communications across all of your devices from a single centralized platform. The KMF's web based client allows you to perform key operations via the interactive and easy to use web based interface from virtually anywhere.

he KMF removes the inherent complexity out of administering and managing encryption keys.

Learn more on our KMF webpage.

For more information, please visit
motorolasolutions.com/astro

MOTOROLA SOLUTIONS