Advances in P25

Standards | Interoperability | Security

RadioResource MissionCritical COMMUNICATIONS | Educational Series

Sponsored by

ASTRONICS TEST SYSTEMS FREEDOM

catalyst communications technologies

Comba keeps you connected

JVCKENWOOD

etherstack wireless innovation

Microlab

P25

STICO ANTENNA SOLUTIONS

VALID8.com Flexible. Affordable. That's Different.

VIAVI VIAVI Solutions

ZETRON

RadioResource MissionCritical COMMUNICATIONS

Contents

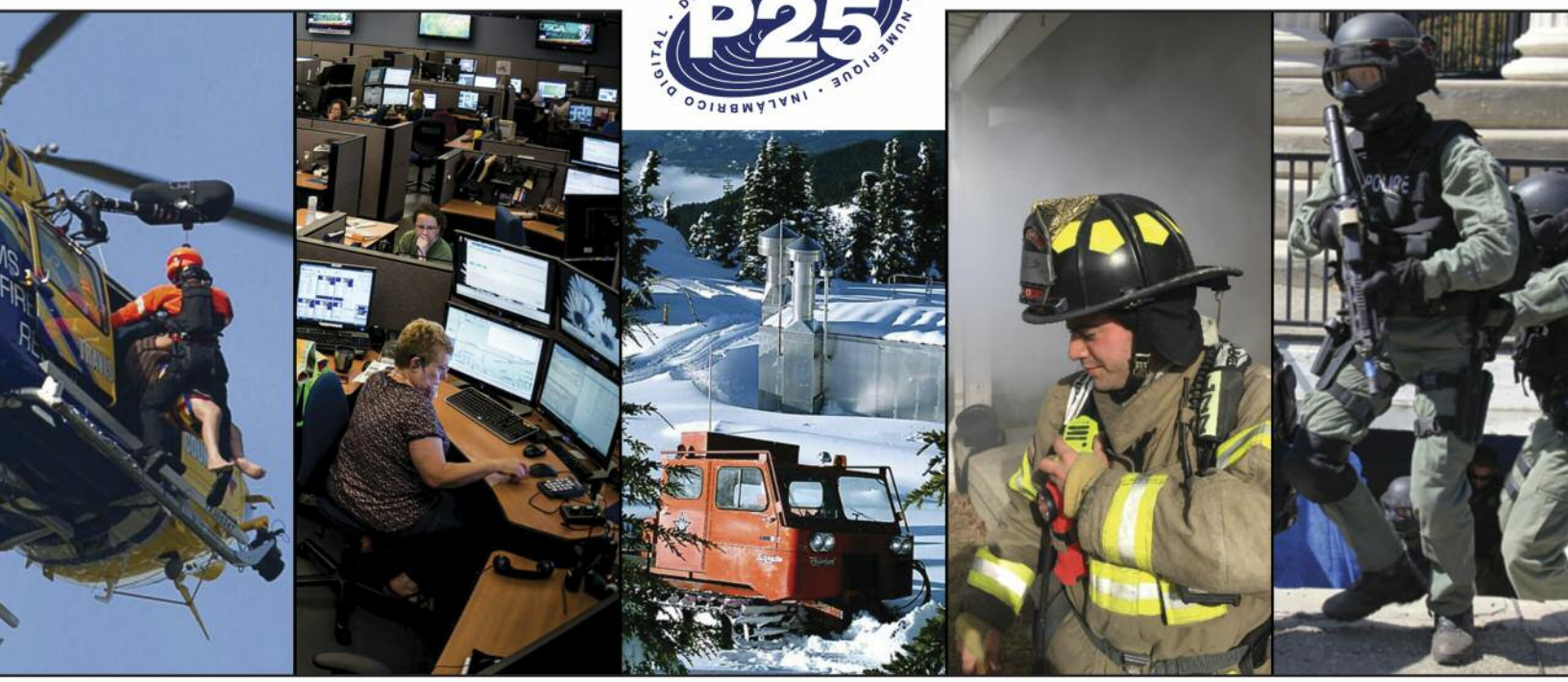
Sponsors

Thank you to the following sponsors for making this eBook possible!

RadioResource MissionCritical COMMUNICATIONS | Educational Series

Pandata Corp., 7108 S. Alton Way, Building H, Centennial, CO 80112. Telephone: 303-792-2390.
Website: www.MCCmag.com

Section 4
Encryption and Security



RadioResource MissionCritical COMMUNICATIONS | Educational Series

How P25 Specification Security Updates Support Public-Safety-Grade Communications

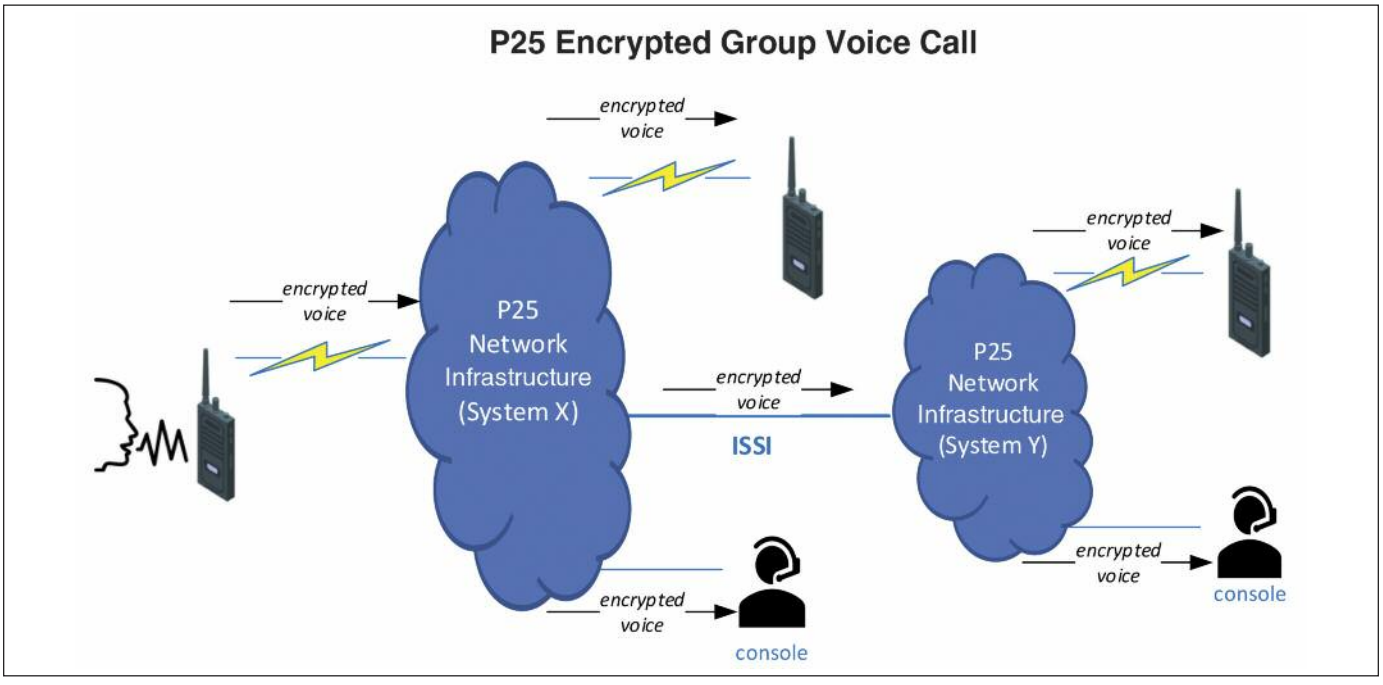
By Tom Senese

Strong communications security is an important attribute of P25 voice services. In many situations, protection of voice communication confidentiality is essential to the successful outcome of a mission or to the safety of radio users. P25 security is comprised of high-grade cryptography and robust key management. Upcoming additions to the P25 standards will enhance the interoperability and efficiency of key management operations.

Voice Encryption

In response to the need for mission-critical voice, the P25 standard defines high-grade, 256-bit encryption for digital voice based on the Federal Information Processing Standard (FIPS) 197 Advanced Encryption Standard (AES). The AES-256 algorithm is approved for use beyond the year 2031.

P25 voice encryption is applied end-to-end between communications endpoints, whether it be a radio or console. The encryption is unbroken on all communication paths within a radio system and between radio systems that are connected through the P25 Inter-RF Subsystem Interface (ISSI). Each communication endpoint encrypts or decrypts digital voice. The use of encryption service is optional with all P25 voice services, including group call, announcement call, broadcast call, systemwide call, conventional call, individual call and telephone interconnect.



P25 voice encryption is applicable to all system configurations, including Phase 1 frequency-division multiple access (FDMA) trunking, Phase 2 time-division multiple access (TDMA) trunking, conventional and direct mode. The P25 block encryption protocol, normatively defined in TIA-102.AAAD-B, describes the application of AES-256 encryption to the P25

full-rate vocoder (Phase 1 FDMA) and to the P25 half-rate vocoder (Phase 2 TDMA). Furthermore, P25 voice encryption has no detrimental effect on audio quality and latency, and works transparently with voice priority pre-emption and late-joining scenarios.

Key Management

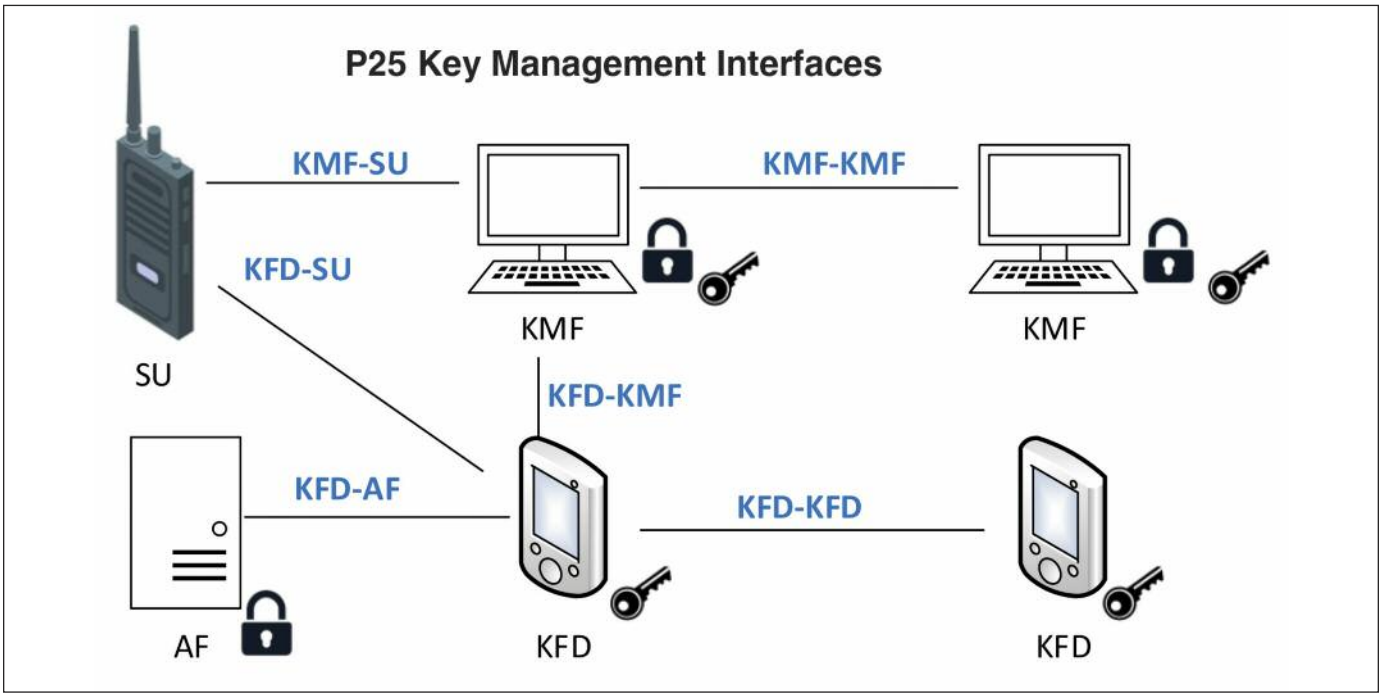
The robustness of the P25 voice encryption service is dependent on the degree of protection and management of the encryption keys. It is commonplace for P25 communications endpoints to use hardware cryptographic modules for persistent key storage, even though the use of cryptographic modules is not required by the P25 standard.

The key management service used by P25 radio systems is over-the-air rekeying (OTAR), normatively defined in TIA-102.AACA-A. Through OTAR, P25 encryption keys are centrally managed by an application server called the key management facility (KMF). The primary functions of the KMF are to manage the lifecycle of keys, map keys to radios and consoles, and remotely deliver the keys to the communication endpoints using key management messages (KMMs). The communications endpoints that a KMF manages are often called OTAR clients.

There are two general categories of keys: traffic encryption key (TEK) and key encryption key (KEK). The TEK is used for media encryption, such as voice and packet data units. The KEK is used to encrypt TEKs that are encapsulated within key management data messages. The TEK is shared amongst all communications endpoints that are members of a communication group. The KEK is generally unique for each communications endpoint.

P25 deployments also use a key fill Device (KFD) to manually upload voice encryption keys and OTAR security objects into the communications endpoints over a wired interface. The KFD interface is normatively defined in TIA-102.AACD-A. Key loading of TEKs based on KFD is used when communication with the KMF is not available or not desired. The OTAR security objects consist of a KEK that is unique to the communications endpoint, a parameter for anti-replay protection and an application identifier for the KMF. A communications endpoint is not able to interact with the KMF until it is configured with the OTAR security objects via KFD.

The OTAR protocol has built-in security for confidentiality protection and message integrity. The keys being delivered in an OTAR message are encrypted with the recipient device's KEK based on an industry-recognized key-wrapping method. An 8-byte cypher block chaining message authentication code (CBC-MAC) is used to ensure message integrity protection of the OTAR KMM. The body of the OTAR KMM is further encrypted with a TEK.



etherstack

Etherstack specialize in Wireless Communications Intellectual Property, Products and Services for clients in Public Safety, Defense, Utilities + Resources industries.

www.etherstack.com

info.na@etherstack.com
info.au@etherstack.com
info.jp@etherstack.com
info.eu@etherstack.com

Exchanging encryption keys between KMFs by use of the P25 KMF-to-KMF Interface, as normatively defined in TIA-102.BAKA, has received a lot of attention from the Federal Partnership of Interoperable Communications (FPIC), due primarily to considerations for interoperable communications. Inter-KMF key exchange involves several use cases, perhaps most notably for interoperable communications between agencies. FPIC is advocating the P25 LMR industry to support TIA-102.BAKA while maintaining manufacturer-specific implementation of the KMF-to-KMF interface. A TEK that will be used for an interoperable communications group is delivered to the KMFs of all agencies that are part of the interoperable group through the standard inter-KMF key exchange procedure. Each agency KMF, in turn, delivers the TEK to the OTAR clients that are under its management.

The important P25 key management interfaces and their associated normative documents are summarized in Table 1 below.

Table 1: Normative Documents for the P25 Key Management Interfaces

Interface	Label	Title	Status
KMF-SU	TIA-102.AACA-A	OTAR Messages & Procedures, Rev. A	Published
KMF-SU	TIA-102.AACA-B	OTAR Messages & Procedures, Rev. B	Draft, in progress
KFD-SU	TIA-102.AACD-A	Key Fill Device Interface	Published
KFD-SU, KFD-KMF, KFD-KFD, KFD-AF	TIA-102.AACD-B	Key Fill Device Interface	Draft, in progress
KMF-KMF	TIA-102.BAKA	KMF to KMF Interface	Published

Radio Authentication

The P25 Link Layer Authentication service, normatively defined in TIA-102.AACE-A, enables the trunking radio infrastructure to validate the authenticity of a P25 radio's subscriber unit ID (SUID). Authentication of the P25 radio prevents against cloning of the radio's SUID on a P25 trunking system. The authentication operation consists of a cryptographic challenge-response exchange between the P25 radio and the authentication facility (AF). The challenge-response exchange takes place on the trunking control channel, usually as part of unit registration. The basis of the cryptographic operation is a secret key, K, that is shared between the P25 radio and AF.

Prior to initial operation on the system, the radio is provisioned with K through KFD upload. The same K is provisioned in the AF. K is stored persistently within the P25 radio.

New Developments

As secure radio operations have evolved in prevalence and sophistication, more expansive key fill use cases have emerged. Etherstack, in collaboration with other vendors, is currently in the process of writing a draft update to the key fill device (KFD) interface document in order to define standards requirements for new interfaces that are associated with the new key fill use cases. The revised KFD interface document, which is expected to be published in the second half of 2021, will define messages and procedures for the following new key fill interfaces:

KFD-KMF. The KFD-KMF interface will support the use case for initializing OTAR security objects in P25 communication endpoints. The KFD downloads the OTAR security objects for a given communication endpoint from the KMF. In a subsequent step, the KFD connects to the P25 communications endpoint and uploads the OTAR security objects originally provided by the KMF.

This interface also supports the use case for OTAR management of P25 communication endpoints without their direct connection to the KMF. The KFD operates as a transport medium between the KMF and the communication endpoint. The KFD can receive KMMs destined for the communication endpoint from the KMF through the KFD-KMF interface, and it can also send KMMs originating from the communication endpoint to the KMF over the same interface. Likewise, the KMMs can be exchanged in both directions when the KFD connects to the P25 communication endpoint through the KFD-SU interface.

The use of interoperable procedures on this interface will allow KFD equipment from different manufacturers to be interchangeable with KMFs. Furthermore, it will allow a security operator to centrally manage the keys of a communication endpoint in a KMF when there is no direct connection from the KMF to that endpoint, either by design or due to temporary loss of coverage. Without central key management under conditions of limited connectivity, the security operator may have to enter the same information in multiple places, thus enhancing risk for misalignment between the KMF and the communication endpoints. The KFD-KMF interface can be supported through direct or remote connection, providing for greater flexibility of deployment.

KFD-KFD. The KFD-KFD interface will support the direct exchange of keys between two KFDs. The use of this interface allows field personnel to directly exchange keys between KFD equipment from different manufacturers. This may be particularly helpful when the field personnel are from different agencies, and key exchange needed for interoperable communication takes place when KMF connections are not available.

KFD-AF. The KDF-AF interface will support provisioning the pairing of the P25 radio identifier and authentication key (K) into the AF. The use of this interface enables remote provisioning of the AF through an interoperable procedure. In some cases, remote provisioning will allow for improved efficiency of operations. Interoperable procedures will allow the use of KFD and AF equipment from different manufacturers in a consistent manner.

The P25 security standards will continue to evolve as new, interoperable interfaces are defined, and as key management operators seek greater efficiencies for their operations. ■

Tom Senese is a network solutions architect with Etherstack. Senese has more than 30 years of systems engineering experience in the LMR business. He is the former chairman of the Telecommunications Industry Association (TIA) TR-8.3 Encryption Subcommittee. He has a master's in electrical engineering from the Illinois Institute of Technology and is a certified information systems security professional (CISSP).

The following sponsors have made it possible for you to download ***Advances in P25: Standards | Interoperability | Security*** FREE of charge. They provide products and services that can help you achieve your communications goals. We encourage you to click on their links to contact them directly for more information.

Astronics Test Systems provides test solutions for mission-critical industries where failure of electronic systems is not an option. We provide test solutions for land mobile and tactical radio communications, mass transit, military and aerospace electronics and many other market segments. The company's FREEDOM-branded communications system analyzers are the industry-leading instruments for the maintenance and repair of LMR radios and infrastructure.

The FREEDOM product family includes the flagship R8000 and R8100 test sets, which have become the standard for the LMR industry. It also includes the R8600 Radio Test Hub for manufacturing applications, and our new R8200 – the first LMR service monitor to include a Vector Network Analyzer (VNA) for diagnosing RF network issues. With the revolutionary R8200, technicians no longer need to carry both a service monitor and separate VNA, saving money and valuable space on the bench or in the van. **https://freedomcte.com/wp-content/uploads/2020/07/ATS-FREEDOM-R8200-DataSheet.pdf**

Catalyst is a leading provider of communications solutions to the first responder community. For more than twenty years, Catalyst has provided dispatch, interoperability and incident command solutions to support mission-critical operations. Recently, Catalyst was awarded a grant from the Department of Homeland Security to research and develop a standards-compliant Interworking solution to enable communications between land mobile radio subscriber devices, including P25, and new mission critical push to talk (MCPTT) applications on smartphones using LTE Networks, including FirstNet™, Push-to-Talk Responder, and other emerging LTE broadband networks offered to first responders. That solution, IntelliLink™ Interworking, is now available from Catalyst. **https://www.catcomtec.com/**

Comba Telecom, Inc., based in Milpitas, California, is a leading supplier of RF communications solutions and equipment to the wireless industry. With R&D innovating in the heart of Silicon Valley and a manufacturing base in Asia, Comba Telecom manufactures cutting edge technologies and cost-effective solutions for OEM, integration, and operator partners. For more information, please visit: **https://www.combausa.com**

EF Johnson Technologies, Inc. is an independent subsidiary of JVCKENWOOD Corporation. Headquartered in Irving, Texas, EFJohnson focuses on innovating, developing and marketing the highest quality secure communications solutions to organizations whose mission is to protect and save lives. The company's customers include first responders in public safety and public service, the federal government and industrial organizations. The company's products are marketed under the EFJohnson and Kenwood brands. For more information, visit **www.efjohnson.com**

JVCKENWOOD is a global manufacturer specializing in Automotive and Professional System Solutions. It was reborn as one company in October 2011 through the merger of Victor Company of Japan, Limited (JVC) and Kenwood Corporation (Kenwood) three years after management integration. JVCKENWOOD operates four business segments, Car Electronics, Professional Systems, Optical & Audio, and Entertainment Software with image, sound, and radio technologies, as well as infotainment and visual software. JVCKENWOOD creates excitement and peace of mind, while aiming to achieve profitable growth and become a business group that is widely trusted by society. For more information, visit **http://www.jvckenwood.com/en.**

Sponsors

Etherstack is the world's leading independent provider of wireless communications software, digital network migration products and cryptographic solutions for defense and commercial clients. Established in 1995 and with offices around the globe, Etherstack offers a complete suite of fixed and tactical P25 network solutions covering terrestrial, satellite and cellular systems interfacing. Etherstack is active in the Project 25 Technology Interest Group and regular contributor to the TIA-102 P25 suite of standards. Clients in public safety, defense, utilities/ resources and cellular industries use Etherstack wireless communication intellectual property (DMR, LTE, SDR Waveforms, TETRA, P25) in many of the world's largest and highest profile mission-critical systems and solutions. To see how Etherstack can help with your digital communications needs, visit us at **www.etherstack.com**

Microlab, a Wireless Telecom Group Company, headquartered in Parsippany, New Jersey, is a leader in low-loss, guaranteed PIM, and custom RF and microwave components, enabling signal distribution and deployment of in-building DAS, wide area, and small cell networks. High-performance components include combiners, directional couplers, tappers, attenuators, terminations, and filters through 6 GHz. The SMART Passives System with embedded IoT technology is a leading-edge public safety DAS monitoring and test and measurement platform replacing typical tappers and couplers. GPS timing and synmil-aero, and medical devices are also supported. **https://microlabtech.com/**

The Project 25 Technology Interest Group (PTIG) is a group of individuals and organizations who share the mutual interest of advancing the refinement, development, deployment, and applications of the digital communications technology represented by Project 25 industry standards. PTIG members include two-way radio communications experts, public safety professionals, and equipment manufacturers. Our members recognize the need for, and have a direct stake in, the continued development of the critical communications capabilities represented in the P25 standards.
For Additional Information contact: **http://www.project25.org/**

STI-CO specializes in designing and manufacturing antenna systems to mission-critical customer specifications. Our custom, high performance antenna systems combine over 50 years of expertise with the latest in technology. STI-CO's antenna systems keep teams safe and securely connected. They proudly serve users in law enforcement, military, homeland security, heavy freight, passenger rail and transportation markets. **https://sti-co.com/**

Valid8 helps the world's networks work by providing the best methods to simulate and test network equipment and communication protocols. With 19 years of proven results, Valid8 believes that testing tools should start with a flexible and affordable base with the ability to customize solutions to needs. Clients should only pay for what they need. Valid8 is dedicated to customer success with a comprehensive support program providing direct access to engineers to assist with training, integration and problem-solving. Over 90% of customer feedback points to Valid8's flexibility and service as the reason they have chosen to partner with the company. Valid8 has succeeded in giving clients a refreshing change from the testing status quo. Learn more at **www.valid8.com**

VIAVI Solutions is a global leader in both network and service enablement and optical security performance products and solutions. Our technologies contribute to the success of a wide range of customers – from the world's largest mobile operators and governmental entities to enterprise network and application providers to contractors laying the fiber and building the towers that keep us connected. **www.viavisolutions.com**

Zetron, a Codan Company, is a trusted provider of mission-critical communications systems worldwide, it's ALL we do. With a comprehensive portfolio of technology solutions, including integrated next generation call taking, dispatch, CAD, mapping, fire station alerting, logging/ reporting, LMR communications and more, Zetron is relied on by customers in federal/state/ local government, public safety, transportation, utilities, healthcare and other markets on all seven continents of the world. Zetron's relentless pursuit of quality, durability and interoperability has made it one of the most enduring and consistently trusted brands in mission-critical communications for decades. Our solutions are backed by world class technical support, training, project management and professional services, as well as a global network of highly capable partners and system integrators dedicated to exceeding the unique needs of Zetron customers. For more information, visit: **www.zetron.com.**