

Continuity of Operations for ASTRO[®]25 Systems

Dynamic System Resilience (DSR) and other strategies to maximize availability, confidentiality and integrity ...when first responders need it most



Public safety personnel require secure, dependable communications at all times. That's why mission critical systems must be designed from the ground up to deliver an extraordinary level of resilience and availability.

Large scale events often overwhelm commercial networks with heavy call volumes, loss of power or damage to network equipment. Unlike a commercial carrier, when you own your own mission critical network, you have the ability to design it for optimum performance during a crisis.

Motorola's ASTRO 25 systems employ a range of capabilities to help ensure that first responders can count on their radios to work the first time and every time. You can select from a range of availability strategies, including the Dynamic System Resilience (DSR) option, to achieve the level of survivability you require today ...and in the future.



A lifeline for public safety

Don't let a fire, flood, storm or other catastrophe shut down your communications. ASTRO 25 systems offer a range of features to maintain continuity of voice and data service to first responders in the field, even under conditions that could cause less robust networks to fail.

Continuity of operations: facing the challenge

For end users, continuity of operations boils down to a simple statement: whenever I need my radio it works. For the managers charged with the responsibility of making that happen, the task is not simple. No agency can achieve perfect 100% assurance that a network will survive every possible event. The challenge is to assess risks accurately and reach the right balance between system survivability and additional costs. It is necessary to look at the complete network and the impact on agency operations.

Continuity of operations is dependent on system availability as well as maintaining the confidentiality and integrity of the network. Confidentiality, integrity and availability all work together to provide a highly resilient and always available solution.

Considerations for maximizing availability

Availability measures the percentage of time when calls are successfully completed. Several parameters must be taken into consideration to maximize availability:

Capacity – The system should be able to connect the call immediately even during events that involve large numbers of personnel. The system can handle the increased call traffic.

Coverage – The first responder will be able to access the system where needed.

System behavior during crisis – The system is designed and tested so it will stand the added user load during a crisis.

Reliability – Needs to be built-in to deliver critical voice communications. The many components involved in making the call, from the user's radio to the repeater site, transport, infrastructure and receiving radio, need to be designed as an integrated part of the system design.

Redundancy – Redundancy configurations should be available for key hardware and software elements in the system.

Recoverability – Failure scenarios must be understood and recovery processes put in place to be quickly executed without impacting the user.

Fallback Operation – When normal service is not available the system offers alternative modes of operation to permit responders to communicate.

When capacity, reliability, redundancy, recoverability and fallback operation are built into the system, the more likely your communications will be available when your personnel—and the citizens they protect—are in greatest need.

ASTRO 25: Proven Operational Performance

Motorola's ASTRO 25 systems are the most widely-used Project 25 compliant communications solutions in the world today. Their resilience has been repeatedly tested under extreme operational requirements in real-life deployments.

Harris County Texas

Harris County is the largest county in Texas and the third largest in the U.S.

"We, as a mission critical organization, must have a system that is available 24 hours a day, seven days a week. We have lives on the line and so consequently we can't be off line. Therefore, the network was designed for high levels of control, security, and redundancy. Tower coverage areas overlap, providing a level of redundancy with service operation. Each radio has a system ID, so if a radio is lost or stolen, it can be taken off line."

— Steven Jennings,
Chief Information Officer
of Harris County and
Executive Director of the
Information Technology Center

Coverage and capacity sized right

ASTRO 25 can be configured to meet the user capacity and coverage requirements with flexible channel and site configurations, plus optimized spectrum and radio coverage so radio users can access the system when and where they need it.

Not only is the system flexible but Motorola has developed specialized tools for voice and data traffic analysis and a very sophisticated tool for coverage design.

Optimized for crisis operations

Motorola's development teams understand that ASTRO 25 will be the life line during a crisis and that the system must continue to operate when under heavy call volumes. Critical features like user priorities, emergency preemption, affiliation throttling and call burst protection all work in conjunction so when 1000's of users must access the system it can be done in a controlled and prioritized manner.

Built-in reliability and redundancy

Reliability is built-in throughout the system. The operating systems are hardened to disable unnecessary services, provide robust system passwords and prevent unauthorized intrusions. Optional hardware and application redundancy is available for voice critical elements. There is an optional geographically redundant configuration in case of catastrophic loss at the core.

Built-in reliability and redundancy allow for changes and expansion to be made without impacting system operation. New base sites can be added without interrupting service to existing sites. At the site base radios can be added by slotting in additional radios where required.

Designed and tested recovery

To further guarantee availability, recovery scenarios are designed-in and tested under heavy call volumes. Transport resilience has been designed and tested so the sites do not go into site trunking when switching to redundant site links. Control channel recovery occurs automatically in case of station failure. PC recovery disks are supplied for each application and backup and recovery applications can be optionally deployed to protect the heart of the system.

Maintaining operations

Fallback operation is another key consideration in maintaining the availability of the system. ASTRO 25 offers built in capabilities to address different failure scenarios so radio communications can be maintained if system elements have been impaired. Some of these fallback operation capabilities include site trunking communications, failsoft operation and the use of consolettes for dispatch.

Protection from unauthorized users

Multiple levels of protection are designed into the system to protect system resources, and the voice and data information in transit.

The ASTRO 25 system can be defended from outside attacks by using a combination of firewalls, Intrusion Detection Sensors (IDS) or by creating a buffer between the customer enterprise and the radio system. ASTRO 25 system resources and voice and data information are only accessible to those users with proper authorization.

Dynamic System Resilience

Not even a catastrophic failure at the system core should be allowed to interrupt your communications. The ASTRO 25 Dynamic System Resilience option can help to maximize availability by enabling your voice and data services to remain operational even if your primary core is destroyed.

DSR is an option for both single and multi-zone ASTRO 25 systems and can be implemented at the time of initial deployment or later as the need arises.

Dynamic System Resilience (DSR) is a new and efficient way to achieve geographic redundancy on an ASTRO 25 system. If an event should cause a power outage, equipment failure, or physical damage to the primary core, DSR enables automatic switchover to a backup core that will continue to deliver the same high level of availability, reliability, and network management capabilities that users expect from their network.

Primary and backup core systems

When deploying Dynamic System Resilience, two cores are deployed: one primary and one backup. These two cores are intended to be geographically separated. Each core has the call management applications, system management servers and networking equipment—everything required to control an ASTRO 25 system.

Every remote site (including RF, dispatch and system management sites) that requires a back-up operation should link to both the primary and backup core. In case of a failure on one T1 and/or Ethernet site link the remote site will continue to operate on either core as long as an alternate path remains operational.

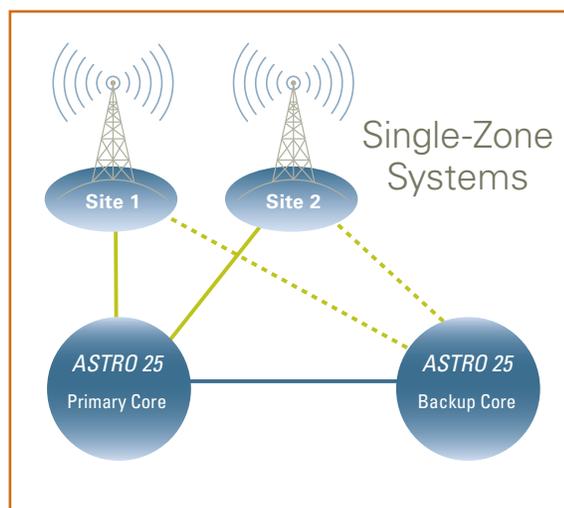
Under normal operating conditions ASTRO 25 cores communicate with each other, exchanging voice and control traffic as well as network health

and management data. Configuration data is synchronized between the cores so both are up-to-date and ready to take over network operations at any time.

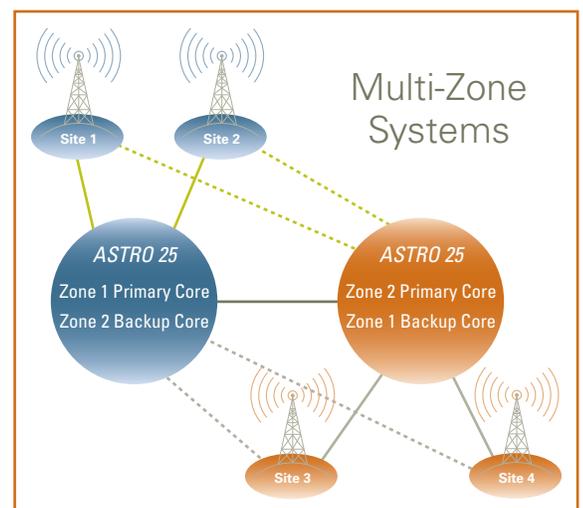
Automatic switch over

If the primary core becomes unavailable for any reason (power failure, equipment fault, damage to facilities, etc.) within seconds the system switches over to the backup core. Switch over requires no action from users or network operators. Remote sites which lose communications with their controller will automatically try an alternate path to access the controller. If the original controller is still active and responds, it will continue to use this controller. If the primary controller is not available, the site will use the backup controller.

Once the primary core is restored to operation, the remote sites will not switch back automatically unless there is a subsequent failure at the backup. This prevents unnecessary switching should the restoration of service be transient or intermittent. It also allows radio system managers to choose the best (and least disruptive) time of day to switch back to the primary core, while still maintaining redundant controller capability.



In a single-zone system with DSR, each ASTRO 25 core has full single zone site and call processing capacity. Under normal operations, the backup core maintains synchronization with the primary core so the backup core is ready to quickly become active at any time.



In a multi-zone system with DSR a core can be configured to act as both a primary core for one zone and a backup core for another zone. Each core has full site control capacity.

Manual switch over

If a situation such as a massive evacuation of the facility occurs the system manager can implement a manual switch over to the backup core maintaining full system operation from an alternate location.

Data services and DSR

If the ASTRO 25 system includes data services (IV&D or HPD) then DSR replicates all of the data sub-system equipment. In the event of a failure within the data sub-system (including the communications path to the customer's data network or CEN), data service will switch to the backup equipment. Failure and recovery of data services is independent of the voice system. Failures in the data sub-system will not cause voice service to be switched over.

Gradual deployment

The DSR configuration is flexible, your agency can introduce it gradually as resources allow. DSR does not necessarily have to be implemented at every remote site, which may help you manage transport costs, prioritize investments, and accommodate RF or console sites that do not support DSR.

A non-DSR remote site operates like any other site on the system as long as it still has connectivity to the primary core. If a failure occurs at the primary core and the non-DSR finds an alternative path to the primary core it will continue to operate. If all connectivity is lost, the non-DSR site will operate in site trunking mode.

Older sites and sub-systems (such as Centracom™ Elite, QUANTAR®, Smart-X and others) can still operate on the ASTRO 25 system but cannot be implemented with DSR. The DSR flexible design allows system configurations to be tailored to the specific requirements of your system.

Motorola quality and support

At Motorola, we understand what “mission critical” really means: the lives of your personnel and the people they protect could be depending on the ability to complete a radio call. We design our products and services to deliver the continuity of operations you should demand when lives are on the line. In addition to system availability, we have a reputation for outstanding quality and robust support services.

Quality control and testing

Motorola designs and builds products with quality at every step. Our processes include extensive pre-release hardware, software and upgrade testing and a rigorous certification process for third-party hardware and software. Our close involvement with user groups and industry standards organizations puts us in direct contact with the people who use

our products and their feedback helps us keep addressing the needs of first-response organizations in the real world.

Consider how we test radios. All Motorola radios and accessories undergo Military Standard 810F (MIL810) testing in 11 different categories: low pressure, high temperature, low temperature, temperature shock, solar radiation, rain, humidity, salt fog, dust, vibration, and shock. This testing was developed by to ensure suitability of equipment in the toughest military conditions—but we apply the same tests to civilian mission critical products.

We even go beyond MIL810 testing to conduct Accelerated Life Testing (ALT) on all our devices and accessories. This testing simulates six years of hard usage in the field. The testing is done during early product development to improve design and quality levels, and again at final approvals to ensure that equipment will function in even the harshest outdoor environments. The tests are designed to give peace of mind that radios and accessories will survive the inevitable knocks and drops, and still keep working.

Supporting services

In addition, Motorola offers a full portfolio of services for every stage in your system's life cycle. We stand by you at every point from needs identification and system design through financing, deployment, training, ongoing maintenance and future upgrades/expansions.

Our comprehensive network planning services can help you design a solution tailored to achieve your desired level of resilience and redundancy. Once your system is operational, we can provide network monitoring and troubleshooting services to keep it at peak performance. Motorola's Network Operation Center is staffed 24x7 every day of the year and has the ability to remotely identify, diagnose, and often fix network problems. When an element cannot be fixed remotely, Motorola repair technicians can travel to your site.

Conclusions

Continuity of operations is a key initiative of Motorola. We apply everything we have learned in over seven decades of working with public safety agencies to provide comprehensive, dependable communications support for public safety agencies around the world. The ASTRO 25 system is designed from the ground up to meet the special mission critical requirements of public safety.

With over 250 mission critical trunked systems deployed, Motorola's ASTRO 25 systems are fully proven for mission critical operations, having survived hurricanes, widespread power failures, and other events that crippled less robust networks.

***For more information about Motorola's ASTRO 25 solution for mission critical networks,
please contact your Motorola representative or visit www.motorola.com/ASTRO25.***



MOTOROLA

Motorola, Inc.
1301 E. Algonquin Road
Schaumburg, Illinois 60196 U.S.A.
www.motorola.com
1-800-367-2346

MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. © Motorola, Inc. (1001)
RO-26-1010