

CRITICAL PAGING SYSTEMS:

SOLUTIONS FOR SAFETY

B I A M P[®]
S Y S T E M S

SAFETY—THE COMMON THREAD	2
THE IMPORTANCE OF THE NETWORK	3
CRITICAL PAGING SYSTEMS: COMPONENT OVERVIEW	4
CONCLUSION	9

SAFETY—THE COMMON THREAD



Facilities and risk managers, and more increasingly IT managers, worldwide share many concerns in the day-to-day operations of the sites they manage. Whether overseeing a hospital, shopping center or sports arena—whether adhering to the standards of Underwriters Laboratories (UL) or the European Committee for Standardization (CE)—**public safety** is a top priority.

Timely and clear communication is paramount in maintaining this goal. One of the most assured ways to achieve this is with a robust, reliable **critical paging system** that clearly and concisely communicates with the public, regardless of the installation size. If you're expanding, retrofitting or planning new construction of a facility—right now or in the future—having a flexible, scalable system will ensure the success in providing safety to those in your building.

In this document, we describe some of the most common requirements and functions of modern critical paging systems, the components that make those functions happen and ways of safeguarding against failure of both individual units and the entire system. We'll show you how Biamp Systems has helped our clients around the world ensure the safety of—and clear communication with—the people who work at and visit their facilities. We call this solution Vocia®—a family of advanced paging products that offer facilities of all sizes a scalable, flexible voice evacuation system.

Traditionally, paging systems have employed discrete audio, data and power wiring. Failure of individual circuits can be circumvented by installing redundant paths; however the resultant systems tend to be unwieldy and offer limited protection against failure. Employing standard IT network infrastructure for all paging system interconnections offers superior fault tolerance and resilience.

THE IMPORTANCE OF THE **NETWORK**

A critical paging system's network must be robust and failsafe. Switches, to which computers and components of the system connect, should be high-reliability, managed types (known as Managed Ethernet Switches). Via computer interface, Managed Ethernet Switches allow you to designate certain settings on the switch to manage network architecture.

Control, audio and power features ride on an Ethernet network, so it is vital that the network is stable and reliable. Fortunately, this is easy to achieve thanks to Rapid Spanning Tree Protocol (RSTP) or Resilient Ethernet Protocol (REP). In a reliable network, RSTP allows for multiple, duplicate paths between Managed Network Switches, which look intelligently at all of the available paths. If a path fails, the switch uses another one. In this kind of reliable network, if a cable is cut somewhere, the network will negotiate a path around the break. The resulting changeover occurs so quickly it is virtually undetected. Thus, RSTP principles are crucial in the design of a secure network.

Switches that connect any critical components of the system should also include a fault relay output. The notification can be made to maintenance staff, indicating the network has encountered an issue that needs attention. Having this system notification is vital, since the network will continue to appear to operate normally even if its integrity has been compromised, requiring immediate investigation and rectification to restore full standby capacity. If the system is required to work during a total power outage, the network switching devices must be powered via an Uninterrupted Power Supply (UPS).

This network should be kept completely separate from any other network traffic, which may compromise the network bandwidth. This is best achieved by physically separating the network from any other facility network with separate switches and cabling. However, segregation can be achieved using shared network infrastructure by utilizing a Virtual Local Area Network (VLAN) for the exclusive use of the paging system and its associated control servers. A high level of experience with networks is vital if deploying the paging system on a shared infrastructure.

CRITICAL PAGING SYSTEMS **COMPONENT OVERVIEW**



Paging systems are important for daily operations, security and evacuation purposes. Among other components, a critical paging system includes **outputs** (such as amplifiers), **inputs** (such as paging stations with microphones), **servers** and **controllers** (such as those which trigger and play pre-recorded announcements and those that interface with fire detection systems). Traditionally, paging systems operate on a separate analog cabling infrastructure, requiring custom cabling that increases material and labor costs. Depending on the country, the system must meet public safety requirements as designated by a third party (i.e., UL in North America and CE in Europe).

OUTPUTS

Amplifier malfunction is perhaps the most common failure in a voice paging system. This can be due to **channel failure** (when one of the amplifier's internal channels connected to a speaker line does not function as required) or **device failure** (when the entire amplifier fails). In a critical paging system, it is important that the amplifier has been designed with several levels of redundancy to proactively protect against failures. These are known as **channel failover**, **device failover** and **network redundancy**:

- **Channel Failover.** The channels of an amplifier can be used for managing loudspeakers in different areas of a building. Some of the channels can be designated for failover purposes. With this safeguard system, if channel one fails, it would failover to channel two. If channel three fails, channel four would serve as its backup. This provides extremely cost-effective amplifier redundancy; however, it does not account for all possibilities of failure within an amplifier (e.g., power supply or network card failure).

- **Device Failover.** In this case, all channels in an amplifier are set up to failover to the channels in another, separate device. If something within an amplifier fails or if the power supply to an amplifier fails, channel failover would be ineffective because the power to both of the channels has failed. The benefit of device failover is that you can ensure the main unit is powered by one feed and the second by another. If one power feed fails but the other is still functioning, you have an added level of protection. This provides total redundancy for the entire frame, including the power supply, network card and digital emergency messages.
- **Network Redundancy.** Amplifiers in a critical paging system should be fitted with what are known as redundant Ethernet ports. These are designed to connect to different Ethernet switches in the redundant network and will ensure that if one network switch fails, the amplifier will continue to be connected to the network.

Several other high-reliability functions are important in an amplifier:

- **Speaker Line Monitoring.** A unit (known as an end-of-line device) connected at the end of the speaker line listens for an inaudible test tone and reports line failure back to the amplifier via the Ethernet.
- **Ambient Noise Compensation.** Placed within an acoustic space, ambient noise sensing microphones measure noise levels in different areas of the building or space. The microphone is connected to an ambient noise compensation device, which prompts the amplifier to adjust the level of voice announcements accordingly. This ensures announcements are always loud enough but never uncomfortably loud during quieter periods.
- **Built-in Emergency Message Storage.** It is critical that Non-volatile Flash Memory is integrated into an amplifier and used to play out emergency messages. This on-board component memory is key to building a networked paging system with no single point of failure. Even during a catastrophic event in which all network connections have been cut to the amplifier, emergency messages would continue to play out, as long as the amplifier is supplied with power.

Amplifiers should be supplied with power via a UPS to ensure full-system functionality during a power outage.

Providing amplifier redundancy (device or channel) and end-of-line monitoring will ensure the highest likelihood the system will be constantly monitored, thus engaging best business practices for the highest

likelihood of being failsafe. Nevertheless, there is always the chance that a speaker on the line or all speakers within a single acoustic space (if the line is shared between several spaces) may fail or become disconnected. To compensate for this scenario, additional speakers may be installed and run from separate lines. Driven from failover devices or channels, they may be run into crucial areas to ensure absolute system failover.



INPUTS

Inputs to a critical paging system may include desk or wall-mounted **paging stations** with microphones, which facilities staff use to make announcements.

Any paging station components exposed to heavy daily use are at risk for damage if dropped or used improperly. The **microphone capsule** (or transducer) is the part of the paging station's microphone that converts sound from the user's voice into an electrical signal. Because it is a sensitive device, over time, it may be particularly at risk of failure. The system should include a means of detecting and reporting such failures.

In order to maintain critical functionality in the event of a paging station failure, it is best business practice to ensure that a minimum of two paging stations reside at each location where important operational and emergency pages will be made (i.e., a reception desk, fire control panel or security control room). The paging stations should be connected to at least two or more different Ethernet switches in case a switch fails. In the event of a power outage, if Ethernet switches are connected via a UPS, the paging stations would continue to be powered via the Ethernet network (also known as Power over Ethernet or PoE).



In high-reliability systems, it is imperative that these components are monitored regularly and automatically by the system, and the system can send an appropriate notification or alarm, allowing facilities staff to proactively replace and repair any component. Vocia paging stations are monitored at all times through the networked structure, and the system automatically raises an alarm if a malfunction is detected.

SERVERS AND CONTROLLERS

Most contemporary paging systems use recorded messages that are released via a **message server** according to some kind of stimulus—a system scheduler or a staff member pushes a button. Message servers support multiple functions within a critical paging system, including storage and playback of pre-recorded messages, time keeping and event scheduling, Voice over Internet Protocol (VoIP) paging interface and more. To ensure a system has full redundancy for all functions at all times, a second message server can be connected and designated as a “mirrored copy” of the primary server. This second server will take over seamlessly in the event of failure of the primary device. It is best practice to physically locate any mirrored copy in a different part of the facility. This protects the system in the event of a disaster. For example, if a fire occurs in the equipment room where the primary message server is located, the second (or mirrored) unit would take over from another location. Message servers should be powered from a UPS if full functionality is required in the event of a power failure.

In order for a critical paging system to connect to an **emergency or fire alarm system**, it will need a device that serves as an **interface** between the two. In the event of a chemical spill or fire, the emergency or fire alarm system alerts the paging system, which then prompts a warning to play over the speakers.

Connections between a fire detection system and a paging system are typically made via a single interface. To comply with European standards (specifically EN54-16), the interface should have built-in redundancies. For example, any fire safety interface device should have the following:

- **Redundant network connection with primary and secondary network ports.** These are designed to be connected to different network switches within the redundant network. If the primary port loses connectivity, the secondary port will automatically activate.
- **Triple redundant power supply.** The primary supply for the interface should include a battery backup and for preference, two such power supplies should be provided (double redundancy). An additional level of power supply is preferable in that the interface can continue to report failure of the primary power supplies.

- **Monitoring of the crucial output ports on the unit.** Output ports on the interface are typically used to report system faults. If a connection to these ports is interrupted or short circuited, the system should provide a fault warning. Similarly, alarm inputs to a life safety interface device (triggers from a fire detection system) are typically monitored by the system.
- **Ability to monitor the health of all paging system devices.** The system should check the integrity of all units involved in the delivery of emergency messages, as well as all relevant network paths (via contact from the network switches). This allows for fault indication of all system parts involved in emergency message delivery.
- **Creation of a dry contact closure that can be used for an external alarm.** If the interface device fails, the unit needs to physically join two wires together so an alarm triggers in another part of the building, indicating unit failure.

OTHER CONSIDERATIONS

Devices within a critical paging system should be designed so that facility maintenance staff can easily maintain and manage the system operation after basic training. This functionality allows for the absolute minimum downtime of the system, as any faulty device can be quickly and safely exchanged by onsite maintenance staff.

Additionally, the Ingress Protection (IP) rating of units in the system is an important requirement. All essential Vocol products are rated to IP-30 for ingress protection of dust, insects and other foreign objects.

CONCLUSION

For more information about international public safety standards, please visit www.ul.com and www.cen.eu.

And for additional information on Biamp's Vocia System, please visit www.biamp.com/vocia.

Important aspects of a critical paging system in a high-reliability environment include:

- Sufficient paging stations in each critical location that are monitored regularly and automatically by the system;
- Amplifiers with channel or device failover, network redundancy, speaker line monitoring, ambient noise compensation and built-in emergency message storage;
- An Uninterrupted Power Supply (UPS) for everything critical (amplifiers, servers, switches);
- Redundant, mirrored servers to ensure the critical functions of those devices (i.e., message playback and VoIP paging interface);
- The inclusion of a life safety interface with built-in redundancies (if the paging system needs to connect to an emergency or fire alarm system);
- Standard network based system interconnections, utilizing Managed Ethernet Switches, Rapid Spanning Tree Protocol (RSTP) principles and a fault relay output. The network should be kept separate from other network traffic;
- Devices should be able to be easily swapped out by maintenance staff, and the Ingress Protection (IP) rating is important.

Whether you're expanding, retrofitting or planning new construction—you need a reliable critical paging and voice evacuation system to ensure the safety of those who work in and visit your space. Keeping these important issues in mind will ensure the design and installation of a robust, stable and expandable solution.

See how Biamp empowers our end-users and partners in the development of networked, critical paging systems with no single point of failure.