Securing the Future of Control Rooms for Next-Generation Operations.

Executive Summary.

Control room environments are under growing pressure to modernize their infrastructure in line with Internet Protocol (IP)-based workflows. This trend is being driven by a range of factors, such as the need for scalable and flexible systems, simplified deployment and management, long-term cost efficiency and achieving better integration with enterprise IT environments, to name a few. Add to that the growing range of inputs used to inform decision-making, and modern control room environments are more complex than ever.

Indeed, going down the AV over IP (AVoIP) route enables centralized control, remote management and interoperability across vendors - capabilities that have become increasingly important in the wake of supply chain disruptions and rising infrastructure complexity. The challenge is that relatively few organizations can afford to replace their entire AV estate in one move, with many still dependent on legacy hardware that must remain operational for the foreseeable future.

This has created a situation in which older AV assets must coexist with new IP-based technologies within an integrated hybrid environment. For those involved in implementing and managing these control room systems, the challenge is to support both formats without introducing unnecessary complexity, performance issues, or limiting future innovation. Success depends on identifying the right bridging technologies and selecting standards-based solutions that allow legacy and IP systems to operate side by side.

Introduction.

From transport networks and emergency response to energy infrastructure and defense, modern control centers are, quite literally, mission-critical. As such, they typically draw on a wide variety of technologies from a host of vendors, with system interoperability, reliability and ease of use central to how well teams can perform.

Indeed, technology integration has always been a defining factor in control center effectiveness, but as more systems move to Internet IP-based infrastructure, ensuring devices, platforms and protocols work together has become significantly more complex. One of the key challenges is that legacy approaches to signalling, where audio and video signals were transmitted over fixed, hardware-defined paths via standard interfaces such as HDMI or SDI, are no longer sufficient for the rigours of modern control centre operations.

Complicating matters even further is that modern control centers use an enormous range of technologies. For operators alone, there are lighting, speaker, and microphone systems that must work alongside high-resolution video walls, IP-based AV distribution, KVM (Keyboard, Video, Mouse) extenders, sensor networks, and, increasingly, AI-powered analytics. Integrated comms platforms, secure network infrastructure and cloud-based infrastructure also play a significant role, alongside tools for processing and routing media across increasingly complex environments. The list goes on.

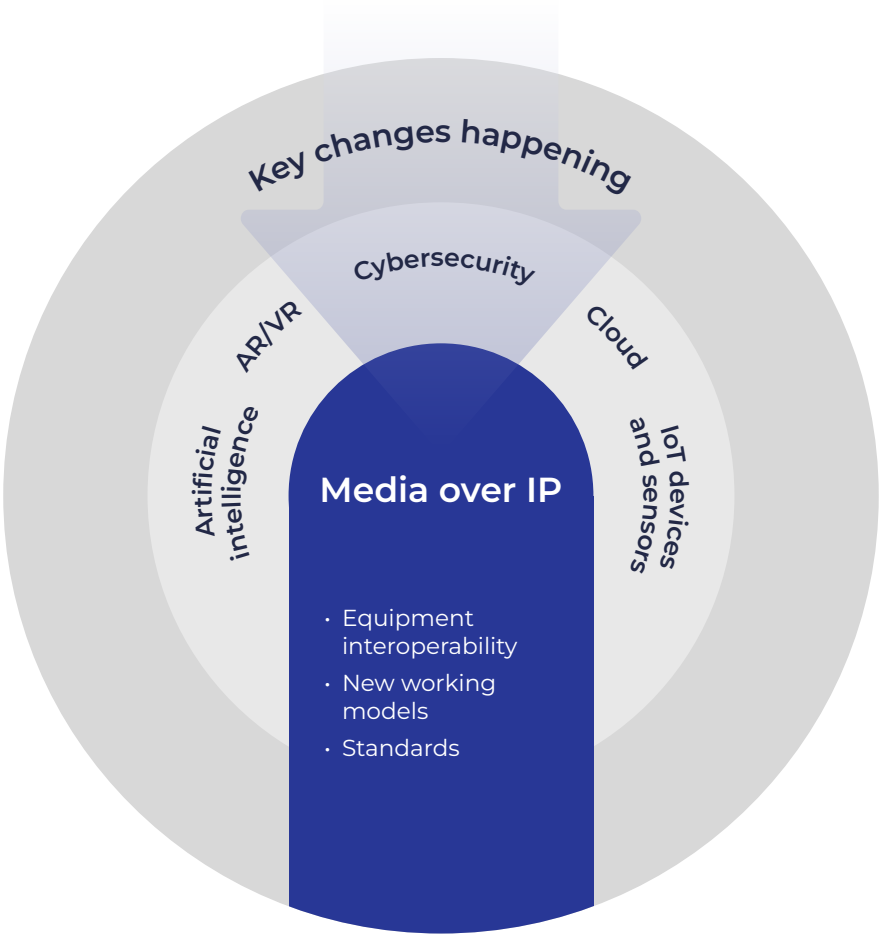
To help organizations address these pressures, this paper explores the shift to IP-based infrastructures, the role of open standards in ensuring interoperability, and why security must be embedded at the protocol level. It also outlines design strategies that enable resilient, future-proof operations. Taken together, these insights provide a framework for balancing performance, scalability and security in the next generation of mission-critical control rooms.

The evolving role of control rooms.

Across these diverse use cases, the role of control rooms continues to evolve. Traditional rooms of dials and gauges have long since given way to computer-based environments and highly visual workflows. The control room employee demographic has also changed, with today's digitally native generation having entered the field. Comfortable handling fragmented data and multiple inputs, they bring a new agility to decision-making, with the FAA's recruitment of gamers perhaps the most striking recent example of the skillsets now valued in control room settings.

The pace of tech-led innovation is accelerating. In many environments, data can now be delivered directly to individual workstations or across sites. Today, organizations have more options than ever before about how information is disseminated among control room teams, with AI, VR, cloud and IoT systems converging to deliver the advanced levels of interoperability, scale and flexibility modern operations demand.

Despite these transformational changes, however, the role of the operator remains paramount. As a result, organizations that build, maintain and run control rooms are faced with some important challenges. How, for example, can they manage information overload and ensure usability in high-pressure environments? Also, how can they build systems that deliver maximum performance while also being secure against cybersecurity risks?



Control room trends

Core control room AV technologies.

At the heart of every control room are the technologies that allow operators to see, interpret, and act on information in real time. While the mix of systems varies by use case and sector, several categories of Pro AV equipment are consistently used across effective operations.

Video walls remain a defining feature of many mission-critical environments. By consolidating multiple streams of information into a single, shared view, they give teams the situational awareness needed to collaborate and respond rapidly. Ongoing improvements in display resolution and IP distribution mean video walls can now integrate a wider variety of content sources, from broadcast-quality video to data visualizations and collaboration platforms. Even as information is increasingly delivered directly to operator workstations, video walls retain their role as a central canvas for decision-making. Video walls are also evolving and new workflows and options are making their use increasingly flexible to suit the needs of different stakeholders, physical room layouts, and individual users. Indeed, the emergence of the personal video wall (at individual stations) continues to rise as well.

Encoders and decoders are equally indispensable. By converting AV signals for transport over IP networks, these devices replace traditional point-to-point cabling to deliver much improved scalability. In these environments, operators can access streams from virtually any source without being limited by distance or physical connectors, while compression options provide the flexibility to balance bandwidth efficiency with latency requirements, ensuring that both routine monitoring and time-sensitive workflows are fully supported.

IP-based KVM systems extend this flexibility to operator interaction. They allow users to control multiple remote servers or applications as if they were local, all from a single workstation. For control centers, this means compute resources can be centralised and secured in equipment rooms or data centres, while operators retain responsive, real-time access. The result is a more ergonomic and efficient working environment, with reduced heat, noise, and clutter at the desk.

These technologies not only enable operators to visualise and manipulate complex data but also support the integration of new IP-based workflows, bridging the gap between legacy systems and next-generation infrastructures. Another important benefit is collaboration and the ability to easily distribute video within a facility or across multiple sites for decision making.

Why open standards matter.

In this context, the migration of audio, video and control to IP networks has become fundamental to modern control room design. As the backbone technology for global contemporary IT, cloud and communications, IP offers a compelling combination of performance, scalability and affordability. Its many advantages over legacy technologies also extend to control rooms by providing the means to deliver distributed workflows and the integration of diverse data streams operators need.

Despite its ubiquitous presence across the technology ecosystem, successfully adopting IP in control room environments is not without challenges. Different device types, from AV and broadcast systems to IT platforms, have adopted IP in inconsistent and often proprietary ways, creating fragmentation that undermines interoperability.

Without open standards, organizations risk costly integration workarounds, added latency and even operational bottlenecks in mission-critical settings. This is why initiatives such as the Internet Protocol Media Experience (IPMX) specifications are gaining traction by offering a common framework for transmitting audio, video and control signals over IP networks.

More specifically, IPMX addresses the ProAV industry's need for a common set of standards and protocols in the transition to IP infrastructures. It does so by delivering a single platform upon which manufacturers can build products that are more standardized and interoperable. Highly flexible and future-proof, IPMX supports SD resolutions and is ready for 8K (or higher) resolutions. Moreover, IPMX is flexible enough to support 1G, 10G, 25G and 100G networks. By aligning previously fragmented technologies under shared protocols, these efforts make it easier for devices from different vendors to work together out of the box.

To ensure open standards don't come at the cost of protection, IPMX also introduces a privacy encryption protocol, which is a method of key exchange that allows different systems to encrypt and decrypt media in a standardized way. This is similar to how High-bandwidth Digital Content Protection (HDCP) technology enables secure media playback in consumer devices, and makes it possible to manage access permissions across brands and platforms while preserving the integrity of the content.

The role of smart gateways.

Even with open standards such as IPMX gaining widespread acceptance, not every control room system speaks the same language. Broadcast equipment, ProAV devices, and IT platforms often use different formats and compression methods. For example, uncompressed broadcast video under SMPTE ST 2110, lightly compressed AV streams and highly compressed IT formats such as H.264 or HEVC all coexist in the same environment. Conversion is therefore unavoidable, and smart gateways provide the means to handle this reliably.

Gateways are primarily about compatibility rather than performance. They provide system designers with the ability to integrate disparate equipment and protocols so they can be managed from the same software platform. While any conversion process can introduce minor latency, gateways are designed to maintain responsiveness at levels operators will not notice. Their key benefit is enabling flexibility across otherwise incompatible systems, allowing integrators to design hybrid environments with confidence.

Securing control rooms at the protocol level.

The ability to integrate diverse systems is, of course, only part of the overall design and implementation equation. In every control room, organizations must also guarantee that every stream of data and video is secure, authenticated, and reliable — especially as operations extend into the cloud and across multiple sites.

Traditional perimeter defenses such as firewalls and physical isolation are no longer good enough to protect modern control rooms and, as AV-over-IP workflows extend across sites and into cloud platforms, data streams must be secured end-to-end as a matter of priority.

As discussed in Section 3, standards such as IPMX incorporate security directly into the protocol, providing standardized encryption. This includes a privacy encryption protocol that allows media streams to be encrypted and decrypted consistently across different vendors' systems. Until now, encryption between equipment from competing brands has not been possible; IPMX changes this by enabling secure workflows in multi-vendor environments.

IPMX also supports High-bandwidth Digital Content Protection (HDCP), ensuring that digital rights–protected material can be managed securely across diverse systems without compromising compliance.

At present, authentication and access control are handled individually by manufacturers, but the standardized exchange of privacy keys across brands is already possible. Manufacturers such as Matrox Video that adhere to the highest standards of authentication add value on top of what IPMX enables, ensuring both encryption and permissions are addressed.

Protocol-level protection is less about cloud distribution and more about guaranteeing that encrypted media streams remain secure when transmitted between different equipment types and brands. For multi-site operations and remote collaboration, this is essential to maintaining trust, compliance, and continuity of service in mission-critical settings.

A practical way to view this is through the operator experience: permissions determine which content can be shared and who has the authority to change those permissions, while encryption ensures that only those with the proper access can view it. IPMX standards and open specifications try to balance between the need for scale in large networks with the need to support encryption across different asset classes from different manufacturers.

Embedding security at the protocol level also addresses the needs of multiple stakeholders. Operators gain reliable access to the information they need, integrators can customize workflows without introducing vulnerabilities, and IT/security teams are assured that AV systems meet organizational security and audit requirements.

Designing resilient and future-proof control rooms.

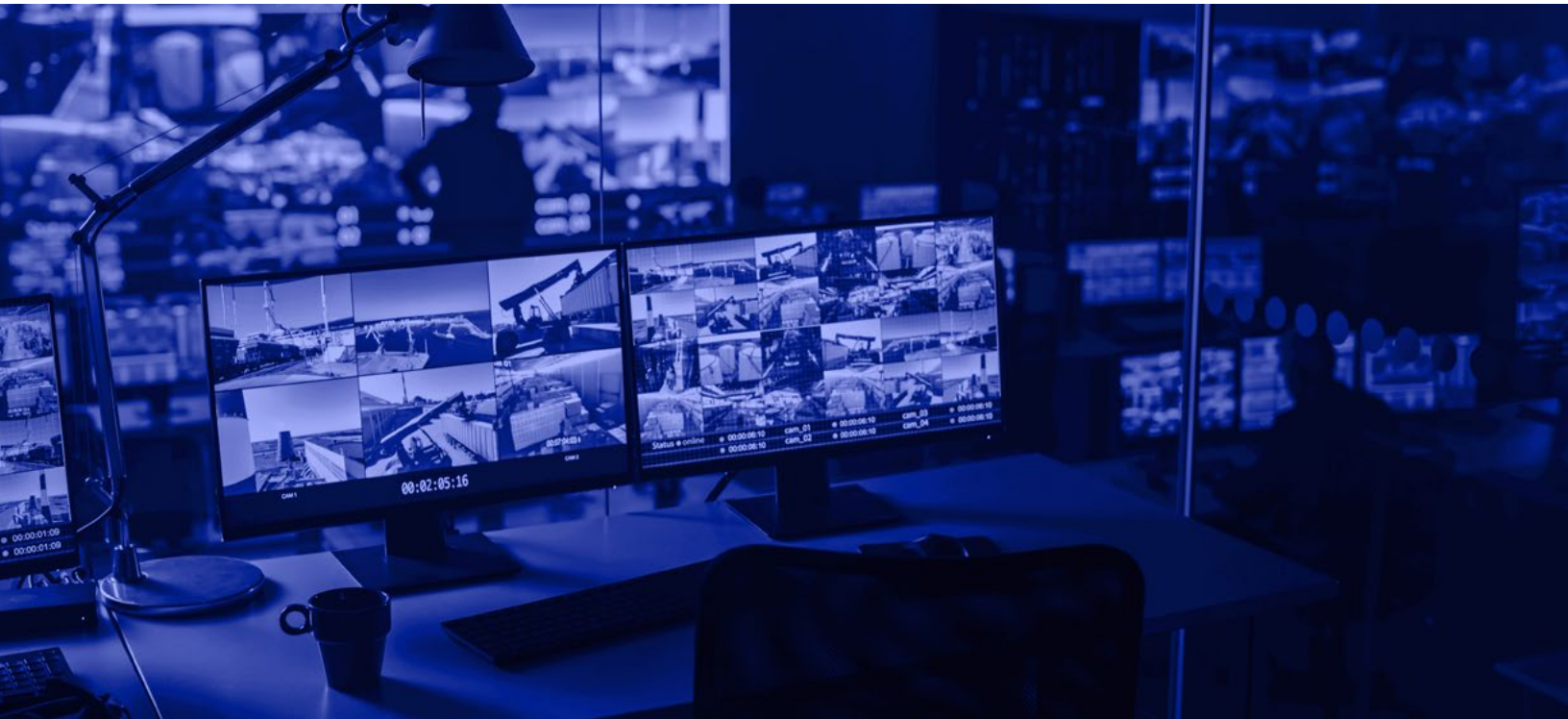
On a practical level, the adoption of IP also changes how control rooms are designed, deployed, managed and scaled. Within a single control room, for instance, priorities typically focus on high performance, real-time and seamless operator control. In these environments, minimal compression and high-bandwidth networks can be used to maintain responsiveness, particularly for audio and video switching or real-time decision-making.

However, as systems scale across multiple rooms or facilities, the equation shifts. Bandwidth efficiency, network security and centralized control become more important, especially when content needs to be shared between departments or across geographic locations. In these scenarios, organisations must consider how to manage media routing, bandwidth constraints and access permissions without compromising performance.

Take the challenges associated with synchronization, for example. In live environments, even slight delays between audio and video, such as when a speaker's voice reaches an audience before or after their image does, can create a distracting and uncomfortable experience. Audio systems in particular often require precise timing, especially when distributing signals across multiple rooms or between left and right speakers, where any misalignment can be problematic, to say the least.

Operational requirements are also changing, with the integration of services such as Teams or Zoom bringing content from IT systems directly into control center AV environments. As a result, the IT department remains indispensable in the design and governance of media infrastructure. For example, when video walls or AV displays are used to show content from collaboration tools, those sources must comply with IT security policies and access controls. This means AV systems must now operate within the same frameworks that govern organizational data, also bringing new considerations around issues such as authentication and network segmentation.

Wherever the specific priorities lie for each control center, however, the underlying requirement is maintaining uptime – they must be able to display the right information, at the right time, without fail. But as protocols evolve and equipment life cycles diverge, technology teams must apply a flexible approach built on a combination of open standards and media and protocol gateways, ensuring systems remain operational and aligned with performance objectives.



Solutions for control rooms from Matrox Video.

In high-stakes control room environments, operators need technologies that deliver reliable performance, enterprise-grade security and seamless scalability. Matrox Video offers a portfolio of IP-based solutions, including KVM over IP, AV encoders/decoders and video wall systems, that are increasingly central to meeting these requirements.

These solutions incorporate advanced security features such as authenticated user access and encrypted communication, ensuring that sensitive information always remains protected. They also deliver high-quality, low-latency video streaming at up to UHD/4K resolutions, supporting workflows while efficiently managing network resources.

Matrox Video solutions are built for flexibility, supporting diverse signal types including HDMI, SDI and HDBaseT, and adhering to open standards such as ST 2110 and IPMX for maximum interoperability. This makes it possible to integrate with existing infrastructure while ensuring a smooth transition to fully IP-based operations. Video wall systems provide stable performance in 24/7 environments, while long product life cycles reduce migration costs and guard against obsolescence.

These capabilities allow control rooms to achieve the high fidelity, security and resilience required for next-generation operations.

To learn more about our sector-specific solutions and products, click here.

Contact Matrox Video
Montreal Headquarters: 1-800-361-4903 (North America), 514-822-6364 (Worldwide) I video.matrox.com/contact
London Office: +44 (1895) 827300, Munich Office: +49 89 62170-444