Beyond Compliance: Building Magnificent Media Infrastructure

The False Choice We've Been Sold

For too long, the professional media industry has been presented with a false dichotomy: either accept proprietary vendor lock-in with "innovative features," or settle for dull, compliance-only IT solutions that destroy the magnificence we've achieved in audio, video, and lighting.

This is nonsense. We can—and must—have both.

What We Actually Want

The User-Centric IP Media Requirements aren't about choosing between excellence and compliance. They're about refusing to accept that choice in the first place.

We want:

- Uncompressed 4K60 RGB at 19 Gbps—full fidelity, no compromise
- Sample-accurate audio synchronization across hundreds of channels
- Lighting control with microsecond precision
- Creative technical innovation from experienced humans who understand the craft
- Bespoke user interfaces built on generations of domain knowledge

And simultaneously:

- NIS2 compliance because it's legally required
- DoD IPv6 mandates because they're procurement reality
- Modern network security because critical infrastructure demands it
- Open standards because vendor lock-in is a supply chain risk

These aren't competing goals. They're complementary requirements for professional infrastructure.

The Necessary Evolution—And Where It Went Wrong

Here's an uncomfortable truth: ****the proprietary "creationist" era was absolutely necessary.****

Around 2008, nothing would have happened without vendor-driven momentum. CobraNet, EtherSound, Dante—these proprietary solutions got the industry moving. They demonstrated what was possible. They built market adoption. They created the foundation we now build upon.

Vendor lock-in, rentierism, and obfuscation of core workings weren't bugs in early audio networking—they were features that enabled initial development and deployment. Without the commercial incentives of proprietary systems, we'd still be running kilometers of copper multicores.

The problem isn't that this happened. The problem is what happened next—or rather, what didn't happen.

The Missed Opportunity

Regulatory frameworks like NIS2 and DoD IPv6 mandates didn't appear overnight. They went through extensive consultation phases. These were opportunities for the media networking industry to engage, to shape requirements, to ensure pragmatic outcomes that balanced security needs with operational reality.

Contrast this with other industries:

- BEIRG (British Entertainment Industry Radio Group) maintained continuous engagement with Ofcom

- Result: Pragmatic regulatory outcomes that reflected industry reality

- A huge force for good through careful, sustained dialogue

What happened in media networking?

- Vendors ignored consultation phases

- Industry associations were absent or ineffective

- Internal backbiting prevented unified response

- No coherent voice representing user needs

The time to address IPv6 requirements, security mandates, and open standards compliance was during consultation. That work was done carefully, with genuine desire for sensitivity to industry needs. Vendors chose not to participate.

Now it's too late.

The legislative path is complete. These aren't proposals—they're enacted requirements with enforcement mechanisms and penalties.

The Landscape Has Hit Bottom

We've floated down the river and reached the waterfall. The industry now faces:

- Regulatory requirements that can't be negotiated away

- Infrastructure built on foundations that can't comply

- Users caught between legal obligations and vendor limitations

- Vendors who still haven't recognized the problem

The evolution we needed:

Proprietary systems → industry engagement during regulatory development → pragmatic transition to compliant standards → continued innovation on modern foundations

What we got:

Proprietary systems → regulatory indifference → legislative completion → compliance crisis

This isn't about open-source ideology. It's about the industry failing to engage when it mattered, and now facing regulatory reality it can't ignore.

What This Industry Actually Does Well

Strip away the vendor lock-in and artificial complexity, and this industry has extraordinary value:

1. Repository of Creative Technical Knowledge

Decades of experience in signal flow, acoustic design, color science, lighting psychology, human perception. This knowledge doesn't exist in generic IT. It's domain expertise refined through generations of practitioners who understand both the art and the science.

2. Bespoke User Experience

A broadcast mixing console isn't a generic UI—it's a tool shaped by decades of understanding how humans work under pressure. Lighting control surfaces embody knowledge about how designers think spatially and temporally. These interfaces represent genuine innovation, not marketing.

3. Integration of Physical and Digital

Media infrastructure exists in real spaces with real constraints—cable paths, equipment racks, cooling requirements, acoustic properties. This industry excels at integrating digital systems into physical reality, something pure IT rarely does well.

This is where the value is.

Not in proprietary networking protocols. Not in vendor lock-in. Not in monetizing artificial limitations.

Networks as "Clever Wire"

The framework repositions networks correctly: as ****utility infrastructure,**** not the hero of the story.

Networks should be:

- **Reliable** - Consistent, predictable, dependable
- **Scalable** - Growth doesn't require rearchitecture
- **Invisible** - Professionals focus on content, not connectivity
- **Standards-based** - Interoperable, auditable, maintainable

This isn't diminishing networking—it's recognizing its proper role. The electrical grid is magnificent infrastructure precisely because it's reliable utility that enables innovation elsewhere. Professional networks should aspire to the same.

When vendors sell networking complexity as a feature, they're selling failure.

IT Infrastructure: Fellow Victims of Missed Engagement

Recent zero-day vulnerabilities in major security appliances demonstrate that IT infrastructure vendors face similar challenges in adapting to modern security requirements.

When critical vulnerabilities emerge in enterprise security products, the pattern is familiar:

- Proprietary implementations that seemed adequate at design time
- Evolving threat landscapes that outpace vendor response
- Customer dependencies that make migration difficult
- Lessons learned painfully through production incidents

IT has been evolving through these challenges.

The shift toward open-source security tools, zero-trust architectures, and infrastructure-as-code isn't ideological—it's pragmatic response to actual operational experience.

The AV industry can benefit from observing IT's evolution

Rather than repeating similar patterns. When IT architects encounter "proprietary networking protocol with closed-source implementation," they recognize the operational risks from experience.

This framework isn't AV dictating to IT. It's both domains recognizing that regulatory requirements and operational scale demand approaches that may differ from what worked in earlier deployment phases.

We're facing similar transitions, learning from each other's experiences.

Media Engineers ARE Network Engineers

Here's an uncomfortable truth for IT vendors: media engineers already understand networking better than they realize.

Signal flow expertise transfers directly:

- Multicore analogue cabling concepts mirror IP routing
- Understanding impedance, termination, and signal integrity translates to network design
- Managing latency budgets in audio is identical to network latency management
- Redundancy strategies in broadcast are more sophisticated than most enterprise IT

The barrier isn't competence—it's jargon.

IT has buried fundamental concepts under acronyms and vendor-specific terminology. Strip away "BGP," "VLAN," "QoS," and "IGMP snooping," and media engineers immediately grasp the underlying concepts because they've been managing equivalent challenges in the analog domain for decades.

This framework recognizes that expertise and removes the jargon barriers that have excluded media professionals from networking decisions about their own infrastructure.

The Business Model That Actually Works

Vendor lock-in and exclusionary practices don't create sustainable value. They extract rent from captive customers while suppressing innovation.

The viable business model is inclusion:

1. Manufacturers provide exceptional hardware

- Superior components that deliver measurable performance advantages
- Innovative form factors and integration approaches
- Genuine engineering that solves real problems

2. Creative technical expertise remains valuable

- System design that optimizes for specific applications
- Integration knowledge that IT generalists don't possess

- Ongoing support from humans who understand the domain

3. Bespoke interfaces and workflows

- User experience design informed by deep understanding of professional practice
- Customization and adaptation to specific operational requirements
- Training and enablement that transfers knowledge

4. Open standards enable ecosystem growth

- More vendors can participate, expanding options
- Users can build hybrid systems optimized for their needs
- Innovation happens faster when it's not blocked by proprietary gatekeepers

This is a bigger market, not a smaller one.

When infrastructure is open and standardized, more participants can build value on top. When it's proprietary and locked, only the gatekeeper can innovate—and they rarely do, because they're already extracting rent.

Regulatory Reality

NIS2 in the EU and DoD IPv6 mandates in the US aren't optional. They're legal requirements with serious enforcement mechanisms and penalties.

The current situation is untenable:

- Critical infrastructure operators face regulatory obligations
- Current vendor offerings make compliance difficult or impossible
- Users are forced to choose between functional systems and legal compliance
- Vendors prioritize sales commissions over users' regulatory obligations

This can't continue. When broadcasters, entertainment venues, and critical infrastructure operators are audited for NIS2 compliance, "my vendor didn't provide IPv6 support" won't be an acceptable defense.

The User-Centric Requirements define what vendors must provide to enable—not obstruct—user compliance.

This isn't opinion. It's not preference. It's regulatory reality. Vendors can argue with the technical approach, but that argument needs to be directed at:

- The U.S. Department of Defense

- The European Commission

- The EU Parliament

- National regulatory authorities

If vendor representatives believe these regulatory bodies are inexpert or have been hoodwinked, they should say so publicly. Otherwise, they need to provide compliant solutions.

The Challenge to Vendors

I'm not your adversary. I'm your customer, representing user requirements.

If these requirements are wrong, incorrect, or impractical, then challenge them—but do so by addressing:

1. Why DoD IPv6 mandates are inappropriate for media infrastructure

2. Why NIS2 security requirements don't apply to professional AV systems

3. Why open standards harm rather than help the industry

4. Why Layer 2 networks are superior to Layer 3 routing for modern scale

Make those arguments technically, publicly, and to the regulatory bodies establishing these requirements.

Alternatively, provide products that meet user needs for both magnificence and compliance. There's an extraordinary business opportunity for vendors who can deliver:

- Exceptional hardware performance

- Standards-based infrastructure

- Genuine innovation in user experience

- Support from knowledgeable humans

The vendors who embrace this will thrive. The vendors who cling to proprietary lock-in models are already obsolete—they just haven't accepted it yet.

What Happens Next

These requirements will be refined through industry consultation. Feedback from manufacturers, users, network architects, and regulatory experts will improve and clarify them.

But the fundamental direction is set by forces larger than any vendor or consultant:

- Regulatory mandates that aren't going away

- Security requirements that will only increase

- Scale demands that proprietary approaches can't meet

- User rejection of vendor lock-in and artificial limitations

The professional media industry can build magnificent systems on modern, compliant infrastructure. We've done harder things. We've built real-time audio networks with sample-accurate synchronization. We've delivered broadcast video to billions of viewers simultaneously. We've created immersive experiences that blur physical and digital reality.

We can absolutely build on IPv6, implement proper security, and maintain technical excellence.

We just need vendors to provide the tools instead of the obstacles.

Kieran Walsh

The User-Centric IP Media Requirements and accompanying presentation are available at www.kdwalsh.com