



The Era of AI Smart Surveillance Is Here:

How the IGR-A804XSM-8PH Solves Five Major Network Challenges

– Building the Network Foundation for AI Surveillance



Growing Demand for AI Surveillance

As AI-powered video analytics rapidly moves into surveillance systems, front-end cameras are evolving from simple “recording devices” into smart sensing terminals capable of object detection, facial recognition, and anomaly detection. According to Fortune Business Insights, the AI video surveillance market is projected to grow from USD 7.04 billion in 2026 to USD 26.9 billion in 2034, at a compound annual growth rate (CAGR) of 18.2%. (Source: *Fortune Business Insights AI In Video Surveillance Market Size and Future Outlook*. Aug. 10, 2026)

As surveillance systems evolve into distributed networks of cameras, sensors, AI computing devices, and back-end platforms, companies face challenges that go well beyond computing power and high-resolution video transmission. The network itself must also keep pace, delivering greater bandwidth, tighter time synchronization, smarter traffic management, and stronger cybersecurity, all at once.

Five Major Challenges of Implementing AI Surveillance:

1. Existing Networks Can't Keep Up with AI Video's Bandwidth Demands

As high-resolution cameras and AI computing devices multiply, multiple video streams flood into NVRs, AI servers, and back-end platforms at once, pushing existing networks past their limits with insufficient upstream bandwidth and transmission bottlenecks. A network built for higher throughput is no longer optional; it's the foundation every AI surveillance deployment depends on.

2. Inconsistent Time Reference Across Cameras and Sensors

When the same event is captured by multiple cameras or sensors at once, a lack of a unified, high-precision time reference can throw off how AI interprets object positions, video captures, and device control. A switch built for high-precision time synchronization keeps every device on the same clock, so results stay accurate and consistent.

3. Critical Data at Risk from Video Traffic Congestion

Surveillance networks carry video, alerts, control commands, and time-sync data all at once. When video traffic spikes, congestion can delay the real-time delivery of critical alerts and control signals. High bandwidth alone isn't enough; AI surveillance needs traffic management that treats data by importance, not just by volume.

4. More Complex Networks Mean Greater Cybersecurity Exposure

AI surveillance depends on a constant flow of video and analytics data between front-end devices, real-time computing systems, and back-end servers. As more devices transmit and get managed at once, the risk of unauthorized access and data tampering climbs right along with it. Every network device sitting at these connection points needs built-in hardware and software protection, plus solid access control.

5. Smart Surveillance Often Means Remote, Hard-to-Reach Deployments

Surveillance systems get deployed at intersections, factories, trackside locations, and public facilities, often far from easy reach. When a network or power failure hits, on-site maintenance eats up time and manpower fast. Equipment needs more than just tolerance for tough environments; it needs network management, redundancy, and automatic recovery to keep maintenance demands in check.

CTC Union Solution

10G High-Bandwidth Transmission and PoE+ Power: IGR-A804XSM-8PH features four 10G SFP slots delivering high-speed fiber uplinks, giving it ample bandwidth headroom to carry multiple 4K/AI video streams to NVRs, core networks, or AI servers. Eight PoE+ ports, each delivering up to 30W within a 240W total power budget, power AI vision sensors, PTZ cameras, PoE illuminators, and other front-end IP devices directly, cutting out the need for separate power supplies and extra cabling.

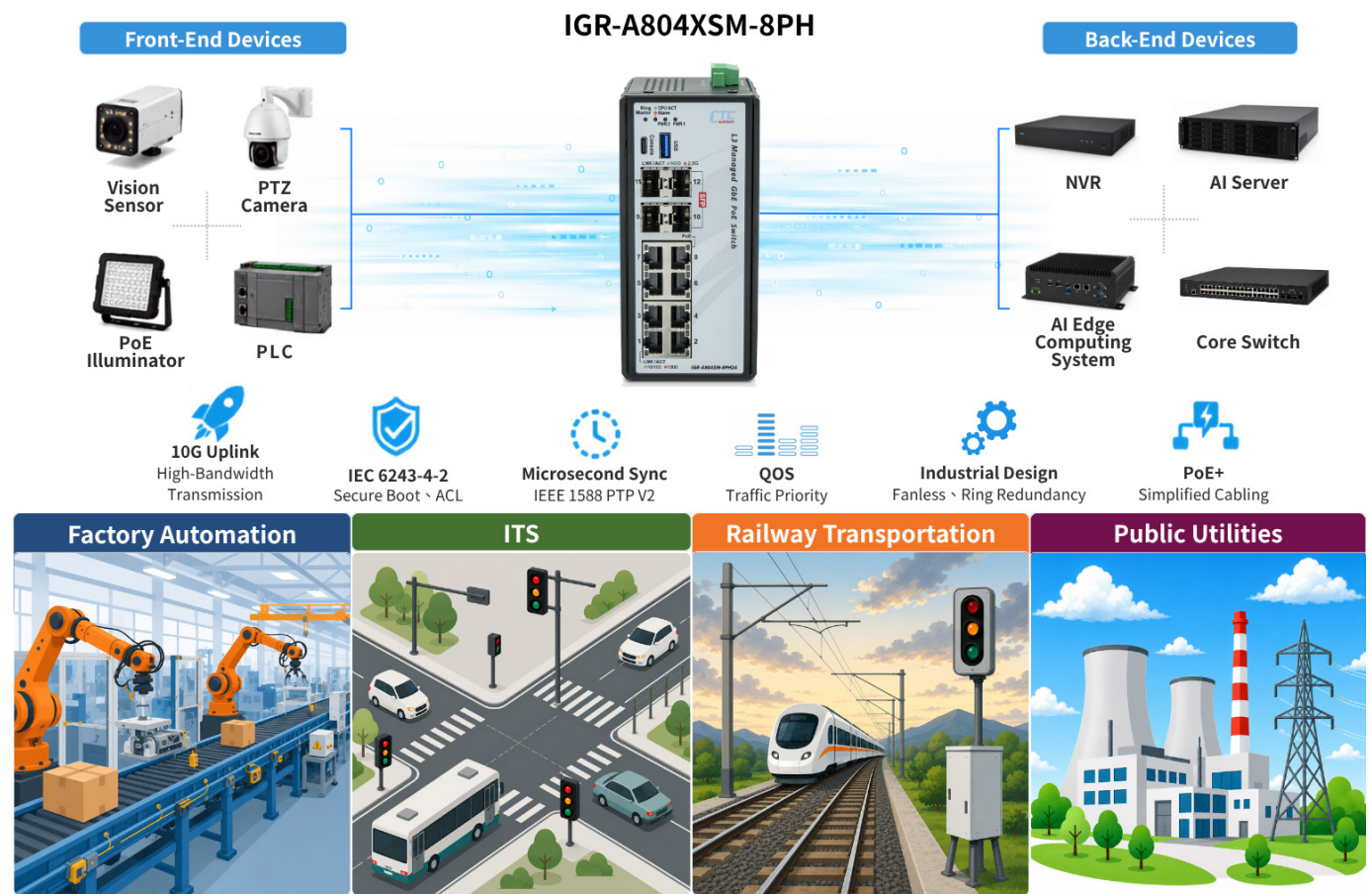
Accurate Time Synchronization: As surveillance expands from a single site to multiple intersections, factory zones, or large transportation hubs, keeping every device's clock in sync becomes mission-critical. The IGR-A804XSM-8PH supports IEEE 1588 PTP v2, delivering precise time synchronization so every camera shares the same time reference, sharpening the accuracy of cross-camera event correlation, incident tracking, and video analysis.

Traffic Management: Built-in QoS lets users set transmission priorities based on data importance, giving critical packets and alerts priority over routine traffic, so the information that matters most gets delivered in real time, every time.

Cybersecurity and Network Access Control: Built to meet the security demands of AI surveillance infrastructure, the IGR-A804XSM-8PH is certified to the IEC 62443-4-2 international cybersecurity standard. Secure Boot and ACL access control with up to 256 rules work together to build a solid line of defense for multi-device networks.

Industrial-Grade Reliability and Remote Management: With an IP30 rugged housing and fanless design, the IGR-A804XSM-8PH meets EN 50121-4 and EN 61000-6-2/-4 standards for transportation and industrial environments, built for automated factories, intelligent transportation systems, warehouses, trackside railway equipment, and public utilities. As a managed switch, it lets teams configure and monitor the network remotely, cutting down on-site maintenance across distributed locations. In addition, PoE fault detection with automatic restart, plus μ -Ring network redundancy, help restore connections fast whenever front-end devices or the network run into trouble, keeping the whole system reliably online.

Application



Conclusion

AI is redefining what front-end surveillance can do, and the network infrastructure behind it has to keep pace. The IGR-A804XSM-8PH combines PoE power delivery, 10G high-speed uplinks, PTP time synchronization, QoS traffic management, and IEC 62443-4-2 cybersecurity protection, giving companies everything they need to tackle the bandwidth, synchronization, traffic, security, and reliability challenges of AI smart surveillance, and building a more stable, scalable foundation for the surveillance networks of tomorrow.

Related Products



Industrial L3 10G Cyber-Secure Managed Ethernet Switch

IGR-A804XSM-8PH

8x GbE RJ45 + 4x 100M/1G/2.5G/10G SFP
with 8x PoE 240W, 48VDC



Industrial L3 Cyber-Secure Managed Ethernet Switch

IGR-A804SM-8PH

8x GbE RJ45 + 4x 100M/1G/2.5G SFP
with 8x PoE 240W, 48VDC



Industrial L3 Cyber-Secure Managed Ethernet Switch

IGR-A804SM-8PH24

8x GbE RJ45 + 4x 100M/1G/2.5G SFP
with 8x PoE 180W, 24/48VDC

• The specification and pictures are subject to change without notice.



CTC UNION TECHNOLOGIES CO., LTD.

8F, No.60, Zhouzi St. Neihu, Taipei 114, Taiwan TEL : +886 2 2659-1021 FAX : +886 2 2659-0237 sales@ctcu.com

© Copyright 2026 CTC UNION TECHNOLOGIES CO., LTD.

CTC UNION and the CTC UNION logo are trademarks of CTC UNION TECHNOLOGIES CO., LTD. All rights reserved. All other trademarks are the property of their respective owners. Specifications & design are subject to change without prior notice. Please visit CTC UNION website for more details.

www.ctcu.com

09/2026 V1.0