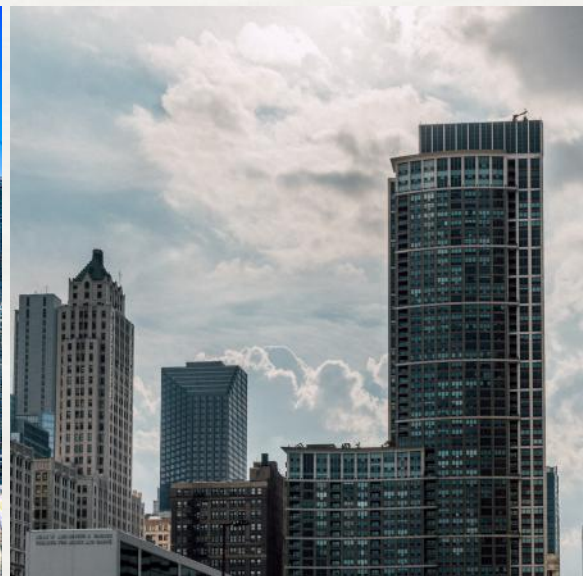
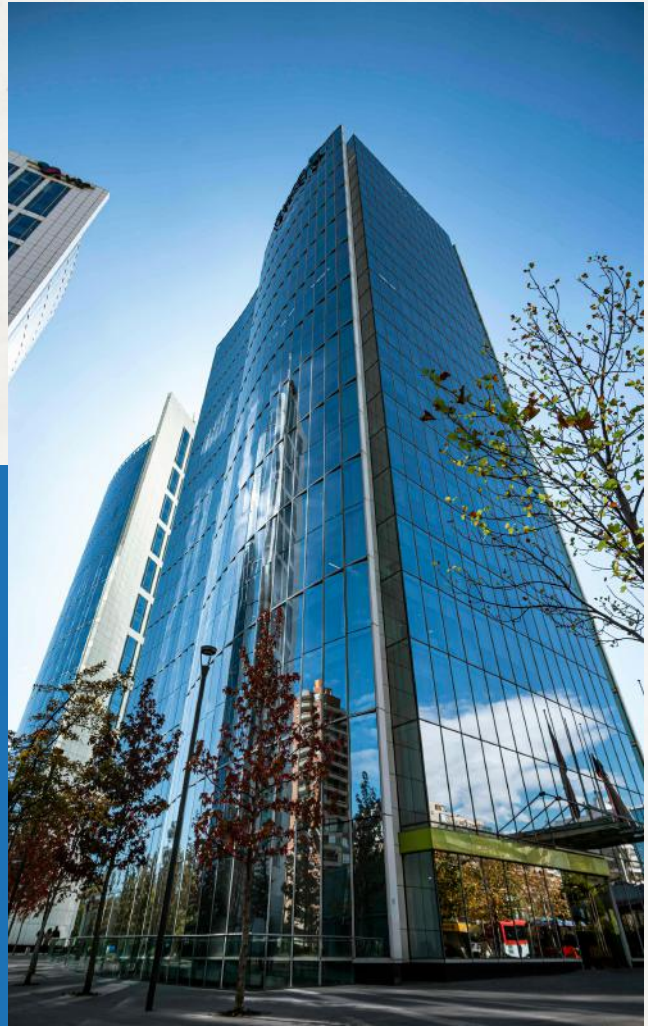


BUILDING TECHNOLOGY BIZBITS

MAY 2026 ISSUE

INBAC ASSOCIATION

Building automation is powered by technology, but driven by a community committed to smarter, safer, and more sustainable buildings.



Community
Connected Buildings by
Connected People

INBAC®
Building Connectivity

www.inbac.org / www.thevital.org

Powerhouse of VITAL opportunities



TABLE OF CONTENTS

- | | |
|--|---|
| <p>01 THE EDITOR'S DESK
By Mehul Joshi
Editor-in-Chief</p> <p>02 THE NEXT GENERATION OF SMART BUILDINGS: NAVIGATING OPERATIONAL TECHNOLOGY CYBERSECURITY IN MODERN BMS
Author: Mr.Abhash Shah
Designation: Business Leader & Technology-Driven Infrastructure Professional
Organization: Forestlinc</p> <p>05 IBMS TRANSITIONING TO AN IP-BASED SOLUTION: THE FUTURE IS CONNECTED
Author: S.R.Manikandan
Designation: Lead CRN,MEP Consultant
Organization: C R NARAYAN RAO</p> <p>07 DATA CONTEXTUALIZATION FOR BUILDING - BMS OR ASSOCIATED SYSTEMS
Author: Mr.Hiren Banker
Designation: Head of Operation: Global Command Centre / Remote Data Analysis
Organization: Siemens (Real Estate).</p> <p>10 ORGATEC ADVERTISEMENT</p> | <p>11 REWIRING THE FUTURE: A NEW APPROACH TO OPEN BUILDING AUTOMATION
Author: Mr.Madhurender Singh
Designation: Building & Energy Management System Expert.
Organization: Mitsubishi Electric India Pvt. Ltd.</p> <p>13 INBAC LEADING THE WAY IN INDIA'S SMART BUILDING REVOLUTION
Author: Mehul Joshi
Editor-in-chief-INBAC BTB magazine</p> <p>15 IGBC RATINGS AND THE FUTURE OF INTELLIGENT BUILDING MANAGEMENT SYSTEMS
Author: Ms.Ekta Sharma
Designation: Sales Director Cyber Group
Organization: Cyber Info Electronic Security System Pvt. Ltd.</p> <p>18 THE FUTURE OF INTELLIGENT TUNNEL & STATION AUTOMATION: SCADA SYSTEMS TRANSFORMING RAILWAY, METRO AND ROAD INFRASTRUCTURE
Author: Dhairya Desai
Designation: Managing Director
Organization: AD Automatos Technologies Pvt. Ltd.</p> |
|--|---|



The Editor's Desk



Dear Inbacers,

We would like to extend our heartfelt congratulations to the entire INBAC team for their outstanding participation at the **Smart Home Expo 2026** as a **Knowledge Partner**, as well as their commendable representation at the **MEP Conclave 2026**. These engagements are a testament to **INBAC's** growing presence and influence in the building technology ecosystem, and we are proud of the team's dedication in carrying forward this mission on every platform.

It is a pleasure to bring you yet another edition of **INBAC Magazine**. This month, we turn our attention to a subject that lies at the heart of the **Building Management Systems (BMS)** industry—one that many of us encounter in every project, yet seldom discuss openly: the need for **standardization** and **closer interoperability** between systems.

Today, a typical building hosts multiple BMS platforms: HVAC controllers, fire alarm systems, access control, energy meters, and more each often operating in its own silo. The result is fragmented data, duplicated effort, and missed opportunities for truly intelligent building operation. The solution is not complex; it begins with a shared commitment to open protocols, common data formats, and agreed-upon integration standards across vendors and disciplines. When systems speak the same language, buildings become smarter, operations become simpler, and the value delivered to end users grows significantly.

We are deeply grateful to our article contributors in this edition, who have shared their perspectives and field experiences on this very topic. Their insights into the practical challenges of system integration and the path toward greater standardization are **invaluable** to our community. It is through such candid, knowledge-driven conversations that we collectively move the **BMS** world forward. We encourage all our readers to engage, share their own experiences, and continue contributing to **BTB Magazine** through the platform of **INBAC**.

Together, let us build a more connected and standardized future for intelligent buildings.

Sincerely,

Mehul Joshi

Editor-In-Chief

Building Technology BizBits Magazine.



THE NEXT GENERATION OF SMART BUILDINGS: NAVIGATING OPERATIONAL TECHNOLOGY CYBERSECURITY IN MODERN BMS

As we progress through 2026, the traditional Building Management System (BMS) has evolved beyond recognition. No longer just a centralized hub for scheduling HVAC and turning off lights, the modern BMS is a highly intelligent, deeply connected nervous system for commercial real estate and industrial facilities. Driven by the need for extreme energy efficiency, ESG (Environmental, Social, and Governance) compliance, and superior occupant comfort, today's smart buildings are entirely data-driven.

However, this hyper-connectivity comes at a cost. The convergence of Information Technology (IT) and Operational Technology (OT) has effectively erased the traditional "air gap" that once protected building infrastructure, introducing severe cybersecurity challenges.

Operational Technology Cybersecurity: Protecting the Physical-Digital Realm

As buildings become smarter, the surface area for cyberattacks expands exponentially. The physical infrastructure of a building (elevators, fire safety, HVAC, access control) is managed by Operational Technology (OT). Because these OT systems are now tethered to IT networks to enable IoT features, cybercriminals have realized that hacking a smart thermostat can be the backdoor into an entire corporate network—or a way to hold a physical building for ransom. Unlike traditional IT attacks that target data (theft of credit cards or emails), BMS attacks target physical outcomes. A compromised BMS can be used to shut down hospital ventilation, overheat data centers, or unlock high-security doors.

Here are the common attack vectors

- The "Front Door" (Exposed Ports): Many BMS controllers are directly connected to the internet for "remote maintenance" without a VPN. This allows attackers to access the entire network.
- Protocol Exploitation: Older protocols like BACnet and Modbus were designed for reliability, not security. They often lack encryption, meaning an attacker on the network can send a "False Command" to a chiller to shut down, and the chiller will obey without question.
- Lateral Movement: Attackers often enter through a "weak" device—like a smart coffee machine or a connected lighting sensor—and move across the network until they reach the Supervisory Level (the server that controls the whole building).
- The Contractor "Sneakernet": Up to 27% of OT incidents originate from contractor laptops or USB drives used to update firmware on-site, bypassing the building's firewall entirely.
- Default Passwords: Almost 90% of OT devices run on default factory passwords. This makes it easy for attackers to bypass the security and access the network remotely.



Implementing Best Practices

Implementing cybersecurity for Building Management Systems (BMS) in 2026 requires a shift from "perimeters" to "resilience." Because BMS controls physical assets (life safety, HVAC, power), the goal is to prevent a digital breach from becoming a physical disaster.

Here are the industry-standard best practices for OT cybersecurity in BMS, aligned with IEC 62443 and NIST 800-82.

1. Network Segmentation: The "Zones & Conduits" Model

The most effective way to stop an attacker is to ensure they cannot move laterally from a compromised lighting sensor to the main electrical switchgear.

- **Establish a DMZ:** Create a "Demilitarized Zone" (DMZ) between the corporate IT network and the BMS OT network. No direct traffic should ever pass between them.
- **Micro-segmentation:** Break the BMS into functional zones (e.g., HVAC Zone, Elevator Zone, Fire & Life Safety Zone). If the HVAC system is breached, the Fire system remains isolated and functional.
- **Protocol Filtering:** Use industrial firewalls that are "BMS-aware." They should inspect traffic to ensure only valid BACnet, Modbus, or LonTalk commands are being sent between zones.

2. Implementation of Zero Trust Architecture (ZTA)

In a Zero Trust environment, "being inside the building" does not mean "being trusted."

- **Always Verify:** Every device—from a high-end server to a simple CO₂ sensor—must authenticate its identity before communicating.
- **Least Privilege Access:** Technicians should only have access to the specific subsystems they are servicing. If a contractor is hired to fix the chillers, their credentials should not allow them to access the security camera feed.
- **Just-in-Time (JIT) Access:** Grant temporary, time-bound access for maintenance. Once the work order is closed, the digital "key" automatically expires.

3. Comprehensive Asset Visibility & Monitoring

You cannot protect what you cannot see. In 2026, "Asset Coverage" is a primary board-level metric.

- **Live Asset Inventory:** Maintain an automated, real-time list of every controller, gateway, and IoT device, including their firmware versions and physical locations.
- **Anomaly Detection:** Use OT-specific monitoring tools that baseline "normal" building behavior. If a boiler controller suddenly starts communicating with an external IP in another country, the system should trigger an immediate alert.

- **Physical Security Integration:** Ensure your cybersecurity logs are correlated with physical access logs. If a server rack is opened physically, the digital monitoring system should flag it.

4. Supply Chain & Lifecycle Management

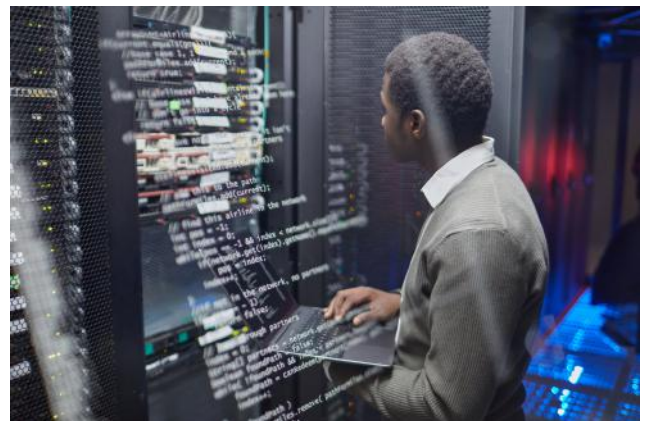
The software running your building often comes from dozens of different third-party vendors.

- **Demand an SBOM:** Require a Software Bill of Materials for every BMS component. This allows you to quickly identify if your building is vulnerable when a new global software flaw (like a future Log4j) is discovered.
- **Secure Remote Access (SRA):** Eliminate traditional VPNs for vendors. Use SRA solutions that provide granular, recorded sessions so you can see exactly what a remote technician changed in the system code.
- **Firmware Hygiene:** Establish a rigorous patch management cycle. Test patches in a "sandbox" or on a non-critical controller before deploying them to the entire building.

5. Governance and Incident Response

Cybersecurity is as much about people as it is about technology.

- **OT-Specific Incident Response (IR):** A standard IT IR plan (which usually involves "shutting everything down") can be dangerous for a building. Your BMS IR plan must prioritize operational continuity—keeping the lights on and the air flowing while isolating the threat.
- **Regular Tabletop Exercises:** Run simulated "Cyber-Fire Drills" involving both IT security teams and the physical facility managers.
- **Golden Backups:** Maintain offline, encrypted backups of all PLC and controller configurations. In the event of a ransomware attack on the building, you must be able to "wipe and restore" the physical hardware quickly.
- **Password Changes:** Change all the default factory password of hardware and software. Avoid using common guessable passwords. Frame a password change policy after 3 months, etc.



Striking the Balance: The Future of Smart Buildings

The BMS landscape of 2026 represents a delicate balancing act. On one hand, advanced IoT and AI integrations are unlocking unprecedented levels of sustainability, operational efficiency, and occupant comfort. On the other hand, the stakes for securing these systems have never been higher.

The most successful commercial real estate owners and facility operators are those who stop treating physical building management and digital cybersecurity as separate disciplines. By adopting "cyber-physical resilience"—where IoT innovation is deployed hand-in-hand with zero-trust OT security—organizations can build facilities that are not only extraordinarily smart but also fundamentally secure.

"The "Golden Rule" of BMS Security: In Operational Technology, Availability and Integrity are more important than Confidentiality. It is better for an attacker to see the room temperature (Confidentiality) than to be able to change it to 50°C (Integrity) or shut off the cooling entirely (Availability)."



AUTHOR: ABHASH SHAH

DESIGNATION: BUSINESS LEADER &
TECHNOLOGY-DRIVEN INFRASTRUCTURE

PROFESSIONAL
ORGANIZATION: FORESTLINC



INBAC[®]
Building Connectivity

JWCC, MUMBAI
NOV 19-21, 2026

BAC E&C
BUILDING AUTOMATION COMMUNITY
EXPO & CONNECT-CONVENTION

6TH EDITION

BAC E&C 2026

BUILDING AUTOMATION COMMUNITY EXPO & CONNECT-CONVENTION

19 - 21 NOVEMBER 2026

VENUE

Jio World Convention Center (JWCC) BKC
Bandra East Mumbai, INDIA



IBMS Transitioning to an IP-Based Solution: The Future is Connected

S. Manikandan, Lead CRN



IBMS TRANSITIONING TO AN IP-BASED SOLUTION: THE FUTURE IS CONNECTED

SMART BUILDINGS & INFRASTRUCTURE - TECHNOLOGY REVIEW

Walk through a hospital building in the 1990s and you'll find—if you look hard enough—a maze of parallel worlds running side by side, a dedicated cable run for HVAC, a separate one for fire alarms, another for access control, each governed by its own proprietary controller talking to nothing else on the floor. Nobody planned it that way. It just grew, system by system, vendor by vendor, over three decades. Today, trying to integrate even two of those subsystems is a project on its own. That experience, repeated across thousands of commercial towers, airports, campuses, and industrial plants worldwide, is exactly what's pushing the industry toward a fundamentally different approach to building management.

The shift toward IP-based Intelligent Building Management Systems (IBMS) is not, at its core, a networking story. It's an operational one. When Information Technology (IT) and Operational Technology (OT) share a single digital backbone, the building stops being a collection of independent subsystems and starts behaving like one coherent platform. That distinction matters because it changes what you can do, not just how the wiring looks. ASHRAE's 2023 guidance on high-performance building systems makes this case plainly: IP convergence is a long-term investment in interoperability, cybersecurity resilience, and operational efficiency that proprietary, siloed architectures simply cannot match.

For most of their history, building systems spoke in dialects nobody else understood. HVAC controllers used one protocol for fire alarm panels, CCTV systems, and other systems, each with its own cabling, its own commissioning process, and critically, its own vendor, whose continued involvement was essentially mandatory.

Kastner et al. (2005) catalogued this fragmentation in detail, noting that proprietary communication stacks were the norm and cross-manufacturer integration was largely aspirational. The arrival of Ethernet and IP networking changed the equation. A single structured cabling plant can now carry HVAC data, access control events, energy meter readings, and video streams simultaneously, and systems from different manufacturers can actually talk to each other without a custom middleware layer sitting in between.

Two open standards sit at the centre of this shift: BACnet/IP and Modbus TCP/IP. BACnet/IP, codified under ASHRAE 135, has quietly become the dominant language of building automation over the past two decades. What made it stick was not just technical merit — the ability to carry HVAC, lighting, fire safety, and security traffic over standard Ethernet and Wi-Fi using UDP/IP is genuinely useful — but more so the fact that ASHRAE actively maintained it and major manufacturers got behind it.

Compared to BACnet MS/TP, which ran over twisted-pair serial links at modest baud rates, the IP variant is faster, easier to reach remotely, and scales to enterprise-class deployments without specialist hardware.



Modbus TCP/IP fills a parallel role in industrial and commercial settings. It takes the classic Modbus protocol, which has been around since 1979 and still deeply embedded

in industrial equipment everywhere, and runs it over standard TCP/IP transport. That means PLCs, sensors, HMIs, and industrial controllers that facilities managers have relied on for years can now participate in a modern IBMS without being replaced outright (Modbus Organization, 2012). For sites carrying legacy equipment, that compatibility is not a minor convenience; it's often what makes the migration financially viable.



Procurement decisions look quite different once you move away from proprietary ecosystems. When HVAC controllers, lighting systems, and energy meters all speak open standards, you are no longer obligated to go back to the original vendor every time you need to expand or upgrade a system. Facilities teams can evaluate products on merit performance, price, and support quality rather than compatibility.

That flexibility compounds over a building's lifetime in ways that are hard to quantify upfront but very apparent over time. Installation is simpler too: a single structured cabling plant carries everything, and technologies like Power over Ethernet (PoE) mean a single cable can deliver both data and electrical power to a device, cutting installation time and reducing infrastructure costs (IEEE, 2018).

Cybersecurity deserves a direct mention here, because it is one of the genuine weak points that critics of IP convergence have raised and not without reason. Putting building automation onto an IP network does increase the attack surface. The answer the industry has arrived at is BACnet Secure Connect (BACnet/SC), introduced by ASHRAE in 2019, which layers TLS encryption and certificate-based authentication onto BACnet/IP communications. It brings building automation networks into rough alignment with the security posture that enterprise IT teams already expect. That does not make the problem disappear, but it gives facilities managers and IT security teams a common framework to work within.

The practical consequence of all this is that it is now realistic not just theoretical to run Fire Alarm Systems, CCTV, access control, emergency evacuation, public address, IP telephony, and energy management on a single shared IP infrastructure.

That is a genuinely different situation from even ten years ago. And because these systems are now on the same network, interactions between them become programmable rather than hardwired: a fire alarm event can automatically unlock emergency exits, trigger PA announcements, and send alerts to building management, without any of that being custom-engineered for the specific site.

Looking further ahead, cloud connectivity and edge processing are extending this further still predictive maintenance based on real operational data, centralised monitoring across multiple buildings, and local processing that keeps critical functions running even when the wide-area network goes down.

The direction of travel is not really in dispute anymore. New builds in most markets are specifying IP-based building management from the outset, and even retrofit projects, where the economics are harder, are increasingly finding that the cost of maintaining legacy proprietary systems over time outweighs the disruption of migration.

BACnet/IP and Modbus TCP/IP have moved from being niche choices to baseline expectations. The question facing most facilities teams today is not whether to move to IP-based IBMS, but how to manage the transition without compromising operational continuity in the process.

“Buildings that work well do not announce themselves. They just run reliably, efficiently, and without the operational headaches that come from systems that refuse to talk to each other.”



AUTHOR: S. R. MANIKANDAN
DESIGNATION: LEAD CRN, MEP CONSULTANT
ORGANIZATION: C R NARAYAN RAO



DATA CONTEXTUALIZATION FOR BUILDING - BMS OR ASSOCIATED SYSTEMS

Trigger/Objective - In today's world everyone is talking about leveraging digital technology, use of AI, Gen AI into a day-to-day business.

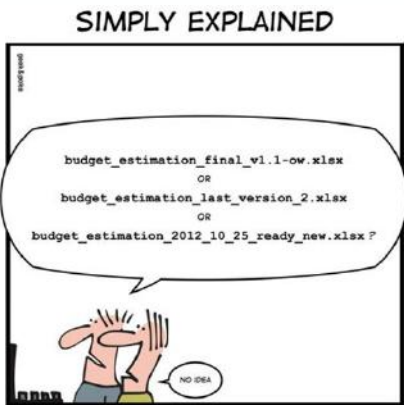
But **data inconsistency** is the **biggest blocker** to speed, quality, and global scale.

Standardized and Consistent **Nomenclature**: key requirement to uniquely identify assets/ data in digital systems to allow correct contextualization, interpretation, and operation.

We should be able to identify every data point uniquely from every Building system e.g., Building Management Solution(BMS), Access Control, CCTV, Fire alarm, networking, other building systems.

Imagine running an office where every employee saves files with random names...

- No one finds anything.
- Work slows down.
- Automation is impossible



Buildings work the same way, however,

- Every building, vendor and system uses different names for the same asset (e.g., AHU1 vs. AHU-01 vs. AirHandler-East)....difficult to analyse/ identify
- This causes confusion, delays, errors in operations and troubleshooting.
- Difficult to run analytics, rule engines, or AI/ML



Key Problem Statements due to unavailability of Naming Convention:

- Ambiguity & Duplication—Multiple teams may use different names for the same asset, causing confusion.
- Data Management Issues—Unstructured naming hinders integration with IT, monitoring, and asset management systems.
- Scalability Constraints—Lack of a systematic approach makes it difficult to expand and organize new utilities efficiently.
- Maintenance & Emergency Delays—Unclear identification slows down troubleshooting and response times.
- Compliance & Standardization Gaps—Inconsistent naming may lead to regulatory and reporting challenges.



Also, Naming Convention influence Driving Digitalization and AI/ML in various assets of the building:

A well-structured naming convention is foundational for successfully implementing digitalization, AI, and machine learning (ML) in Asset/utility management. Here's why we should have naming convention to drive digitalization journey:

Data Consistency & Standardization:

- AI/ML models require clean, structured, and standardized data to generate meaningful insights.
- Identify the data point uniquely from any building IT systems.
- A uniform naming convention ensures consistent data labeling, reducing errors in data processing.

Improved Data Integration & Interoperability

- Utilities often operate across IoT sensors, SCADA, BMS, digital twins, and cloud platforms.
- A standardized naming system enables seamless integration across AI/ML tools, predictive analytics, and automation platforms.

Enhanced Searchability & Data Retrieval

- AI and automation depend on fast and accurate data access.
- A structured naming system makes it easier for AI models to query, analyze, and categorize utility assets effectively.

Scalability for AI/ML Models

- A scalable naming convention allows for efficient expansion of AI-driven utility monitoring.
- Ensures that new assets, sensors, and digital records can be added without disrupting existing AI workflows.
-

Reliable Predictive Maintenance & Fault Detection

- AI/ML models for anomaly detection, predictive maintenance, and fault diagnosis need well-structured data.
- A standardized naming convention ensures that historical data aligns with real-time sensor inputs, improving model accuracy.

Compliance & Regulatory Alignment

- AI-driven asset/ utility management requires accurate reporting for system uptime, sustainability, energy efficiency, asset management and compliance audits.
- A clear naming structure ensures traceability and regulatory adherence.

Without a well-defined naming convention, AI/ML applications in asset/ utility management face data inconsistencies, integration challenges, and reduced accuracy. A standardized approach ensures better automation, predictive insights, and digital transformation success.

Way forward:

To develop a structured, scalable, and standardized naming convention that enhances asset/ utility management, ensures seamless integration across platforms, and improves operational efficiency.

Definition of Data contextualization (Naming Convention)

A naming convention for assets and utilities in real estate buildings is a structured and standardized system for assigning unique and consistent names to various infrastructure components. This convention ensures clarity, organization, and interoperability across facility management, digital systems, and automation platforms.

Uniqueness – Each asset or utility should have a distinct identifier to avoid duplication.

Hierarchy & Categorization – Names should reflect the type, location, function, and system (e.g., HVAC, electrical, networking, fire and security).

Scalability – The system should support future expansion as buildings and infrastructure evolve.

Integration with Digital Systems – Names should align with BMS, IoT sensors, AI/ML models, and digital twins for seamless automation and analytics.

Compliance & Standardization – Naming should align with industry standards (e.g., ISO 55000 for asset management, IFC for BIM).

Example Naming Structure: [Country code], [Location Code], [Building Code], [Floor code], [Room code], [Asset Type & No], [Abbreviation for sensor data point], [Free text if needed].

Spatial Info... + Building Info...	Country	Location code	Building code/ ID	Floor	Room
	A. Asset		B. Sensor		C. Free Text
	AST		SRN		FRT

Note: In certain cases, system-specific constraints—such as character limits—may restrict the inclusion of all required information within a single field. However, by leveraging additional available fields or implementing an appropriate hierarchical (tree) structure, the intended objective can still be effectively achieved.



Conclusion:

Standardized data contextualization (nomenclature) is not merely a documentation exercise—it is the foundational layer for digital transformation in buildings.

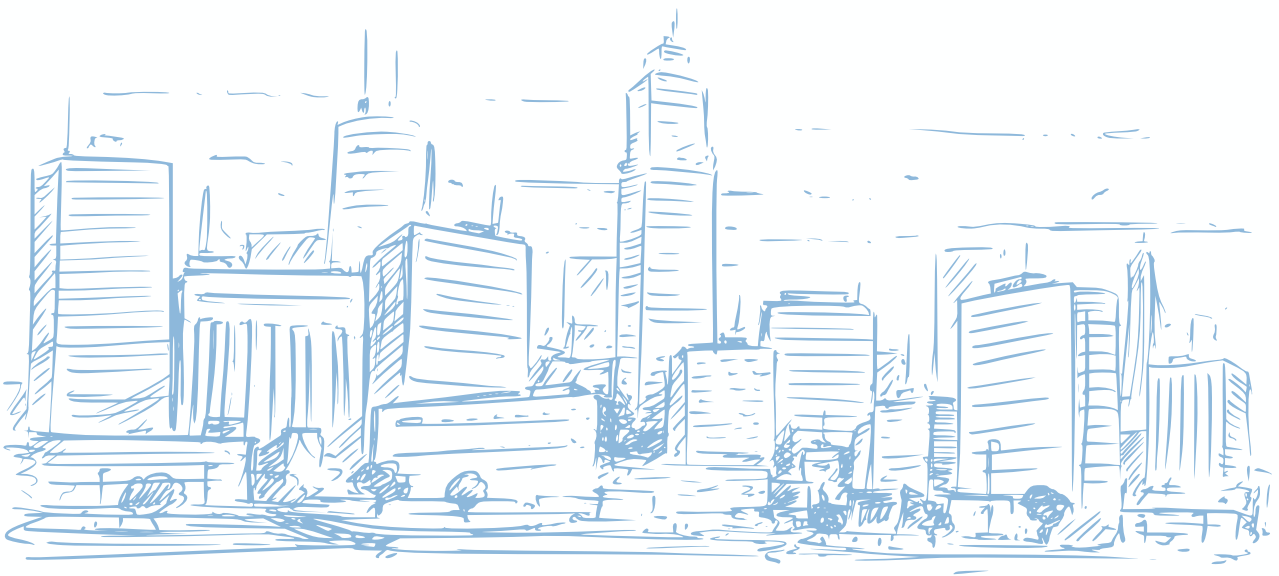
Without structured and consistent naming, automation remains fragmented, analytics remain limited, and AI-driven operations remain aspirational.

By institutionalizing a unified naming framework across all building systems, we establish a scalable backbone for interoperability, data intelligence, and autonomous control. This initiative directly enhances operational efficiency, improves asset transparency, reduces risk, and accelerates innovation.

In essence, nomenclature is the first step toward transforming conventional buildings into intelligent, self-optimizing assets.



AUTHOR: MR.HIREN BANKER
DESIGNATION: HEAD OF OPERATION:
GLOBAL COMMAND CENTRE / REMOTE
DATA ANALYSIS
ORGANIZATION: SIEMENS (REAL ESTATE).





INDIA'S ONLY EXHIBITION REDEFINING THE **FUTURE OF WORKSPACES**

**19-20-21
NOV 2026**

JIO WORLD CONVENTION
CENTRE, MUMBAI



**2025
Highlights**

9,417
Visitors

101
Exhibitors

18
Country
Representations

10,000
sqm Exhibition
Space

100
Speakers &
Thought Leaders

Join us in shaping the future of workspaces. Get in touch:

For Sales & Sponsorship

Manoj Nandiot
M: +91 98339 31376
E: m.nandiot@koelnmesse-india.com

For Marketing & Alliances

Akshata Ayare
M: +91 80971 26313
a.ayare@koelnmesse-india.com

Stay Connected: www.orgatec-india.com

koelnmesse



REWIRING THE FUTURE: A NEW APPROACH TO OPEN BUILDING AUTOMATION

Rethinking Openness in Building Automation Systems

Is Any BAS Truly “Open”?

For decades, the building automation industry has been obsessed with the promise of the “open” system. Today, nearly every major BAS/BMS platform claims to be open, interoperable, and future-ready. But talk to any building owner or facility manager, and they’ll tell you a different story: the reality rarely lives up to the marketing.

The bottleneck is no longer communication. Most modern systems can talk to each other just fine. The real issue is control. True openness isn’t just about protocol compatibility; it’s about engineering freedom, long-term flexibility, and finally breaking free from proprietary vendor lock-in.

Communication vs. True Openness

Today, almost every BAS platform supports standard protocols like BACnet, Modbus, and MQTT. Because of this, getting HVAC, lighting, and fire systems to talk to each other is easier than it’s ever been.

But just because a system can share data doesn’t mean it’s actually open.

The industry constantly confuses communication with control. There is a massive difference between a system that can speak a common language and one that gives you the freedom to engineer, modify, and manage it yourself.

The Missing Piece: Universal Engineering Standards

The biggest hurdle to a truly open system is that every manufacturer still builds and programs their controllers differently. Unlike the IT world, which runs on standardized environments and open APIs, the building automation industry is a mess of different software tools, licensing models, and proprietary workflows.

This means that even if your systems share data perfectly, you are still handcuffed to the vendor at the controller level. You might successfully pull all your equipment into one beautiful dashboard, but the moment you need to change a sequence, upgrade a controller, or commission a new unit, you still have to call the original vendor.

Integration Platforms: The Closest Step Toward Openness

Over the last ten years, integration platforms have brought us closer than ever to an open architecture. Modern software can pull HVAC, lighting, security, and IoT data into a single screen for centralized alarms, trends, and reports.

Operationally, this is a massive win.

The catch is that these platforms only scrape the surface. They live at the supervisory layer. Underneath that pretty interface, the actual logic running inside the field controllers remains locked away inside the manufacturer’s software.

In short: your data is open, but your control is still trapped.

The Business Reality Behind Proprietary Systems

This isn’t just a technical debate—it’s a financial one.

For decades, BAS manufacturers have built their entire business models around proprietary software, licensing fees, and long-term service contracts. But for building owners, this setup usually means expensive vendor lock-in and zero flexibility when it comes time to upgrade or make changes.





Because of this, the industry is stuck in a constant tug-of-war between two competing priorities: giving owners the openness and freedom they want, versus maintaining the security and control that manufacturers claim they need.

Conclusion

The BAS industry has come a long way with compatibility, but 'open' is still a relative term, not a reality.

Right now, systems are great at sharing data and connecting at the top level, but they still lock you down when it comes to programming the actual controllers. A truly open BAS would mean any technician could program any controller using standard, readily available tools—without vendor restrictions or hidden licensing fees.

Until we get there, a completely open system is more of a marketing pitch than a practical reality.

The future of smart buildings isn't about wiping out proprietary tech entirely. It's about finding a fair balance—one where security and stability don't come at the expense of an owner's freedom.



AUTHOR: MR.MADHURENDER SINGH
DESIGNATION: BUILDING & ENERGY
MANAGEMENT SYSTEM EXPERT.
ORGANIZATION:MITSUBISHI ELECTRIC INDIA
PRIVATE LIMITED



INBAC LEADING THE WAY IN INDIA'S SMART BUILDING REVOLUTION

A recap of milestones at the Smart Home Expo and MEP Conclave 2026

The year 2026 has been a milestone chapter for the INBAC Association. As the collective voice of India's smart building sector, INBAC stepped into the spotlight at two of the country's most essential industry gatherings: the 7th Smart Home Expo 2026 in Mumbai and the 9th MEP Conclave 2026 in New Delhi. These events gave INBAC an excellent platform to share knowledge, advocate for new industry standards, and push forward the future of automation across India.

Instead of just participating from the sidelines, INBAC brought a diverse, highly energized delegation of senior professionals, technical experts, regional chapter leads, and talented young practitioners. This strong presence highlighted INBAC's role as India's leading hub for smart building professionals, driving deep conversations on how to better integrate automation with traditional building services.

"INBAC continues to serve as the vital bridge between real-world industry innovation and professional standards. Our active presence at leading national platforms like the Smart Home Expo and the MEP Conclave is a true testament to our mission—and reflects the incredible commitment of our members."

— INBAC Leadership

The 7th Smart Home Expo—Mumbai

Jio World Convention Centre, Mumbai | April 28–30, 2026

The 7th edition of the Smart Home Expo returned to Mumbai's iconic Jio World Convention Centre (JWCC) in Bandra Kurla Complex.

Known as one of Asia's largest tech exhibitions for smart homes, this year's massive event drew over 14,000 trade visitors and showcased more than 450 leading Indian and international brands across a sprawling 15,000 square metres.

INBAC made a powerful statement by sending a dedicated delegation for all three days of the expo. Instead of just walking the floor, they jumped right into the action—collaborating with tech vendors, speaking at Tech Talks, and hosting roundtables to emphasize the value of unified technology standards with key players across the construction and tech sectors.

The delegation was led by Mrs. Sakhee Chandrayan, a highly respected leader in India's smart building field. Mrs. Chandrayan was instrumental throughout the expo, meeting with technology vendors and fellow industry leaders to pitch INBAC's clear vision: a future built on fully integrated, standards-driven smart home ecosystems.

"The Smart Home Expo gave us a direct window into exactly where this industry is heading. At INBAC, our job is to make sure this rapid progress is built on a solid foundation of robust standards, highly skilled professionals, and true system interoperability."

— Mrs. Sakhee Chandrayan, INBAC Founder & President

INBAC also used the expo's momentum to preview three exciting upcoming initiatives tailored specifically for India's growing real estate and construction sectors:

- A new Vital certification programme designed to validate and level up professional skills.
- A comprehensive model specification guide to streamline complex Integrated Building Management Systems (IBMS) projects.
- A brand-new Smart Building Rating Framework, built ground-up to evaluate modern Indian infrastructure.

The 9th Edition MEP Conclave — New Delhi

Hyatt Centric, New Delhi | May 19, 2026

Shortly after the Mumbai expo, INBAC travelled north for the 9th Edition of the MEP Conclave, organized by Convolign Media at the Hyatt Centric in New Delhi. This elite, one-day event is widely recognized as India's top knowledge and networking hub for the Mechanical, Electrical, and Plumbing (MEP) industries. It gathered an elite crowd of MEP consultants, contractors, HVAC experts, plumbing engineers, project managers, BIM specialists, and real estate developers all under one roof for serious technical discussions.

Mrs. Sakhee Chandrayan was once again leading the charge for INBAC in Delhi. She took center stage during an important panel discussion titled 'MEP Projects: Standards, Scope, and Integration Challenges.' Her insights struck a chord with the crowd of consultants and builders.

During the session, Mrs. Chandrayan made a strong case for creating clearer industry guidelines to define project scope within MEP contracts. She also strongly advocated for a uniform national standard for IBMS system commissioning—a critical cause that INBAC has actively championed for several years. Her clear, practical insights sparked great follow-up engagement and networking sessions with developers and consultants in the audience, closing out a highly successful season of national advocacy for the association.



AUTHOR: MEHUL JOSHI
DESIGNATION: EDITOR-IN-CHIEF,
INBAC BTB MAGAZINE





IGBC RATINGS AND THE FUTURE OF INTELLIGENT BUILDING MANAGEMENT SYSTEMS

How Intelligent Automation is Redefining Sustainable Building Operations

A decade ago, green buildings were primarily defined by energy-efficient lighting, water-saving fixtures, and sustainable construction materials. Today, however, the definition of sustainability has evolved far beyond construction practices alone.

Modern buildings are now evaluated not only by how efficiently they are designed—but by how intelligently they operate throughout their lifecycle.

This transformation has positioned Building Management Systems (BMS) as one of the most critical technologies driving sustainable infrastructure and IGBC-oriented developments.

Sustainability Is No Longer Only About Construction

Traditionally, green building discussions focused heavily on architectural design and material selection. While these elements remain important, operational efficiency has now become equally critical.

A building may use premium insulation, energy-efficient equipment, and advanced façade systems, but without proper operational monitoring and control, actual performance can gradually deviate from design expectations.

Sustainability today is not measured only by design intent — it is measured by actual building performance throughout the operational lifecycle.

The Growing Importance of BMS in IGBC-Oriented Projects

A modern Building Management System acts as the centralized operational platform of a facility. It enables monitoring, control, analytics, and optimization of multiple building services from a unified environment.

In IGBC-oriented projects, BMS platforms commonly integrate:

- HVAC systems
- Energy meters
- Lighting controls
- Water management systems
- Ventilation systems
- Indoor air quality monitoring
- Renewable energy integration

Advanced BMS infrastructures increasingly support open communication protocols such as BACnet, Modbus, and IoT-enabled integrations, allowing seamless interoperability between multiple building systems and smart devices.

From Energy Saving to Intelligent Efficiency

Modern BMS platforms are evolving into decision-support tools for facility management teams.

By converting raw building data into actionable insights, facility operators can make informed decisions related to:

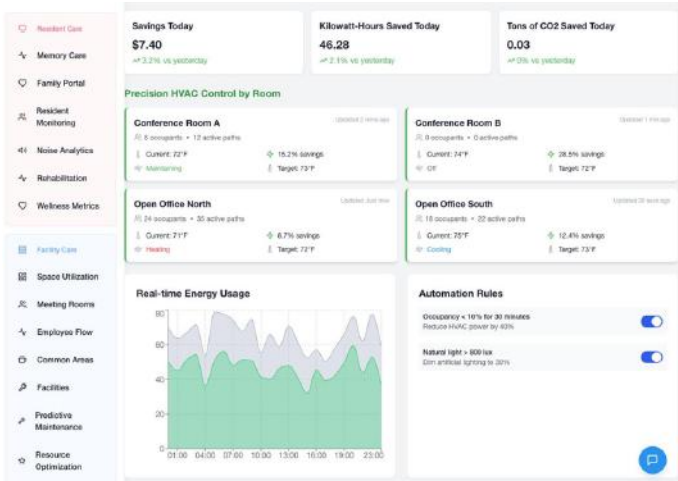
- Energy optimization
- Preventive maintenance
- Operational scheduling
- Tenant comfort
- Resource utilization

As many industry professionals now say:

“A sustainable building is not the one that consumes less energy only on paper—it is the one that continuously learns how to operate more efficiently.”

1. Smart Building Dashboard with Live Energy Analytics

•Real-time HVAC monitoring



•Real-time HVAC monitoring

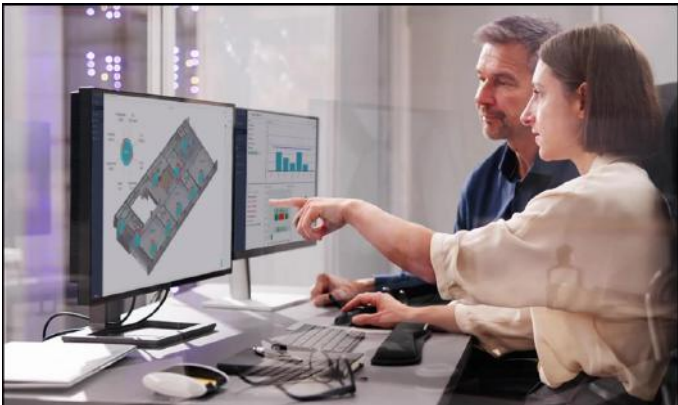


2. Modern Commercial IGBC Certified Building
Glass façade green buildings



3. BMS Control Room and Monitoring Screens

•Engineers monitoring systems



4. HVAC Automation and Intelligent Cooling Systems

- Chiller Plant manager



5. Green Infrastructure with IoT Integration

- IoT-connected buildings



The Future of Smart Buildings

The future of building automation is being shaped by next-generation technologies that are revolutionizing the way buildings operate and interact.

Conclusion

Building Management Systems are no longer just operational tools—they are the driving force behind intelligent, sustainable, and future-ready infrastructure.

By integrating automation, real-time analytics, energy optimization, and smart technologies, BMS empowers organizations to achieve operational excellence while enhancing sustainability and occupant experience.

As the world moves toward smart cities and digital infrastructure, building automation will continue to play a transformative role in shaping the future of modern living and intelligent engineering.



AUTHOR: MS.EKTA SHARMA
DESIGNATION: SALES DIRECTOR | CYBER
GROUP
ORGANIZATION: CYBER INFO ELECTRONIC
SECURITY SYSTEM PVT LTD





THE FUTURE OF INTELLIGENT TUNNEL & STATION AUTOMATION: SCADA SYSTEMS TRANSFORMING RAILWAY, METRO AND ROAD INFRASTRUCTURE

Modern transportation infrastructure is no longer limited to civil engineering and rolling stock alone. Today's railway tunnels, underground metro systems, elevated stations, and road tunnels depend heavily on intelligent automation platforms capable of ensuring operational continuity, passenger safety, energy optimization, and real-time centralized control. At the center of this transformation lies SCADA (Supervisory Control and Data Acquisition) technology integrated with high-availability PLC systems, redundant communication networks, and advanced third-party subsystem integration.

As India accelerates infrastructure development through mega projects such as Himalayan railway tunnels, metro corridors, elevated rapid transit systems, and smart road tunnels, the role of integrated SCADA architecture has become mission-critical.

SCADA in Railway Tunnel Automation

Railway tunnels are among the most complex infrastructure assets from an operational and safety perspective. Unlike conventional railway stations, tunnels operate in confined environments where smoke management, ventilation, drainage, emergency response, and power reliability directly impact passenger safety.

Modern Tunnel SCADA systems are designed to centrally monitor and control:

- Tunnel ventilation systems
- Jet fans and axial fans
- Fire detection and suppression systems
- Tunnel lighting
- Drainage and sump pumps
- HT/LT electrical distribution
- Environmental monitoring systems
- UPS and DG systems
- Emergency evacuation systems

In long railway tunnels, particularly those crossing mountainous regions, multiple Tunnel Control Centers (TCCs) are deployed locally, while a centralized Main Tunnel Control Center (MTCC) supervises the entire route through redundant optical fiber communication networks. A high-availability SCADA architecture with redundant PLCs, redundant historians, and dual communication networks ensures that tunnel operations continue even during communication or hardware failures. In critical transportation infrastructure, single point failures are unacceptable.



Road Tunnel SCADA: Safety-Centric Intelligent Automation

Road tunnel automation differs significantly from railway applications due to continuous vehicular movement, variable pollution levels, and dynamic traffic conditions.

Road Tunnel SCADA systems focus heavily on:

- Carbon monoxide (CO) monitoring
- Nitrogen oxide (NOx) monitoring
- Visibility measurement systems
- Traffic control systems
- Emergency telephones
- CCTV integration
- Variable message signs (VMS)
- Fire & smoke extraction systems

The SCADA platform continuously processes environmental sensor data and dynamically controls ventilation systems based on traffic density and air quality conditions.

Advanced PLC logic algorithms are used to determine:

- Fan operation sequences
- Smoke extraction zones
- Tunnel pressurization strategies
- Emergency evacuation modes

In emergency scenarios such as fire incidents, the automation system executes predefined cause-and-effect matrices within milliseconds, enabling coordinated operation of ventilation systems, dampers, alarms, and emergency lighting.



Metro Tunnel SCADA and Underground Station Automation

Underground metro systems present an even more sophisticated automation challenge due to high passenger density, interconnected subsystems, and stringent operational requirements.

Modern Metro SCADA systems typically integrate:

- Environmental Control Systems (ECS)
- Tunnel Ventilation Systems (TVS)
- Station ventilation and air conditioning
- Fire alarm systems
- Lift and escalator systems
- Electrical SCADA
- Platform screen doors
- Water management systems
- Tunnel lighting systems

The SCADA architecture for metro projects is usually based on distributed PLC systems connected over redundant industrial Ethernet networks using PRP, MRP, or ring topologies.

One of the most critical engineering aspects is the implementation of complex PLC logic for emergency ventilation and fire management.

For example, during a fire event inside an underground station or tunnel section, the PLC must instantly:

- Identify the fire zone
- Activate smoke extraction fans
- Pressurize escape routes
- Shut down non-essential ventilation
- Coordinate with fire alarm systems
- Trigger evacuation sequences
- Interface with OCC (Operation Control Center)

These operations require deterministic, fail-safe, and SIL-rated control architectures.



Elevated Station SCADA: Distributed Automation for Modern Urban Transit

While elevated stations may appear operationally simpler than underground systems, they involve extensive integration of distributed electrical and mechanical systems.

Elevated station SCADA systems typically monitor and control:

- HVAC systems
- Electrical panels
- UPS systems
- DG systems
- Lighting systems
- Lift and escalator controls
- Fire alarm systems
- Water pumping systems
- Energy monitoring systems

These operations require deterministic, fail-safe, and SIL-rated control architectures.

With the growing emphasis on energy efficiency and centralized operation, many metro operators now prefer integrated SCADA platforms capable of real-time analytics and predictive maintenance.

A modern elevated station may include hundreds of data points originating from different OEM devices and communication protocols. Therefore, interoperability and third-party integration capability have become essential selection criteria for SCADA systems.

Third-Party Integration: The Real Engineering Challenge

One of the most underestimated yet technically demanding aspects of infrastructure SCADA projects is third-party device integration.

A typical railway or metro SCADA system may need to integrate with:

- Fire Alarm Systems (FAS)
- Building Management Systems (BMS)
- Public Address Systems (PAS)
- CCTV systems
- Energy meters
- Variable Frequency Drives (VFDs)
- Intelligent Electronic Devices (IEDs)
- Weather monitoring systems

These devices often use different communication protocols such as:

- Modbus TCP/IP
- Modbus RTU
- BACnet
- OPC UA
- IEC 61850
- SNMP

Developing stable and cybersecure communication interfaces among multiple OEM systems requires deep engineering expertise in industrial networking, protocol mapping, and data synchronization.

In many cases, the success of a SCADA project depends more on integration engineering than on the SCADA software itself.



Redundancy and High Availability: Mandatory for Critical Infrastructure

Modern tunnel and metro SCADA systems are increasingly adopting:

- Redundant PLC architectures
- Dual redundant communication networks
- PRP-enabled Ethernet systems
- Redundant historians
- Redundant SCADA servers
- Dual power supply systems



The objective is simple: No single hardware or communication failure should interrupt tunnel or station operation.

This philosophy becomes especially important in long railway tunnels and underground metro systems where communication loss or ventilation failure can lead to severe operational and safety risks.

SCADA Redevelopment in Existing Railway and Metro Infrastructure

Across India and globally, many railway stations and metro facilities still operate on aging PLC and SCADA systems installed more than a decade ago.

These systems often face:

- Obsolete hardware
- Unsupported communication protocols
- Limited cybersecurity
- Non-redundant architectures
- Lack of remote diagnostics

SCADA redevelopment projects are now becoming increasingly common, where legacy systems are upgraded with:

- Modern Ethernet-based PLCs
- Redundant SCADA servers
- Virtualized infrastructure
- Advanced historians
- Cybersecurity-compliant architectures

Redevelopment projects are particularly challenging because migration must often occur without disrupting live operations.

Engineering teams must carefully manage:

- Database migration
- Signal mapping
- Interoperability with existing field devices
- Live cutover strategies
- Phased commissioning

The Road Ahead

The future of railway, metro, and tunnel automation will increasingly revolve around:

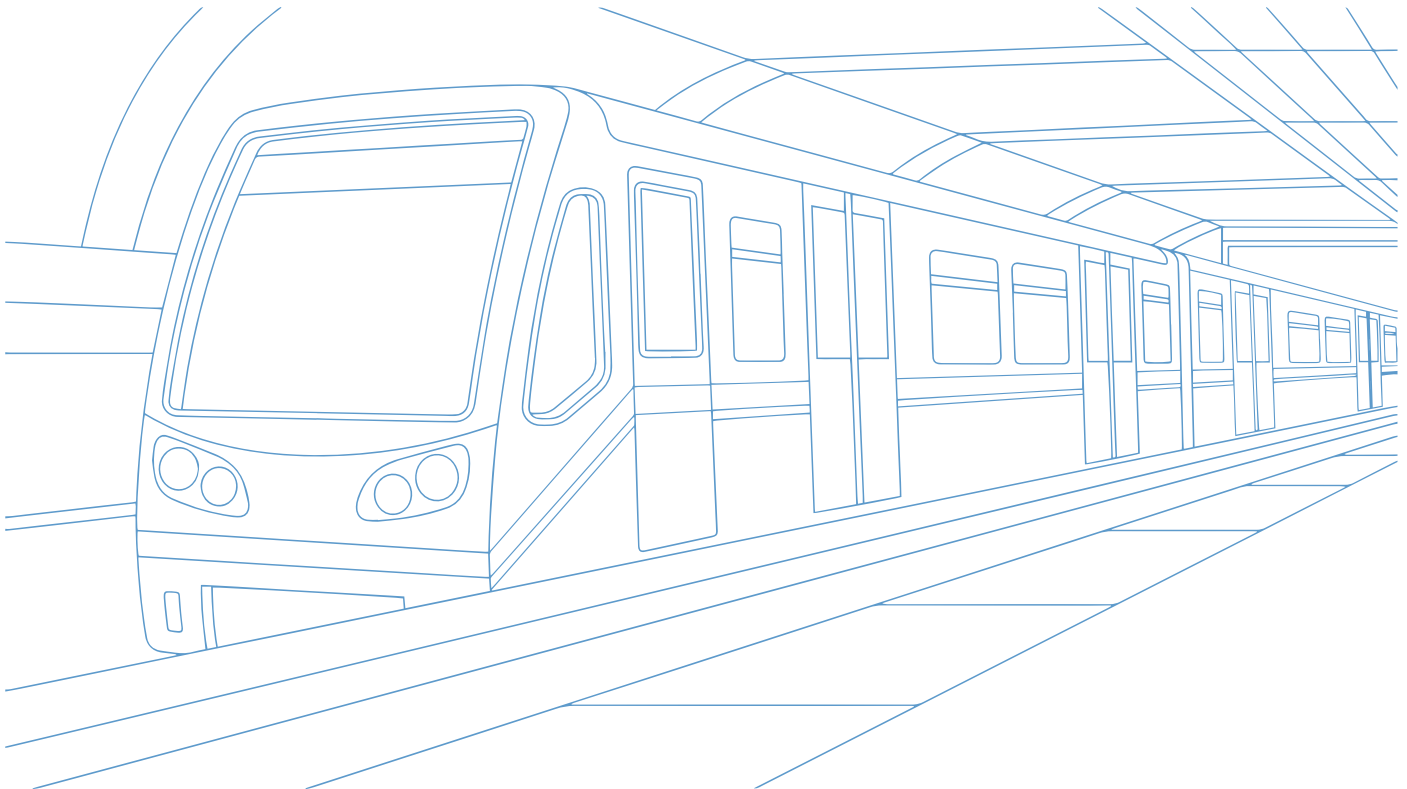
- Intelligent analytics
- AI-assisted diagnostics
- Predictive maintenance
- Digital twins
- Cybersecure industrial networks
- Cloud-enabled historians
- Edge computing architectures

However, the foundation of all intelligent infrastructure remains a robust SCADA and PLC architecture capable of delivering deterministic control, high availability, and seamless integration.

As transportation infrastructure becomes smarter and more interconnected, SCADA systems will continue evolving from simple monitoring tools into intelligent operational platforms driving safety, reliability, and efficiency across modern transit ecosystems.



AUTHOR: DHAIRYA DESAI
DESIGNATION: MANAGING DIRECTOR
ORGANIZATION: AD AUTOMATOS
TECHNOLOGIES PVT. LTD.



BUILDING TECHNOLOGY BIZBITS TEAM

Statutory Note

All content, including articles and images, published in this magazine is provided by individual contributors and remains their intellectual property. The publisher assumes no legal responsibility for any copyrighted material submitted. This publication is intended solely for educational and informational purposes, with no commercial objectives.



**Innovation and intelligence in every space -Team
BizBits at the heart of transformation.**

Write to us: editor@inbac.org