WHITEPAPER

Why Smart Water Metering Projects Fail in ASEAN

And How to Fix Them

A Practical Guide for Utilities, Governments, and Smart Infrastructure Leaders

Author	**Vincent Wong (Wong Yew Hon)**
Published	27th May 2026
Category	Smart Water Infrastructure / Utility Digitalization / AMI
Version	1.0 — First Edition

Executive Summary

Across ASEAN, utilities are under mounting pressure to reduce Non-Revenue Water (NRW), modernise aging infrastructure, improve billing accuracy, and deliver on national smart city mandates. Smart water metering — and the broader category of Advanced Metering Infrastructure (AMI) — has emerged as a centrepiece of that transformation agenda.

The investment case is compelling. Yet despite growing capital commitments across the region, a significant proportion of smart water metering deployments fail to achieve their intended outcomes. Some never scale beyond the pilot stage. Others produce unreliable data, suffer premature hardware failures, or become mired in integration disputes that were entirely predictable — and preventable.

The core problem is not the technology. While smart meter technologies have matured significantly, project outcomes often depend less on the device alone than on how the wider AMI ecosystem is designed and managed. In practice, failure most often originates from how projects are conceived, procured, planned, and executed. Common root causes include poor requirement definition, misaligned procurement decisions, inadequate network planning, unrealistic battery life assumptions, weak integration architecture, fragmented operational ownership, and a systematic underestimation of what it takes to run a large-scale digital infrastructure program.

This whitepaper examines eight categories of failure in depth, drawing on practical experience supporting AMI deployments across ASEAN — particularly in NB-IoT and sub-GHz RF environments — combined with broader regional industry observation. For each failure mode, concrete remediation strategies are provided. The analysis concludes with practical readiness questions that utilities can use to stress-test their own AMI programs before committing to mass rollout.

Key Finding

Multiple industry studies point to systemic underperformance in IoT deployments globally. Cisco's 2017 research found only 26% of IoT initiatives were completed successfully — a 74% failure or stall rate *(Cisco, 2017)*. Microsoft's IoT Signals report observed roughly 30% of projects fail at proof-of-concept stage, primarily due to high implementation costs or unclear business value *(Microsoft, 2022)*. An IDC study of industrial firms found 31% of IoT/IIoT projects yielded only minimal payback, failing to meet expected ROI *(IDC, 2022)*. In ASEAN, where environmental conditions are demanding and procurement models heavily cost-driven, the risk of underperformance is particularly acute for utilities that treat AMI as a hardware purchase rather than a long-term digital infrastructure program.

1. The ASEAN Smart Water Metering Opportunity

Southeast Asia presents one of the most compelling regional cases for smart water infrastructure investment. The Asian Development Bank reports that most Asian utilities average a 30% NRW loss, with some losing up to 65% of daily production (ADB, 2023). Country-level data underscores the scale of the problem: in 2018, NRW rates in Malaysia, Indonesia, and Vietnam stood at 36.5%, 32.75%, and 21.5% respectively, with individual Malaysian states reaching as high as 63.1% (Tan et al., 2023). These figures compare starkly against best-in-class benchmarks of approximately 10% achieved by leading utilities in Denmark, and 5.6% in Singapore (ADB, 2023; Liemberger & Wyatt, 2019). The gap represents both a significant financial liability and a powerful incentive for modernisation.

Rapid urbanisation is compressing infrastructure upgrade timelines while simultaneously expanding the scale of the challenge. Aging pipeline networks, increasing per-capita water demand, and growing citizen expectations for service quality are creating pressure from multiple directions simultaneously.

Manual meter reading, which remains the operational norm across much of the region, compounds these problems. It is labour-intensive, prone to error, slow to detect tampering or leakage, and increasingly difficult to sustain as field workforce availability tightens. Smart metering promises to address all of these pain points through remote reading, automated billing, real-time leak detection, consumption analytics, and exception-based field operations.

Yet while the value proposition is clear on paper, real-world deployment in ASEAN involves a set of physical and operational challenges that are substantially more demanding than those encountered in the European or North American markets where many AMI products were originally designed and tested. The region's tropical climate, dense high-rise urban environments, underground meter chambers, flood-prone installation sites, variable cellular coverage, multi-language operational contexts, and cost-sensitive procurement cultures all create conditions that require deliberate, localised deployment strategies — not imported assumptions.

The utilities most likely to succeed are not those with the largest budgets. They are those that invest the most care in planning, vendor governance, and operational readiness before the first meter is installed.

2. Failure #1 — Treating AMI as a Hardware Procurement Exercise

The single most common pattern observed in underperforming smart metering projects across ASEAN is a procurement strategy that evaluates the program primarily on device price. Requests for Proposal are structured around meter unit cost, communication module specifications, and battery rated life. Lowest-bid evaluations dominate. OPEX and lifecycle costs are either modelled superficially or ignored entirely.

This approach is understandable — procurement rules in many ASEAN utilities are designed to enforce cost discipline, and device cost is tangible and easy to compare. But it can produce a significant mismatch between what is purchased and what is actually needed. A smart water metering system is not a meter. It is an integrated digital infrastructure platform spanning devices, firmware, connectivity, Head-End-Systems (HES), Meter Data Management Systems (MDMS), APIs, analytics platforms, cybersecurity controls, and device lifecycle management processes. Optimising for CAPEX on one component while ignoring the rest of the system often produces higher total cost over a 10-year lifecycle.

Utilities that discover this late in the project often find that integration costs dwarf device costs, firmware customisation is contractually difficult, vendor lock-in prevents scalability, and data quality is inconsistent because no one defined quality standards at procurement time.

How to Fix It

Procurement frameworks may benefit from being redesigned to evaluate AMI as a digital transformation program, not a device purchase. This means defining measurable technical and operational KPIs before issuing any RFP, and embedding contractual enforcement mechanisms for those KPIs throughout the contract lifecycle.

KPI Category	Illustrative Requirements
Data Availability	Measurable targets for daily and monthly reading success rates, defined against the utility's operational requirements
Latency	Maximum acceptable delay from meter event to HES delivery, defined per alarm class
Firmware OTA	OTA campaign success rate target, with a defined completion window and exception-handling process
Battery	Defined life under specified RF conditions, reporting frequency, and temperature range, as agreed at procurement
Support SLA	Tiered fault response and resolution timelines, matched to operational severity classification
Scalability	System architecture must support the defined target population with open, documented APIs

The cheapest meter is rarely the lowest-cost system over ten years. In many deployments, procurement decisions made without lifecycle cost analysis produce higher long-run costs than initially anticipated.

3. Failure #2 — Unrealistic Battery Life Expectations

'10-year battery life' is one of the most consistently misunderstood specifications in the smart metering industry. Utilities across ASEAN regularly discover — only after pilot deployment — that real-world battery performance differs materially from the figures presented during vendor demonstrations or procurement evaluations.

This is not necessarily the result of deliberate misrepresentation. Battery life specifications are typically measured under idealised laboratory conditions: controlled temperature, strong signal quality, standard reporting frequency, and minimal retries. In ASEAN field deployments, almost none of these conditions reliably hold.

In NB-IoT deployments, battery consumption is heavily influenced by signal quality metrics including RSRP (Reference Signal Received Power) and SINR (Signal-to-Interference-plus-Noise Ratio), as well as network configuration parameters such as eDRX (Extended Discontinuous Reception) and PSM (Power Saving Mode) cycles. Research confirms that smart water devices are often located underground, where wide coverage is required and RSRP directly determines battery lifetime outcomes (Roosipuu et al., 2023). A 2026 experimental evaluation of NB-IoT power consumption found that signal strength and standby current variability have a major impact on battery life, with standby currents varying between devices from 6.7 μA to 23 μA — a range with compounding multi-year implications (Anttila et al., 2026). Field experience in ASEAN deployments is consistent with published research: devices operating in poor-signal underground environments consume substantially more energy than equivalent devices in good surface-level coverage, with high retry rates compounding this further (Lim et al., 2021).

Similarly, reporting frequency has a direct and non-linear relationship with battery consumption. A project that configures hourly uploads, frequent alarm transmissions, and aggressive diagnostic polling — without modelling the power trade-offs — may reduce expected battery life from ten years to three or four.

How to Fix It

Vendors may be asked to provide documented battery life simulation models that specify the RF conditions, reporting frequency, retry assumptions, and temperature ranges underlying any life estimate. In well-structured procurement, these assumptions form part of the performance specification rather than remaining as marketing footnotes.

Pilot programs may benefit from being designed to stress-test battery performance in the most challenging installation environments anticipated in the full deployment — underground chambers, basement plant rooms, high-rise riser ducts, and rural edge-coverage zones. A pilot conducted only in favourable surface-level conditions provides no meaningful battery life data for difficult deployment sites.

Practical Consideration: Evaluating Battery Life Assumptions

Utilities may benefit from understanding the operating assumptions underlying vendor battery life estimates, including reporting frequency, communication conditions, retry behaviour, and environmental factors.

4. Failure #3 — Poor Connectivity Planning

Connectivity is frequently treated as a secondary consideration — something to be confirmed after the core hardware decision has been made. In ASEAN deployments, this approach consistently produces communication instability, high retry rates, poor data availability, and battery drain that was never anticipated in the project budget.

Technology selection is particularly prone to trend-following rather than engineering analysis. Projects select LoRaWAN without planning for gateway infrastructure ownership, maintenance, and coverage validation. Projects select NB-IoT without verifying that operator coverage penetrates the underground and indoor environments where meters are actually installed. Projects assume that a single communication technology will serve all deployment zones — dense urban cores, residential high-rise estates, semi-rural service territories, and industrial areas — when in practice each environment may require a different architecture.

Coverage maps provided by mobile network operators are a particularly unreliable guide to real-world NB-IoT performance. Published maps reflect outdoor signal levels at ground level. They say nothing about penetration into underground meter chambers, sub-surface vaults, or the interior of reinforced concrete buildings — which is precisely where ASEAN water meters are most commonly installed.

How to Fix It

RF site surveys are worth treating as a formal pre-deployment activity, not an afterthought. Signal quality measurements are most useful when taken inside the actual meter installation environments — not estimated from outdoor coverage maps. Surveys may usefully record RSRP, SINR, and observed retry rates across a representative sample of installation conditions, including the worst-case sites that are easiest to ignore during planning.

Deployment zones may benefit from segmentation based on site survey findings, with communication architecture selected per zone. NB-IoT may be well-suited to urban areas with strong operator coverage. LoRaWAN with utility-owned gateways may be more appropriate for campus environments or areas with poor cellular penetration. Hybrid architectures are often the most operationally resilient approach in mixed-condition service territories.

Rather than specifying a communication technology in procurement documents, utilities may consider specifying measurable data delivery outcomes — for example, defined data delivery targets with agreed latency parameters — and allow vendors to demonstrate how their proposed connectivity architecture achieves those outcomes under realistic field conditions.

5. Failure #4 — Weak Integration Architecture

Experienced AMI practitioners will recognise a common project pattern: the device works. Data reaches the Head-End System. But nothing happens with it. Billing integration is incomplete or error-prone. Alarms are generated but never actioned. The MDMS receives data but cannot reconcile it against customer accounts. Field teams lack the mobile tools to act on the information the system is producing.

This pattern — technically successful device-to-network communication combined with operationally useless data — is the defining characteristic of a weak integration architecture. It is one of the most expensive failure modes because it is discovered late, after devices are installed, and remediation typically requires significant rework across multiple systems and vendor relationships.

Common causes include data model mismatches between systems (different timestamp formats, unit conventions, alarm structures, and meter identifier schemas), incomplete or poorly documented APIs, proprietary integration dependencies that create long-term vendor lock-in, and the absence of end-to-end testing that covers the full chain from physical meter to billing system to customer invoice.

How to Fix It

Integration architecture is most effectively designed and validated before mass deployment begins, rather than during it. A useful starting point is a formal integration blueprint that maps every data flow in the system: from meter to network to HES to MDMS to billing to customer portal to field mobile application. Each interface benefits from having a defined data model, documented API specification, and agreed error handling behaviour.

Utilities may find value in prioritising open APIs, standardised payload structures, and webhook support. REST-based integrations with published documentation are far easier to maintain, extend, and audit than proprietary integration layers built to a single vendor’s specification.

Pilot success is best defined not as “the meter is sending data” but as “the utility can operationally use the data end-to-end.” This means validating automated bill generation, alarm workflow execution, dispute resolution access, and field team tooling before any system is declared production-ready.

6. Failure #5 — No Clear Operational Ownership

Large AMI programs typically span multiple organisational functions: IT manages the software platforms; Operations manages meter installations and field teams; Procurement manages vendor relationships; Finance controls budget releases; and the mobile network operator manages connectivity. In many ASEAN utilities, no single function owns end-to-end system performance.

This fragmentation produces predictable outcomes. When data availability drops, IT blames the network operator, the network operator points to device configuration, and the device vendor attributes the issue to installation quality. Resolution timelines stretch from days to weeks. KPIs are ambiguous because no one entity is accountable for the full chain. Executive visibility is limited because there is no single performance dashboard and no defined escalation path.

The problem is compounded by the tendency to treat AMI governance as a project-phase activity that ends at commissioning. In reality, a deployed AMI system requires ongoing management — firmware update campaigns, data quality monitoring, device lifecycle tracking, alarm threshold tuning, and cybersecurity patch management — that demands dedicated operational ownership indefinitely.

How to Fix It

Many utilities find it valuable to establish a dedicated AMI operations function with clear accountability for system performance across its full technical scope: device health, connectivity performance, data quality, software platform availability, vendor SLA enforcement, and cybersecurity posture. This function would typically own a unified performance dashboard and have defined escalation authority across all vendor relationships.

Contracts that align SLA obligations across all vendor relationships — device vendors, connectivity providers, software vendors, and system integrators — tend to reduce ambiguity around accountability. When contractual interdependencies are explicit, finger-pointing between vendors becomes far less tenable.

7. Failure #6 — Pilots Are Managed. Scale Is Not.

AMI pilots in ASEAN consistently outperform subsequent mass deployments. This is not a paradox. Pilots succeed because they are managed with an intensity that cannot be sustained at scale: devices are manually monitored, deployment sites are hand-selected for favourable conditions, vendor support teams are on-site, and sample sizes are too small to reveal systemic weaknesses in network architecture or backend performance.

When the program scales from 200 meters to 10,000, the hidden problems become visible. Firmware update campaigns that were manageable manually become operationally unworkable without automated orchestration. Network congestion emerges as thousands of devices synchronise their upload schedules. Installation quality becomes inconsistent as field crews expand and training depth decreases. Alarm volumes grow beyond the capacity of operations teams to review and action manually.

This pattern is consistent with broader IoT research findings: Gartner identifies scalability failure as a primary cause of approximately 30% of IoT project failures — solutions that worked with dozens of devices cannot handle thousands (Gartner, 2023). Scaling failure is characteristically an operational and architectural problem, not a hardware problem. The meters that performed well in the pilot often perform identically in mass deployment — but the systems around them were never designed to handle the volume.

How to Fix It

Pilot programs may benefit from being deliberately designed to stress-test the conditions most likely to cause problems at scale. This means intentionally including difficult installation sites, weak coverage zones, diverse building types, and a large enough sample size to generate statistically meaningful performance data. A pilot of 200 devices in a utility's best-coverage area proves almost nothing about a deployment of 10,000.

Backend systems are worth load-testing against projected full-deployment volumes before mass rollout begins. This includes simulating mass simultaneous uploads, firmware update campaigns across large device populations, alarm spike scenarios, and graceful degradation under partial network outage conditions.

Operational processes — alarm triage workflows, device replacement procedures, data exception handling, maintenance scheduling — are best designed and documented during the pilot phase, not improvised during mass deployment.

8. Failure #7 — Neglecting Workforce and Organisational Readiness

Technology deployment without organisational transformation produces limited and often short-lived value. This is one of the most consistently underestimated dimensions of AMI project planning across ASEAN — and one of the most difficult to remediate after deployment has begun.

The most common manifestation is a utility that has deployed an advanced AMI system and continues to operate in the same way it did before. Field teams distrust automated readings and continue manual verification. Billing staff override system-generated bills because they lack confidence in the data. Data analytics capabilities go unused because no internal function has been trained to interpret or act on consumption insights. IT and Operations continue to operate as separate silos, each managing their portion of the system without coordinating on system-wide performance.

Data literacy is a particularly acute gap. Utilities may successfully configure their MDMS to receive hourly interval data from every meter in the network — and then find that no one in the organisation has the analytical capability to use that data for anything more sophisticated than replacing the manual bill read. The full value of AMI — predictive maintenance, demand forecasting, pressure zone optimisation, NRW attribution — remains unrealised.

How to Fix It

Workforce readiness investment is most effective when it begins during the planning phase, not after commissioning. This typically includes structured training in AMI operations, data analytics, connectivity troubleshooting, firmware management, cybersecurity awareness, and alarm management for relevant staff across IT, Operations, and Finance.

Business processes are often worth redesigning around the operational model that AMI enables — exception-based field dispatch, automated billing, remote tamper investigation, predictive maintenance scheduling — rather than adapting the new system to fit legacy manual workflows. The utility that digitalises its processes alongside its infrastructure consistently outperforms the utility that simply adds a new technology layer on top of unchanged ways of working.

9. Failure #8 — Underestimating Cybersecurity Risk

Cybersecurity is frequently treated as a compliance checkbox in ASEAN AMI procurement — a section in the RFP response that vendors tick without detailed scrutiny, and that utilities rarely have the internal capability to evaluate rigorously. This is changing, but not fast enough.

The risk profile of a large-scale smart metering network is substantially different from that of a conventional utility IT environment. Academic research on AMI security vulnerabilities identifies data breaches, unauthorised access, data manipulation, denial-of-service attacks, and malware introduction as the primary cybersecurity risk categories (Garg et al., 2019). A successfully compromised AMI system can serve as an entry point into wider utility operational technology networks — including distribution management and SCADA systems — with documented potential for attackers to cause blackouts or issue harmful control commands (CLOU Global, 2025). The consequences extend beyond financial loss to public service reliability.

In ASEAN, the risk is amplified by several regional factors: the prevalence of multi-vendor supply chains with limited visibility into firmware provenance, the use of shared mobile network infrastructure for device communication, inconsistent national cybersecurity regulation across the region, and limited in-house OT security expertise within most utilities.

Example Security Considerations Utilities May Evaluate

Utilities may benefit from seeking documented evidence — rather than relying on vendor attestation alone — across key security domains at procurement stage. The following considerations may help utilities assess commonly discussed security expectations during procurement and deployment planning.

Security Domain	Minimum Consideration
Device Authentication	Mutual TLS or equivalent; unique per-device credential management
Data Encryption	End-to-end encryption for all meter-to-platform communications
Firmware Integrity	Cryptographic signing of all firmware; secure OTA update mechanism
Vulnerability Management	Defined patch release timelines; CVE disclosure policy
Access Control	Role-based access to HES/MDMS with audit logging
Incident Response	Documented breach response procedures with defined notification timelines
Third-Party Assessment	Independent penetration testing of device and platform within prior 12 months

Cybersecurity obligations embedded in vendor contracts, with defined update and disclosure responsibilities throughout the system lifecycle, tend to provide stronger protection than point-in-time procurement requirements alone. This is an area where ongoing governance — not just initial specification — determines real-world outcomes.

10. The ASEAN Context — Why Regional Deployments Are Different

ASEAN utilities may find it useful to approach AMI program design with caution around importing deployment assumptions from European or North American programs. The technical and operational contexts differ in ways that matter significantly for project design.

Tropical climate exposure — high humidity, sustained elevated temperatures, and flooding events — creates environmental stresses on metering hardware that are largely absent from temperate-region deployments. IP68 ingress protection ratings are a necessary starting point, not a sufficient specification. Installation site conditions across the region routinely include submerged chambers during monsoon events, temperatures exceeding 40°C in outdoor installations, and humidity levels that degrade connector and terminal integrity over time.

Urban density in major ASEAN cities creates signal attenuation challenges that are qualitatively different from those encountered in European deployments. Multi-storey residential blocks with reinforced concrete construction, underground car park meter chambers, and service riser ducts in high-rise towers all present RF penetration challenges that require site-specific connectivity solutions rather than coverage-map assumptions.

Regulatory fragmentation across ASEAN's ten member states adds a further layer of complexity for utilities operating across borders or seeking to standardise procurement across jurisdictions. Data localisation requirements, telecommunications licensing constraints, smart meter technical standards, and consumer data protection frameworks vary significantly between Malaysia, Indonesia, Vietnam, the Philippines, and Thailand. Multi-country AMI programs may need to account for this regulatory diversity explicitly in their architecture and compliance planning.

Finally, ASEAN procurement cultures — characterised by extended tendering cycles, price-sensitivity, and complex multi-stakeholder approval processes — create project timeline pressures that often compress the planning and pilot phases that most determine long-run success. Utilities and their procurement advisers may find it worthwhile to resist the pressure to abbreviate these phases in the interest of faster deployment commencement.

11. What Successful Projects Have in Common

Across ASEAN, the smart water metering programs that consistently achieve their intended outcomes share a recognisable set of characteristics — none of which depend on deploying the most expensive technology or working with the largest vendor.

They begin with operational objectives, not devices.
Before any technology evaluation begins, successful utilities define what they are trying to achieve — a specific NRW reduction target, a billing error rate threshold, a field workforce reduction — and use those objectives to define the technical requirements their AMI system must meet.

They define measurable KPIs before procurement and align them contractually.
Data availability rates, battery performance thresholds, integration uptime requirements, and support response SLAs are specified in procurement documents and embedded in vendor contracts with consequence provisions.

They design pilots to stress-test, not to demonstrate.
Pilot deployments include deliberately difficult sites, diverse installation conditions, and large enough sample sizes to generate actionable performance data. Success criteria are defined at the outset, not calibrated after the fact.

They invest in integration architecture early.
The data model, API specifications, and end-to-end system test plan are finalised before mass deployment begins. Operational use of data — not just data availability — is the definition of a successful pilot.

They build cross-functional ownership.

IT, Operations, Procurement, Finance, and Executive leadership share accountability for AMI program outcomes under a unified governance structure with clear escalation paths and a single performance dashboard.

They treat cybersecurity as a design requirement, not a procurement checkbox. Security controls are specified, validated, and maintained throughout the system lifecycle.

12. Practical Readiness Questions Before AMI Deployment

The following questions may help utilities assess readiness before committing to large-scale AMI deployment. Each dimension reflects one of the failure modes identified in this paper.

Readiness Dimension	Pre-Deployment Questions
Procurement Strategy	Have operational objectives and measurable KPIs been defined before issuing the RFP? Does the evaluation criteria weight lifecycle cost, not only device price?
Battery Life Validation	Has battery life been validated under worst-case RF and environmental conditions in the actual deployment environment, not laboratory conditions?
Connectivity Planning	Have RF site surveys been conducted at a representative sample of installation sites including underground and indoor locations?
Integration Architecture	Is the end-to-end integration blueprint documented? Has the full chain from meter to billing system been tested in a staging environment?
Operational Ownership	Is there a designated AMI operations function with defined accountability for system performance across all vendor relationships?
Scalability Testing	Has the backend been load-tested against full-deployment volumes? Have operational processes been documented and rehearsed at pilot scale?
Workforce Readiness	Have operations, IT, and analytics teams completed AMI training? Have business processes been redesigned around the AMI operational model?
Cybersecurity	Has independent penetration testing been conducted? Are firmware signing, encryption, and vulnerability disclosure obligations contractually defined?
Regulatory Compliance	Have data localisation, telecommunications, and consumer privacy requirements been assessed for all jurisdictions in scope?

Utilities that can answer these questions affirmatively — supported by documented evidence rather than assumptions — may be better positioned for large-scale deployment. Those that identify gaps may find it useful to treat those gaps as the highest priority items on their pre-deployment workplan.

Conclusion

Smart water metering has genuine transformative potential across ASEAN. Smart metering technologies have matured significantly. The operational benefits — reduced NRW, automated billing, real-time leak detection, lower field workforce dependency, better demand management — are well-demonstrated in markets that have deployed AMI effectively. In many deployment contexts, the investment case can be compelling when implementation assumptions and operational readiness are realistic.

The problem is not that the technology does not work. The problem is that the conditions required for the technology to work are consistently underestimated, underprepared, and underinvested. Projects encounter difficulties at the seams — between procurement and operations, between the pilot and the full deployment, between the device network and the billing system, between the technology program and the organisational capability required to use it.

The utilities that will define the next generation of smart water infrastructure in Southeast Asia will not necessarily be those that deploy the most meters. They will be those that operationalise smart metering most effectively — transforming connected devices into management capability, billing accuracy, network insight, and measurable NRW reduction.

That outcome requires deliberate planning, rigorous vendor governance, honest assessment of organisational readiness, and a willingness to define success in operational terms rather than installation volume. The investment in getting the foundations right is always less expensive than fixing the consequences of getting them wrong.

References

Asian Development Bank. (2010). The issues and challenges of reducing non-revenue water. ADB. https://www.adb.org/publications/issues-and-challenges-reducing-non-revenue-water

Asian Development Bank. (2023). Curbing Asia's nonrevenue water. ADB. https://www.adb.org/publications/curbing-asias-nonrevenue-water

Anttila, J., et al. (2026). Experimental evaluation of NB-IoT power consumption and energy source feasibility for long-term IoT deployments. IoT, 7(1), 7. https://doi.org/10.3390/iot7010007

Cisco Systems. (2017). The journey to IoT value: Challenges, breakthroughs, and best practices. Cisco.

CLOU Global. (2025). Cybersecurity for smart meters and AMI: Practical risks and real-world protections. https://clouglobal.com/cybersecurity-for-smart-meters-and-ami-practical-risks-and-real-world-protections/

Garg, S., et al. (2019). Smart meter security: Vulnerabilities, threat impacts, and countermeasures. ResearchGate. https://www.researchgate.net/publication/333305127

Gartner. (2023). Market trends: IoT endpoints will need new technologies to achieve scale. Gartner.

IDC. (2022). IoT and IIoT project outcomes study. IDC.

Liemberger, R., & Wyatt, A. (2019). Quantifying the global non-revenue water problem. Water Supply, 19(3), 831–837. https://www.researchgate.net/publication/326238463

Lim, D., et al. (2021). Real-world evaluation of power consumption and performance of NB-IoT in Malaysia. IEEE Access. https://ieeexplore.ieee.org/document/9627879/

Microsoft. (2022). IoT signals report. Microsoft Corporation.

Roosipuu, P., et al. (2023). Evaluating the energy consumption savings at 450 MHz band for NB-IoT devices. In Proceedings of the 14th International Conference on the Internet of Things. ACM. https://dl.acm.org/doi/10.1145/3703790.3703825

Tan, C., et al. (2023). Key challenges to urban water management in ASEAN. In Water resource management in ASEAN. Springer. https://link.springer.com/chapter/10.1007/978-981-19-8677-2_2

World Bank. (2006). The challenge of reducing non-revenue water in developing countries. World Bank. https://documents1.worldbank.org/curated/en/385761468330326484

Disclaimer

The views and observations expressed in this paper are the author's own and are intended for general industry discussion and educational purposes. They are based on publicly available research, practical engineering experience, and regional industry observations, and do not represent the official position, product commitments, customer relationships, or commercial practices of any employer, client, utility, or affiliated organisation. Utilities should evaluate deployment decisions within their own operational, technical, regulatory, and procurement context.

About the Author

Vincent Wong (Wong Yew Hon)

Vincent Wong brings over **25 years of engineering and product leadership experience** across industrial infrastructure and technology sectors, with the past decade focused on smart metering, Advanced Metering Infrastructure (AMI), and NB-IoT deployment strategies in ASEAN utility environments. As a senior engineering and product development executive, his work spans hardware engineering, connectivity systems, and utility digitalization initiatives. His writing focuses on the practical operational, connectivity, deployment, and governance realities of smart utility programs in Southeast Asia.

Connect on LinkedIn: linkedin.com/in/vincentwongmy