SAARC ENERGY CENTRE · REGIONAL WEBINAR

Cyber Security Training and Auditing for Smart Grid

Auditing Smart Grid Performance

Linking Operational Reliability with Cyber Resilience

Toufiq Rahman

Certified Energy Auditor | SREDA, Government of Bangladesh

30 June 2026 · SAARC Energy Centre, Islamabad

AGENDA

What We Will Cover

1	The Threat Landscape	Why smart-grid cyber risk is escalating across SAARC	Slides 3–7
2	The Core Idea	Auditing as the bridge between performance and cyber resilience	Slides 8–11
3	Evidence from the Field	Documented incidents and the economics of a breach	Slides 12–15
4	The Audit Method	Framework, evidence, risk, controls, and detection	Slides 16–21
5	The Regional Path	Standards, maturity, and recommendations for SAARC	Slides 22–26

PART 1

The Threat Landscape

Why smart-grid cyber risk is escalating across SAARC — and what makes the grid exposed.

THE TREND IS NOT SUBTLE

Cyberattacks on Utilities Are Accelerating

+70%

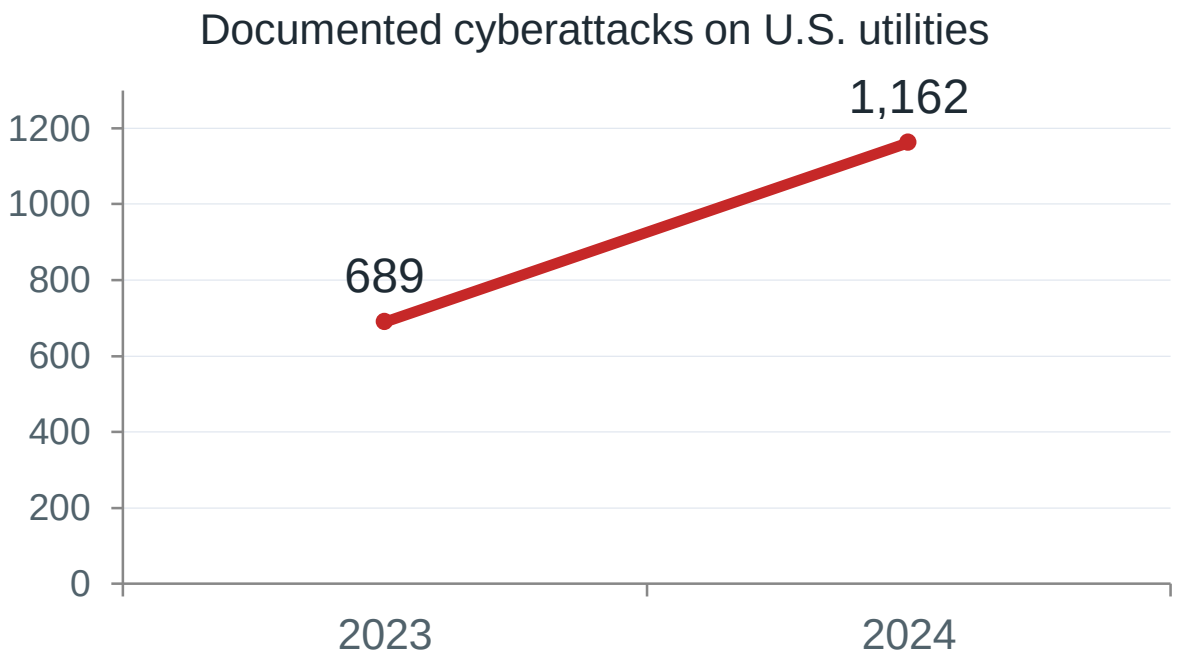
utility attacks, 2023→24

+146%

sites with disruption, 2024

67%

energy orgs hit by ransomware



Source: Check Point Research / Reuters (2024); Sophos (2024); Industrial Cyber (2024).

CONTEXT

Why Smart-Grid Cyber Risk Is a SAARC Issue

Expanding attack surface

OT–IT convergence multiplies entry points

Physical, high-cost failures

Blackouts, equipment damage, national-security risk

Regional propagation

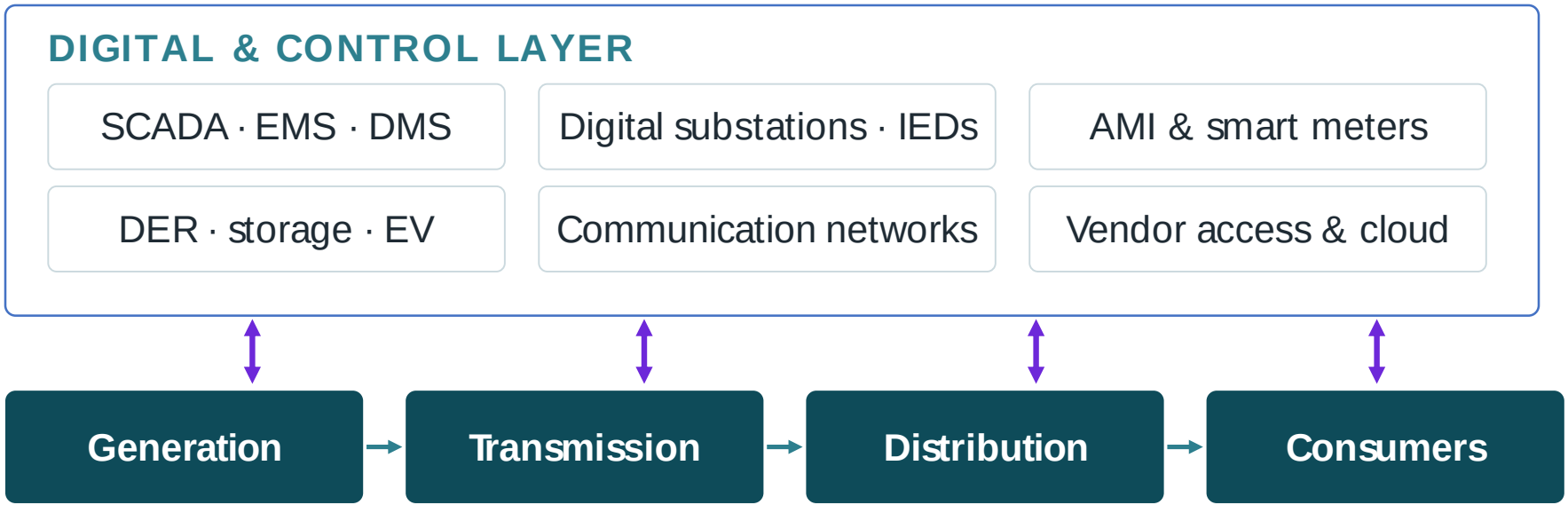
One weak utility becomes its neighbours' risk

The binding constraint: a 42% shortfall in energy-sector cybersecurity personnel.

Source: Boston Consulting Group, via MHI Spectra (2025). || *OT- Operation Technology*

THE TERRAIN

What Makes a Grid "Smart" Also Makes It Exposed



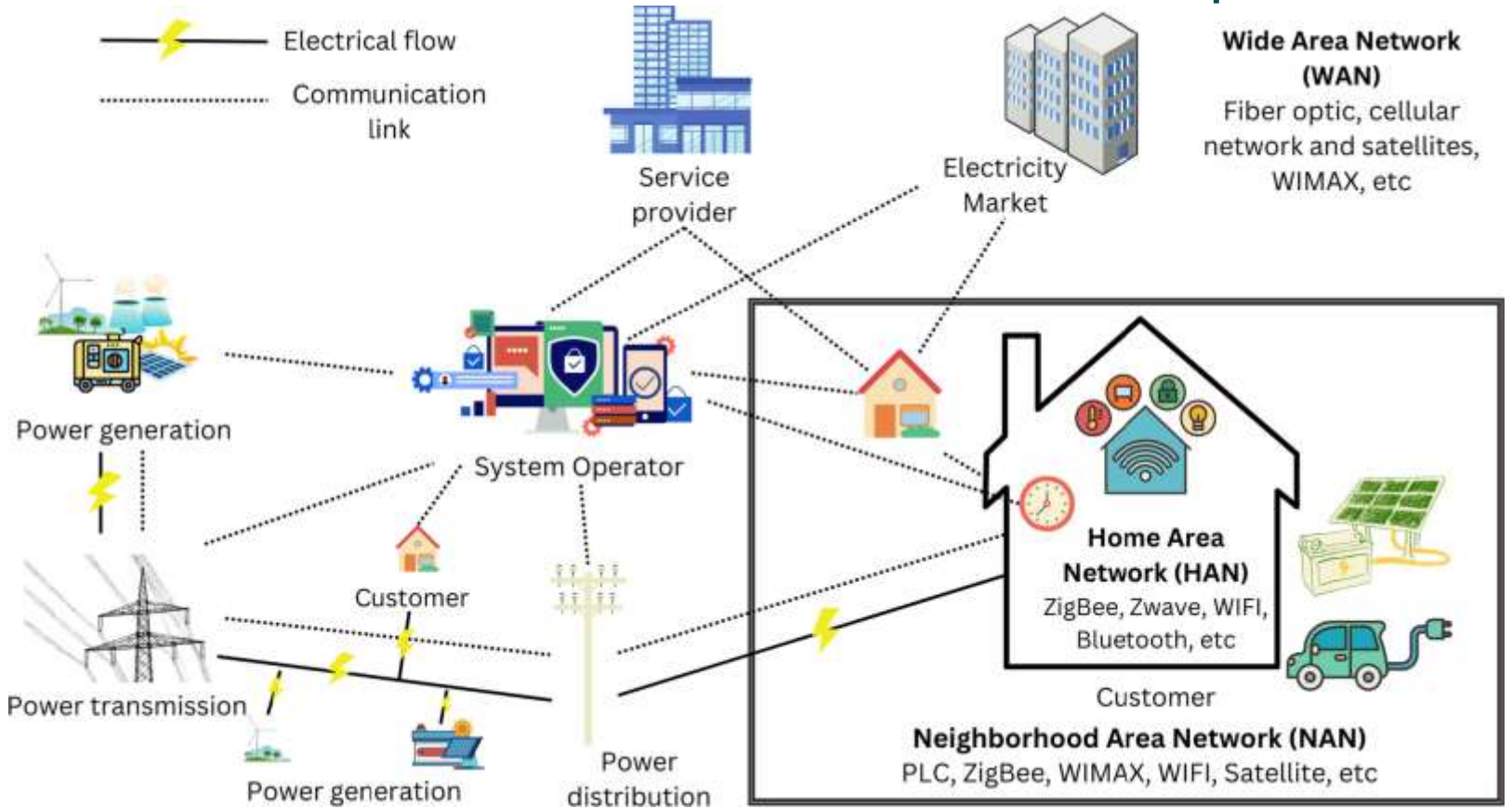
Every two-way connection is an entry point. *80% of solar-inverter flaws (3 yrs) rated high/critical.*

Source: Forescout Vedere Labs, SUN:DOWN (2025).

SCADA — Supervisory Control & Data Acq.
EMS / DMS — Energy / Distribution Mgmt Sys.

IED — Intelligent Electronic Device
AMI — Advanced Metering Infrastructure
DER — Distributed Energy Resources

What Makes a Grid “Smart” Also Makes It Exposed



Source: Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges, 2024, Batoul Achaal et. al.

THREAT LANDSCAPE

Speak Threats in the Language of Operations

False data injection
Wrong dispatch; billing loss

SCADA / EMS intrusion
Unsafe switching; forced outages

Ransomware on utility IT
Frozen billing; delayed restoration

Denial-of-service on comms
Operators go blind

Vendor remote-access compromise
A trusted backdoor into OT

Manipulated relay settings
Protection defeated; equipment risk

Explain every threat by its operational consequence — not by exploit jargon.

PART 2

The Core Idea

Auditing as the bridge between grid performance and cyber resilience.

THE THESIS

Two Audits, One Shared Evidence Base

"You cannot secure what you do not measure, map, monitor, and audit."

Performance audit asks

- Is the grid reliable?
- Are data, control, comms accurate?
- Is automation delivering value?
- Are anomalies escalated?

Cybersecurity audit asks

- Are assets, access, control protected?
- Are risks classified and monitored?
- Can incidents be detected and recovered?

Many cyber risks first appear as performance anomalies.

WHAT TO AUDIT

Six Performance Dimensions of a Smart Grid

1 · Reliability

SAIDI, SAIFI, restoration, FDIR

2 · Power quality

Voltage, frequency, harmonics

3 · Communication

Latency, packet loss, redundancy

4 · Data

Accuracy, time-sync, integrity

5 · Control

Command timing, config changes

6 · Cyber-resilience

Visibility, access, logging, backups

Dimensions 1–3 reveal the grid's health. 4–6 reveal whether you would notice an attack.

SAIDI — Avg. Interruption Duration Index, **SAIFI** — Avg. Interruption Frequency Index, **FDIR** — Fault Detection, Isolation, Restoration

THE BRIDGE IN PRACTICE

Performance Gaps Are Early Cyber Warnings

Audit finding	Cyber-risk signal
Incomplete asset inventory	Unmonitored entry points
Poor time synchronization	False data undetectable
Unexplained config changes	Possible unauthorized access
Missing SCADA / IED logs	No forensic readiness
Untested backup	Ransomware becomes a crisis
Unprioritized alarm flood	Real events drown in noise

The audit converts technical abnormalities into risk signals leadership can act on.

PART 3

Evidence from the Field

Documented incidents and the economics of a breach — what really happened, and what it cost.

DOCUMENTED CASE · REAL INCIDENT

Ukraine, Dec 2015 — First Grid Blackout by Cyberattack

225,000	customers lost power
3	utilities hit at once
~30	substations switched off
1–6 hrs	outage duration

How it unfolded — every step maps to an audit control

1. Phishing → malware on IT
   Access control, training
2. VPN → SCADA; breakers opened
   Remote-access MFA, segmentation
3. KillDisk wipes; UPS disabled
   Backup & recovery testing
4. Call-centre denial-of-service
   Comms resilience planning

Source: E-ISAC / SANS (2016); CISA IR-ALERT-H-16-056-01; U.S. CRS R48067 (2024).

DOCUMENTED CASE · REAL INCIDENT

Colonial Pipeline, 2021 — When IT Ransomware Stops OT

$4.4M	5,500 mi	45%	6 days
ransom paid	pipeline shut	of E-Coast fuel	to resume

The decisive detail

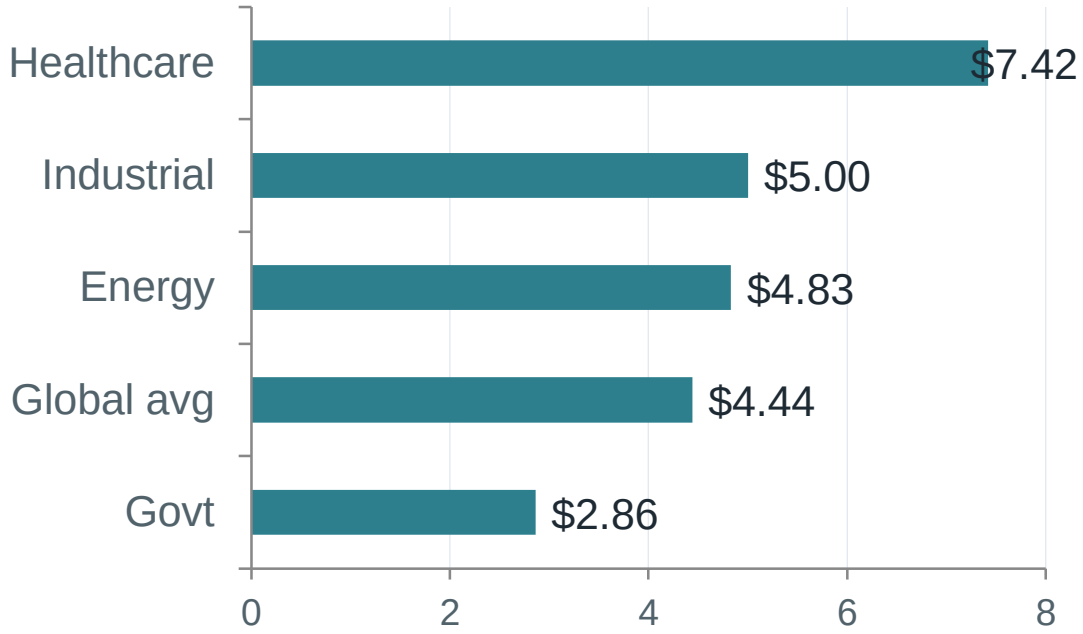
The OT pipeline was never compromised. Ransomware hit IT billing; OT was shut down precautionarily because IT and OT were not segmented. Entry: one legacy VPN account **with no MFA.**

Audit lessons: IT/OT segmentation · MFA on every path · tested recovery · retire legacy access.

Source: U.S. DOE/CESER; U.S. Senate testimony (2021); CISA-FBI AA21-131A.

THE ECONOMICS

What a Breach Costs — and What Prevention Saves



$4.83M

avg energy-sector breach, 2025

Prevention pays

$19M saved + **80 days** faster containment via automation.

Source: IBM / Ponemon, Cost of a Data Breach 2025.

PART 4

The Audit Method

A seven-step framework — from evidence and risk to controls and live detection.

HOW TO AUDIT

The Seven-Step Audit Framework

1 Define scope

Incl. vendor access

2 Map assets

Flows, owners, links

3 Baseline

Performance & logs

4 Identify gaps

Access, patching, backups

5 Classify risk

Likelihood × consequence

6 Prioritize

By criticality & cost

7 Verify

Re-audit, drills, review

The audit is not finished at the report — Step 7 is where resilience is built.

EVIDENCE COLLECTION

An Audit Is Evidence-Based, Not Opinion-Based

Architecture

- Asset inventory
- Network & SCADA maps
- Config change records
- Segmentation policy

Operations

- Event & alarm logs
- Outage reports
- Power-quality reports
- Patch records

Governance

- Access-control policy
- Vendor-access records
- Backup test records
- Incident plan & drills

If a utility cannot produce these within days, that absence is itself a critical finding.

PRIORITIZATION

Classify Risk by Grid Criticality — Not by Fear

CRITICAL	Blackout, unsafe switching, cross-border impact
HIGH	Control-centre, substation, restoration capability
MEDIUM	Data quality, reporting, localized operation
LOW	Administrative or documentation gaps

Not every cyber gap deserves the same investment. Budget must follow criticality.

WHAT TO FIX FIRST

Priority Controls: Governance, Technical, Operational

Governance

- OT policy with clear ownership
- Vendor-access governance
- Periodic audit & review

Technical

- Inventory & segmentation
- MFA for remote access
- Log monitoring
- Patching & tested backups

Operational

- Training & drills
- Alarm prioritization
- Corrective-action tracking

Start with three: visibility, access, recoverability.

DETECTION · THE LIVE EARLY-WARNING LAYER

Intrusion Detection & Anomaly Monitoring

272

days, on average, to detect + contain an industrial breach (199 + 73).

Every undetected day, the attacker is inside.

What monitoring watches in OT

- **Network baselining** — Flag unexpected device or protocol
- **Command anomalies** — Switching outside normal sequence
- **Data-integrity checks** — Impossible values, time-sync drift
- **Prioritized alarms (SOC)** — Surface the real signal, not the flood

The audit defines the baseline; monitoring enforces it continuously.

Source: IBM / Ponemon — industrial-sector detect/contain timelines.

PART 5

The Regional Path

Standards, the maturity reality across member states, and recommendations for SAARC.

FROM FINDING TO RESILIENCE

A Regional Success, and an Illustrative Pathway

REGIONAL PRECEDENT · REAL

Containment through preparedness

Pakistan Petroleum (2025) contained ransomware by isolating IT early. Contrast a SE-Asian provider disabled **18 days** (NightSpire, $8M). Same threat; opposite outcome.

Differentiator: detection speed + IT/OT segregation.

ILLUSTRATIVE MODEL (not a real utility)

- **Finding:** Unknown devices; no MFA; untested recovery
- **Risk:** Unauthorized access; slow restoration
- **Action:** Inventory; MFA; monitoring; backup test

Outcome: Visibility; faster detection; accountability

Total new hardware: almost none. Gains come from visibility, discipline, verification.

Source: Asimily, Top Utilities Cyberattacks of 2025.

FROM FINDING TO RESILIENCE

Bangladesh & SAARC: Why This Risk Is Immediate

Smart-grid exposure is no longer theoretical

Bangladesh

Grid digitalization: SCADA, automation, digital substations Smart/prepaid metering expanding rapidly Solar, DER and inverter-based assets increasing Cross-border electricity trade already active

SAARC

Different grid-maturity levels Shared interconnections create shared cyber risk One weak control point can affect regional reliability

Digitalization improves efficiency — but every connected asset must be mapped, monitored, secured and verified

TECHNICAL EXPLAINER · 1

Demand Response & Smart Meters (AMI)

Demand Response (DR)

Shifting or shedding load on grid or price signals — turning consumers into a controllable resource that flattens peaks.

AMI / smart & prepaid meters

Two-way metering: remote read, remote connect/disconnect, prepaid vending, tamper & outage telemetry — the data backbone for DR.

BANGLADESH TODAY

10.66 lakh

smart prepaid meters installed by DPDC (of ~19.1 lakh consumers)

5–7%

non-technical loss the prepaid rollout targets

Audit hook: Every meter is a two-way endpoint with a remote disconnect — an audit must verify who can issue that command, and how it is logged.

Source: DPDC / BSS (Oct 2025); Bangladesh Power Division prepaid-metering programme.

TECHNICAL EXPLAINER · 2

Grid Stability: AGC, Governor Mode & Nuclear Band

AGC

Automatic Generation Control — the control centre continuously trims generator output to hold 50 Hz and balance supply with demand.

FGMO

Free Governor Mode of Operation — governors react automatically to frequency. Historically inactive in Bangladesh; trialled post-2014 with encouraging results.

Nuclear band

Rooppur NPP is base-load with a low ramp rate and stringent margins — it needs frequency held tightly near 50 Hz to operate safely.

THE REGIONAL REALITY

Bangladesh: nominal 50±0.5 Hz, but routinely 48.9–51.2 Hz (48.7–51.5 under contingency). **India:** IEGC band 49.5–50.3 Hz. **Tie:** asynchronous HVDC back-to-back link.

Audit hook: Frequency, AGC set-points and governor response are performance signals — spoofed or manipulated, they threaten stability; an audit must confirm their integrity.

Source: IEEE PESGM 2018 (FGMO trials); BAERA / TBS (2026); CERC IEGC.

TECHNICAL EXPLAINER · 3

Industrial Energy: Factory EnMS & Building EMS

Factory EnMS

Energy Management System (ISO 50001) — meters, sub-meters and controls that monitor and optimise industrial energy use.

BEMS

Building Energy Management System — automates HVAC, lighting and loads in commercial buildings for efficiency.

Both are IT–OT systems with controllers, networks and remote access — both are energy-audit territory

Continuous metering

Sub-metered loads, demand profiles, KPIs

Automated control

Setpoints, schedules, demand limiting

Networked & remote

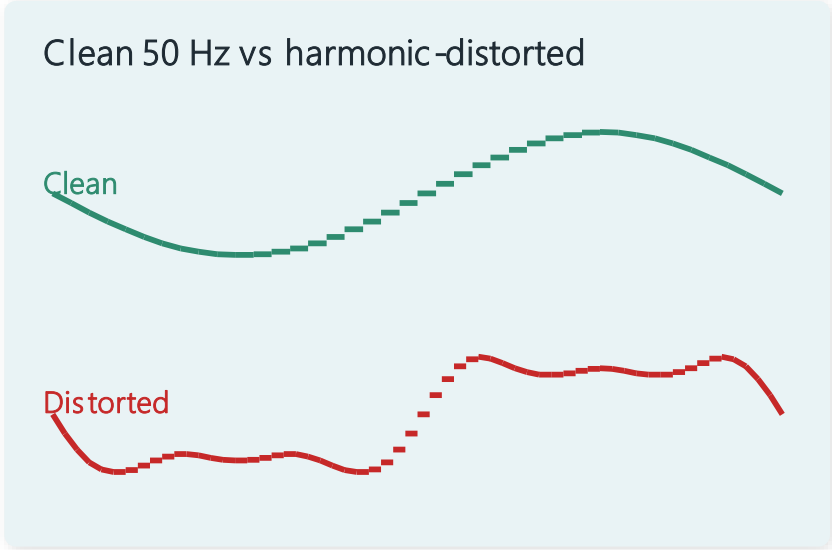
BACnet / Modbus, vendor cloud dashboards

Audit hook: EnMS/BEMS data proves efficiency — but their controllers and vendor links are unmonitored OT entry points an audit should scope in.

Harmonics: Generation & Injection into the Grid

What harmonics are

Distortions of the pure 50 Hz sine wave at multiples (150, 250 Hz…). They overheat equipment, trip protection and corrupt measurements.



Where they come from

- Solar / DER inverters
- VFDs & industrial drives
- EV chargers & SMPS loads

Audit hook: Power-quality data (THD, distortion) is an audit metric — an attacker injecting harmonics or faking PQ readings hides behind it.

Source: IEEE 519 harmonic limits; IEC 61000 power-quality standards.

ANCHOR TO RECOGNISED STANDARDS

You Do Not Have to Invent the Baseline

IEC 62443
OT / control-system security

ISO/IEC 27019
Energy-sector information security

IEC 62351
Power-system protocol security

NIST SP 800-82 / CSF
OT guidance — freely available

NERC CIP
Mandatory regulatory reference

ISO/IEC 27001
Information-security management

For SAARC: extract one harmonized minimum baseline — not full certification on day one.

Source: IEC, ISO/IEC, NIST and NERC published standards (2026).

WHY HARMONIZATION IS HARD — AND NECESSARY

Member States Sit at Different Maturity Stages

STAGE 1 Ad hoc	STAGE 2 Developing	STAGE 3 Defined	STAGE 4 Managed
No policy; no inventory	Basic controls; first audits	Policy, segmentation, MFA, audit	Continuous monitoring; drills

Interconnection means the region's security equals its least mature connected utility — so lift the floor.

THE WAY FORWARD

Recommendations for the SAARC Region

Policymakers & regulators

- Minimum cyber-audit requirements
- Mandate inventories & risk registers
- Harmonize standards regionally
- Build OT-security capacity
- Incident-reporting mechanisms

Utilities

- Integrate performance + cyber audit
- Start with critical assets
- Live corrective-action dashboard
- Run cyber-physical drills
- Treat cyber as governance

KEY TAKEAWAYS

1. Cybersecurity is inseparable from grid performance.
2. The threat is escalating fast — ~$4.8M per energy breach.
3. Real incidents failed on standard audit controls, not exotic attacks.
4. Performance anomalies are early cyber warnings.
5. Structure: evidence → classification → action → verification.
6. SAARC needs harmonized cyber-audit practice — now.

"The most secure smart grid is not the one with the most technology — it is the one with the strongest visibility, discipline, accountability, and verified resilience."

FOR REFERENCE

Glossary of Key Abbreviations

Control & operations

OT / IT — Operational / Information Technology
SCADA — Supervisory Control & Data Acq.
EMS / DMS — Energy / Distribution Mgmt Sys.
ADMS — Advanced Distribution Mgmt Sys.

Field devices & assets

RTU / IED — Remote Terminal Unit / Smart Device
AMI — Advanced Metering Infrastructure
DER — Distributed Energy Resources
EV — Electric Vehicle

Cybersecurity terms

MFA — Multi-Factor Authentication
SOC — Security Operations Centre
SIEM — Security Info & Event Mgmt
VPN / DoS — Private Network / Denial of Svc

Reliability & standards

SAIDI — Avg. Interruption Duration Index
SAIFI — Avg. Interruption Frequency Index
FDIR — Fault Detection, Isolation, Restoration
IEC / NERC — Grid-security standards bodies

Full standards references on the next slide. A complete glossary is in the Presenter Pack.

Thank You

Toufiq Rahman · Certified Energy Auditor · Energy Analyst - *questions welcome*