SAARC Webinar

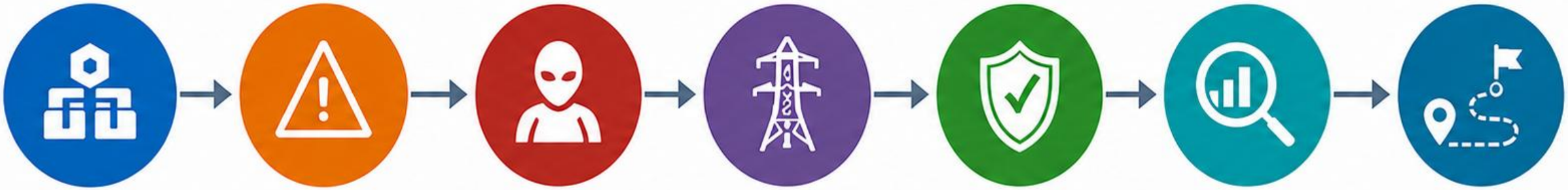
Cybersecurity of Smart Grids

From digitalization risk to cyber-physical resilience

Burhan Hyder
Cybersecurity Engineer
Pacific Northwest National Laboratory
Washington, USA

30 June 2026

Agenda



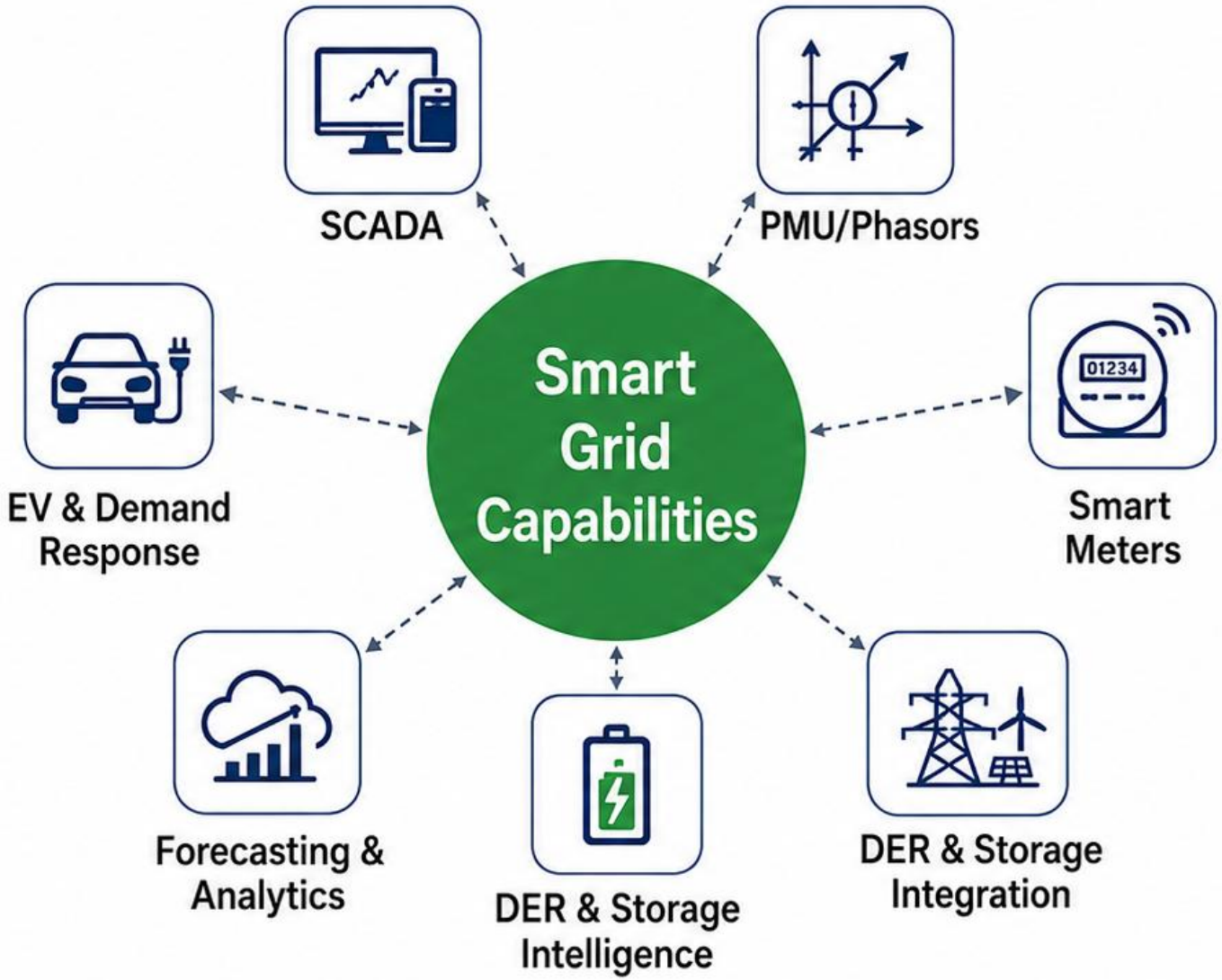
- Understand the system
- Why risk is growing
- How attacks happen
- What can go wrong
- How we defend
- How we validate
- Way forward

Smart Grids: Why the Grid Became Digital

Digitalization delivers better visibility, faster control, higher reliability, DER integration, and stronger customer engagement.

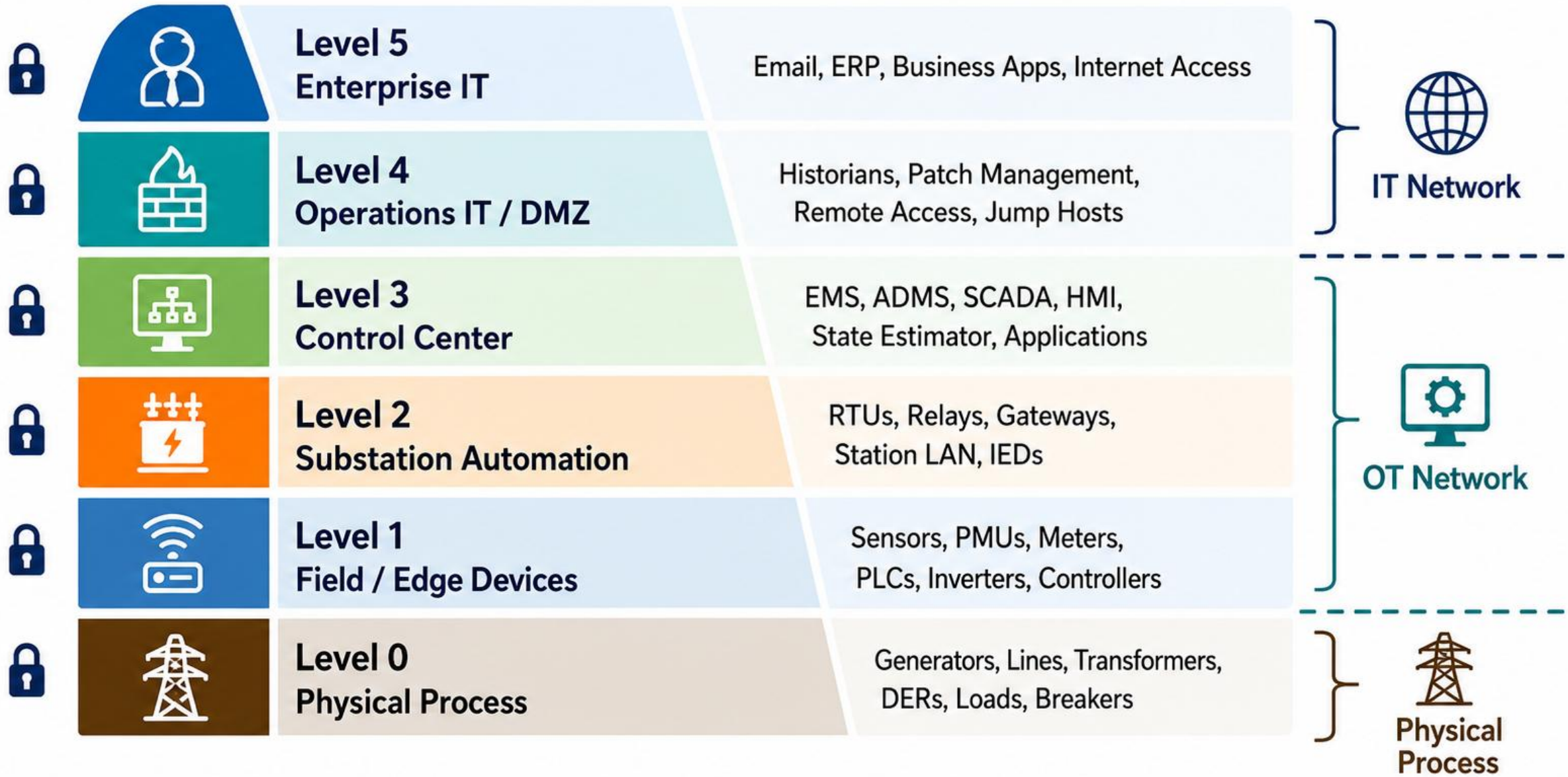
Need for:

- ✓ Better visibility
- ✓ Faster control
- ✓ Higher reliability
- ✓ Integration of DERs
- ✓ Operational efficiency
- ✓ Customer engagement



Smart Grid as a Cyber-Physical System

(Purdue Model Inspired)



Why the Energy Transition Increases Cyber Risk

More Devices
DERs, meters, PMUs, inverter controls

More Communications
cellular, cloud, internet, RF, VPN

More Data & Software
analytics, forecasting, platforms, APIs

More Automation
remote control, DER coordination, auto patching or auto switching

More Third Parties
vendors, aggregators, cloud, integration

More connectivity and digitalization expand the attack surface and increase risk exposure.

What Attackers May Try to Achieve

Steal

credential, data, diagrams, settings, network maps, operational procedures

Disrupt

ransomware, DoS or DDoS, communication loss, data-availability disruption

Deceive

false data, replay, alarm suppression, time spoofing, state-estimation bias

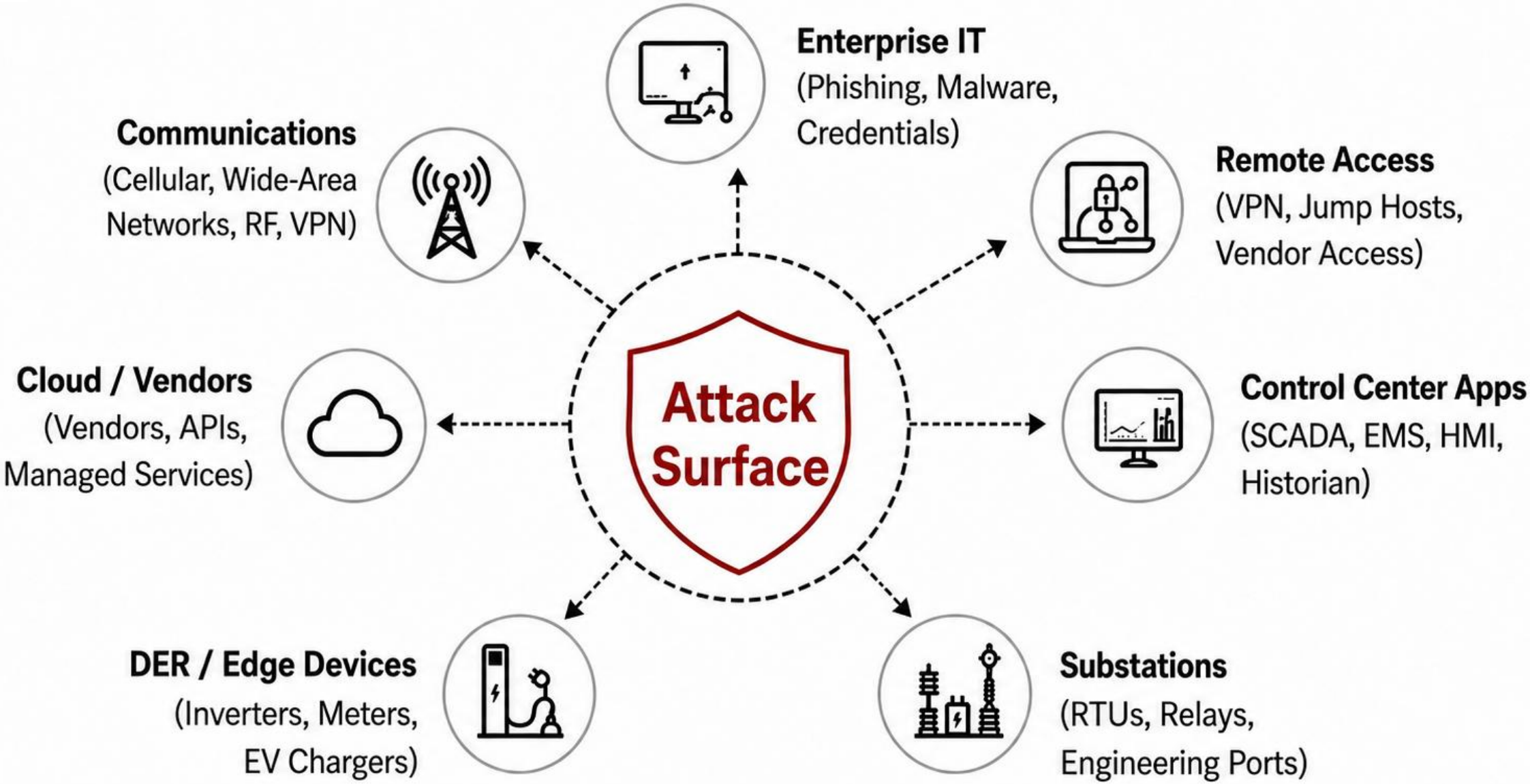
Control

unauthorized commands, setpoint changes, relay setting changes, DER/inverter control

Delay Recovery

wipe systems, lock backups, disable tools, disrupt vendor access

Where Attackers Can Get In



From Cyber Attack to Physical Consequence

1 Initial Access

- Phishing
- Stolen credentials
- Vulnerable or exposed access

2 Lateral Movement

- Move to OT
- Access servers or workstations
- SCADA gateways

3 Process Manipulation

- False telemetry
- Bad commands
- Setting changes
- Disable protection

4 Operational Effect

- Wrong decisions
- Unstable control
- Loss of visibility
- Delayed response

5 Physical Consequence

- Outage
- Equipment stress
- Voltage or frequency violations
- Unsafe restoration
- Cascading risk

DEFENDER GOAL: Detect and disrupt the chain before process manipulation occurs.

Why Grid Cybersecurity Is Different

Typical IT Security		Grid / OT Security
Confidentiality focus	VS.	Availability and integrity focus
Best-effort availability		Real-time constraints
Homogeneous systems		Heterogeneous and legacy systems
User workflows		Physics-aware operation
Backup often sufficient		Recovery must be tested

Cybersecurity in power systems must respect physics, protection, safety, and operations.

How We Tackle the Problem

Planning Perspective
(Before)

- Risk assessment
- Attack-defense modeling
- Asset criticality
- Investment prioritization

Operations Perspective
(During)

- Monitoring and detection
- Situational awareness
- Incident response
- Safe decision making

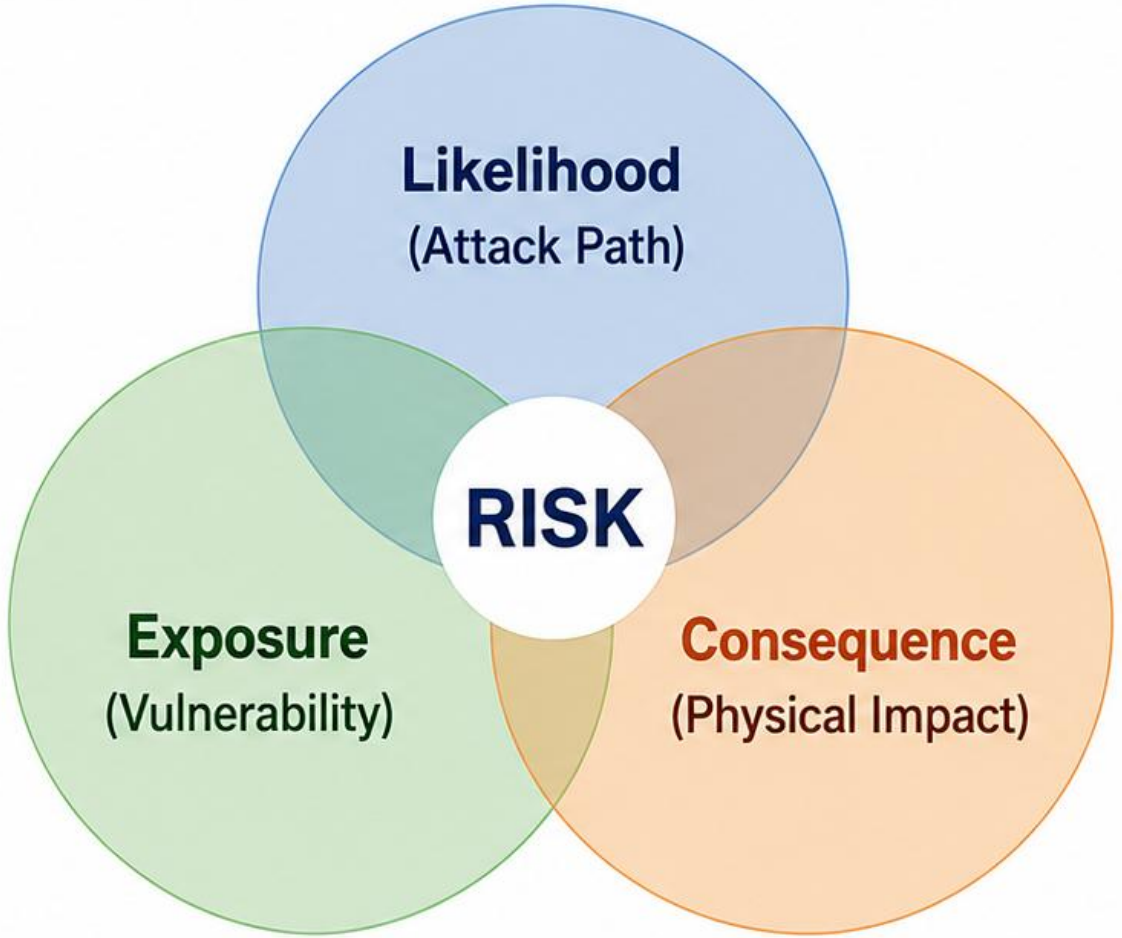
Resilience Perspective
(After)

- Business continuity
- Backup and recovery
- Exercises and drills
- Learn and improve

Prevent → Detect → Respond → Recover

Planning Perspective: Invest Where Cyber Risk Becomes Grid Risk

1. **Asset Inventory**
   What do we have?
2. **Attack Modeling**
   How can it be attacked?
3. **Impact Analysis**
   What could happen?
4. **Investment Decision**
   Where to invest?



Risk = Likelihood × Exposure × Consequence × Recovery Difficulty

Operations Perspective: Detect, Decide, Respond

Observe

- SCADA
- PMU
- Logs
- Flows
- Event Alarms

Detect

- Anomaly Detection
- Rules & Signatures
- Protocol Checks
- Physics Validation

Triage

- Cyber or Physical?
- Data Quality?
- Impact Assessment

Respond

- Isolate / Contain
- Block / Restrict
- Manual Fallback
- Safe Actions

Recover

- Restore Systems
- Validate Configs
- Lessons Learned
- Improve Detection

 Trusted Situational Awareness →  Safe Control →  Reliable Operation

Resilience Perspective: Prepare, Absorb, Adapt, Recover, Learn

1 Prepare

Plans, Roles, Backups, Drills

2 Absorb

Segmentation, Limit Access, Fail-safe Design

3 Adapt

Manual Fallback, Alternate Paths, Degraded Mode

4 Recover

Restore, Validate, Reconnect Safely

5 Learn

Lessons Learned, Improve Defenses

Operate with Preparedness. Absorb with Control. Adapt with Agility. Recover with Confidence. Learn to Get Stronger.

Essential Protection Strategies

Governance

- Policies
- Ownership
- Compliance
- Risk Management

Zones & Conduits

- Segmentation
- Firewalls
- DMZ
- Controlled Paths

Identity & Access

- MFA
- Least Privilege
- PAM
- Access Review

Secure Engineering

- Patching
- Hardening
- Backups
- Change Control

Monitoring & Detection

- Logs
- Alerts
- IDS/IPS
- Correlation

Incident Response

- Playbooks
- Coordination
- Containment
- Recovery

Defense-in-Depth Across People, Process, and Technology.

Tools & Frameworks: What Can Help

FRAMEWORKS

NIST
CSF
(Cybersecurity Framework)

IEC
62443
(Industrial Cybersecurity Standard)

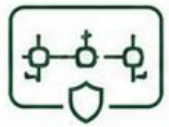
CISA
CPGs
(Cybersecurity Performance Goals)

DOE
C2M2
(Cybersecurity Capability Maturity Model)

NERC
CIP
(Critical Infrastructure Protection Concept)

TOOLS

Asset Discovery



Network IDS

SIEM/ SOAR

Protocol Analyzer

OT Endpoint

ENGINEERING & VALIDATION

Power System Simulation

Co-Simulation & HIL Testbeds

Digital Twins & Cyber Ranges

Data & ML Analytics

KEY TAKEAWAYS

Frameworks organize and prioritize programs.
They align efforts with proven standards and maturity models.

Tools provide visibility and detection.
They help identify risks, monitor assets, and respond faster.

Engineering validation grounds cybersecurity in grid operations.
It ensures readiness through realistic models, testbeds, and analytics.

Why Testbeds and HIL Matter

Power System Layer

- Transmission
- Distribution
- DERs / Inverters
- Protection Models
- Faults & Events

Communication Layer

- DNP3 • IEC 61850 • Modbus • C37.118
- Networks, Routers, Firewalls, VPNs

Control Layer

- SCADA • EMS • HMI • Historian • ADMS
- DERMS • State Estimator

HIL / Devices

- Relays • PMUs • RTUs • PLCs • Controllers
- Real I/O with OPAL-RT / Real-Time Simulators

Attack & Defense Experiments

- False Data
- Replay
- DoS/DDoS
- Command Injection
- Ransomware
- GPS Spoofing

Data Generated

- SCADA, PMU
- Waveforms
- Events, Logs
- PCAPs, Flows

Test → Validate → Train → Improve

Examples from the Energy Sector: Key Lessons

Ukraine Power Grid Attack (2015 & 2016)

- Remote access compromise
- HMI interaction
- Breaker operations
- Recovery disruption

Lesson: Segmentation, monitoring, manual operation, drills

Ransomware in Energy Sector

- Business systems disrupted
- Operations affected indirectly

Lesson: Backups, identity security, business continuity

DER / Cloud / Vendor Exposure

- Aggregator compromise
- Insecure APIs
- Supply chain risk

Lesson: Third-party interfaces, validation

A Practical Roadmap for SAARC Stakeholders

Phase 1 Foundations (0-6 months)

- Governance
- Asset inventory
- Risk assessment
- MFA & access control
- Segmentation basics
- Backups & logging

Phase 2 Visibility (6-18 months)

- Network monitoring
- Log collection
- Baseline behavior
- Threat intelligence
- Detect anomalies

Phase 3 Resilience (12-36 months)

- Incident playbooks
- Recovery testing
- Tabletop exercises
- Manual fallback
- Configuration mgmt
- Drills & training

Phase 4 Ecosystem (36+ months)

- Testbeds & labs
- Workforce dev
- Info sharing
- Regional exercises
- University-utility collaboration

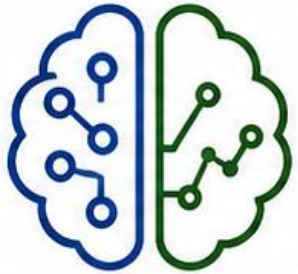
Build Capacity → Strengthen Resilience → Secure the Future

What the Future Looks Like

Zero-Trust OT Access

- Strong identity
- Least privilege
- Continuous verification
- No implicit trust

Physics-Aware AI & Analytics



- Anomaly detection
- Power-system constraints
- Validation
- Fewer false alarms

Secure DER Orchestration

- Authenticated commands
- Validated setpoints
- Fail-safe behavior

Digital Twins & Cyber Ranges

- Model-based validation
- Attack simulation
- Operator training

Regional Collaboration

- Info sharing
- Common standards
- Exercises
- Workforce pipeline

Continuous Security • Intelligent Automation • Resilient Grid

Key Takeaways

1. **Smart grids are cyber-physical systems.** Security must protect both information and physical grid behavior.
2. **Digitalization expands the risk surface.** More devices, connectivity, automation, vendors, and cloud increase dependencies.
3. **Attack impact depends on coupling.** Focus on what cyber compromise can influence physically.
4. **Defense needs three perspectives:** Planning, Operations, and Resilience.
5. **Testbeds turn claims into evidence.** Validate cyber-physical impact and defenses before deployment.
6. **SAARC capacity can be built incrementally** through collaboration, training, testbeds, and shared lessons.

NIRC
CYBERSECURITY RESEARCH & CAPACITY FRAMEWORK

IEC
62443
(Industrial Cybersecurity Standard)

ENHANCE
360 Testbeds & Digital Twins

Incident Reports & Case Studies

Academic & Research

Selected Sources

1

NIST Cybersecurity Framework 2.0

Program structure: Govern, Identify, Protect, Detect, Respond, Recover

2

ISA/IEC 62443

Industrial control system security, zones and conduits

3

DOE C2M2

Energy-sector cybersecurity maturity model

4

CISA Cybersecurity Performance Goals

Baseline cybersecurity practices

5

MITRE ATT&CK for ICS

Adversary tactics and techniques for ICS environments

6

NERC CIP Concepts

Critical asset identification, access control, monitoring, recovery

7

Power-System Simulation & Testbed Literature

Co-simulation, HIL, digital twins, cyber-physical validation

8

Incident Reports & Case Studies

Operational lessons from real cyber events in energy systems

Reference anchors for architecture, threat modeling, resilience, and validation.

Thank you!

Questions?

Email: burhan.hyder@pnnl.gov