Thematic Session-3
CYBER SECURITY FOR THE DIGITALIZED GRIDS

P.K. Agarwal,
Former Director & CISO
Power System Operation Corporation Ltd.

Grid is Transforming

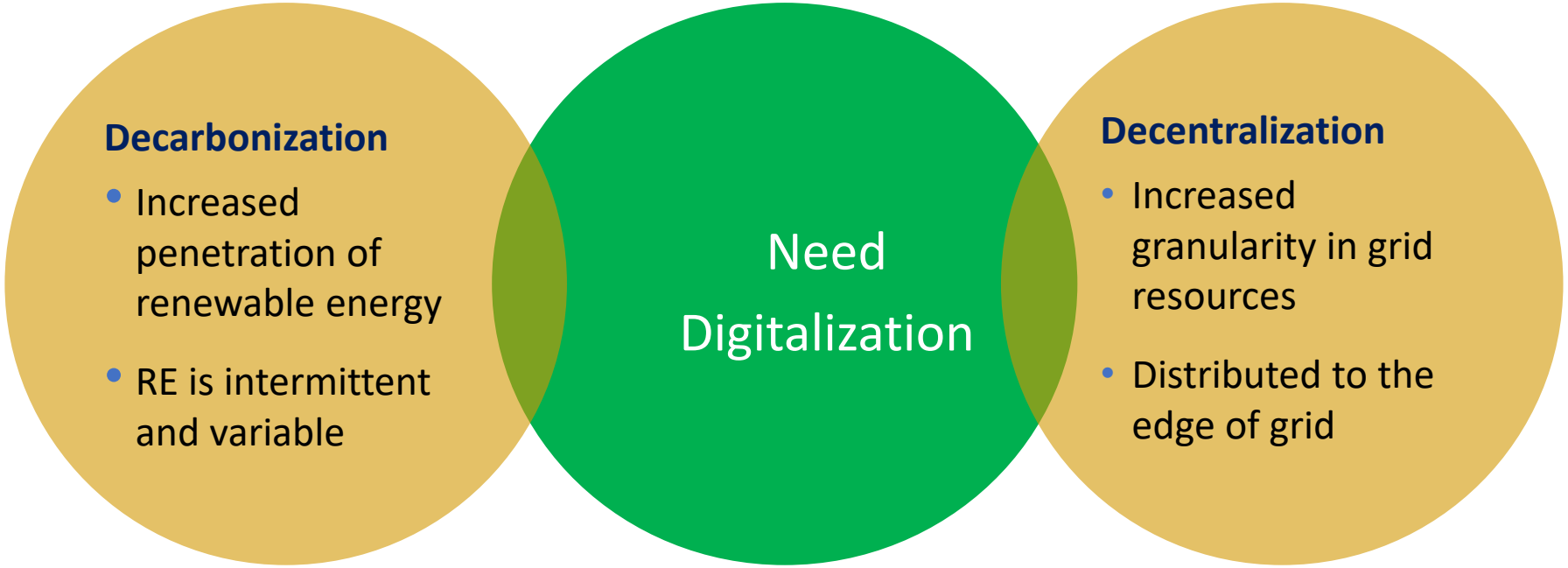
The electric grid is now transitioning to its fourth version .

- **Grid 1.0**– Localized generation and distribution – Local Grid.
- **Grid 2.0**– Inter-connected and dispersed generation resources through transmission system - Connected Grid.
- **Grid 3.0**– Convergence of electric network with information and communication network. - Smart Grid
- **Grid 4.0**– Decarbonized, Decentralized and Digitalized Grid – Digital Grid.

Digital Grid is next to Smart grid

A fundamental shift in the global energy landscape.
Decarbonisation, Decentralisation, and Digitalisation are transforming the future of the power sector.

Central is Digitalization



Digitalization causes cybersecurity issue.

Low Frequency High Impact Events

Availability **Integrity** **Confidentiality**

Trojan horse Black Energy – Ukraine Power System.

An electrical power station in Ukraine's was targeted. Affected colossal impact on eighty thousand (80,000) people at risk by putting them in the dark.

Stuxnet – Iran Nuclear facility

Targeted the Supervisory Control and Data Acquisition (SCADA). A misbehaving functional command injected in PLC of SCADA. Caused damages to thousands of centrifuges of nuclear establishment

WannaCry Ransomware – Many

A devastating programme WannaCry Ransomware caused a global cyber-attack on well-known organisations, including Renault, FedEx and crashed thousands of regular users' computers.

People Process Technology

Technology – No problem – Quite Objective

People & Process need attentions – They are subjective

People

Awareness

- Responsibility of all.
- Culture of being aware.
- Culture of questioning attitude.
- Sense of ownership.
- Sense of responsibility.
- Awareness of rules & policies.

Mock Drills

- Periodic mock drills.
- Pre-informed.
- Surprise.
- Analysis – missing actions.

Continuous Training

- Simple and practical training.
- Repeat to reinforced learnings.
- Policy for action on wrong doing.
- Cybersecurity to be a mainstream job.

Process

Policies & Procedures

- Cyber Security policy.
- Use policy
- Asset disposition procedure.
- Password Policy.
- Internet usage policy.
- Email policy.
- Back-up procedure.
- ISO 27001 compliance

Organizational

- Cybersecurity as mainstream.
- Cyber risk approach.
- Support new initiatives.
- Commit resources.
- Regular board agenda on status, events and actions.
- Map business risks with cyber attack. Need not to dig technical details.
- Avoid over compliance.

Leading in Crisis

- Lead instead of fault finding.
- Digital Stewardship.
- Inculcate confidence in working staff.
- CISO as coordinator not the only responsible person.
- Cybersecurity is responsibility of all.
- Manage attack surface.

Use Case/Case Study

- Case of Ransomware Attack on One of the control center in India
- Integration of control center data from outside country

Recommendations

- Minimize number of interfaces and paths with enterprise network. Use of unidirectional security gateways. **Every new path through a firewall is an attack vector.** **Monitor Attack Entry.**
- Use of segmented network for digital systems. Different zones per security requirements. **Manage attack surface.**
- Allow minimal required traffic between zones. **Fortified attack path**.
- Be aware most cyber attacks starts with intrusion from enterprise network. **Monitor connected enterprise network.**
- Think of cyber risks in the context of the business risks that cyberattacks can cause. **Make it a part of ERM.**
- Treat cyber security as mainstream business function. **Make it responsible to the board**

Key Takeaways

- Human element is the strongest link but weakest if not aware. Awareness training is the key.
- Adversary need to get entry to your control system for a successful cyber attack. Protect and monitor all entry points.
- Early detection and quick response prevents from further consequences. Security Operation Center enables it.
- A risk-based approach to cyber security enhances the involvement of decision maker. Make it a part of regular board agenda.
- View cybersecurity controls from the perspective of the business activities they protect. Understandable by board members.

Thank You

For discussions/suggestions/queries email: www.indiasmartgrid.org
www.isgw.in
Links/References (If any)

P.K. Agarwal

You can find me at

@pkagar
~/pkagar
pkagarwal@gmail.com
www.pkagarwal.info

India Smart Grid Forum
CBIP Building, Malcha Marg,
Chanakyapuri,
Delhi-110021
Website: www.indiasmartgrid.org