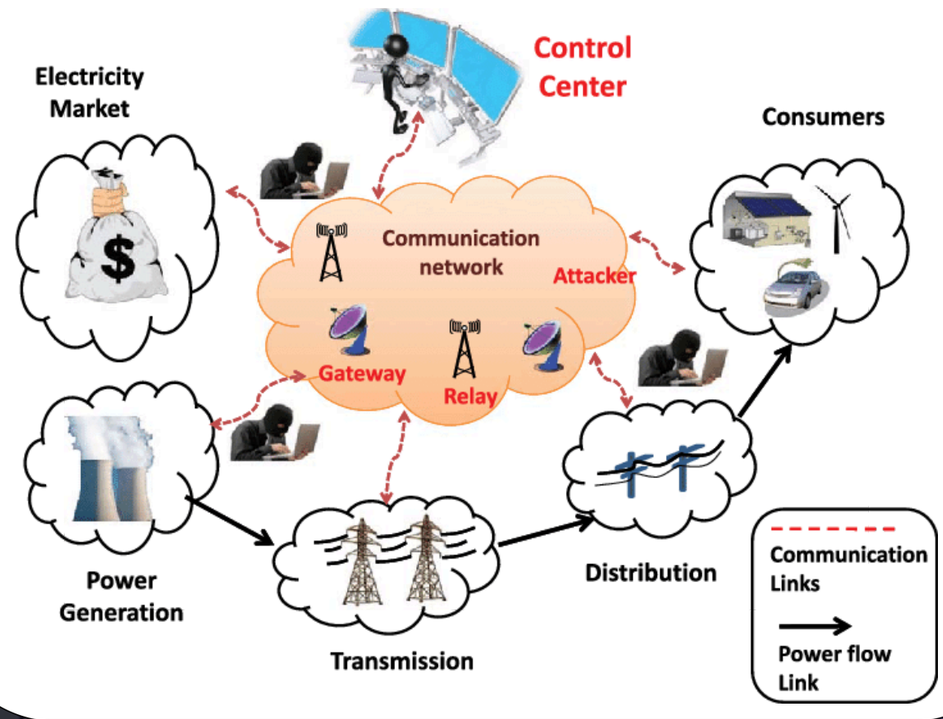
POWERGRID
CENTER OF EXCELLENCE
IN CYBER SECURITY

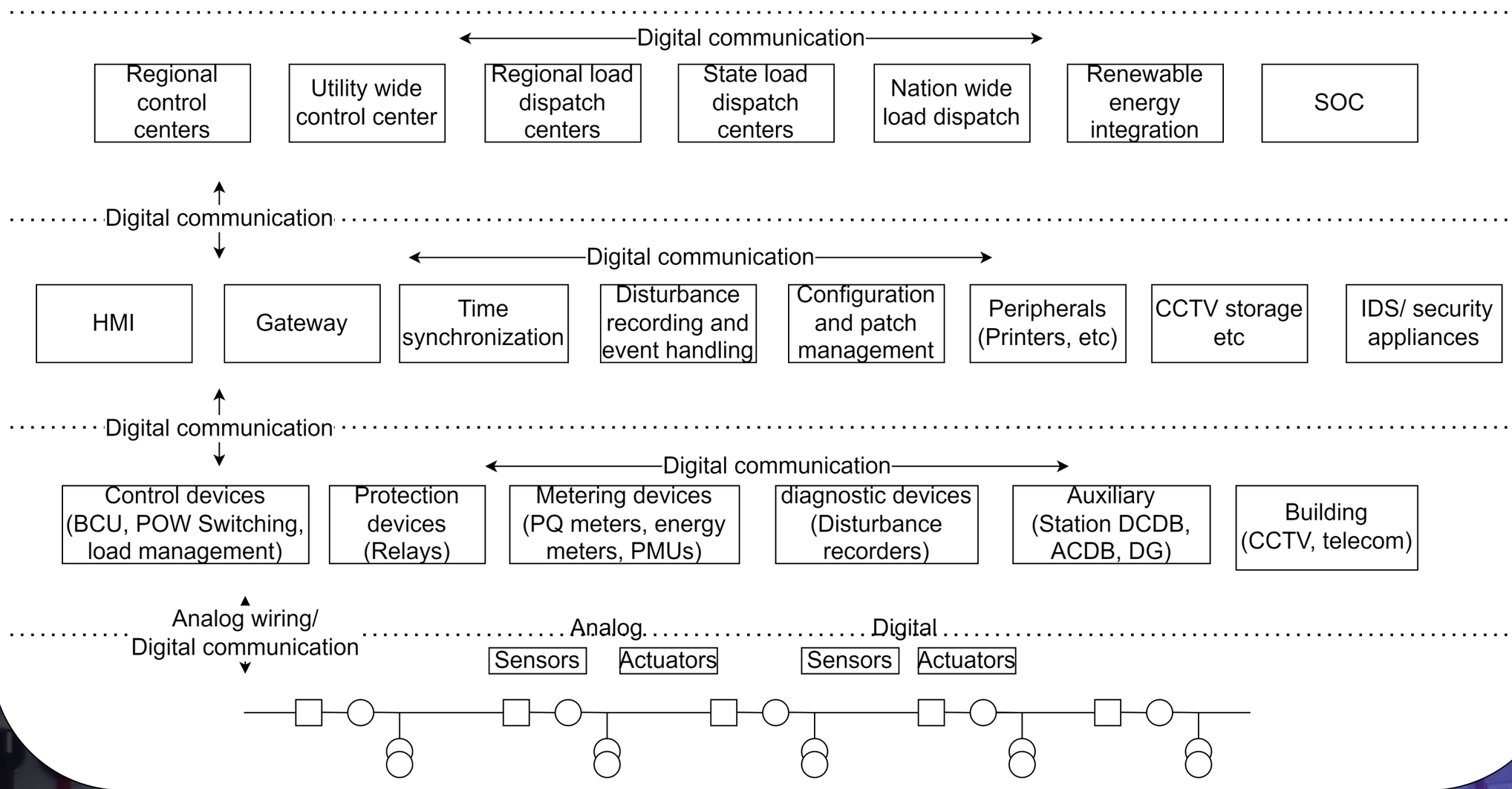
# PowerGrid Center of Excellence in Cyber Security

## Need for Cyber security of OT systems in Power grid




## Types of Attacks


## Existing Infrastructure




## Center of Excellence: Offerings

**Problems from utilities, main stream research, and Advisory board - Present and future challenges and measures**

**Risk and Vulnerability assessment of Communication Infrastructure**

- Artificial intelligence
- Machine learning
- Big data analytics
- Issue identification and Protection

**OT Security management**

- Compliance mechanism
- Audit mechanism and conformance
- Research Threat landscape
- Asset management

**OT Security Framework**

- Testing
- Supply chain risk mitigation
- Intrusion detection solution
- Network Monitoring

**OT Security analytics / event management**

- Forensic data analytics
- Anomaly detection

**OT Security capacity building**

- Skill development
- Training
- Workshops
- Seminar
- Academic
- Indsutry

Get in touch with us on :

# PowerGrid Center of Excellence in Cyber Security

POWERGRID
CENTER OF EXCELLENCE
IN CYBER SECURITY

## Advanced Cyber Physical Modelling Framework for Contingency Planning

1. Assessment of risk from automation system on the power system operations

2. Asset mapping of critical infrastructure

## Test bed for evaluation of Cyber Security of operations

1. Development of Realistic Testbed

2. Development of the synthetic test simulators for IEC 104 and IEC 61850, extended to make a test bed manager

## Machine Learning models based Intrusion / Attack detection and mitigation systems

1. IDS and knowledge base Framework

2. Application of AI / ML in the context of OT Security

## Cyber security in Substation Automation System - Hardware / software / firmware / communication threats on Intelligent Electronic Devices (IEDs)

1. Testbed for device testing on cybersecurity

2. Appliance for securing operations in utility automation

3. Cyber security Threat Landscape in the power transmission and grid operation

## Embedded Systems Security of Field Devices

**a) Electronic Component Analysis to identify the design weakness and hardware Trojan analysis of PCBs**

**b) Field Technician Interface Analysis to identify weak points like port or physical interfaces**

**c) Firmware Binary Analysis to identify vulnerabilities**

1. Analytics based on the CVE list

2. Detection of Vulnerabilities in Firmware Images