GIAN Short course

Cyber-Physical Security for the Smart Grid

Indian Institute of Technology, Bombay, India

Coordinator: Prof. R. K. Shyamasundar

Manimaran Govindarasu

Dept. of Electrical and Computer Engineering

Iowa State University

Email: gmani@iastate.edu

http://powercyber.ece.iastate.edu

March 5-16, 2018

Course Agenda

Day 01	• Module 1: Cyber Threats, Attacks, and Security concepts
Day 02	• Module 2: Risk Assessment and Mitigation & • Overview of Indian Power Grid
Day 03	• Module 3: Attack-resilient Wide-Monitoring, Protection, Control
Day 04	• Module 4: SCADA, Synchrophasor, and AMI Networks & Security
Day 05	• Module 5: Attack Surface Analysis and Reduction Techniques
Day 06	• Module 6: CPS Security Testbeds & Case Studies
Day 07	• Module 7: Cybersecurity Standards & Industry Best Practices
Day 08	• Module 8: Cybersecurity Tools & Vulnerability Disclosure
Day 09	• Module 9 : Review of materials, revisit case studies, assessments
Day 10	• Module 10: Research directions, education and training

Module 2:
Risk Assessment and Mitigation

Risk Assessment and Risk Management Process

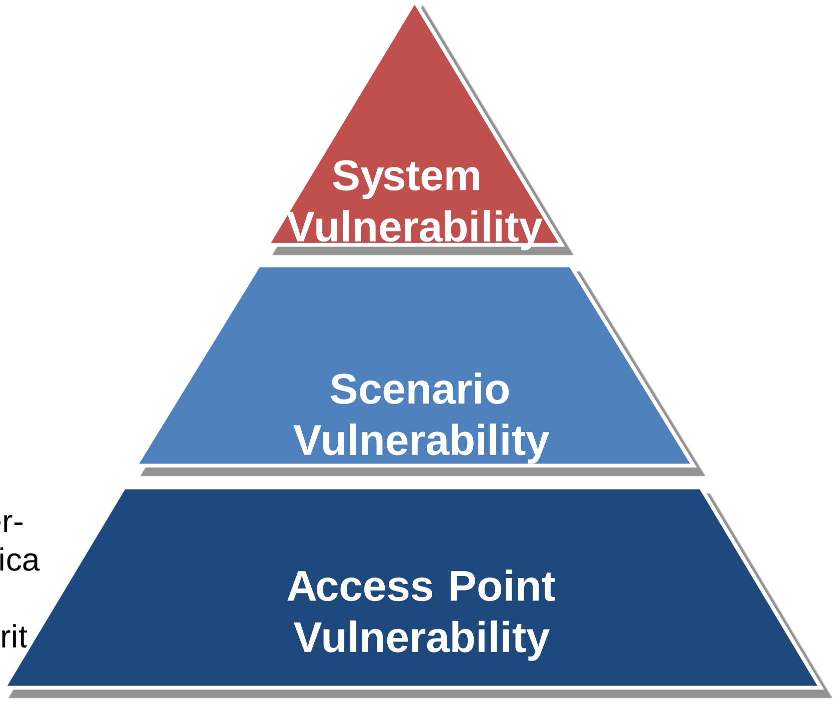
Qualitative and Quantitative Risk Assessment

Risk Mitigation process overview

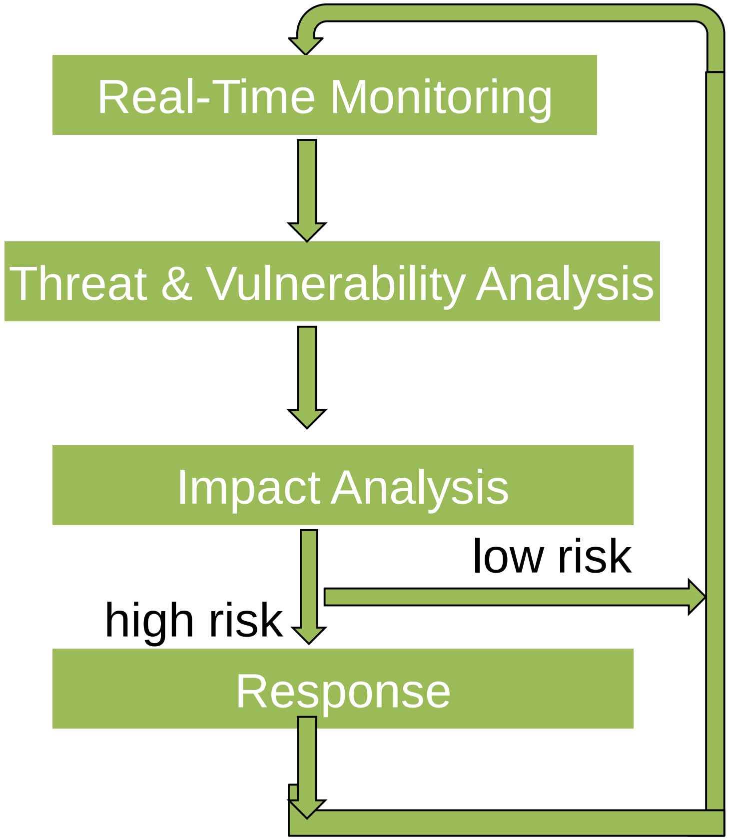
2.1 Risk Assessment and Risk Management Process

Risk Modeling and Mitigation Framework

- **Risk Assessment & Risk Mitigation**
- **Security Investment Analysis**



Hierarchical modeling



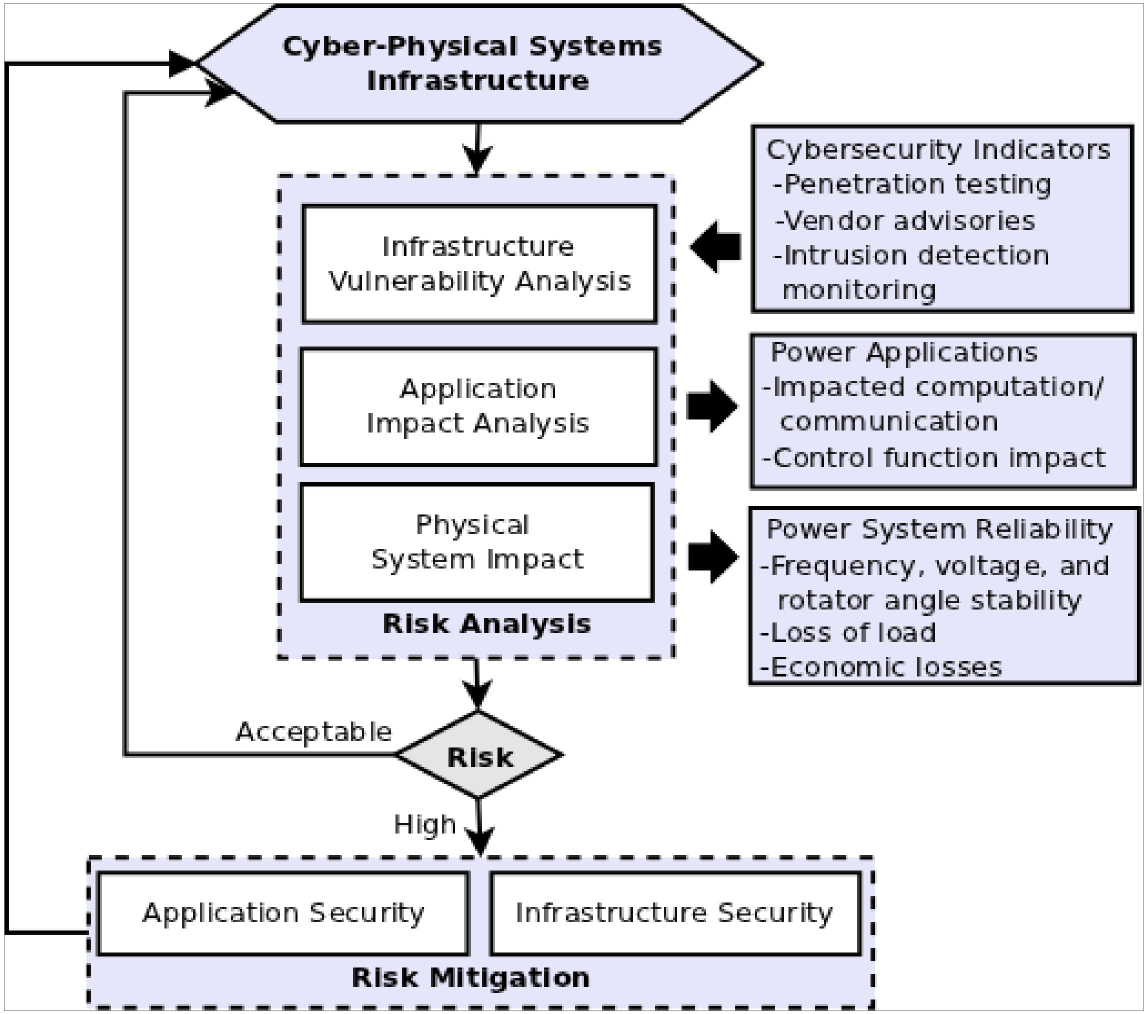
Cyber Risk

Risk = Threat X Vulnerability X Impacts

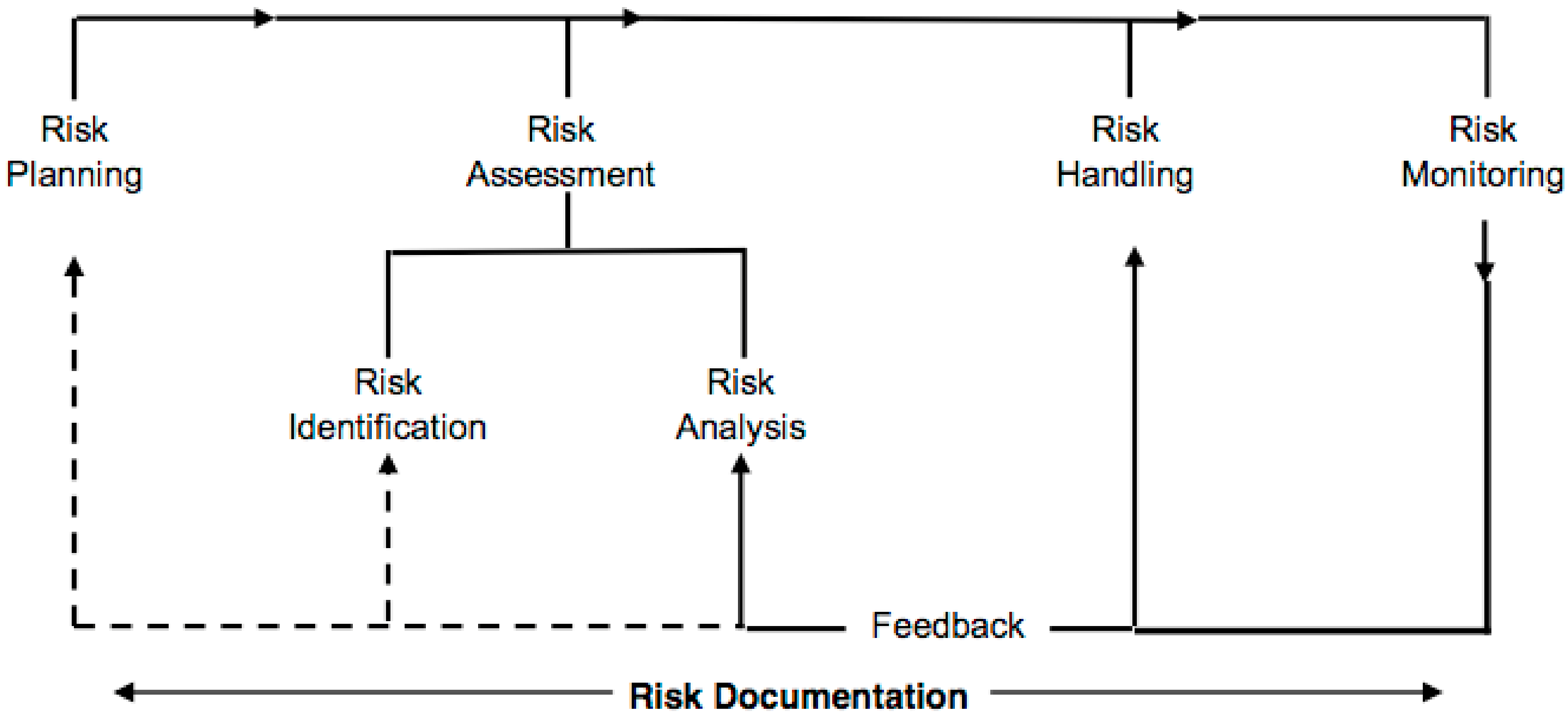
- Risk: Probability (likelihood) of a certain event happening multiplied by the consequence (impacts) of that event
- Event Probability: probability that an adversary exploits vulnerability in the cyber system
- Impacts: the consequence of the event in terms of load loss, equipment damage, stability violation, blackout, or economic loss
- Enumeration of all the plausible events to determine associated risks
- Modeling the threat is not well understand; it's still an art than science.

Risk Assessment & Mitigation

Risk = Threat x Vulnerability x Impacts

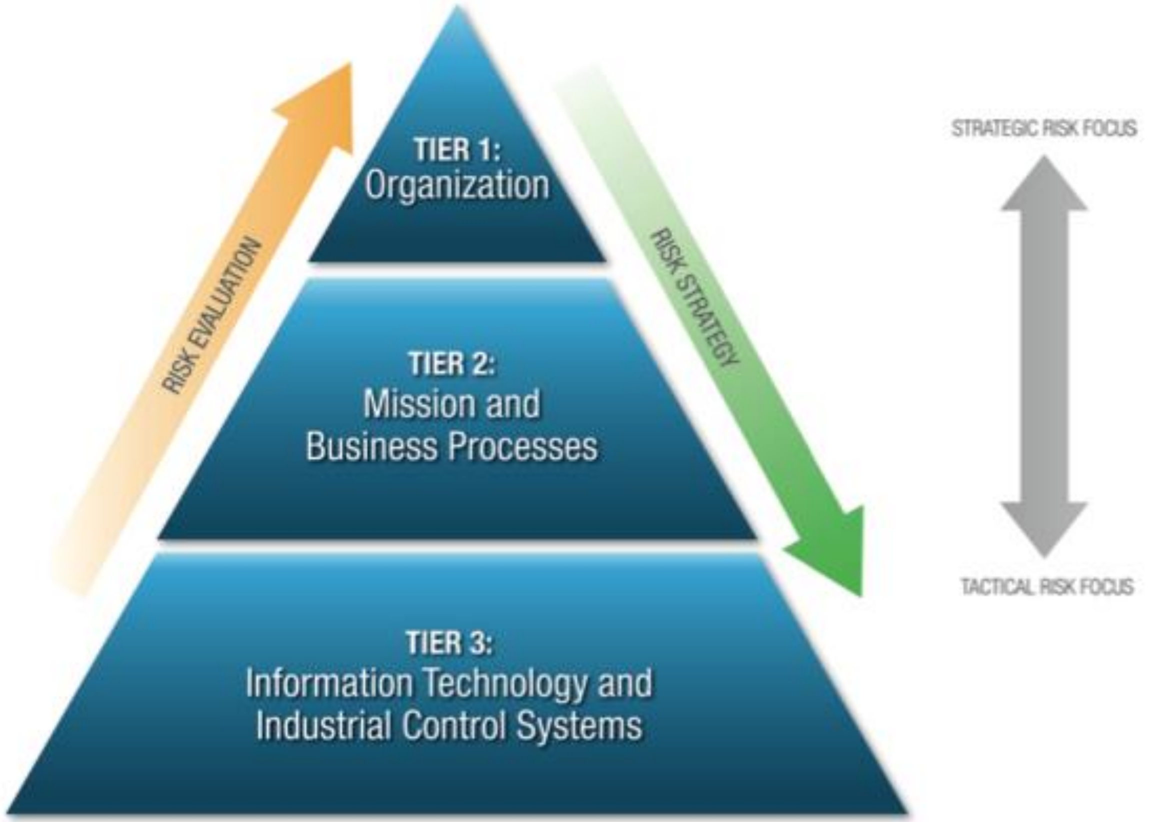


Risk Management Process



Source: **Risk Management Guide, DOE Jan 2011**

Hierarchical Risk Management Model



Source: **ELECTRICITY SUBSECTOR CYBERSECURITY RISK MANAGEMENT PROCESS, DOE May 2012**

Risk Management Process Overview

	TIER 1	TIER 2	TIER 3
RISK FRAMING	**Section 3.1** Produce a set of organizational policies, governance structure, and guidance that form the basis for the Risk Management Strategy	**Section 4.1** Establish risk assessment methodology and define the cybersecurity components of the enterprise architecture	**Section 5.1** Develop the cybersecurity plan that identifies the components, systems, hardware, and software of the IT and ICS
RISK ASSESSMENT	**Section 3.2** Determine risk to an organization's operations	**Section 4.2** Develop prioritized list of mission and business processes	**Section 5.2** Conduct risk assessment and develop cybersecurity risk assessment report
RISK RESPONSE	**Section 3.3** Decide on the appropriate courses of action to accept, avoid, mitigate, share, or transfer risk.	**Section 4.3** Using the prioritized list of processes, establish cybersecurity program and architecture	**Section 5.3** Develop and implement risk mitigation plan
RISK MONITORING	**Section 3.4** Determine the ongoing effectiveness of risk response measures	**Section 4.4** Measure the effectiveness of and level of conformance with the cybersecurity architecture	**Section 5.4** Monitor changes and measure effectiveness of cybersecurity controls

Source: **ELECTRICITY SUBSECTOR CYBERSECURITY RISK MANAGEMENT PROCESS, DOE May 2012**

2.2 Qualitative and Quantitative Risk Assessment

Qualitative Risk Analysis Matrix

*Combines the **probability** and **consequence** of a risk to identify a **risk rating** for each individual risk.*

- **Risk ratings**
  - Represents a judgment as to the relative risk to the project
  - Categorizes each risk as
    - Low
    - Moderate
    - High

Qualitative Risk Matrix – A sample template

Consequence --> /Probability	Negligible	Marginal	Critical	Catastrophic
Very High	Low Risk (S1)	Medium Risk	High Risk	High Risk
High	Low Risk	Medium Risk (S2)	High Risk (S4)	High Risk
Medium	Low Risk	Low Risk	Medium Risk	High Risk
Low	Low Risk	Low Risk	Medium Risk	Medium/High
Very Low	Low Risk	Low Risk	Low Risk	Medium Risk

Process

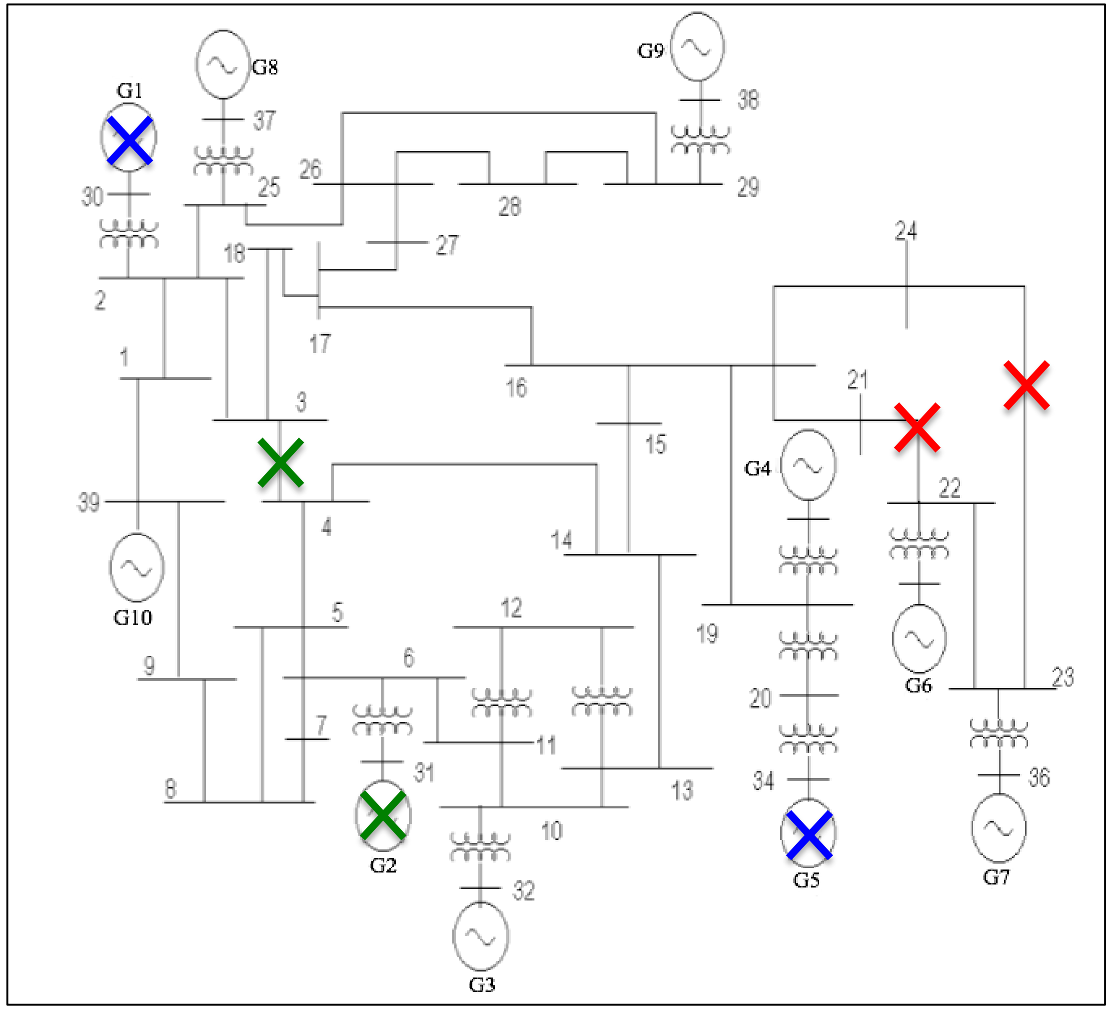
- Domain expert enumerates all the scenarios: S1, S2, S3, S4, …
- Map the scenarios into appropriate cells of the Risk Matrix
- For all scenarios whose "Risk" is higher than acceptable threshold, mitigation must be done

- Risk mitigation: either by reducing the probability or the severity of consequence; or both
- Cost-benefit needs to be accounted in risk mitigation

Risk Evaluation – Example

Risk = Threat x Vulnerability x Impacts

Attacker can control: Space: where to attack? Time: when to attack?



Evaluating $\mathcal{G}$ – Impact Estimation

- Coordinated Attack Groups
  - ✓ Gen + Gen
  - ✓ Gen + Trans
  - ✓ Trans + Trans
- Optimal power flow simulation
- $\mathcal{G}$ = load shedding for OPF solution

Results

X → $\mathcal{G}$ = 363 MW

X → $\mathcal{G}$ = 163 MW

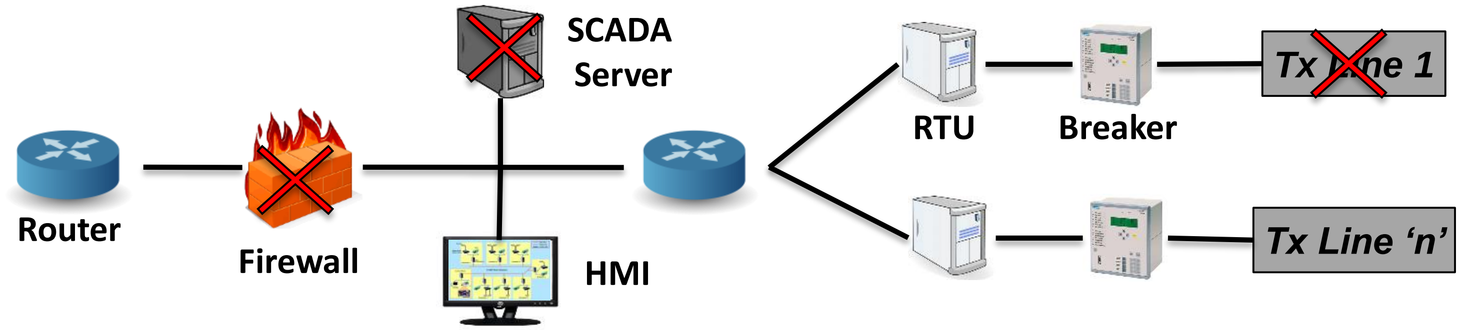
X → $\mathcal{G}$ = 110 MW

Coordinated Cyber Attack Scenarios

Attack Type	***Attack vectors***	***Attack Target***	***Impacted Application***	***Coordination***	***Impacts***
Data Integrity	Via SCADA network, RTU, IED access	SCADA status and analog measurements	State Estimation (**Wide – Area Monitoring**)	Space, same time	Poor situational awareness, Line overloads, Market Impacts
Data Integrity, DoS, Combination	Via SCADA network RTU access	Frequency, Tie-line power flow measurements	Automatic Generation Control (**Wide – Area Control**)	Space, same time	Frequency Imbalance, Operational reliability, Market Impacts
Data Integrity and DoS Combination	Via Substation LAN remote access	IEC 61850 GOOSE messages	Remedial Action Schemes (**Wide – Area Protection**)	Space, staggered time	Operational reliability, Potential to cascading outages

Quantitative Risk Evaluation

Risk Estimation Example



- ***Attack Template -*** Tripping two generators in New England 39-bus system

Attribute	*Type*	*Target*	*Variable*	*Timing*	*Impact*
Attack 1	Fabricate	FW + SCADA Server	Gen 1 status	Simultaneous	Load Shedding
Attack 2			Gen 5 status		

- ***Result :***

$$\pi(Gen_1 + Gen_5) = 0.03 * 0.01 = 0.0003$$

$$\lambda = LoadShed = 163MW$$

$$\boxed{risk = 0.0003 * 163 = 0.0489}$$

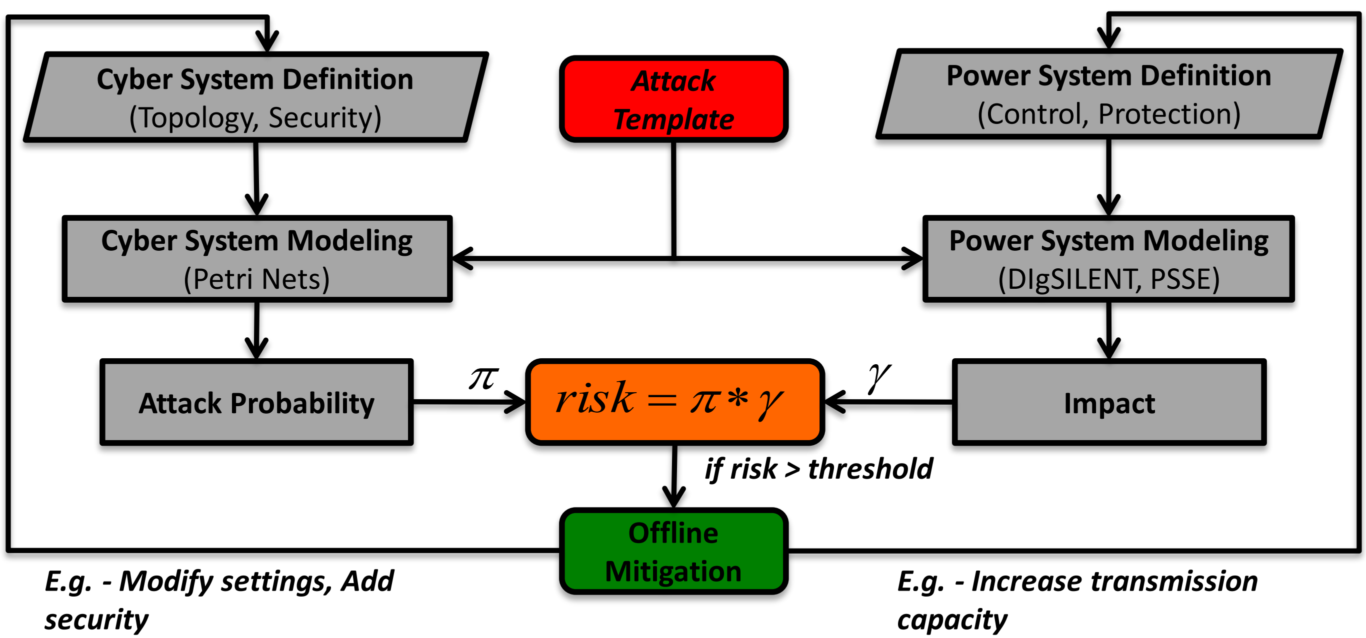
S. Sridhar, G. Manimaran, C-C. Liu, Risk Analysis of Coordinated Cyber Attacks on Power Grid, chapter in edited book "Control and Optimization Methods for Electric Smart Grids," Springer Series on Power Electronics and Power Systems, Vol. 3, 2012.

Risk modeling and mitigation

Mitigation of Coordinated Attacks

- Approach 1 → ***Offline:*** *Risk Modeling and Mitigation*
- Approach 2 → ***Online:*** *Alert Correlation and Mitigation*

Approach 1: Risk Modeling and Mitigation



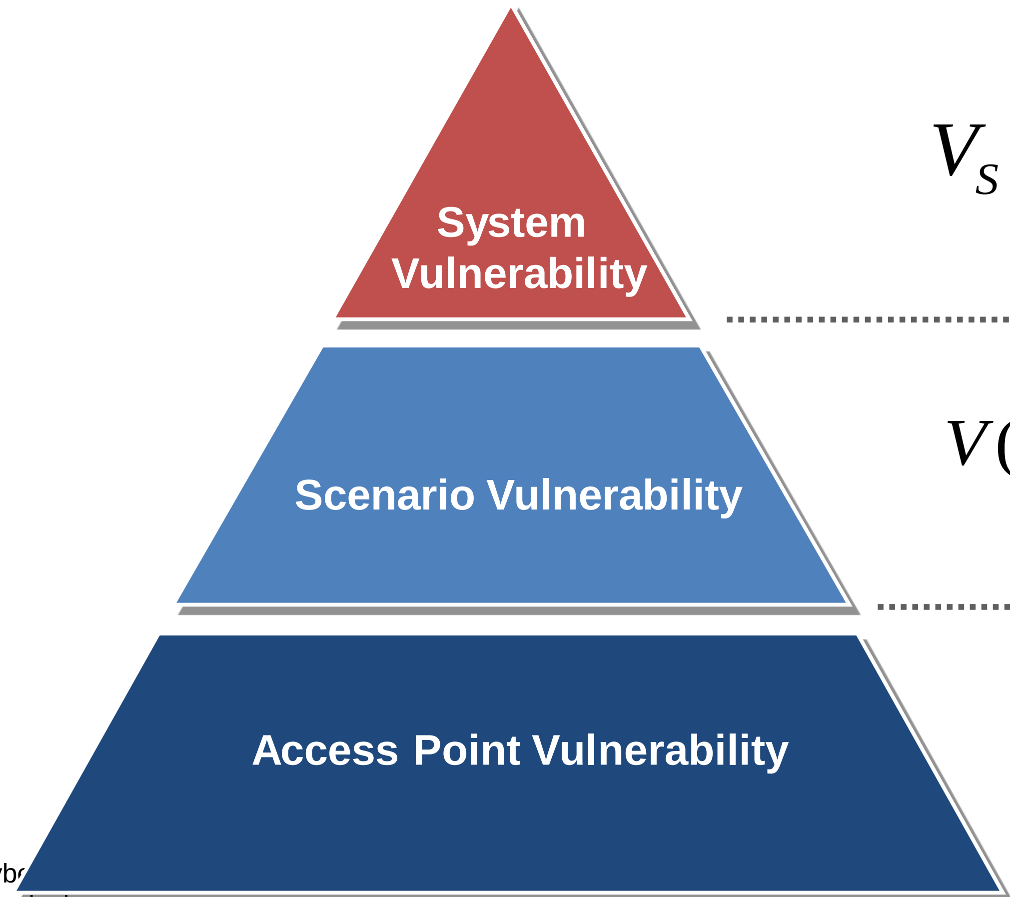
2.2 (a) Quantitative risk assessment - A case study

Source:

Chee-Wooi Ten; Chen-Ching Liu; Manimaran, G., "Vulnerability Assessment of Cybersecurity for SCADA Systems," IEEE Trans. on Power Systems, vol.23, no.4, pp.1836,1846, Nov. 2008.

Risk Modeling of Intrusions …

A hierarchical relationship among ***system***, ***scenario***, and ***access point*** vulnerability



$$V_S = \max\left(V(I)\right)$$

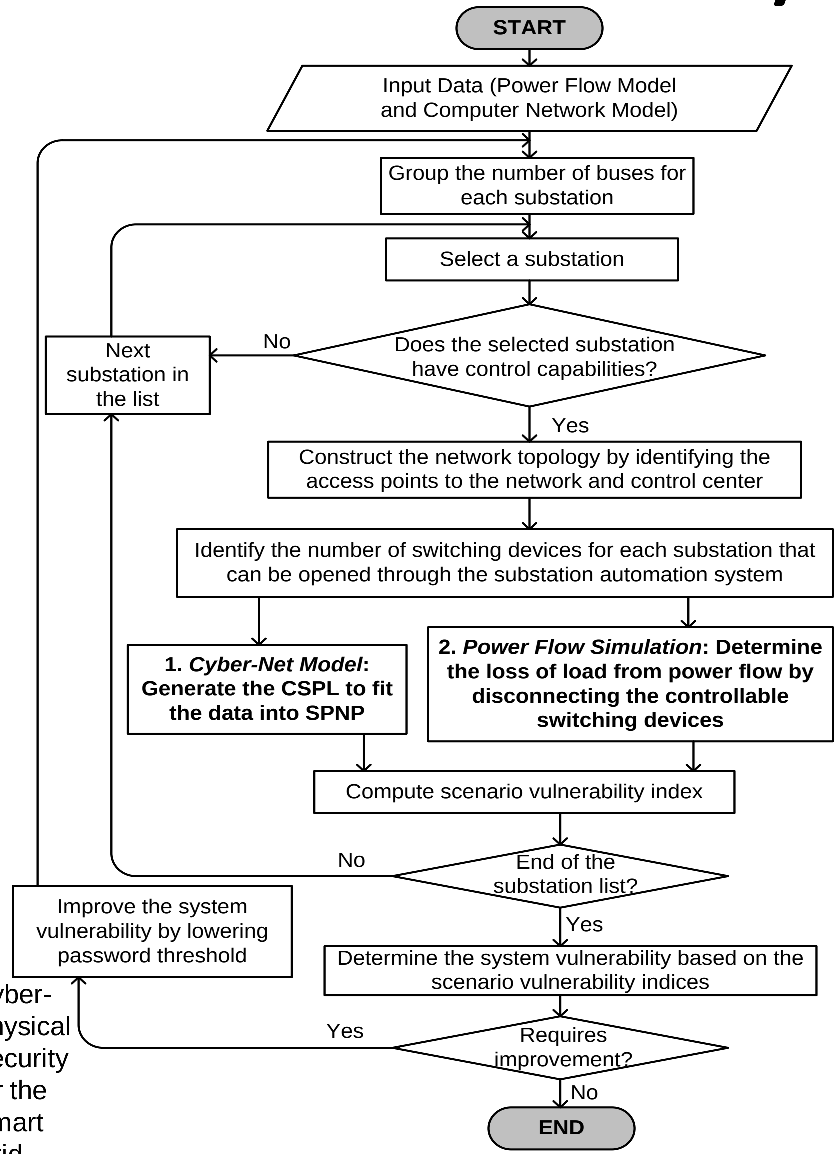
$$V(I) = \{V(i_1), V(i_2), \ldots, V(i_K)\}$$

$$V(i) = \sum_{j \in S} \pi_j \times \gamma_j$$

π_j **Probability of intrusion** thro access point ***j***

γ_j **Impact** due to compromise of substation ***j***

Risk Analysis Framework



Key steps

1. Construct a **cyber-net model**

   - model the access points & associated vulnerabilities

2. Construct a GSPN (Petri Net)

   - compute steady state probabilities (of attacks)

3. Perform **impact analysis** for the most likely scenarios

   - using Power Flow Simulation

4. Calculate Risk

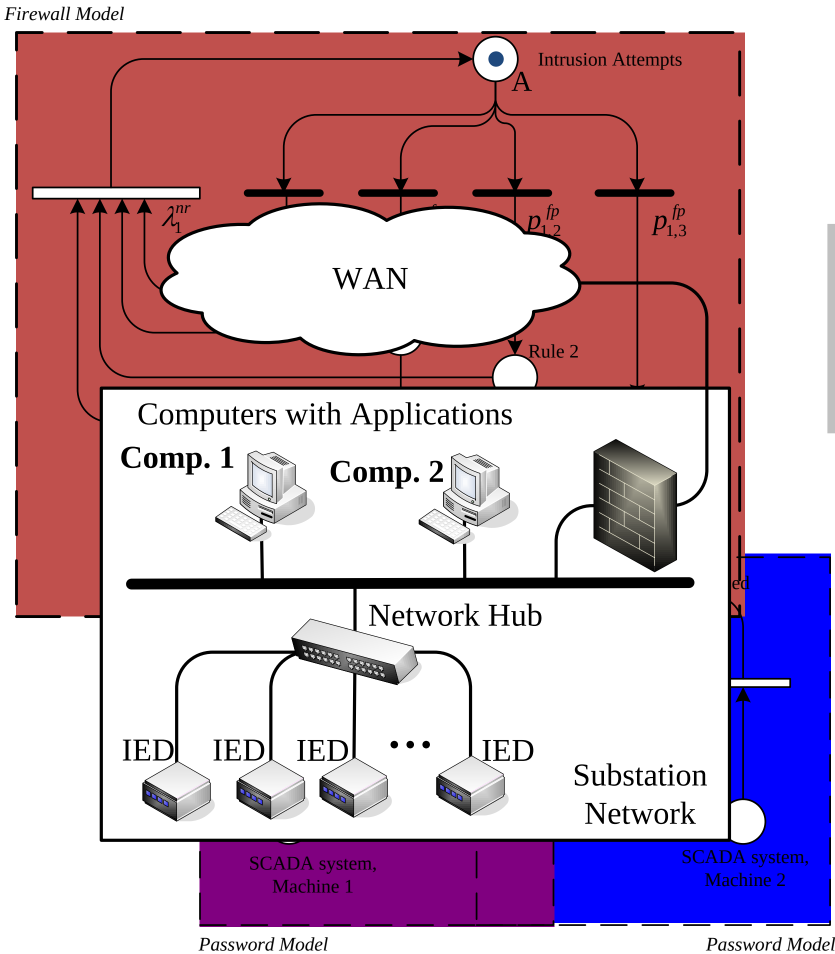
Case Study: PetriNet model of a substation

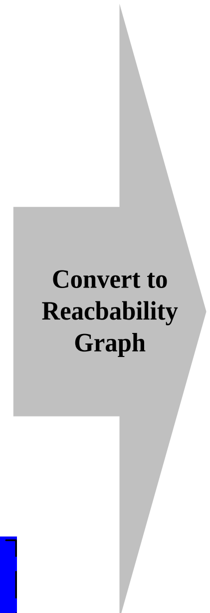
- Substation model consists of
  - Firewall model - one firewall
  - Password model - two machines

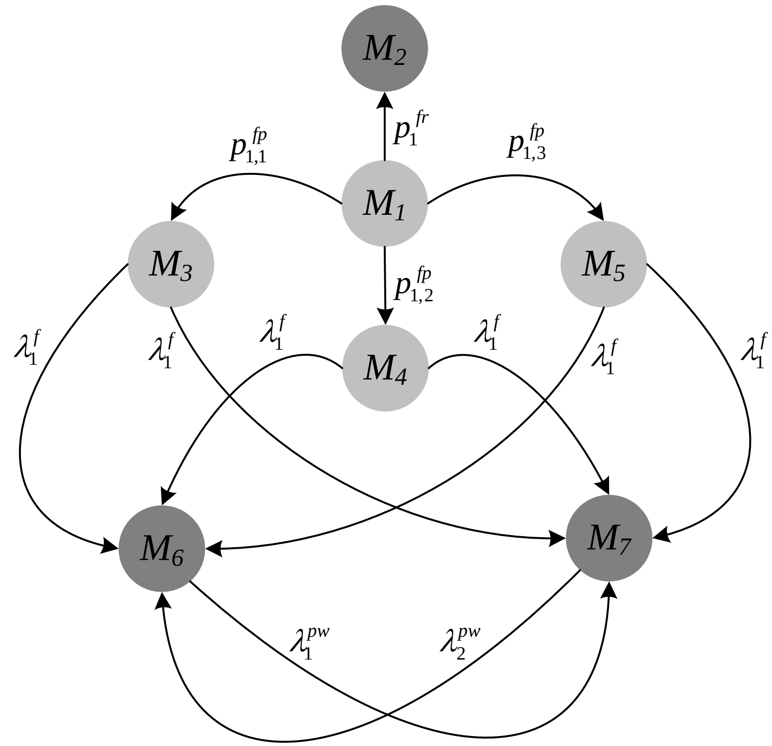
- The cyber-net intrusions are modeled by a GSPN model
- The states of the stochastic process are the status of intrusions to a network that are inferred from the abnormal activities
- These include malicious packets flowing through pre-defined firewall rules and failed logon password on the computer system

- Sample data logs were mined, the values for model parameters (e.g., transition probabilities) were obtained through it

One-Firewall-Two-Machines (substation)







M_1=[1 0 0 0 0 0 0 0]

M_2=[0 1 0 0 0 0 0 0]

M_3=[0 0 1 0 0 0 0 0]

M_4=[0 0 0 1 0 0 0 0]

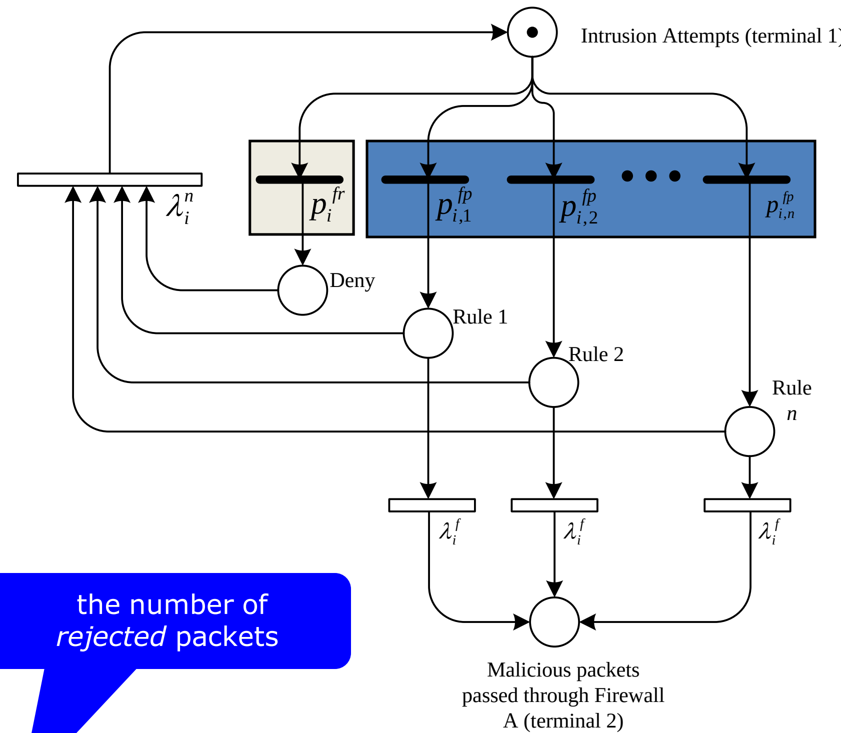
M_5=[0 0 0 0 1 0 0 0]

M_6=[0 0 0 0 0 0 1 0]

M_7=[0 0 0 0 0 0 0 1]

Firewall Model

- **The firewall model depicted** includes ***n*** **paths corresponding to *n* rules** in the firewall model
- The submodel consists of circles that are the states **representing the denial or access of each rule**
- Malicious packets **traveling through policy rule *j* on each firewall *i* is taken into account.**



$$p_{i,j}^{fp} = \frac{f_{i,j}^{fp}}{N_{i,j}^{fp}}$$

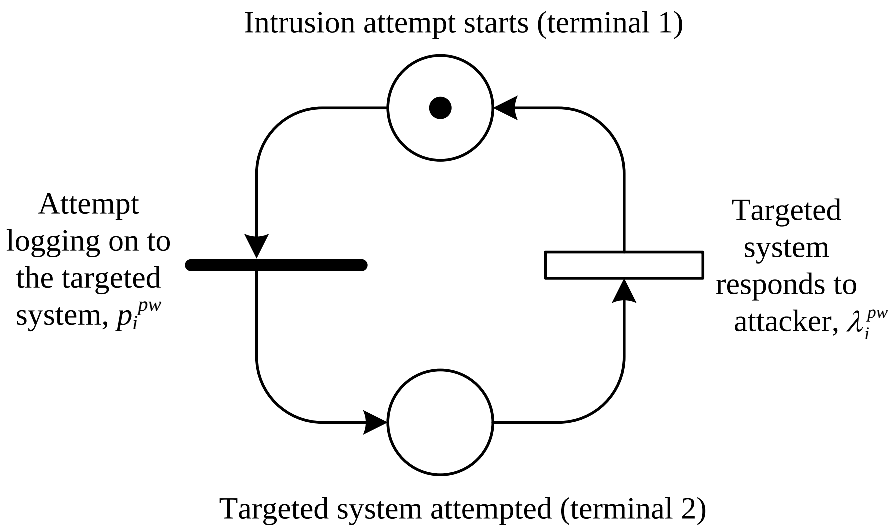
- $p_{i,j}^{fp}$: probability of malicious packets traveling through a firewall rule
- $f_{i,j}^{fp}$: denotes the frequency of malicious packets through the firewall rule
- $N_{i,j}^{fp}$: total record of firewall rule *j*.

$$p_i^{fr} = \frac{f_i^{fr}}{N_i^{fr}}$$

- p_i^{fr}: probability of the packets being *rejected*
- f_i^{fr}: the number of *rejected* packets
- N_i^{fr}: denotes the total number of packets in the firewall logs

Password Model

- The **intrusion attempt to a machine** is modeled by a transition probability associated with a solid bar. An empty bar represents the *processing execution* rate that responds to each attack event
- **An account lockout feature**, with a limited number of attempts, can be simulated by initiating the ***N* tokens** (password policy threshold).



the intrusion attempt probability of a computer system, *i*

$$p_i^{pw} = \frac{f_i^{pw}}{N_i^{pw}}$$

number of intrusion attempts

total number of observed records

Impact Factor Evaluation

Definition of Impact Factor

- Impact factor for the attack upon a SCADA system is:

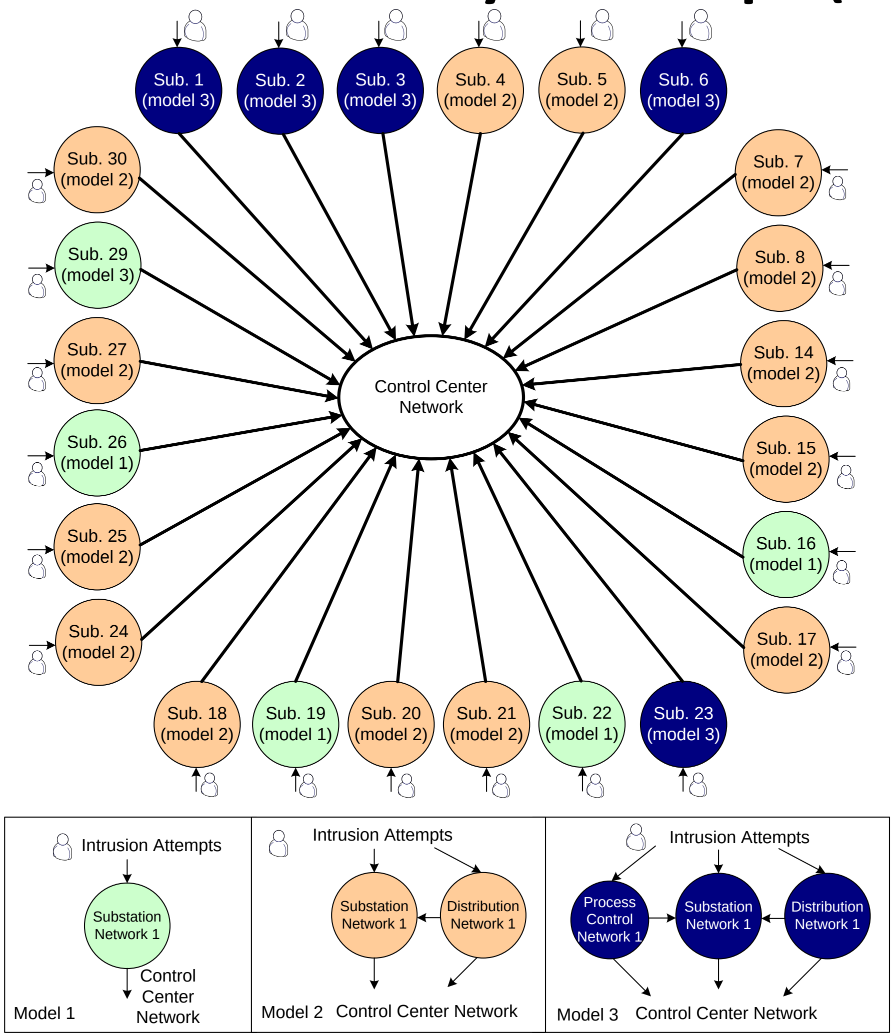
$$\gamma = \left(\frac{P_{LOL}}{P_{Total}} \right)^{L-1}$$

LOL: the loss of load for a disconnected substation

To determine the value of *L:*

- Start with the value of *L*=1 at the substation
- Gradually increases the loading level of the entire system without the substation that has been removed
- Stop when power flow diverges

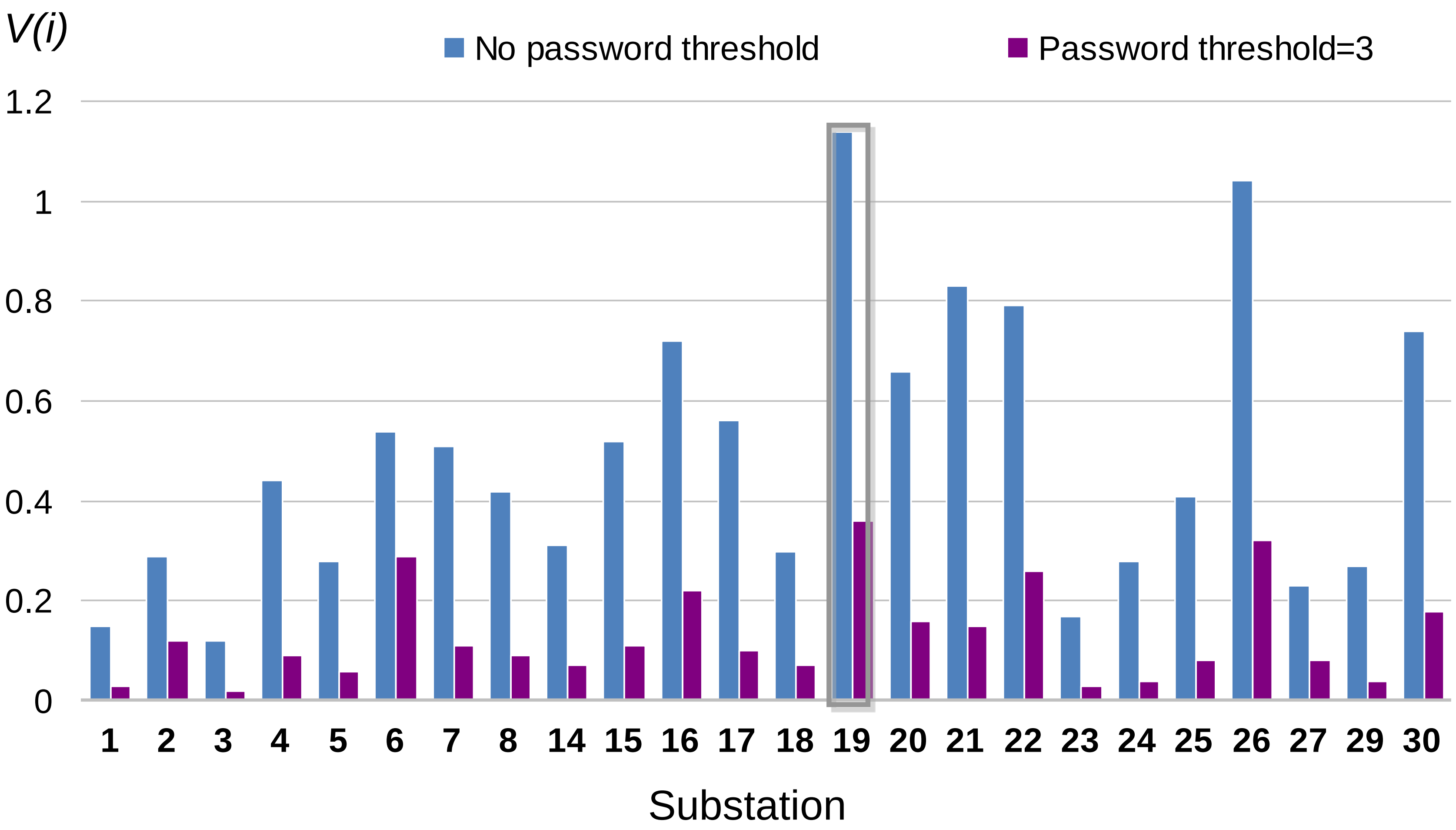
Case Study Setup (IEEE 30 Bus System)



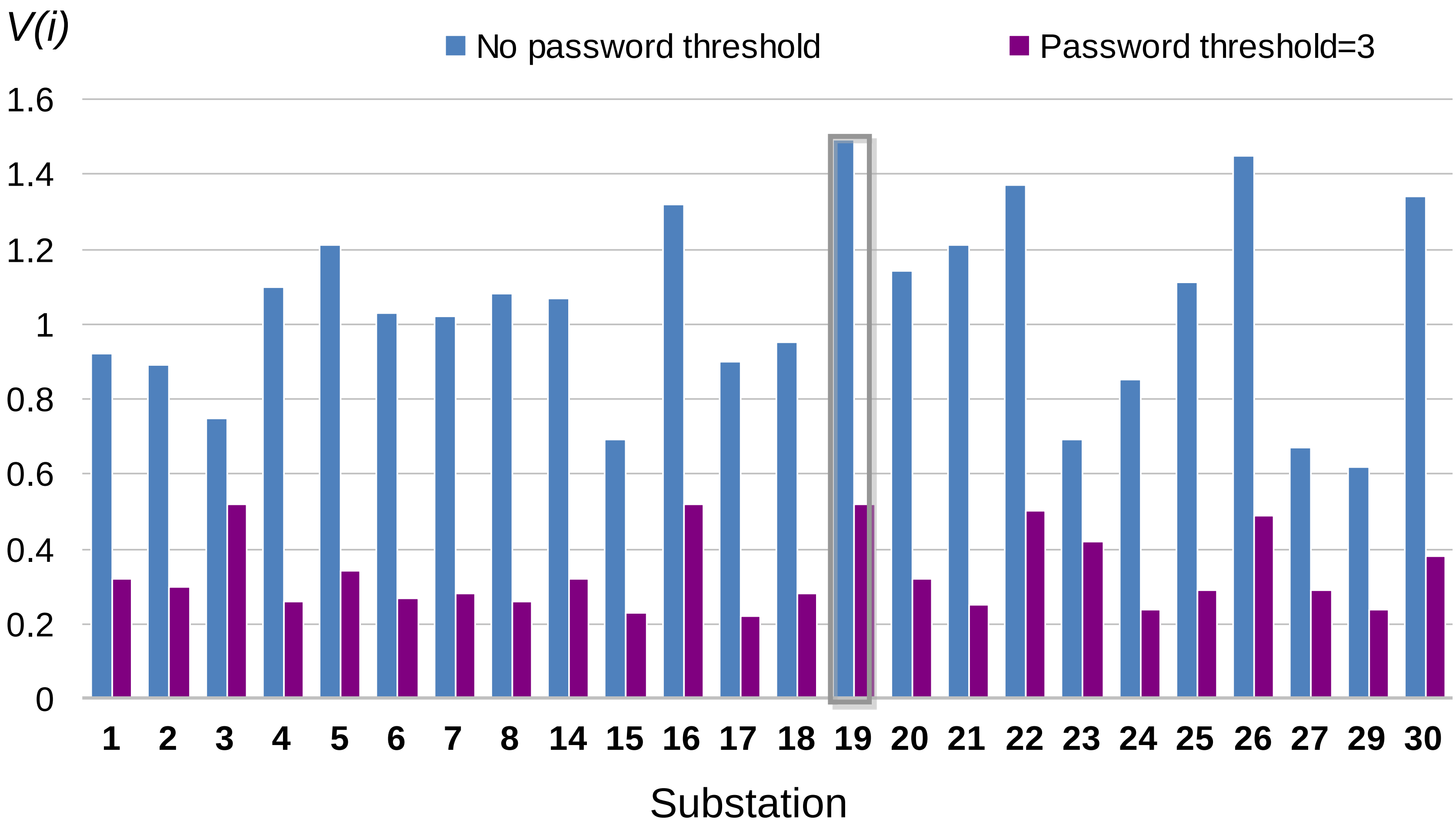
Communication between Control Center and Substation Networks

- **24 Substations** associated to 30 buses
- Model 3: 3 possible access points to the networks
- Model 1 and 2: Without substation network
- Each consists of ***Firewall*** and ***Password*** submodels.
- Two cases for vulnerability evaluations are considered
  - An attack from outside the substation-level networks
  - An attack from within the substation networks

Vulnerability Evaluation - Outside Network

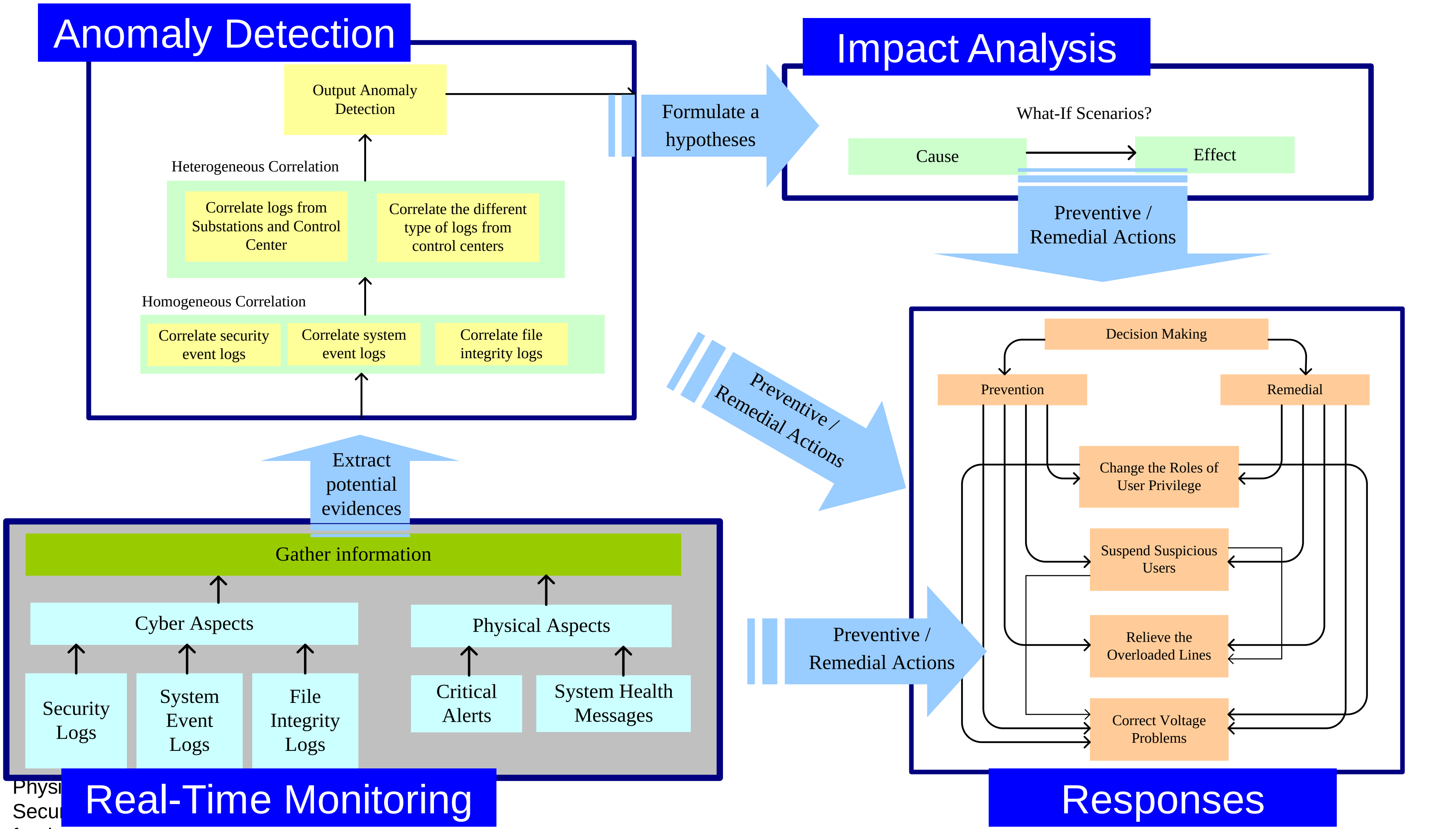


Vulnerability Evaluation - Within Network



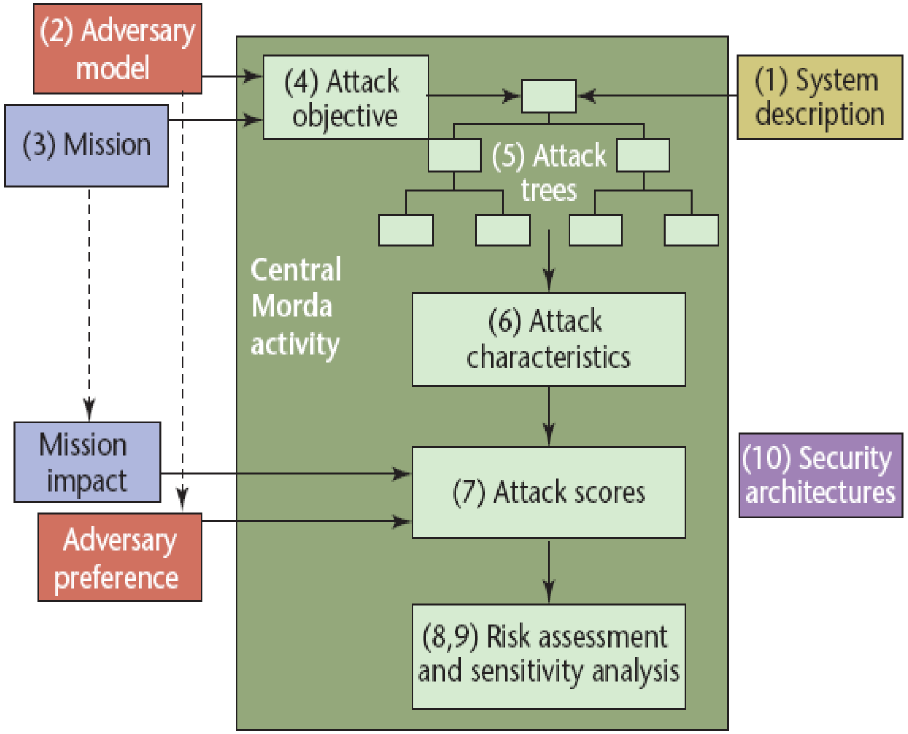
2.3 Risk mitigation

A Real-Time Risk Analysis Framework



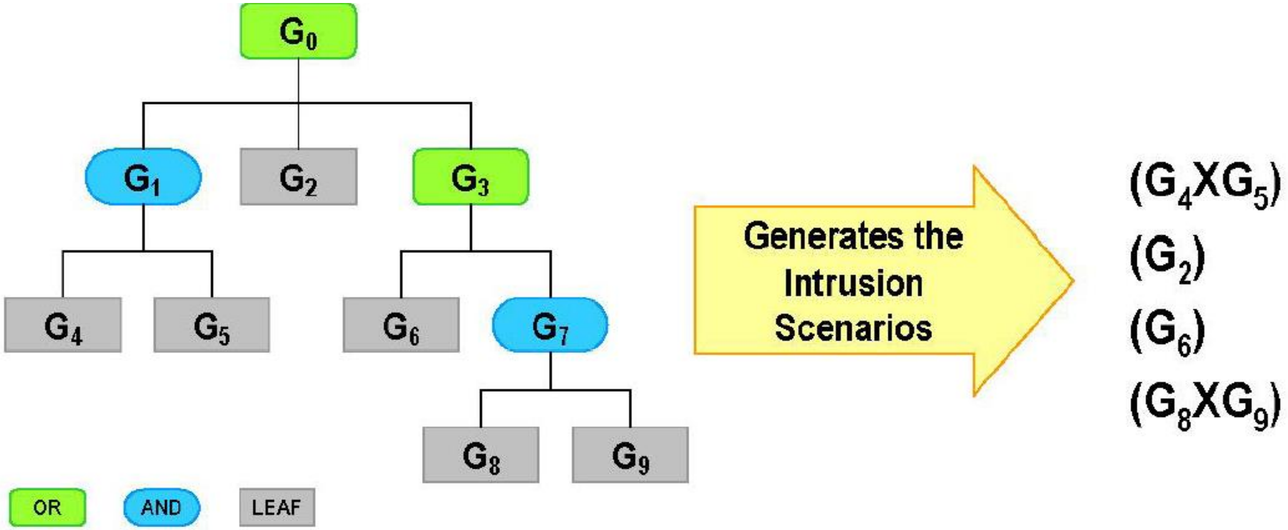
A Mission Oriented Risk and Design Analysis (MORDA)

1	Develop an analysis-focused system description.
2	Define the system threat and model the adversary.
3	Identify relevant missions and impact.
4	Identify adversary attack objectives.
5	Derive attacks to meet adversary attack objectives.
6	Characterize attack steps in terms of parameters that influence the adversary's attack strategy.
7	Calculate attack scores based on attack characteristics adversary preferences, and mission impact.
8	Assess system risk based on calculated scores.
9	Assess sensitivity of input data.
10	Develop security architectures based on risk analysis results.



Attack Trees

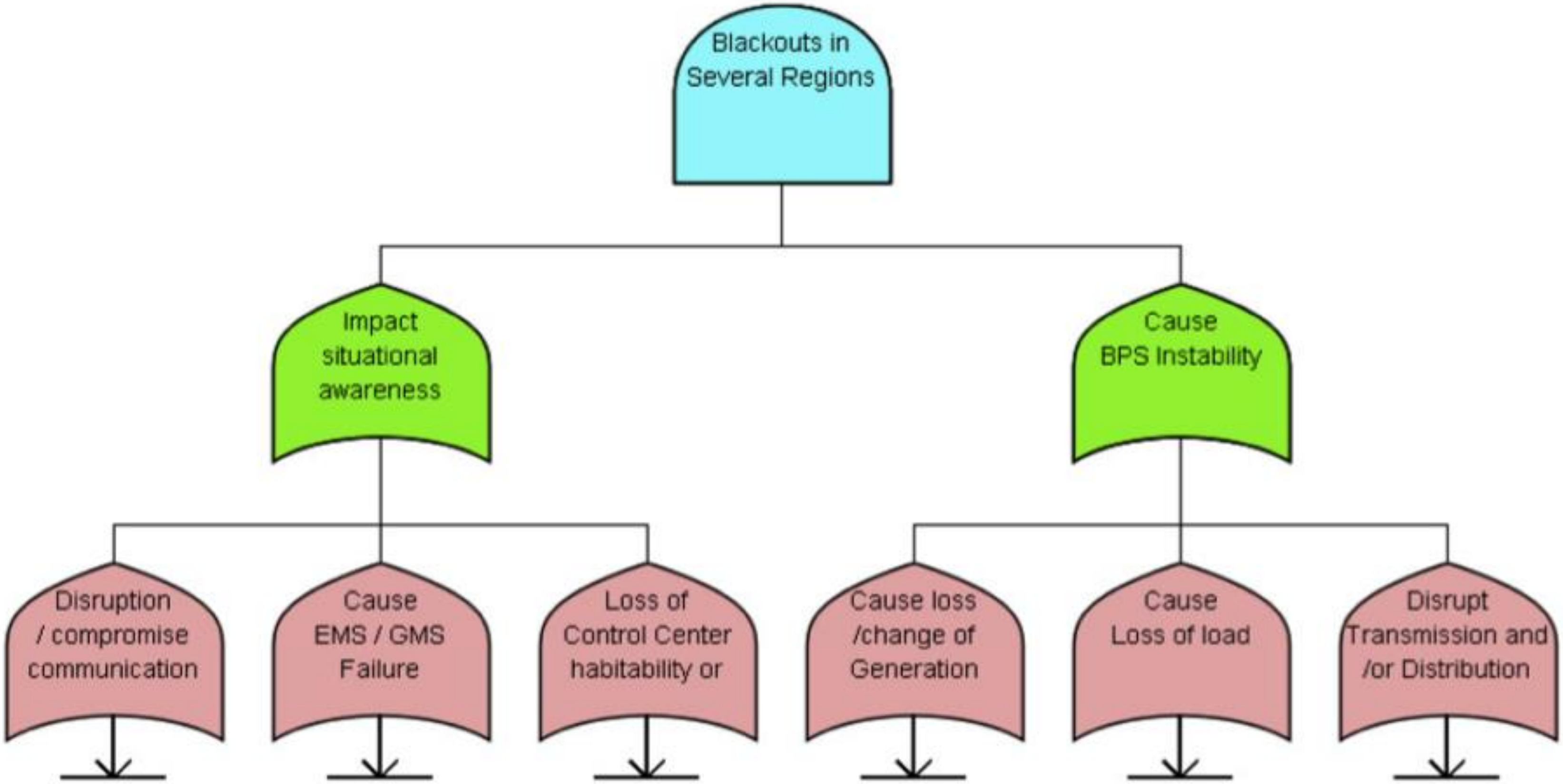
- Graph connects more than one attack leaf from each node
- Consist of multi-level hierarchy in predecessor-successor structure
- Top node is the ultimate goal
- The predecessors of each leaf attributed with "AND" or "OR"



- **G0: mission objective from the attacker's viewpoint.**
- **To compromise G0, one of G1, G2, or G3 needs to be compromised**
- **To compromise sub-goal G1, both G4 and G5 need to be compromised**

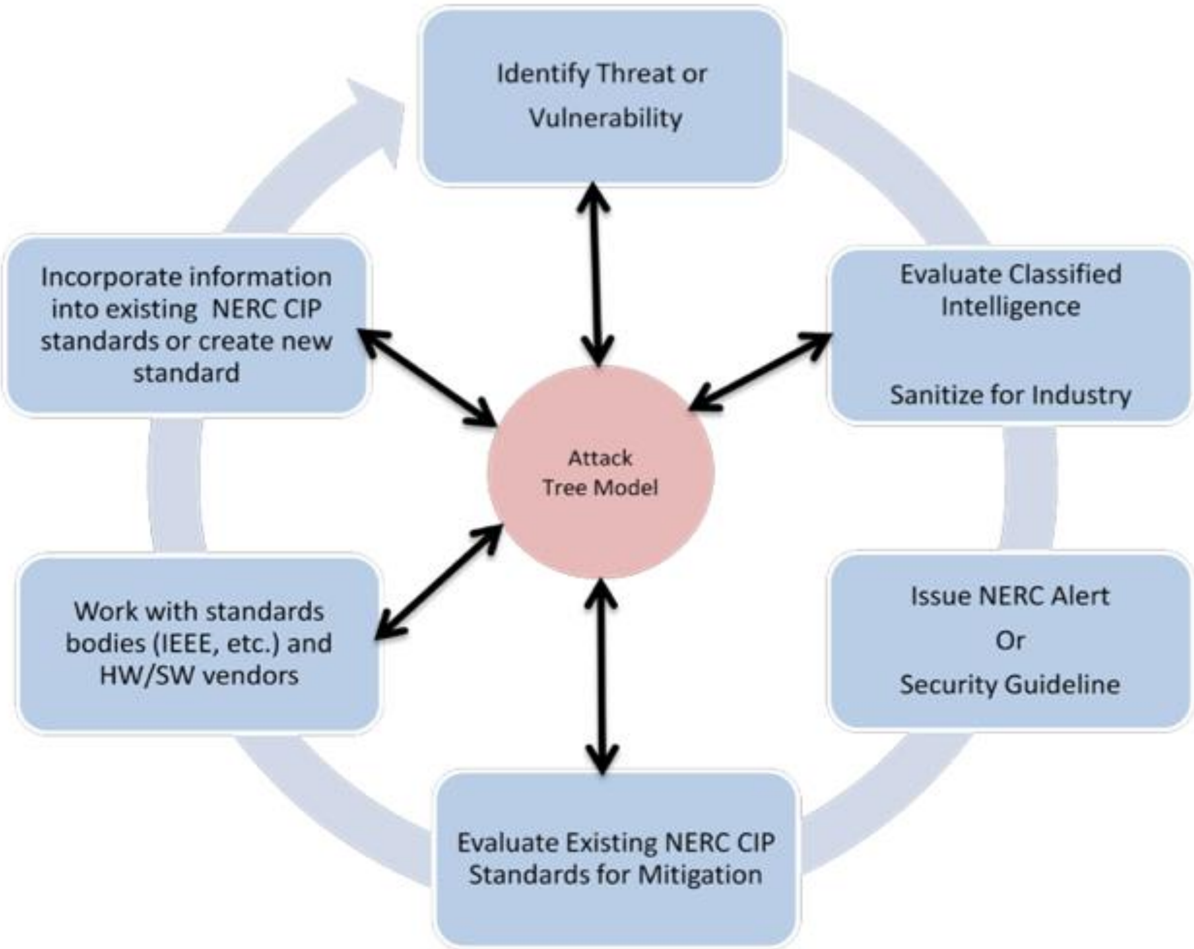
Attack Trees

Attack Tree for HILF Coordinated Cyber Attack (sample)



Source: NERC Cyber Attack Task Force report, May 2012 (www.nerc.com)

NERC CATF Risk Mitigation Framework



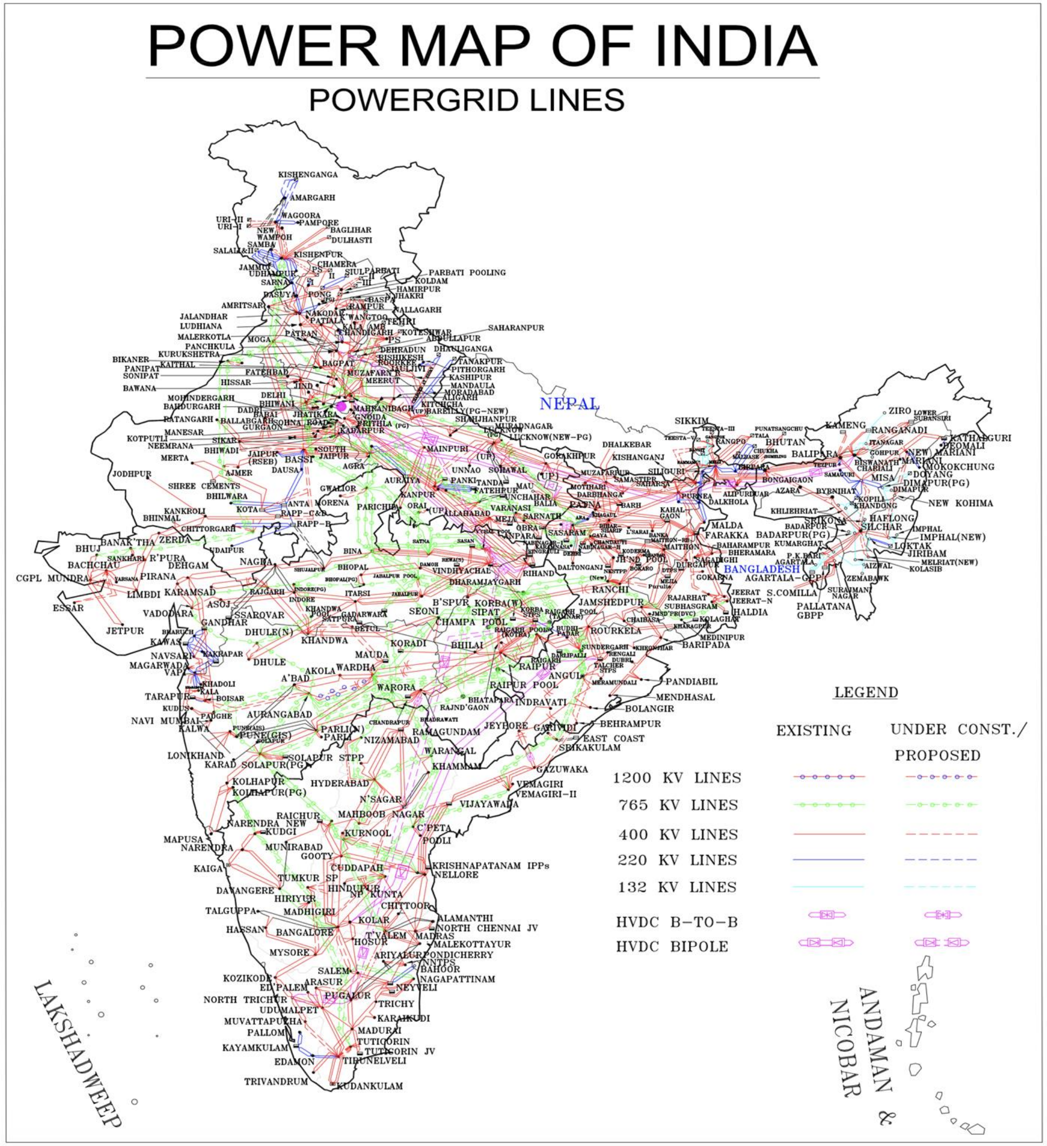
Source: NERC Cyber Attack Task Force report, May 2012 (www.nerc.com)

Summary

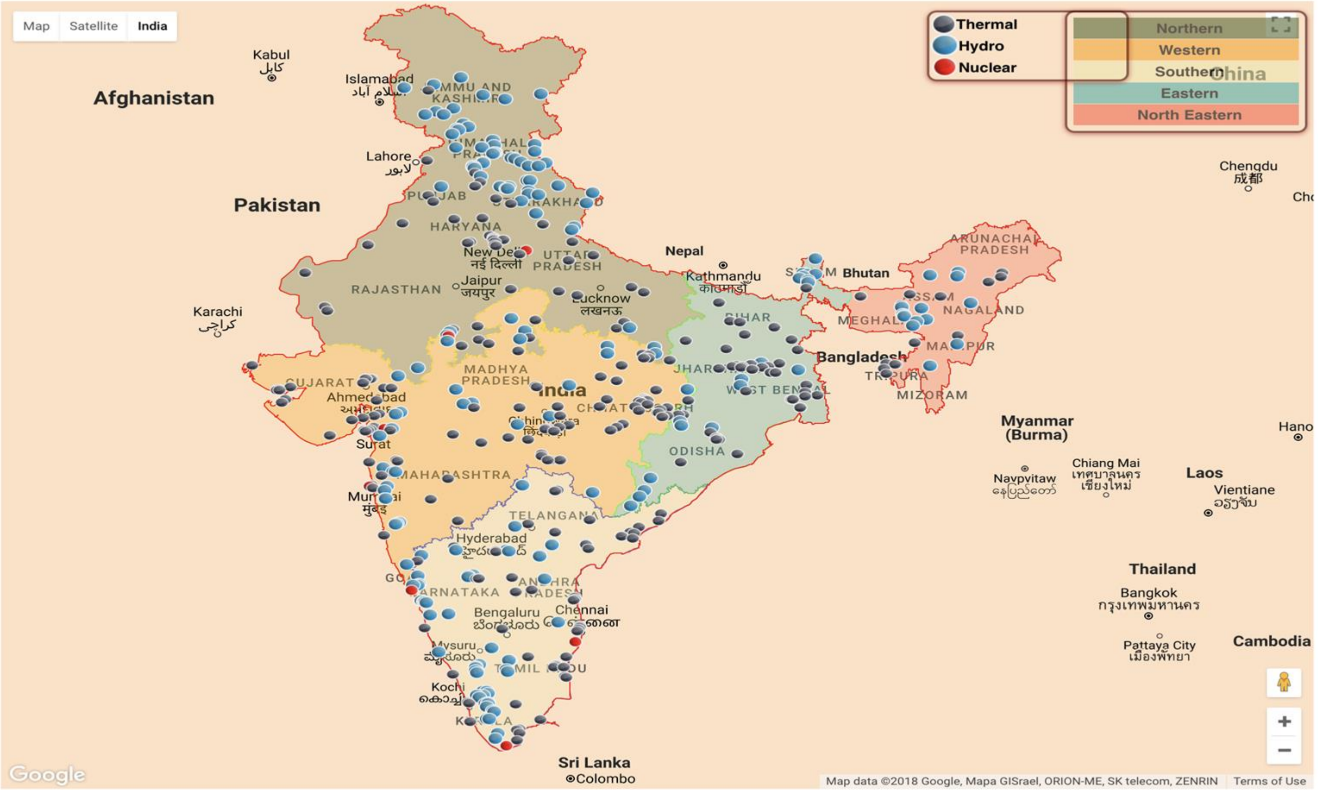
- Risk Assessment methodology
- DOE Risk Management Process
- Qualitative Risk Assessment
- Quantitative Risk Assessment
    - Case study
- Risk Mitigation
    - Mission Oriented Risk and Design Analysis framework
    - Attack Trees and NERC CATF Attack Tree Risk mitigation framework

Indian Power Grid – An Overview

March 2018

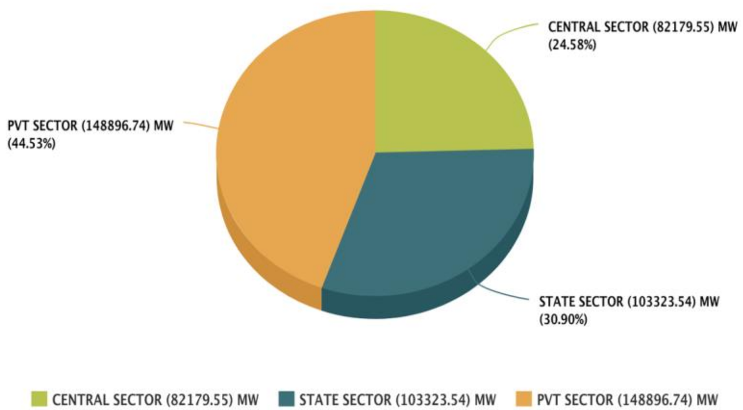

POWER MAP OF INDIA
POWERGRID LINES
NEPAL
BHUTAN
BANGLADESH
LAKSHADWEEP
ANDAMAN & NICOBAR
LEGEND
EXISTING
UNDER CONST./ PROPOSED
1200 KV LINES
765 KV LINES
400 KV LINES
220 KV LINES
132 KV LINES
HVDC B-TO-B
HVDC BIPOLE

All India Status (Generation source-wise)

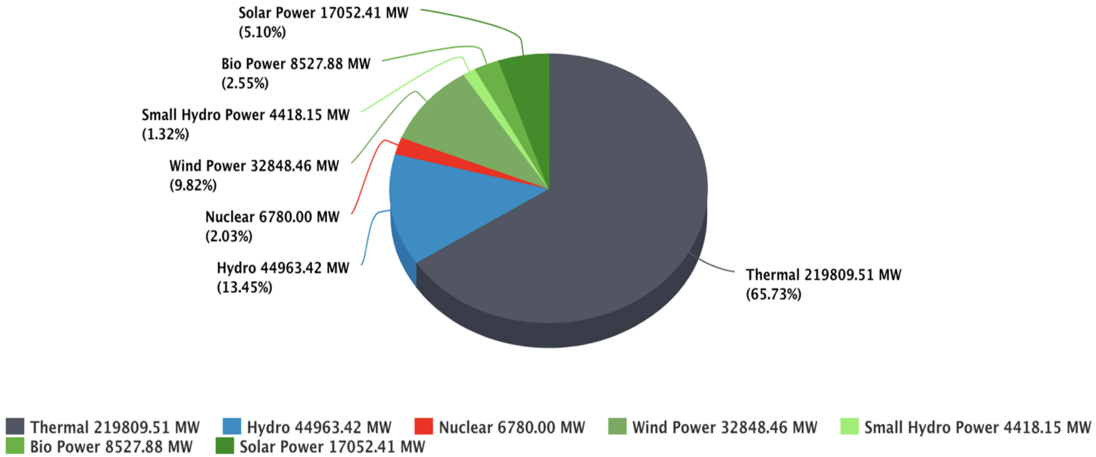


Source: http://npp.gov.in/

Sector wise - Installed Generation Capacity (11/02/2018)

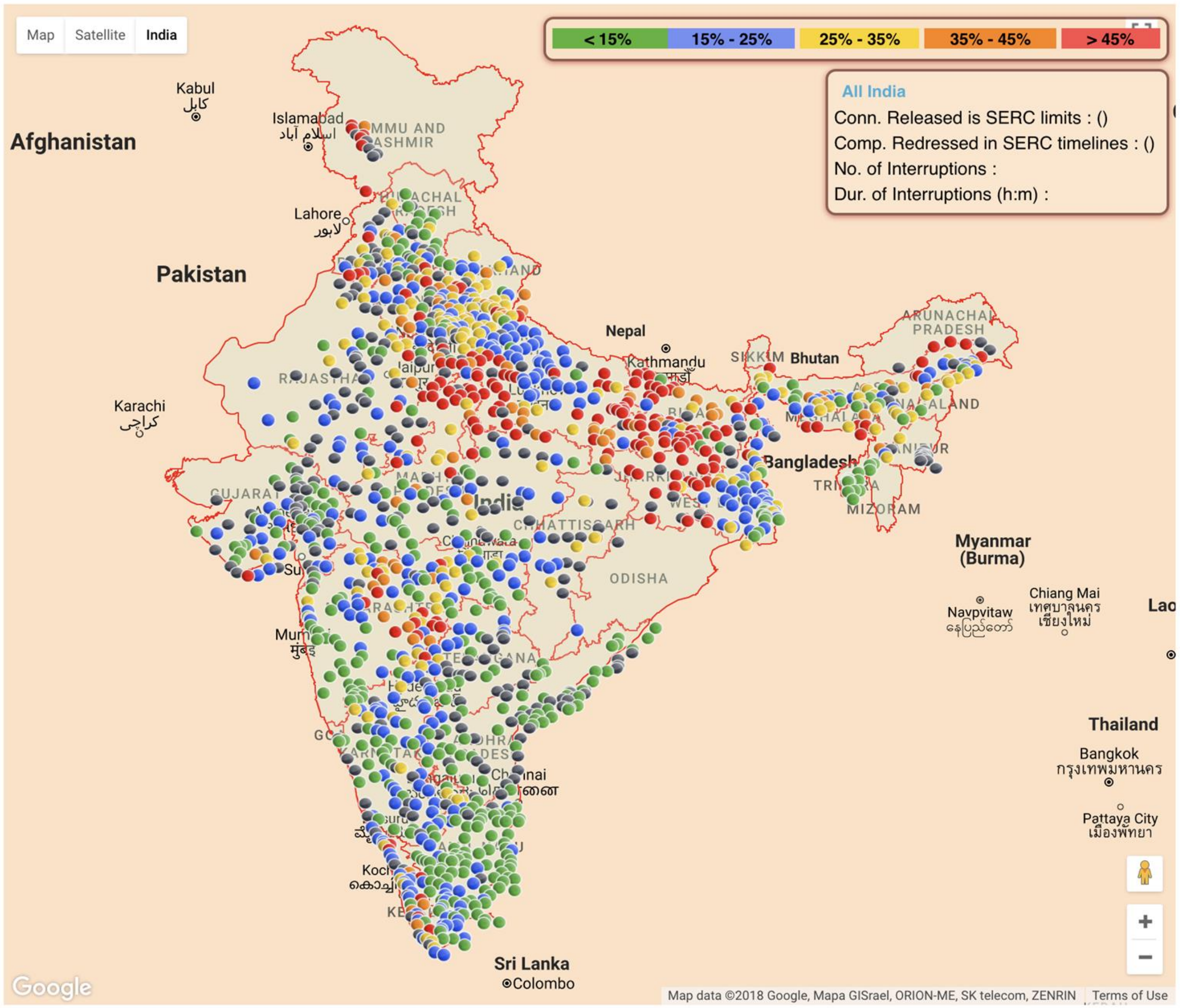


Category wise - Installed Generation Capacity (11/02/2018)



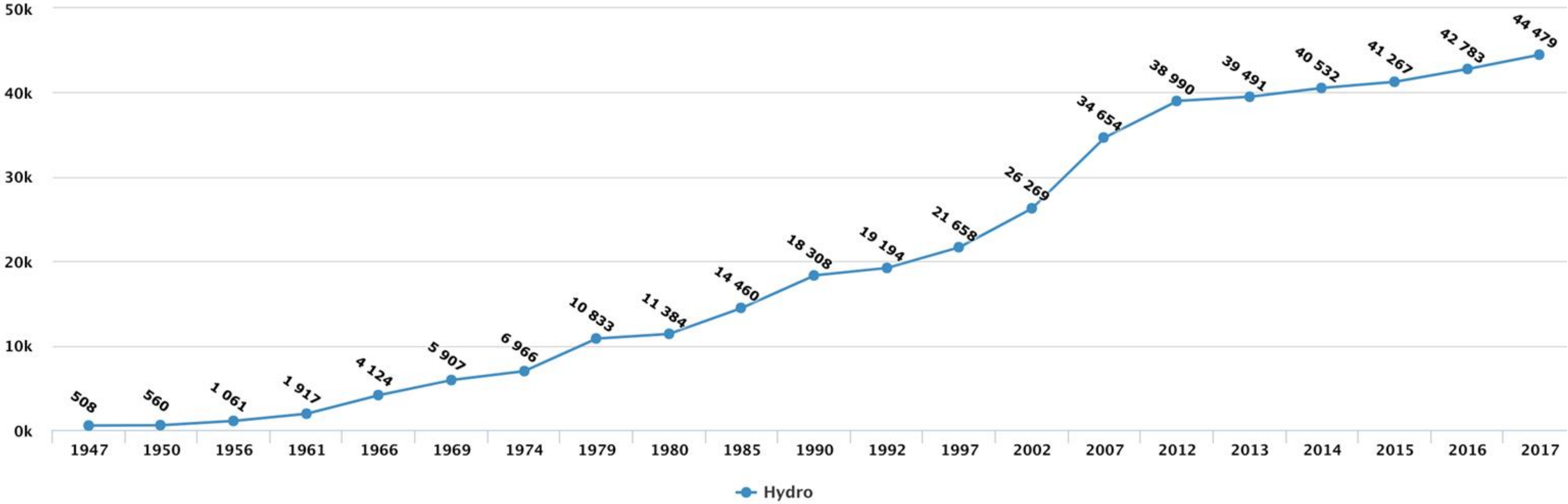
Source: http://npp.gov.in/

All India Aggregate Technical and Commercial Losses (AT & C Losses)



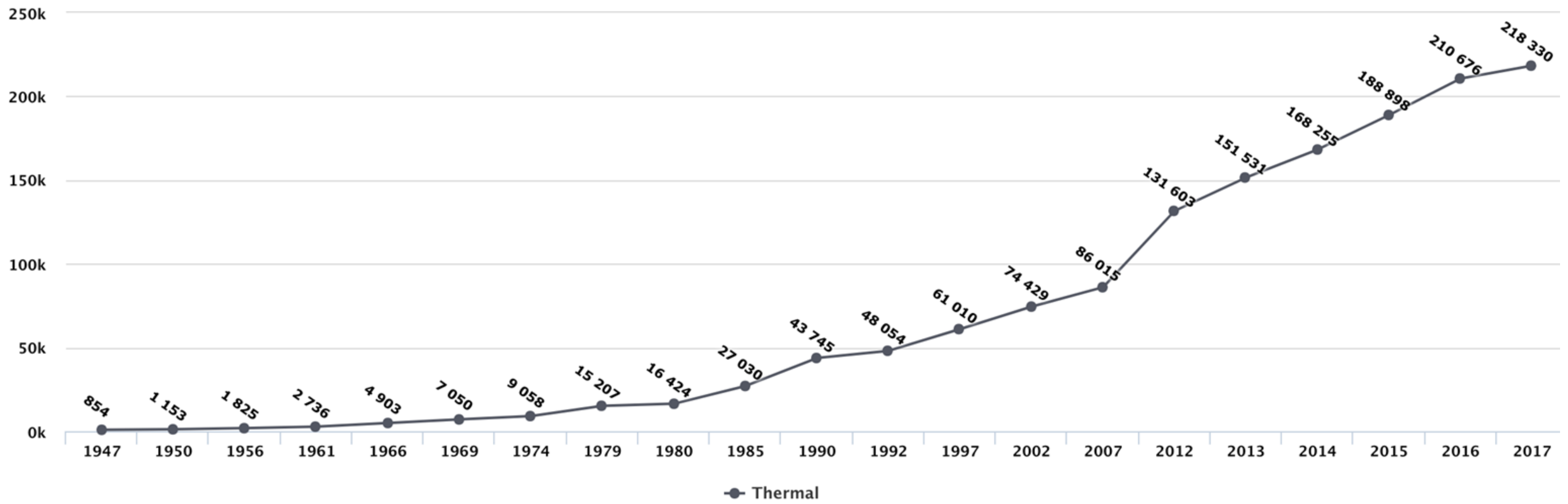
Source:
http://npp.gov.in/

Historical Data : Growth of Electricity Generation of India



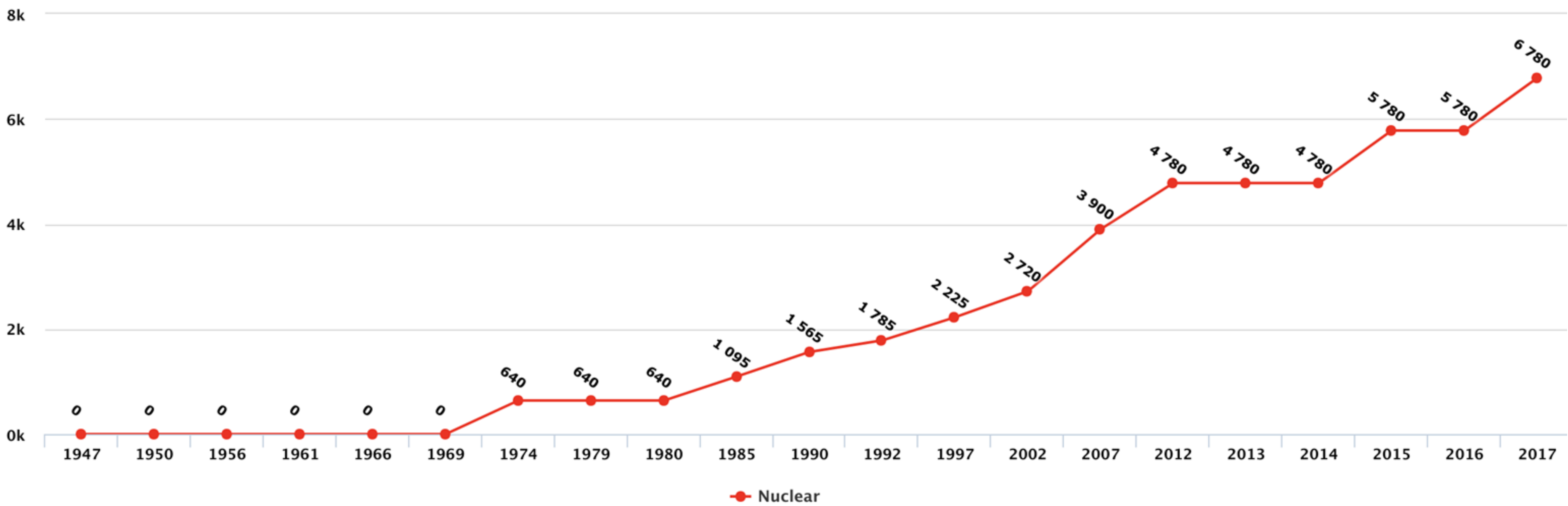
Growth of Installed Capacity (Hydro) in MW

Source:
http://npp.gov.in/



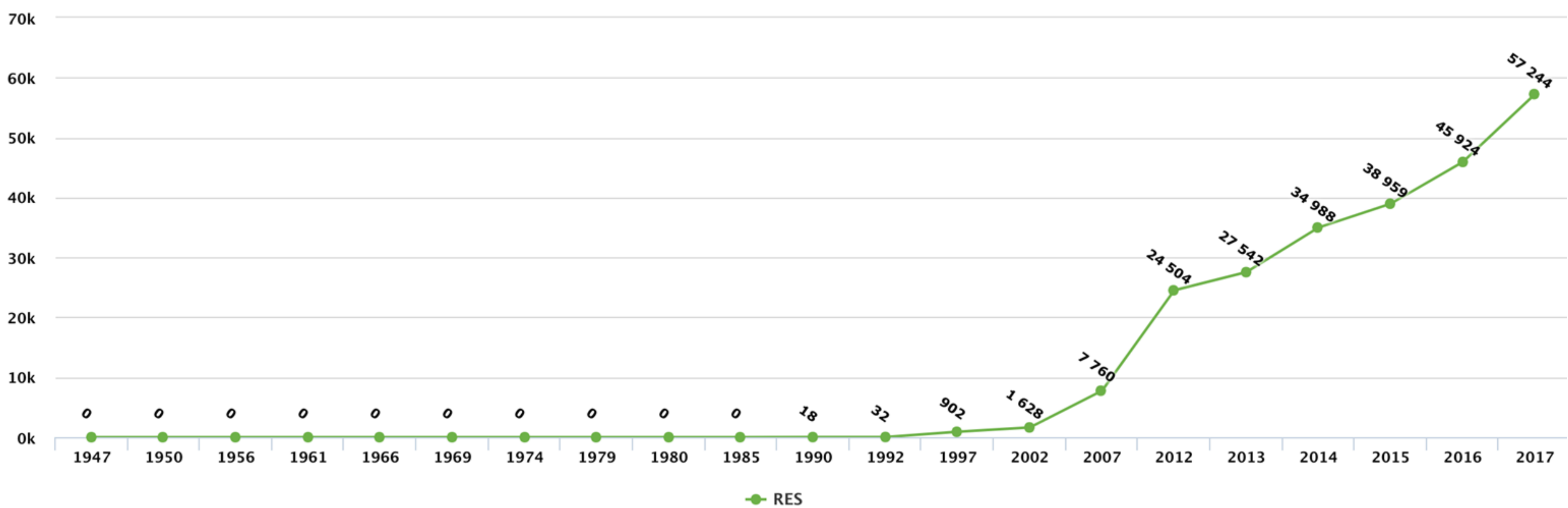
Growth of Installed Capacity (Thermal) in MW

Source:
http://npp.gov.in/



Growth of Installed Capacity (Nuclear) in MW

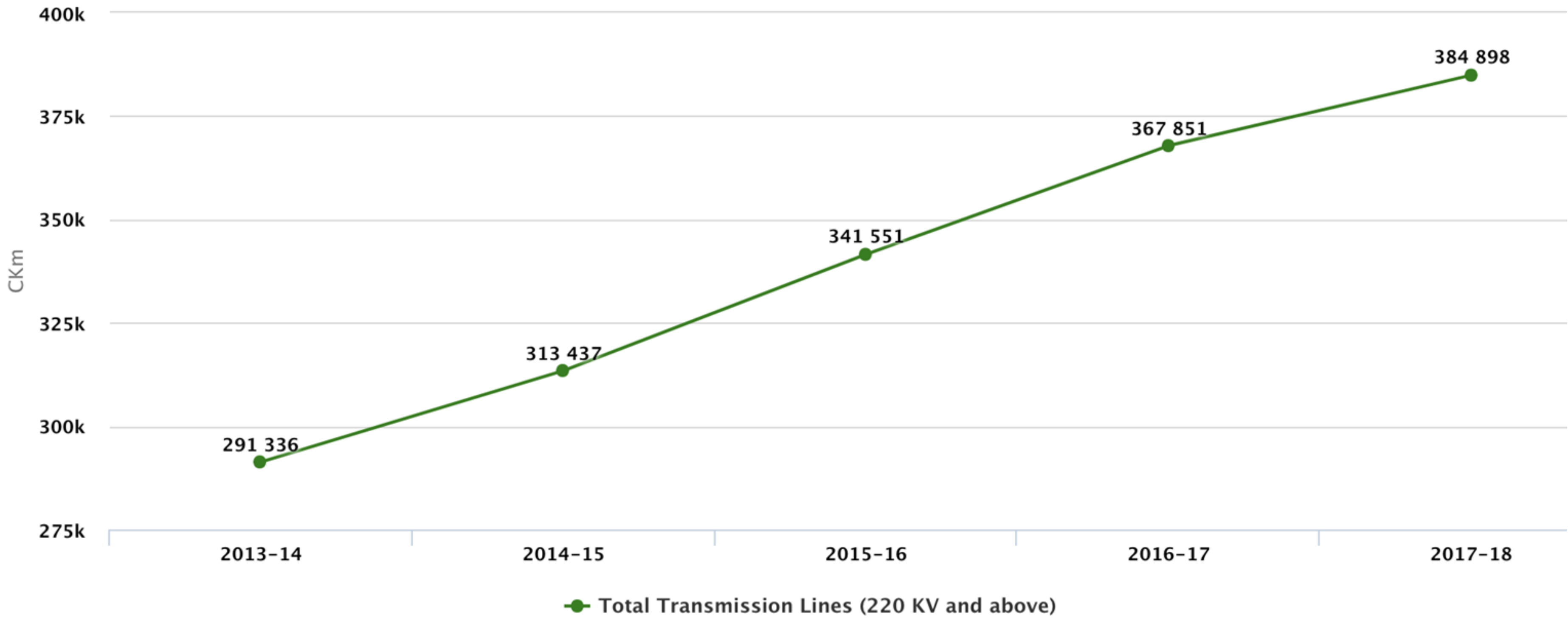
Source: http://npp.gov.in/



Growth of Installed Capacity (Renewables) in MW

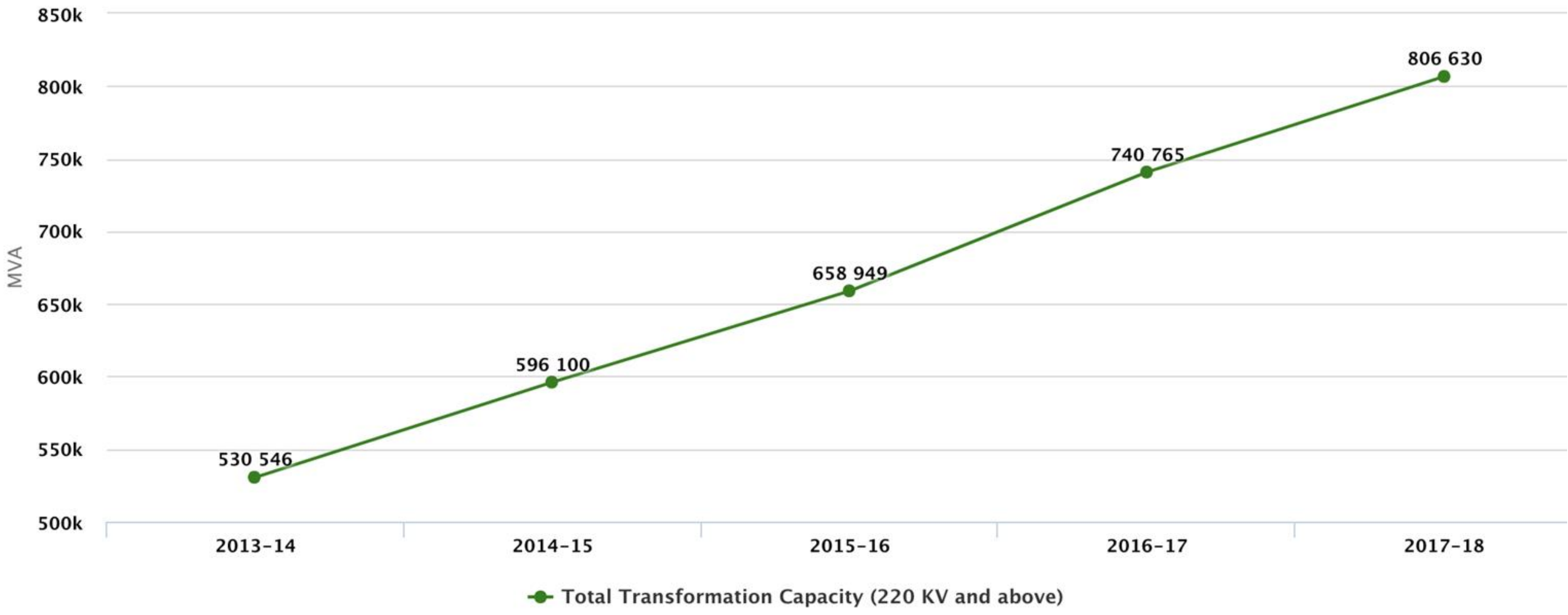
Source: http://npp.gov.in/

Historical Data : Power Transmission



TRANSMISSION LINES(CKM) UPTO JAN-2018

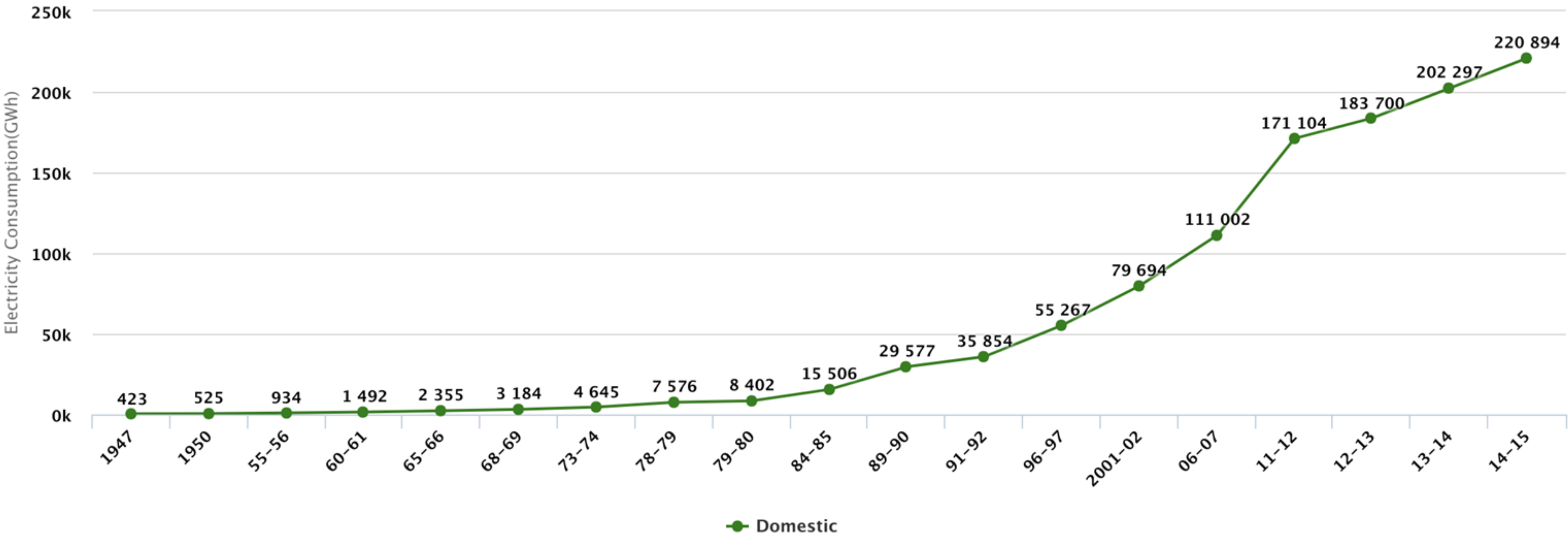
Source: http://npp.gov.in/



TRANSFORMATION CAPACITY(MVA) UPTO JAN-2018

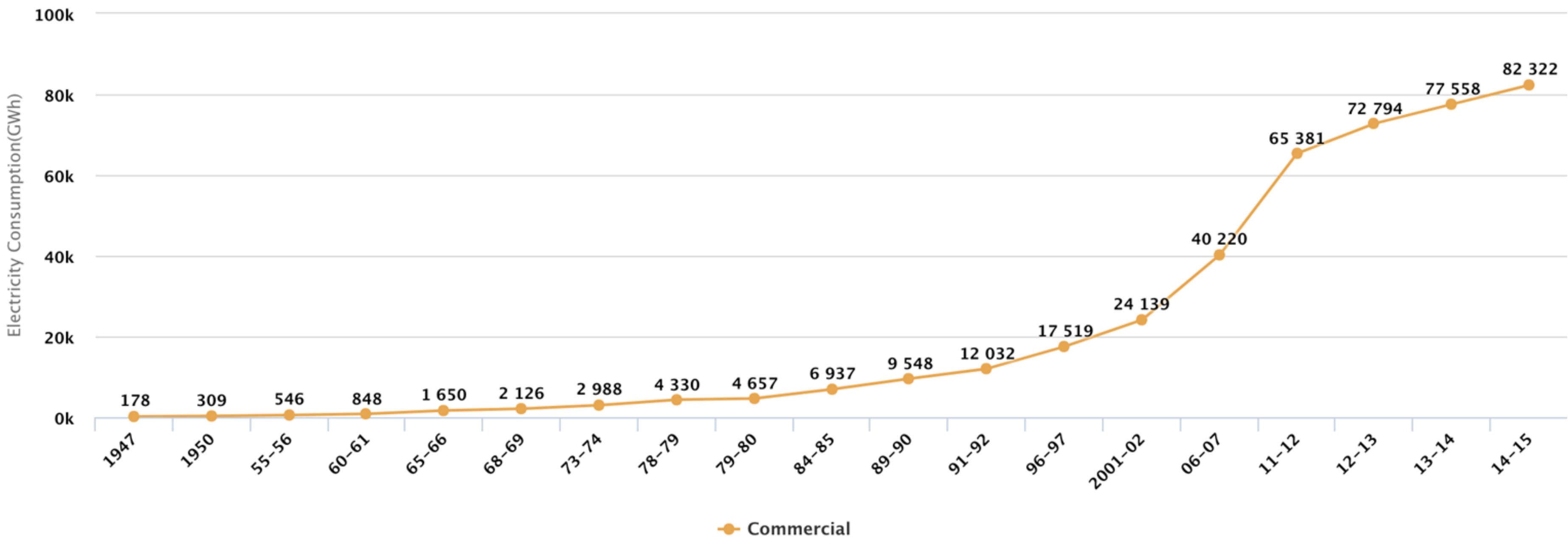
Source:
http://npp.gov.in/

Historical Data: Growth of Electricity Consumption



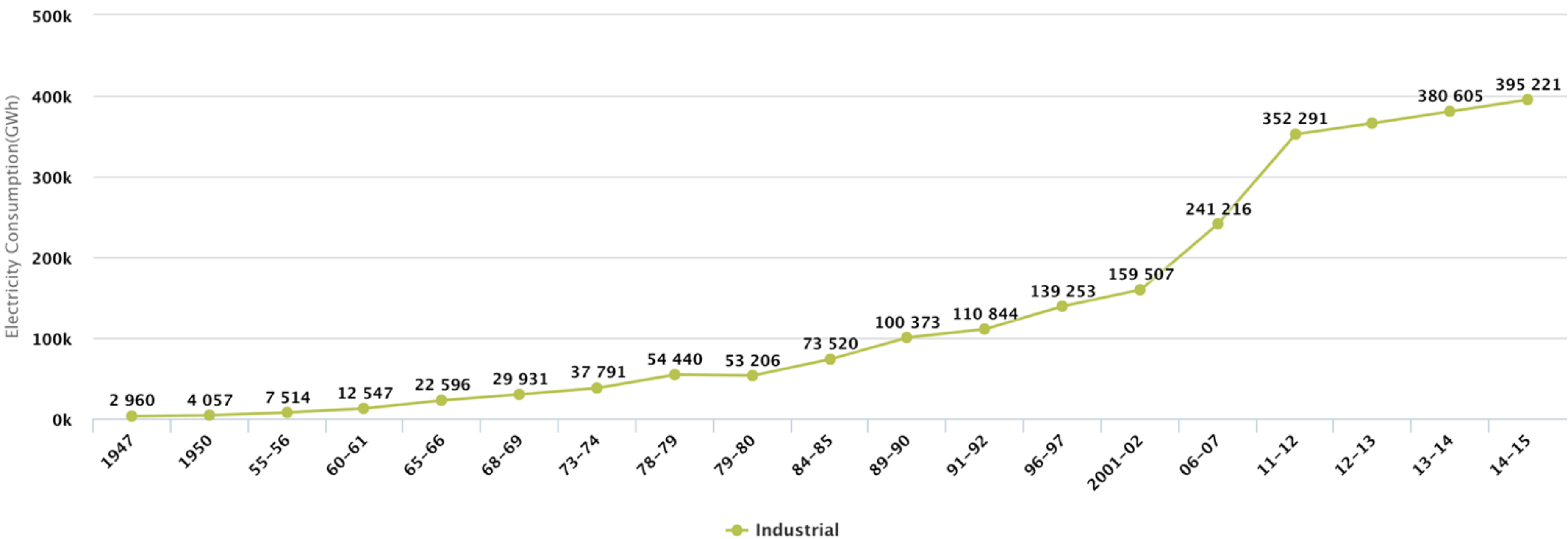
DOMESTIC

Source:
http://npp.gov.in/



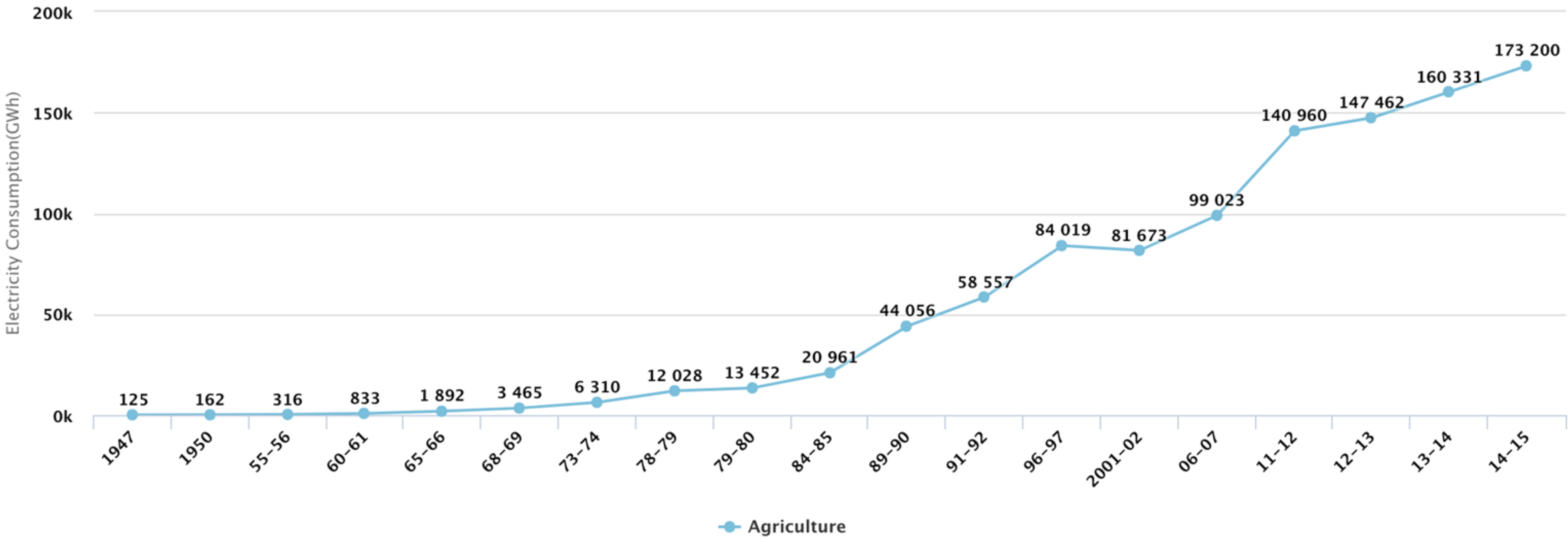
COMMERCIAL

Source: http://npp.gov.in/



INDUSTRIAL

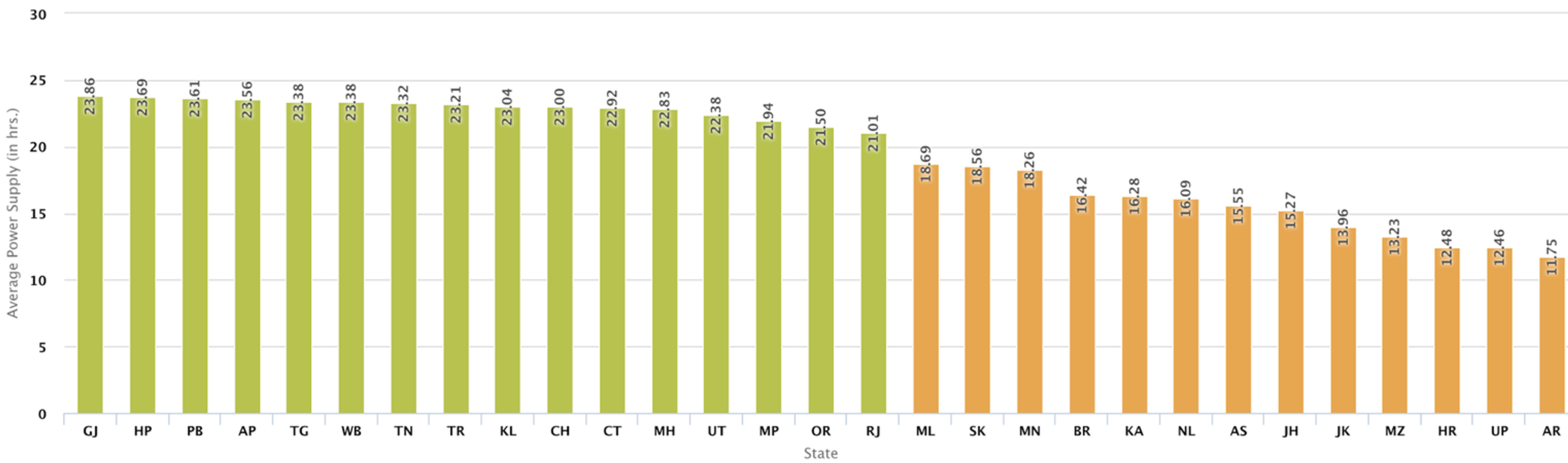
Source:
http://npp.gov.in/



AGRICULTURE

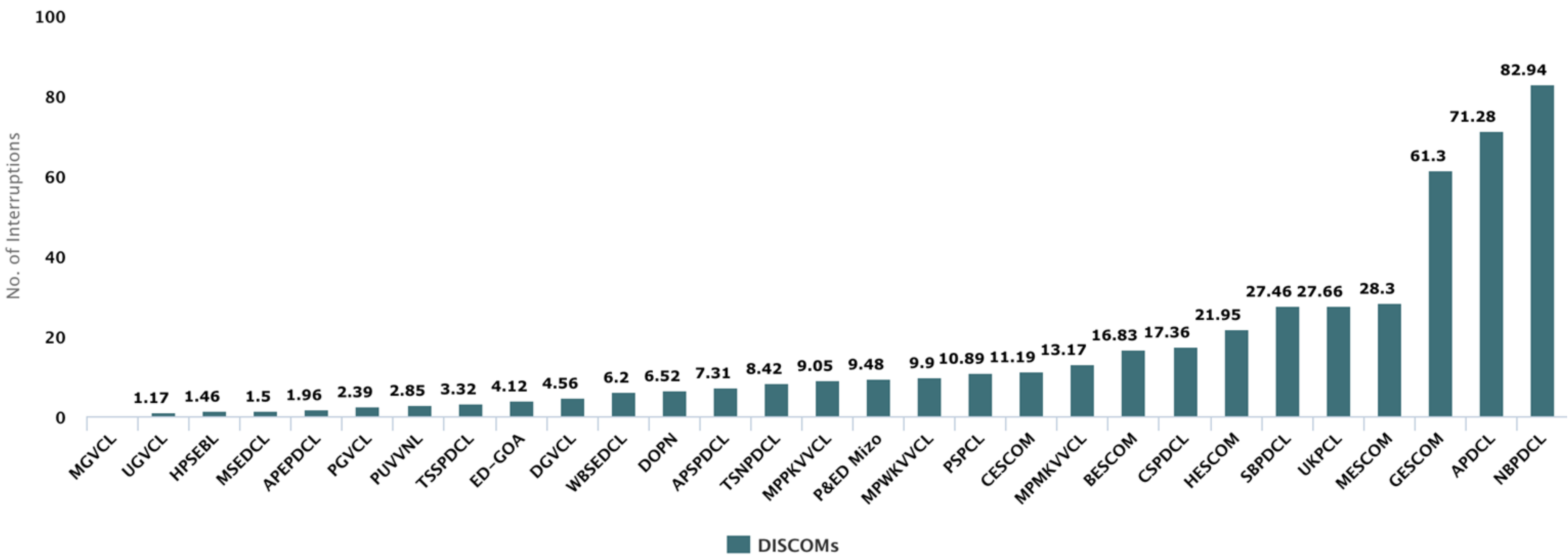
Source:
http://npp.gov.in/

Status of Rural Distribution



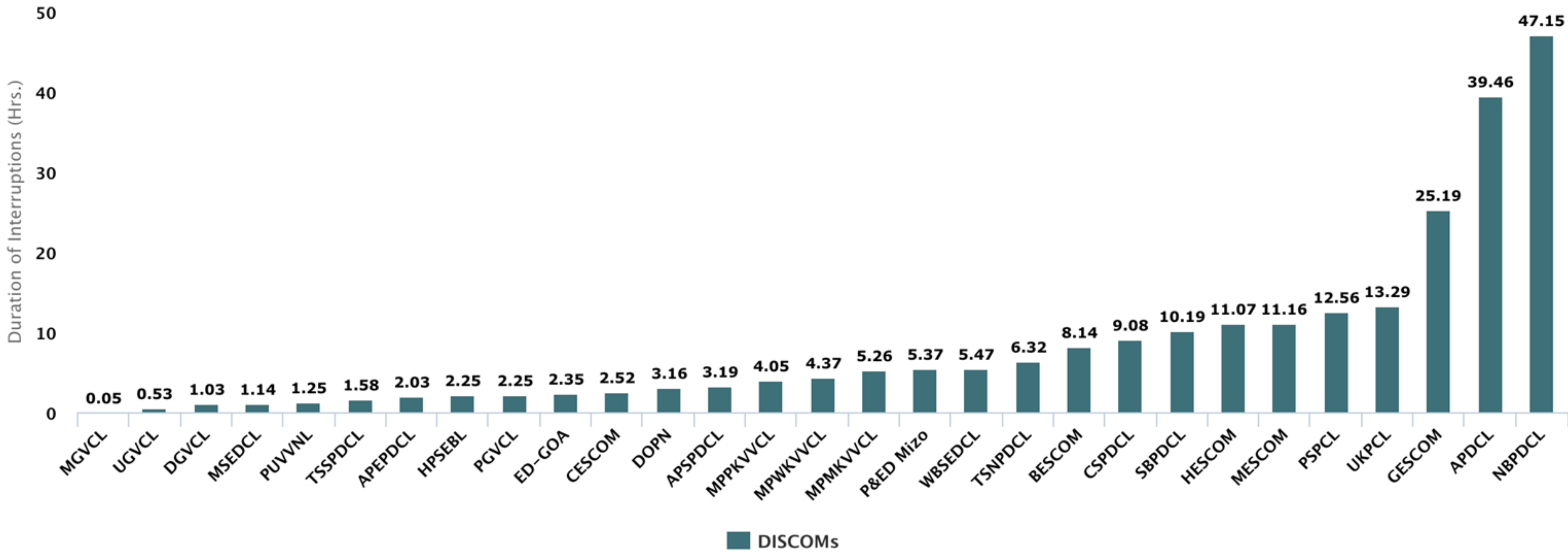
STATUS OF RURAL POWER SUPPLY (JUL-2017)

Source:
http://npp.gov.in/



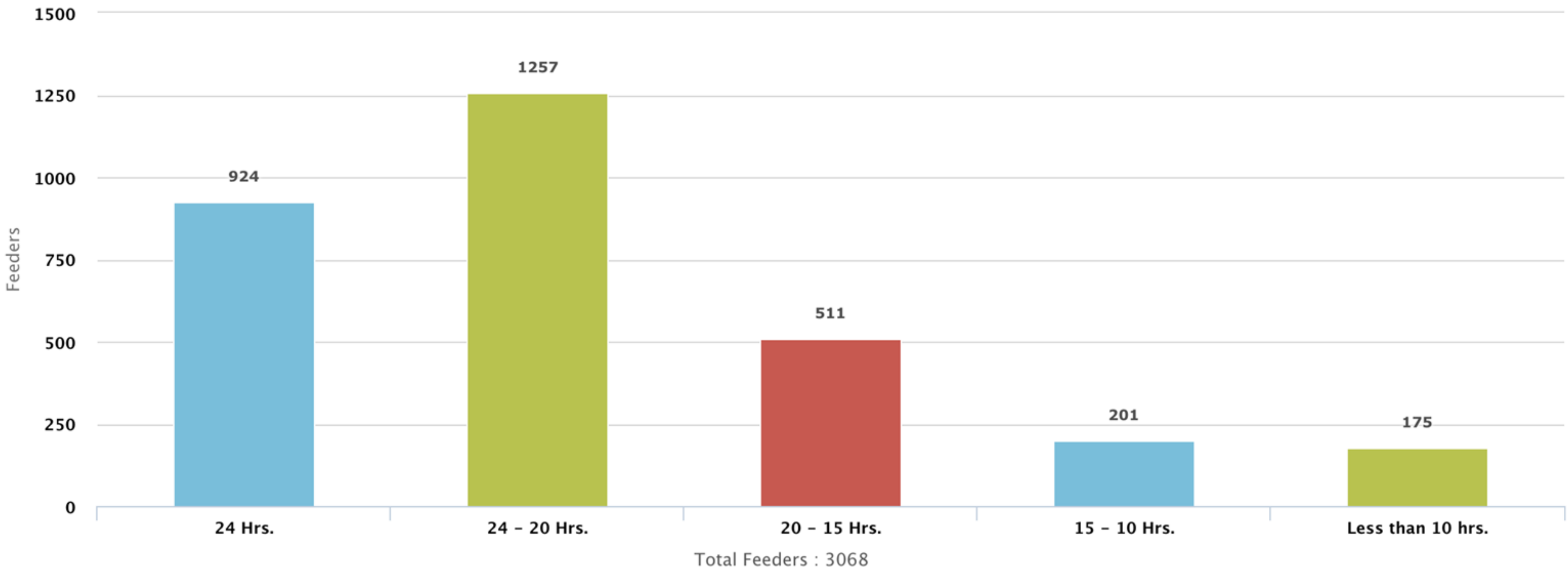
NO. OF INTERRUPTIONS (POWER SUPPLY OUTAGE) FOR (NOV-2017)

Source: http://npp.gov.in/



DURATION OF INTERRUPTIONS (POWER SUPPLY OUTAGE) FOR (OCT-2017)

Source: http://npp.gov.in/



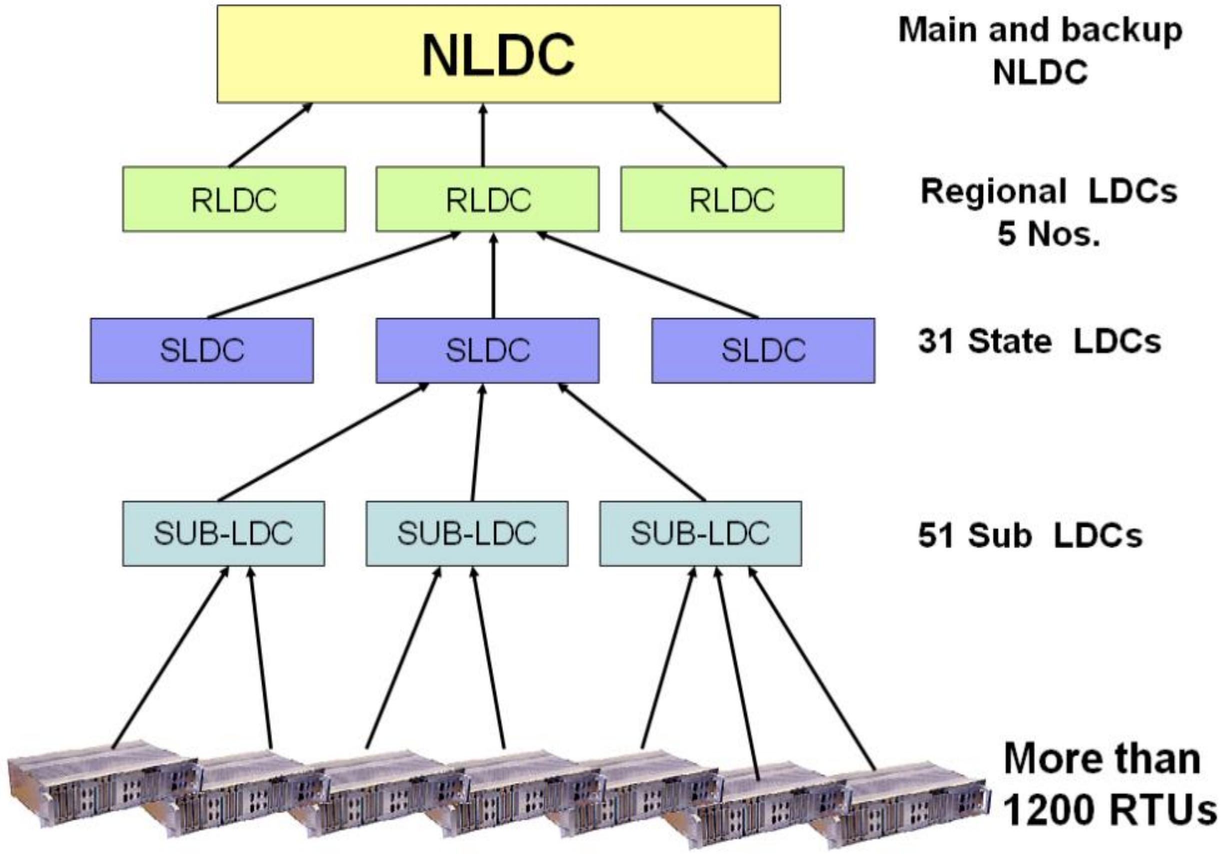
POWER SUPPLY MONITORING STATISTICS (IN HRS) (TILL - JAN-2018)

Source:
http://npp.gov.in/

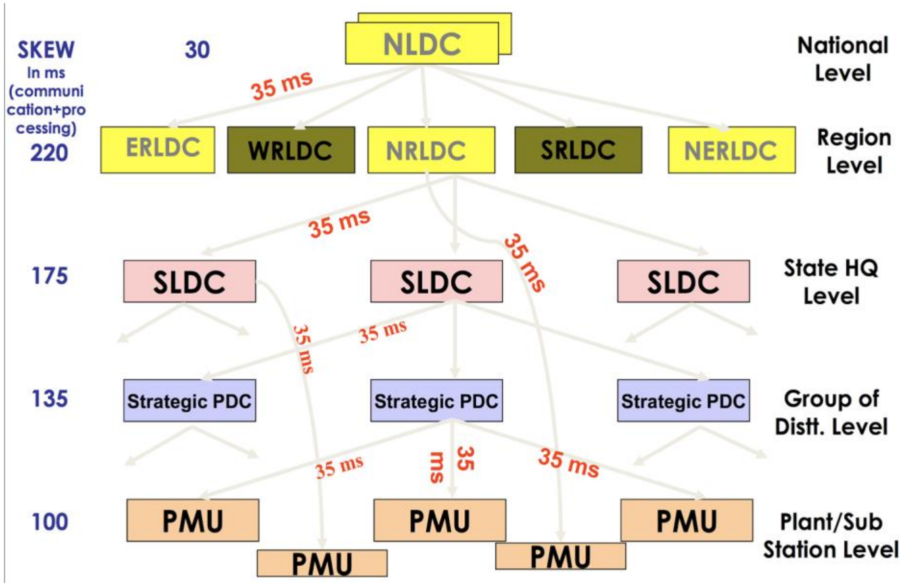
Cyber System for Indian Power Grid – An overview

March 2018

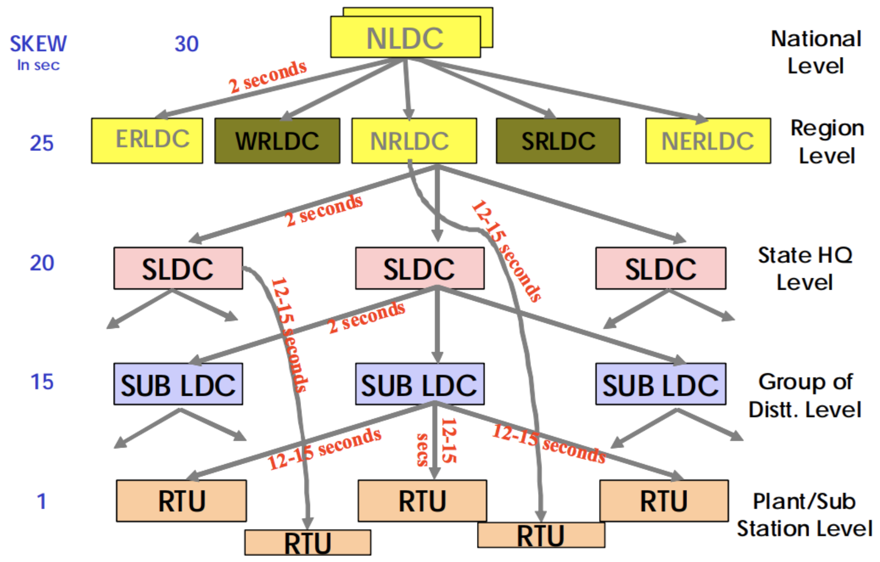
Hierarchy in Grid Operation management:



Latency in WAMS (PMUs)



Latency in SCADA (RTUs)

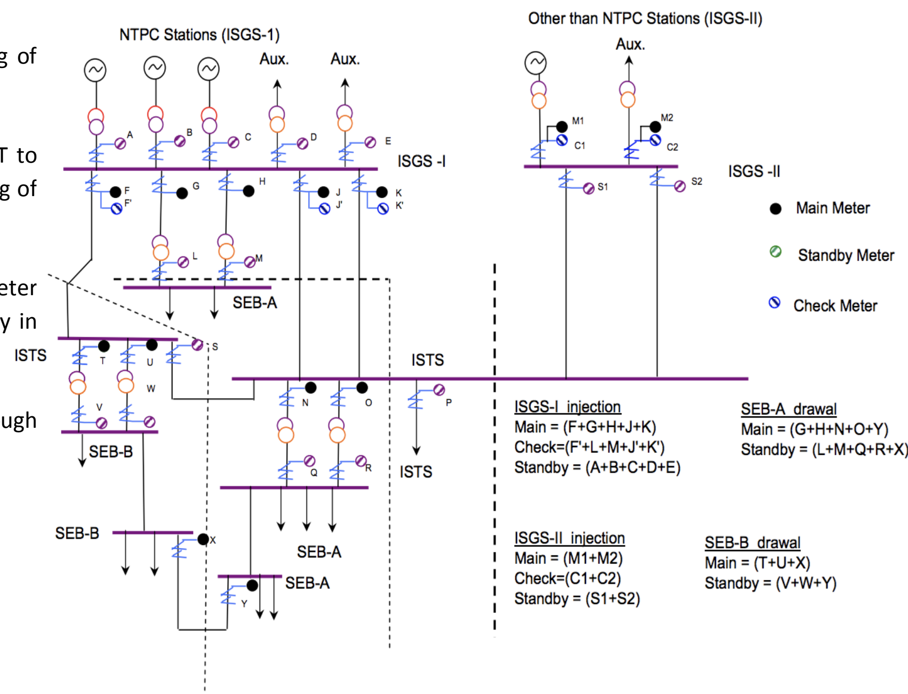


Special Energy Meter

Functionality of SEM

- Main Meter :
  - means a meter, which would primarily be used for accounting and billing of electricity.
- Check Meter :
  - means a meter, which shall be connected to the same core of CT and PT to which main meter is connected and shall be used for accounting and billing of electricity in case of failure of main meter.
- Standby Meter :
  - means a meter connected to CT and VT, other than those used for main meter and check meter and shall be used for accounting and billing of electricity in case of failure of both main meter and check meter;
- Data Processing in SEM [Source]
  - Raw data is sent to RLDCs every week by Tuesday noon from sites through email.
  - Raw data is converted to text files.
  - All text files are appended to a single text file.
  - Korba end SEM is used as master frequency meter.
  - Actual energy is calculated by a software as per configured fictitious meter.
  - Daily Output MWh pertaining to drawal/injection/IR exchange is created.
  - Daily Regional output file for the week period is created.
  - Regional loss is calculated after processing.
  - RLDCs send processed SEM data to respective RPCs.
- Manual on SEM, Data Processing and Computation can be found at [Source]

Typical SEM configuration



Status: Cyber Grid for Power Systems

Communication options and Regulatory provisions

Communication Options

- PLCC - Power Line Carrier Communication is the oldest communication technology used for power system.
- Microwave – Is the second oldest communication system used for power system.
- Copper Wire – generally used for local area communication.
- Fiber Optic – Is the latest and most efficient communication system for modern power system aka smart grid.

Indian Electricity Grid Code (Regulatory provisions - Voice)

5.2 System Security Aspects

- "Each User, STU, RLDC, NLDC and CTU shall provide and maintain adequate and reliable communication facility internally and with other Users/STUs /RLDC/SLDC to ensure exchange of data/information necessary to maintain reliability and security of the grid. Wherever possible, redundancy and alternate path shall be maintained for communication along important routes, e.g., SLDC to RLDC to NLDC."

Major Projects on Cyber Infrastructure at the All India Level

Project on
National Transmission Asset Monitoring Centers (NTAMC)

- Aims for centralized Monitoring, Operation and Management of POWERGRID Substations.
- Remote operation and Management of the POWER GRID Transmission Assets leading to unmanned substation
- Reduction of O&M cost
- Improved Reliability
- **Requirement of Bandwidth**
    - 100 Mbps between the various control centers and backbone network
    - 10 Mbps between Substations and backbone network
    - Redundancy required

Project on
Unified Real time Dynamic Measurement System (URTDSM)

- The Project addresses several questions and concerns such as:
    - How do we know what is going on in the grid where SCADA cannot monitor?
    - Was there an Event? When, where, what kind, after-effects?
    - Is the system really stressed? What are real-time margins?
    - Are there unstable oscillatory modes in the system?
    - What issues will arise when the percentage of Renewable Energy, an intermittent source of power, will increase to 20-30%?

National Transmission Asset Monitoring Centers (NTAMC)

National Transmission Asset Monitoring Centers (NTAMC)
Network Topology and Cyber Grid Requirements

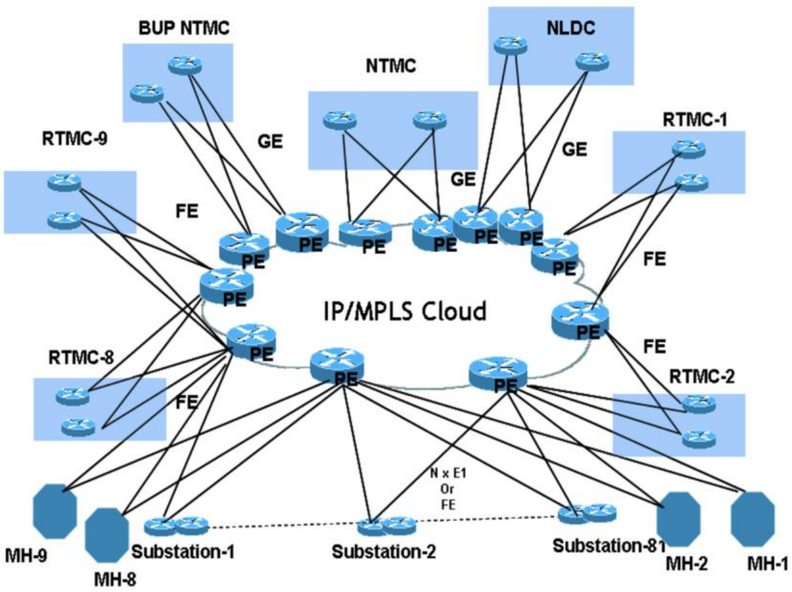
Procurement of Bandwidth

- Services from POWERTEL (MPLS technology, IP/Ethernet based, VPNs)
- Use of ULDC fibre network (up to nearest S/S having connectivity with POWERTEL)
- Lease line from other Telecom Service Providers (up to nearest S/S having connectivity with POWERTEL)

Requirement of Bandwidth

- 100 Mbps between the various control centers and backbone network
- 10 Mbps between Substations and backbone network
- Redundancy required

Network Topology



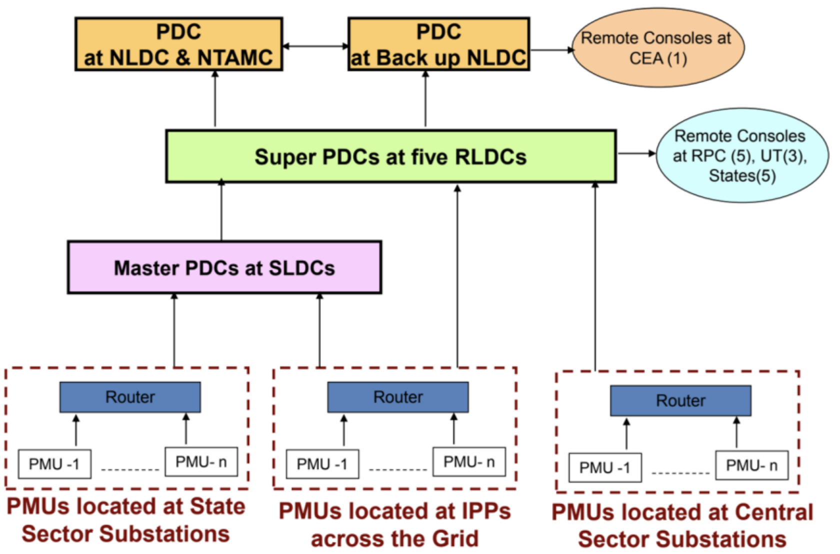
Unified Real time Dynamic Measurement System (URTDSM)

Unified Real time Dynamic Measurement System (URTDSM)

Project Details

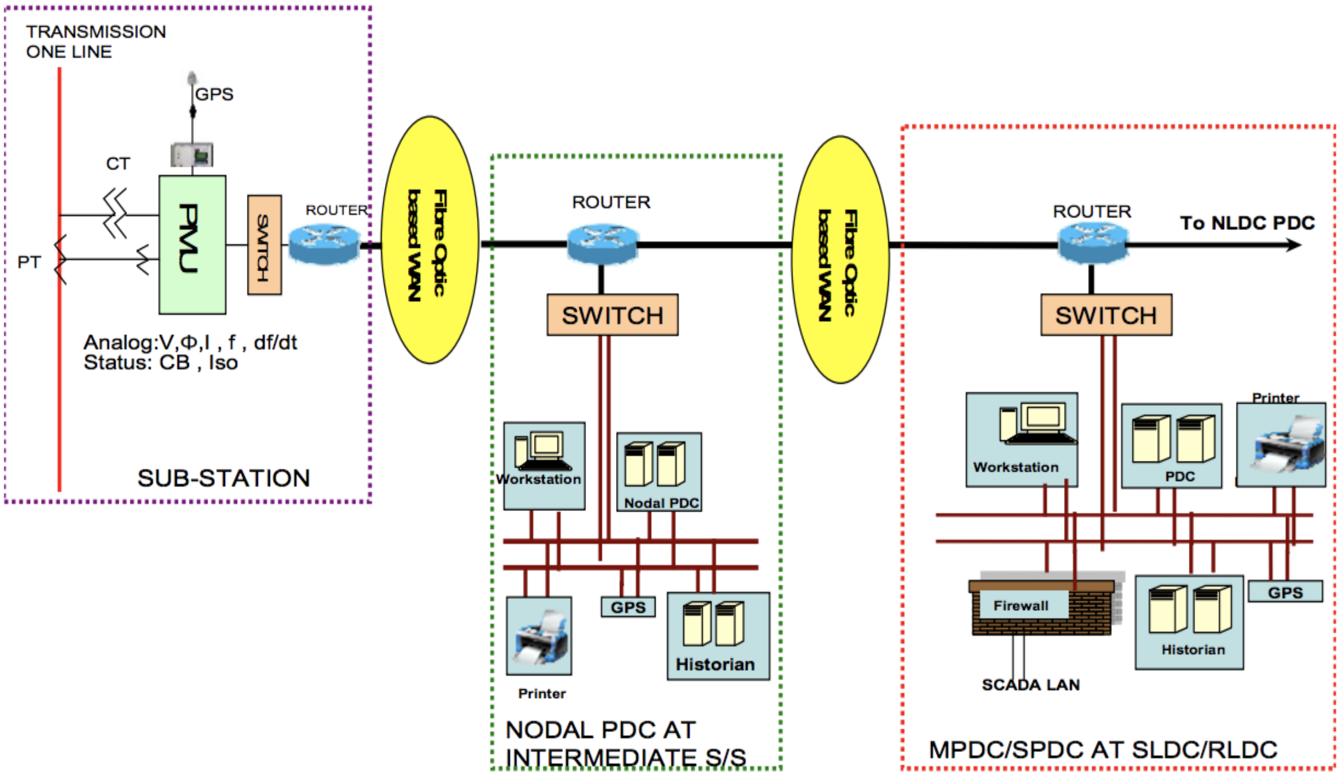
- Phase-1
  - LOA: 15.01.2014 to M/s Alstom
    - Completion Schedule: -24 Months (Jan 2016)
    - Scope: Installation of PDCs at 34 Control Centres
    - Installation of 1186 PMUs across 354 Substations
      - PMUs at substations/generating stations of ISTS/STU connected through OPGW network.
      - PDCs at SLDCs/RLDCs/NLDC/NTAMC (34 nos.)
  - Package-I: (NR, ER, NER, NTAMC & NLDC)
    - Supply: - Rs. 158.22 Crore;
    - Services: - Rs.72.82Crore
    - Total: - Rs. 231.04 Cr
  - Package-II: (SR, WR)
    - Supply: - Rs. 82.61 Crore Services: - Rs.43.75Crore
    - Total: - Rs. 126.36 Cr
- Phase-II
  - Installation of approximately 554 PMUs at Substations and Power Plants
  - Installation of 11530 Km of OPGW and associated items mainly on state/ other utilities lines
  - Installation of 326 SDH equipments and associated items at substations and Power Plants
  - Installation of 215 Auxiliary Power Supply Equipments at substations and Power Plants

URTDSM System Hierarchy



Unified Real time Dynamic Measurement System (URTDSM)

Typical Information Flow and Data Collection in URTDSM



- Total latency : about 100 ms
- Approximately 1 TB data per month from 120 PMUs

Smart Transmission-Communication System

Wideband Communication

- POWERGRID established Wideband Communication Network as a part of Unified Load Despatch and Communication (ULDC) Project comprising of Fiber Optic Communication and Digital microwave Communication System.
- Fiber Optic Communication System was based primarily on Aerial Cables i.e. OPGW cable and few links on ADSS and Wrap Around Cable technology.
- Majority of the installations of Aerial Cables was carried out using Live Line Installation Technique.
- Requirements
  - High Bandwidth
  - High Reliability
  - High Availability
  - Security of highest order
  - Least latency

Optical Ground Wire OPGW

- Implementing OPGW based Communication System under various project such as Microwave Replacement Project (MRP), Fibre Optic Expansion Projects (FEP) and other projects
- Around 35000 km of OPGW under implementation
- Around 65000 km of OPGW network to be implemented to meet the requirement

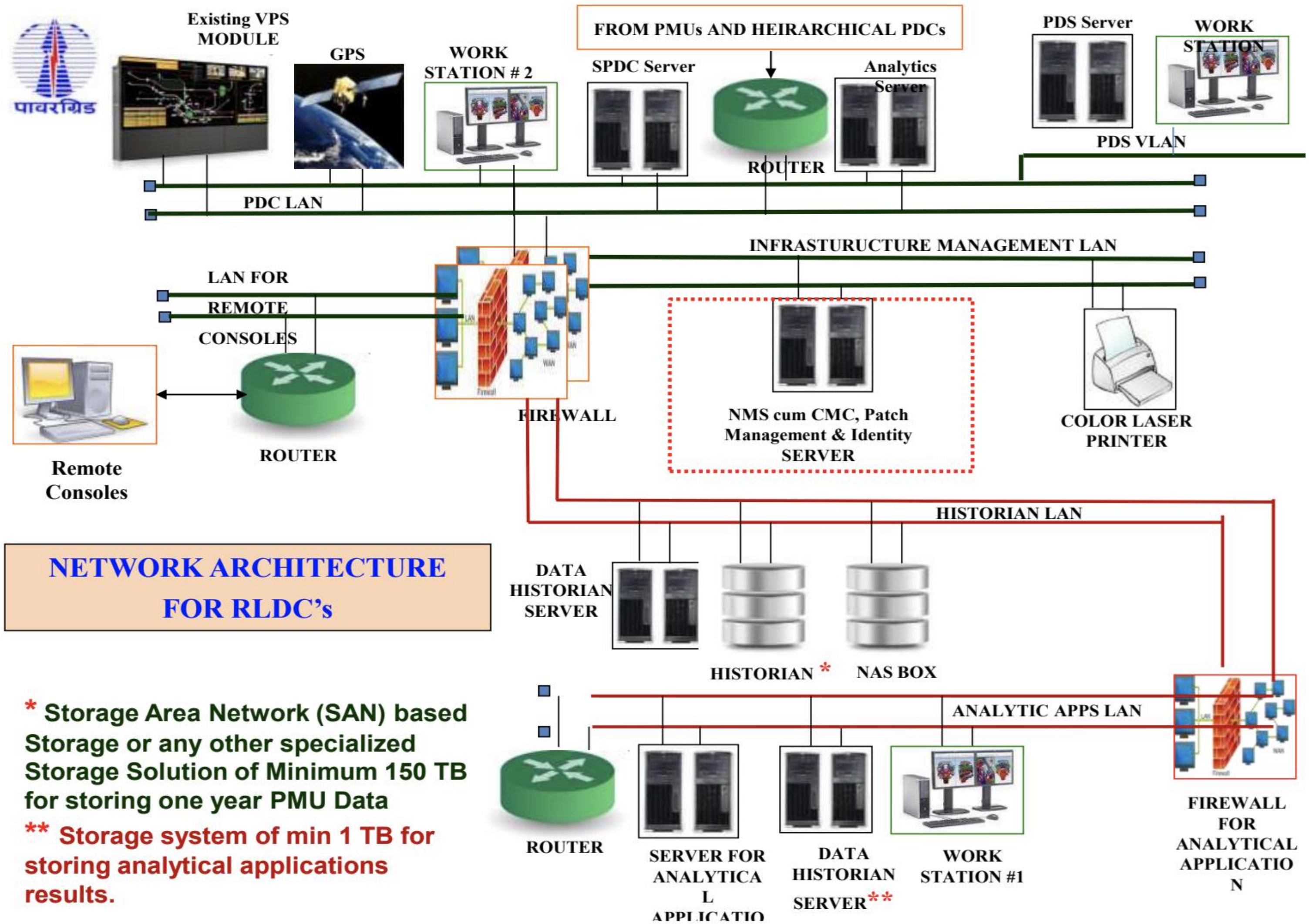
Communication Equipment

- Communication equipment with minimum bit rate of STM-4/STM-16 is being implemented as part of expansion network for nodes falling in linear section and ring network respectively.
- Provision for both E1 & Ethernet interface in the OLTE equipment
- Both equipment protection as well as path protection

Status of PMU Supply and Integration with CC as on 30th July 2016

Region	Scope		Dispatch		Installation & Commissioning		Integrated with CC	
	S/s	PMUs	S/S	PMUs	S/S	PMUs	S/S	PMUs
NR-I	70	206	43	129	41	124	18	63
NR-II	44	120	31	109	30	103	5	18
ER-I	20	88	0	0	0	0	0	0
ER-II	39	114	15	52	11	40	7	29
ORISSA	26	79	8	25	8	25	4	17
SR-I	30	96	22	89	17	69	4	17
SR-II	41	129	31	103	24	77	12	46
WR-I	19	80	2	2	1	1	0	0
WR-II	37	157	9	51	6	38	3	18
CHG	14	68	6	55	2	11	2	11
NER	14	49	11	42	9	35	0	0
Total	354	1186	178	657	149	523	55	219

Network Architecture For RLDC's with Firewall security:



Wide Area Technology Development

Status from PMU Pilot Projects

Applications of Synchrophasor data at RLDCs and NLDC

Visualizations

- Magnitude, angle of all three voltage/current phasor
- Sequence components of voltage/current phasor
- Frequency & Frequency difference
- Rate of change of frequency
- Angular separation between pair of nodes
- 1-phase auto reclosing in EHV transmission line
- Subsystem synchronization during restoration by using standing phase angle separation and phase sequence
- Forensic analysis of faults/grid incidents
- Post Dispatch Analysis of Grid Operation
- Detection and Analysis of Oscillations in Power System

Observations

- Inter area oscillations were observed, and were captured by the WAMS system of NR.
- The phase angle across nodes has helped in determining the stress in the grid and its proximity to instability.
- On further analysis of frequency data, from PMU it has been experienced that difference in frequency exist at different locations even in the synchronous system and this difference is very pronounced during transients, tripping of generating unit or major load throw off conditions. Such difference in frequency was not visualized through SCADA system due to 10 second data.
- High rate of change in frequency of the order of +1 Hz to 1.5 Hz were also observed during initial fault period, which dies down after 100 to 120 millisecs.

Applications of Synchrophasor data at RLDCs and NLDC

Visualizations

- Magnitude, angle of all three voltage/current phasor
- Sequence components of voltage/current phasor
- Frequency & Frequency difference
- Rate of change of frequency
- Angular separation between pair of nodes
- 1-phase auto reclosing in EHV transmission line
- Subsystem synchronization during restoration by using standing phase angle separation and phase sequence
- Forensic analysis of faults/grid incidents
- Post Dispatch Analysis of Grid Operation
- Detection and Analysis of Oscillations in Power System

Observations

- Inter area oscillations were observed, and were captured by the WAMS system of NR.
- The phase angle across nodes has helped in determining the stress in the grid and its proximity to instability.
- On further analysis of frequency data, from PMU it has been experienced that difference in frequency exist at different locations even in the synchronous system and this difference is very pronounced during transients, tripping of generating unit or major load throw off conditions. Such difference in frequency was not visualized through SCADA system due to 10 second data.
- High rate of change in frequency of the order of +1 Hz to 1.5 Hz were also observed during initial fault period, which dies down after 100 to 120 millisecs.

Special Protection Schemes (SPS) Project

Applications of Synchrophasor data at RLDCs and NLDC

Visualizations

- Magnitude, angle of all three voltage/current phasor
- Sequence components of voltage/current phasor
- Frequency & Frequency difference
- Rate of change of frequency
- Angular separation between pair of nodes
- 1-phase auto reclosing in EHV transmission line
- Subsystem synchronization during restoration by using standing phase angle separation and phase sequence
- Forensic analysis of faults/grid incidents
- Post Dispatch Analysis of Grid Operation
- Detection and Analysis of Oscillations in Power System

Observations

- Inter area oscillations were observed, and were captured by the WAMS system of NR.
- The phase angle across nodes has helped in determining the stress in the grid and its proximity to instability.
- On further analysis of frequency data, from PMU it has been experienced that difference in frequency exist at different locations even in the synchronous system and this difference is very pronounced during transients, tripping of generating unit or major load throw off conditions. Such difference in frequency was not visualized through SCADA system due to 10 second data.
- High rate of change in frequency of the order of +1 Hz to 1.5 Hz were also observed during initial fault period, which dies down after 100 to 120 millisecs.

Applications of Synchrophasor data at RLDCs and NLDC

Visualizations

- Magnitude, angle of all three voltage/current phasor
- Sequence components of voltage/current phasor
- Frequency & Frequency difference
- Rate of change of frequency
- Angular separation between pair of nodes
- 1-phase auto reclosing in EHV transmission line
- Subsystem synchronization during restoration by using standing phase angle separation and phase sequence
- Forensic analysis of faults/grid incidents
- Post Dispatch Analysis of Grid Operation
- Detection and Analysis of Oscillations in Power System

Observations

- Inter area oscillations were observed, and were captured by the WAMS system of NR.
- The phase angle across nodes has helped in determining the stress in the grid and its proximity to instability.
- On further analysis of frequency data, from PMU it has been experienced that difference in frequency exist at different locations even in the synchronous system and this difference is very pronounced during transients, tripping of generating unit or major load throw off conditions. Such difference in frequency was not visualized through SCADA system due to 10 second data.
- High rate of change in frequency of the order of +1 Hz to 1.5 Hz were also observed during initial fault period, which dies down after 100 to 120 millisecs.

Summary

- Demand is increasing
- Generation is increasing
- Transmission capacity is increasing
- Rural electrification is expanding
- Smart grid deployment is underway – pilot projects