

# **Reliability Considerations in Cyber-Power Dependent Systems**

**Visvakumar Aravinthan**

**Wichita State University**

(visvakumar.Aravinthan@Wichita.edu)



PSERC Webinar  
April 17, 2018



# Acknowledgement

- **This work was part of PSERC project T-53**
  - **Reliability Assessment and Modeling of Cyber Enabled Power Systems with Renewable Sources and Energy Storage**
  - **Collaborative work between Texas A&M & Wichita State**
- **The following students contributed to this work**
  - **Mohammad Heidari**
  - **Mojtaba Sepehry**
  - **Thanatheepan Balachandran**
  - **Suvagata Chakraborty**



# Presentation Outline

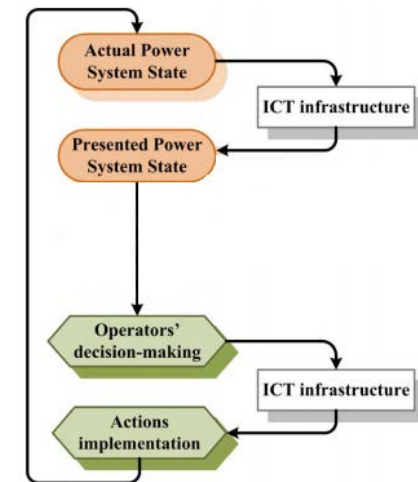
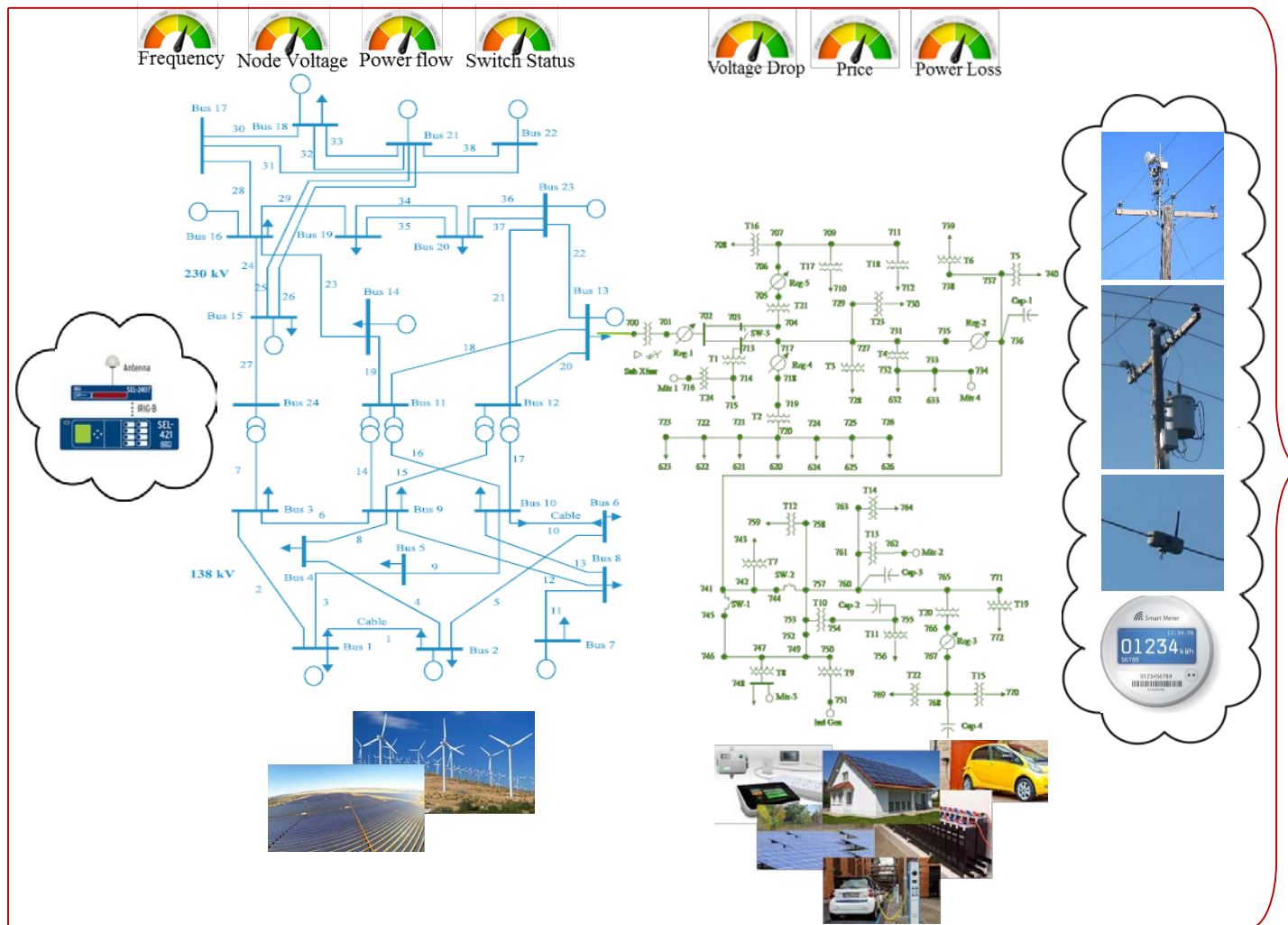
- **Background and Motivation**
- **Monitoring & Preventive Maintenance**
- **Effect of Communication**
- **Cyber System Failure Modeling**
  - Scenario 1: Cyber unavailability
  - Scenario 2: Cyber attack
- **Dependent System Modeling Tools: A Need**
- **Final Remarks and Future Needs**



# Presentation Outline

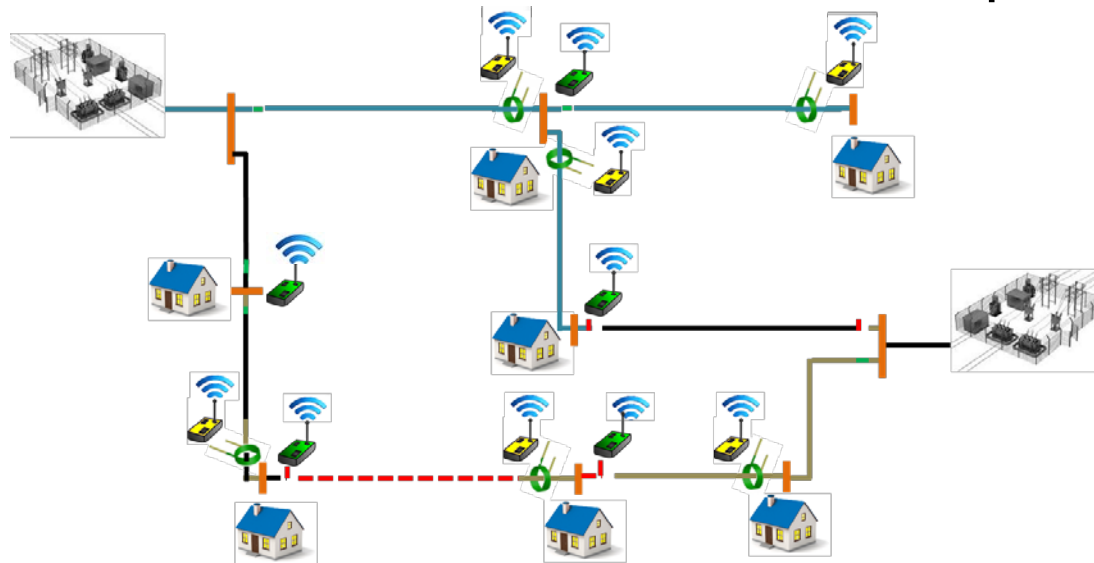
- **Background and Motivation**
- Monitoring & Preventive Maintenance
- Effect of Communication
- Cyber System Failure Modeling
  - Scenario 1: Cyber unavailability
  - Scenario 2: Cyber attack
- Dependent System Modeling Tools: A Need
- Final Remarks and Future Needs

# Background & Motivation



# Background & Motivation

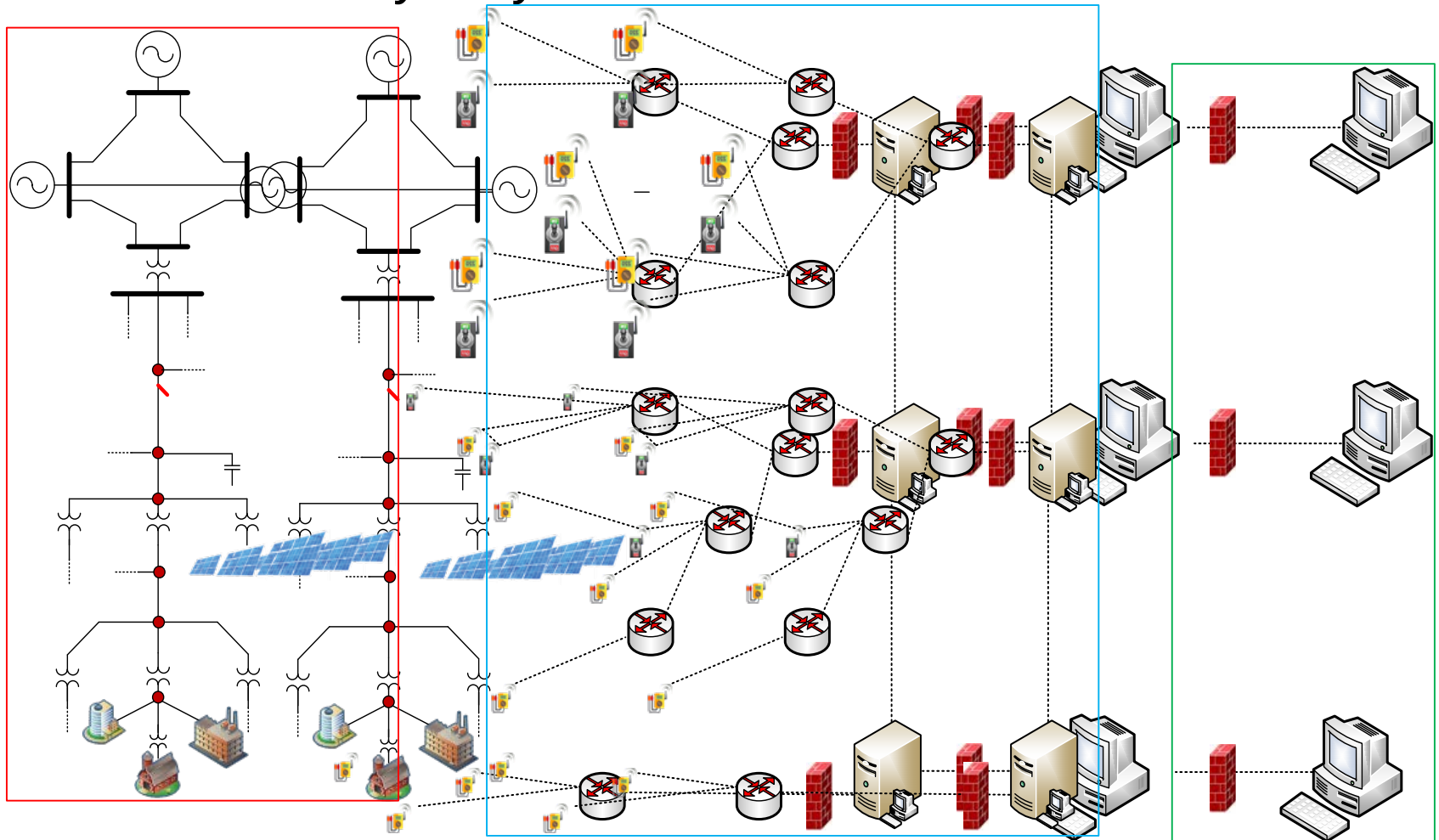
- **A simple example of cyber-power system**
  - Automated fault isolation as the example



- **This process depends on**
  - Communication
  - Automatic decision

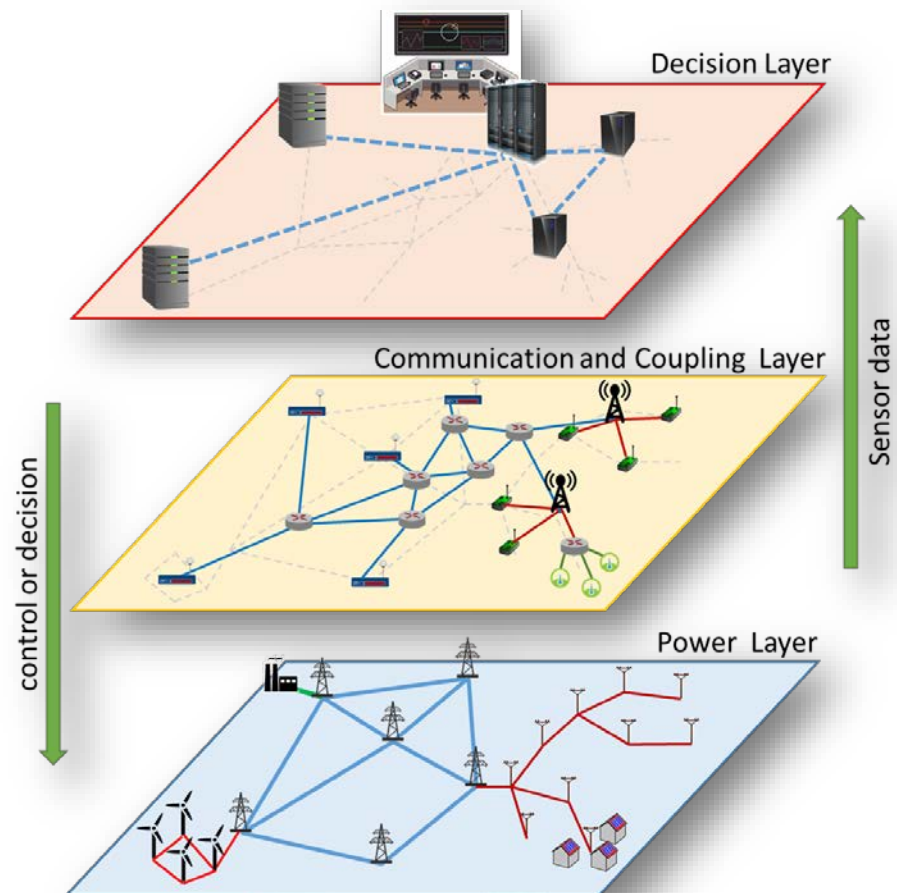
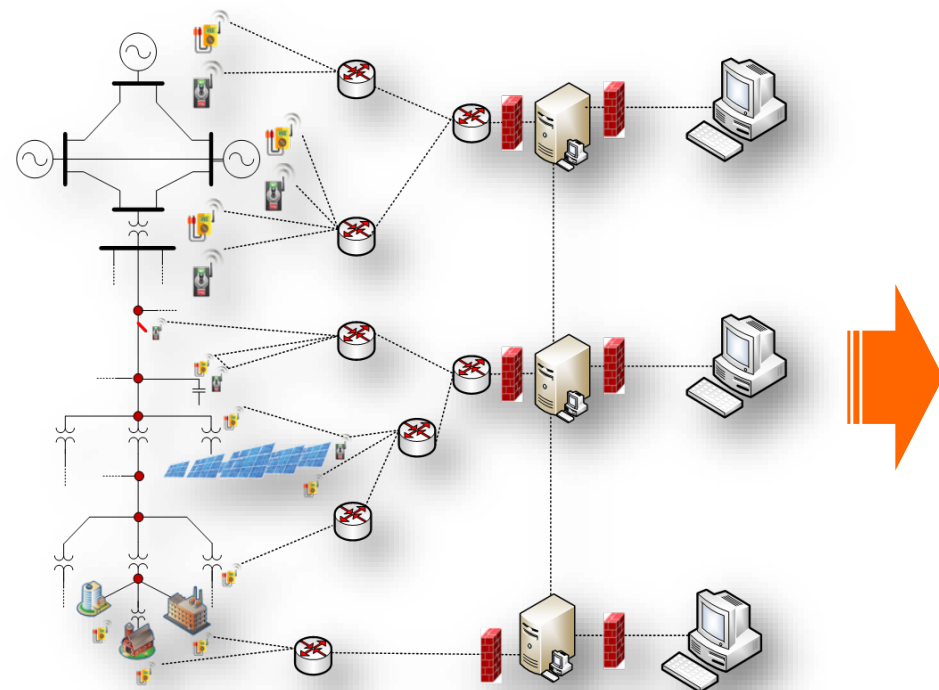
# Background & Motivation

- The cyber-power system can be modeled as
  - A three layer system



# Background & Motivation

- Three layer system



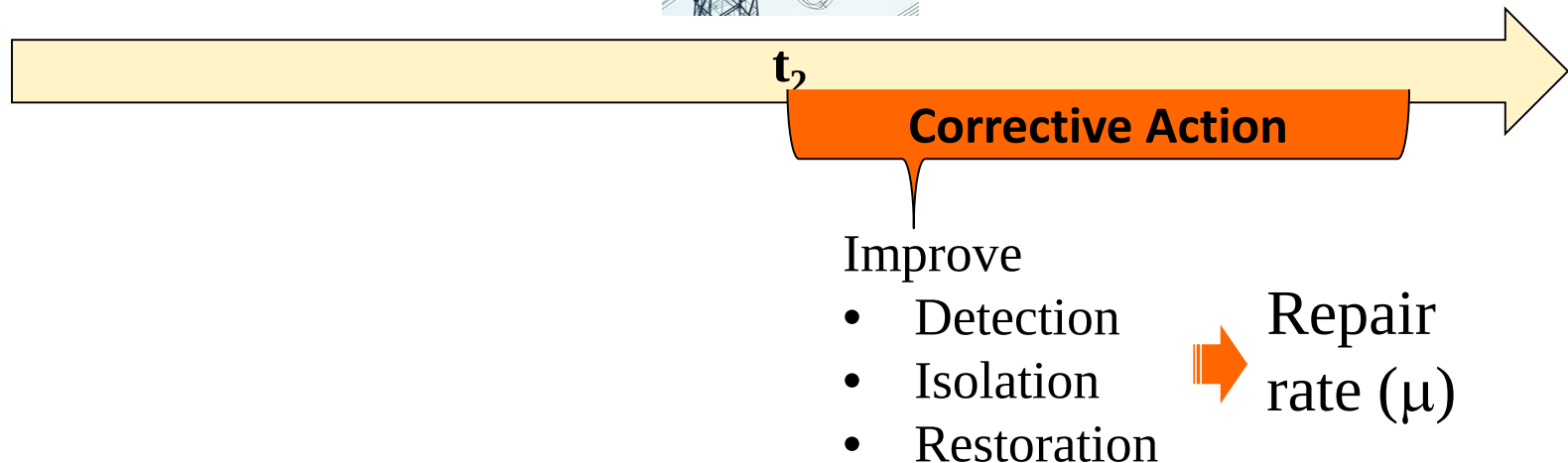


# Presentation Outline

- Background and Motivation
- **Monitoring & Preventive Maintenance**
- Effect of Communication
- Cyber System Failure Modeling
  - Scenario 1: Cyber unavailability
  - Scenario 2: Cyber attack
- Dependent System Modeling Tools: A Need
- Final Remarks and Future Needs

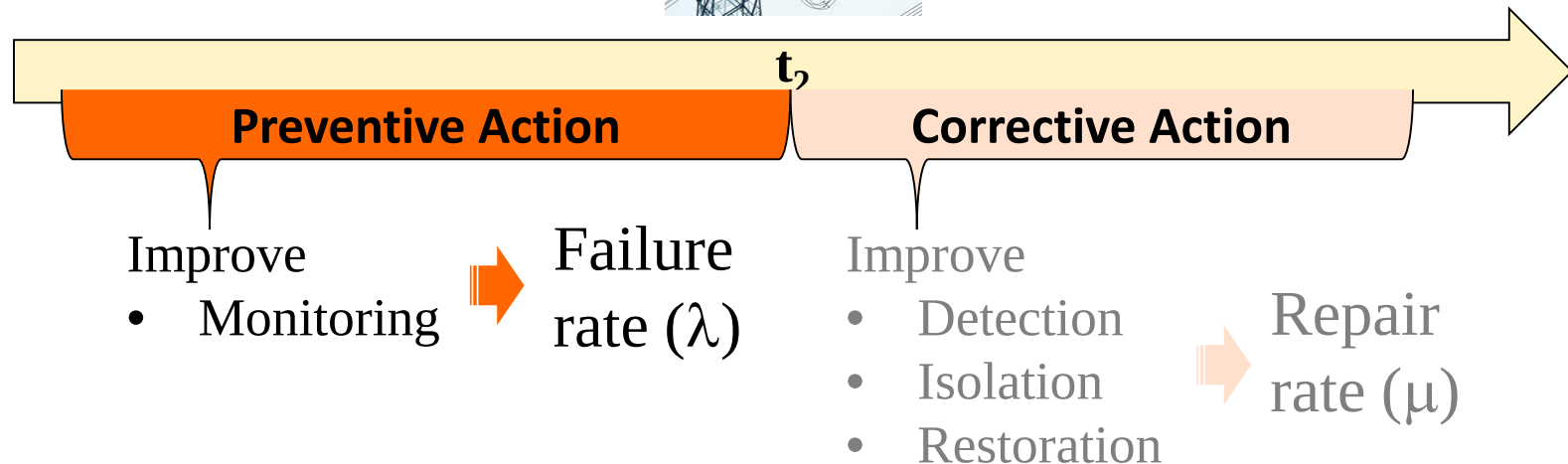
# Monitoring & Preventive Maintenance

- **A simple example for motivation**
  - Improved monitoring
- **Traditional equipment failure management**



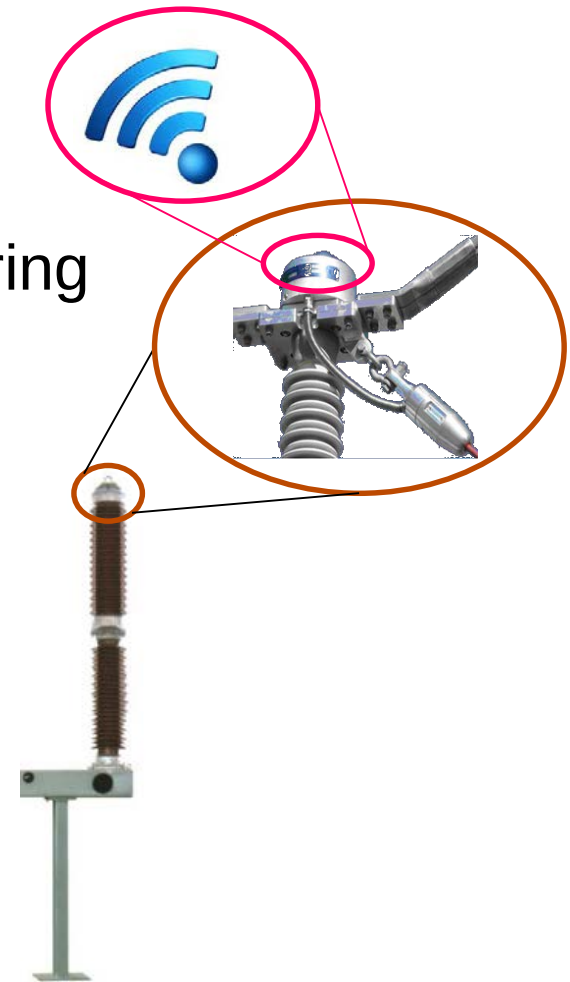
# Monitoring & Preventive Maintenance

- A simple example for motivation
  - Improved monitoring
- Preventive equipment failure management



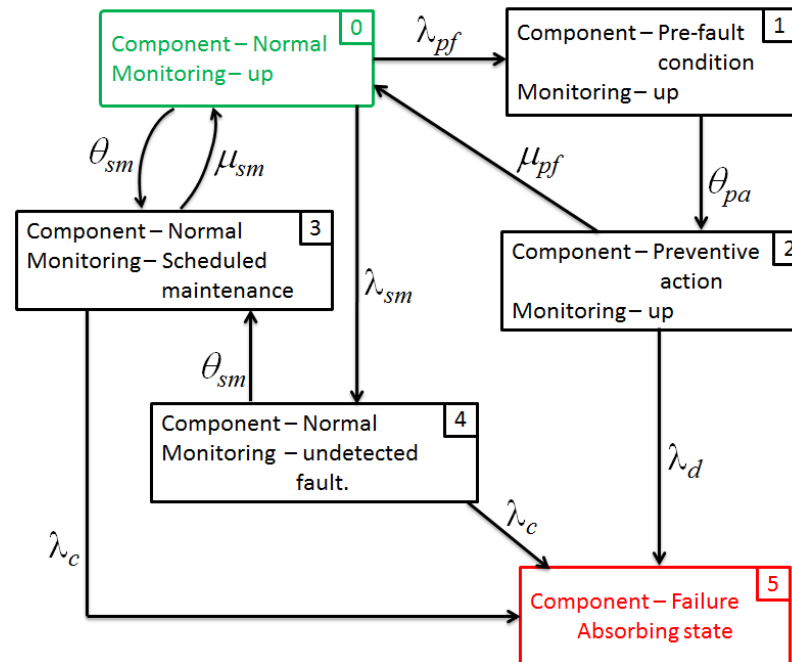
# Monitoring & Preventive Maintenance

- A simple example for motivation
  - Improved monitoring
- **Smart component:**
  - Combination of electrical & monitoring
    - Electrical equipment
      - Normal
      - Preventive action
      - Failure
      - Scheduled maintenance
    - Monitoring
      - Normal
      - Failure
      - Scheduled maintenance



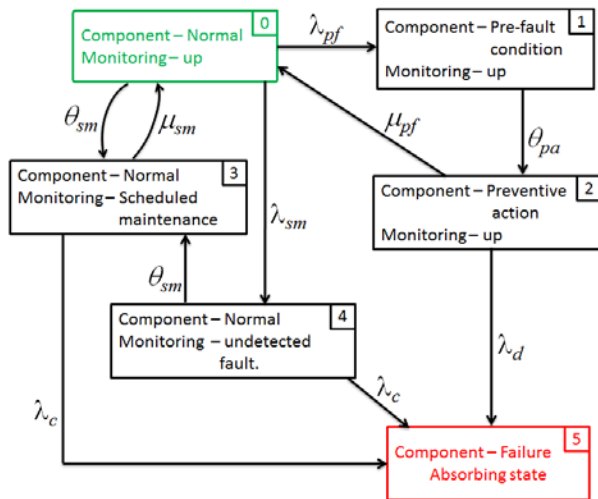
# Monitoring & Preventive Maintenance

- A simple example for motivation
  - Improved monitoring
- **Smart component:**
  - State transition model for reliability evaluation



# Monitoring & Preventive Maintenance

- A simple example for motivation
  - Improved monitoring
- **Smart component:**
  - Failure rate of the smart component (Markov Model)



State transition

$$\left\{ \begin{array}{l} \text{State 0: } p_0(\theta_{sm} + \lambda_{sm} + \lambda_{pf}) = p_2(\mu_{pf}) + p_3(\mu_{sm}) + P_5(\mu_0) \\ \text{State 1: } p_1(\theta_{pa}) = p_0(\lambda_{pf}) \\ \text{State 2: } p_2(\lambda_d + \mu_{pf}) = p_1(\theta_{pa}) \\ \text{State 3: } p_3(\lambda_c + \mu_{sm}) = p_0(\theta_{sm}) + p_4(\theta_{sm}) \\ \text{State 4: } p_4(\lambda_c + \theta_{sm}) = p_0(\lambda_{sm}) \\ \text{State 5: } p_5(\mu_0) = p(\lambda_d) + p_3(\lambda_c) + p_4(\lambda_c) \end{array} \right.$$

Smart component failure rate

$$\lambda_{sys} = \lambda_d p_2 + \lambda_c p_3 + \lambda_c p_4$$

Can be shown that  
if  $p_0 > 0$

$$\lambda_{sys} < \lambda_c$$

**Failure rate decreases**



# Presentation Outline

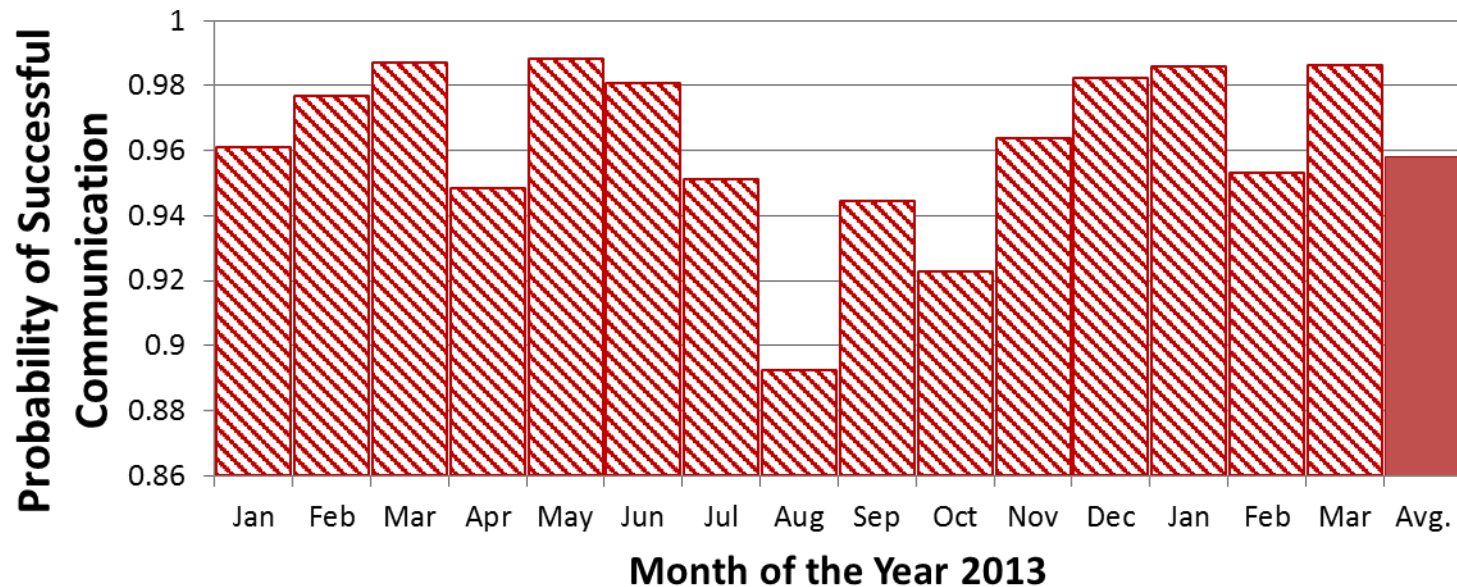
- Background and Motivation
- Monitoring & Preventive Maintenance
- **Effect of Communication**
- Cyber System Failure Modeling
  - Scenario 1: Cyber unavailability
  - Scenario 2: Cyber attack
- Dependent System Modeling Tools: A Need
- Final Remarks and Future Needs

# Effect of Communication

- **Communication network**

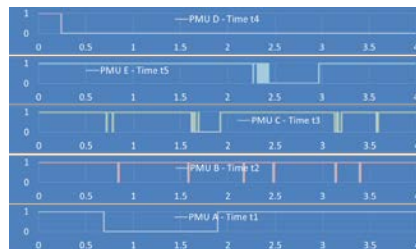
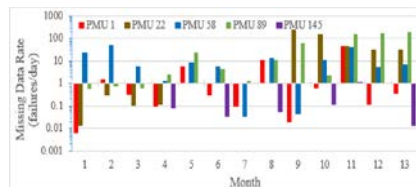
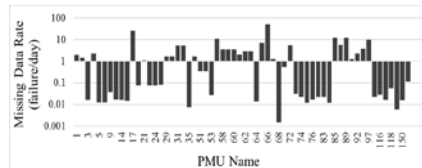


- **Successful data received rate**



# Effect of Communication

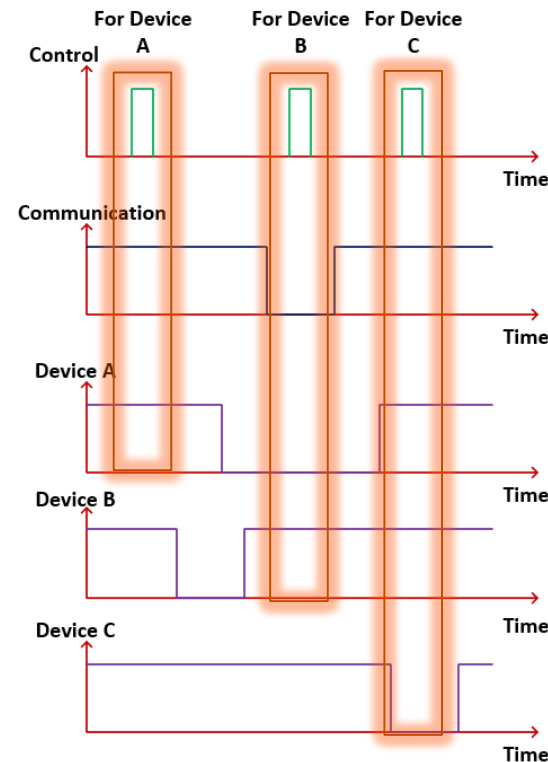
- Communication network
  - Failure data:



|                          |                         |
|--------------------------|-------------------------|
| <b>Data Availability</b> | 0.9582                  |
| <b>Missing Data Rate</b> | 3.2212 failures per day |
| <b>Recovery Rate</b>     | 0.3555 second           |

# Effect of Communication

- **Communication network**
  - How communication failure affects power system:
    - **Example: Event driven communication**
      - Application: Automatic switches

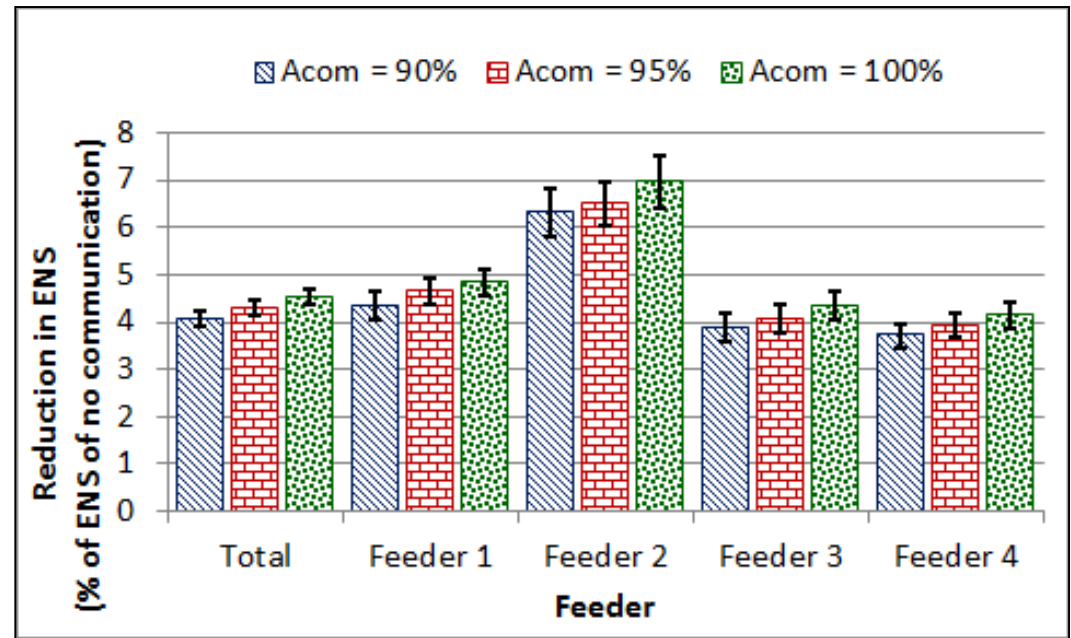
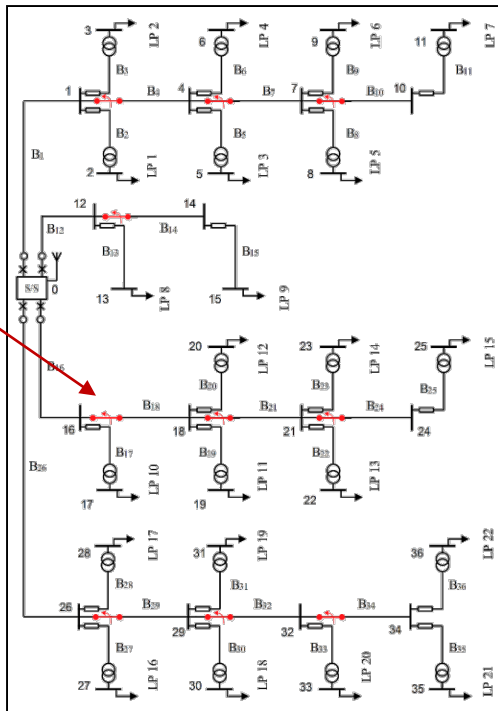


Critical to  
understand the  
dependency

# Effect of Communication

- **Communication network**
  - How communication failure affects power system:
    - **Example: Event driven communication**
      - Application: Automatic switches

Communication  
enabled  
switches



Time sequential Monte-Carlo simulation  
Unavailability based approach

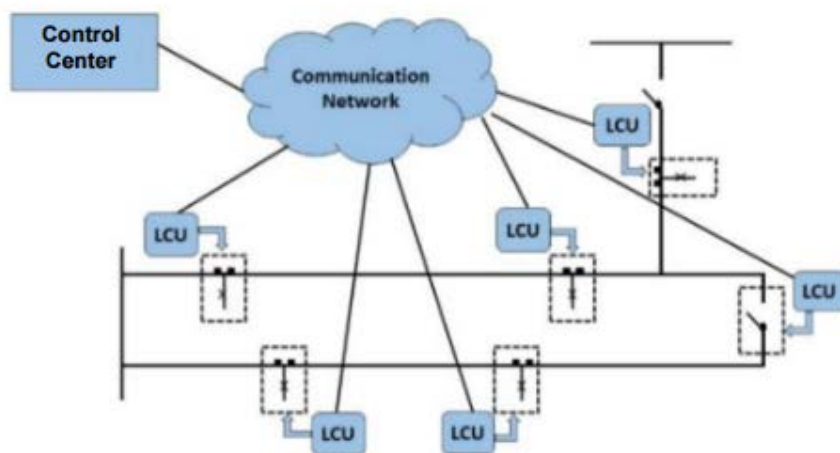


# Presentation Outline

- Background and Motivation
- Monitoring & Preventive Maintenance
- Effect of Communication
- **Cyber System Failure Modeling**
  - Scenario 1: Cyber unavailability
  - Scenario 2: Cyber attack
- Dependent System Modeling Tools: A Need
- Final Remarks and Future Needs

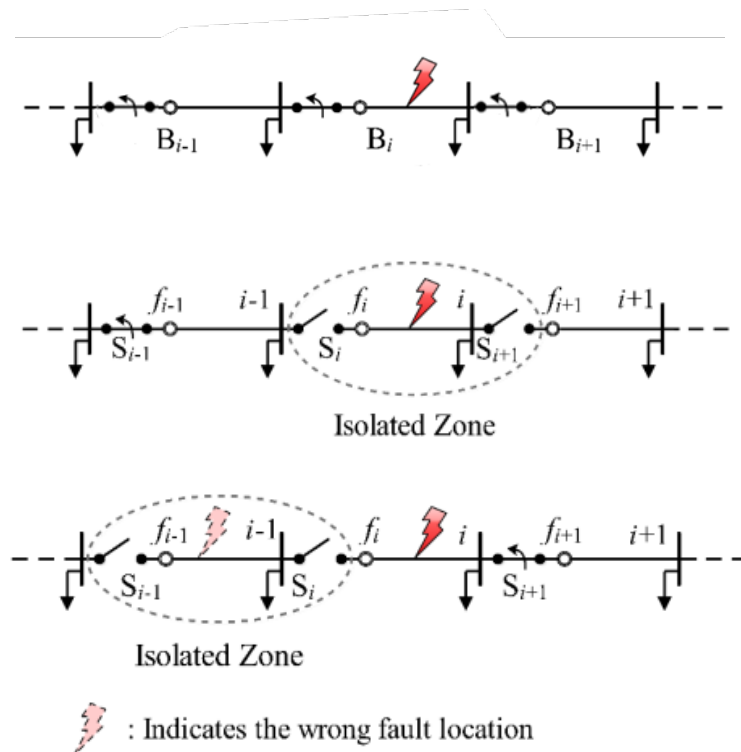
# Cyber System Failure Modeling

- Failure of cyber system
  - Scenario 1:
    - Data unavailability



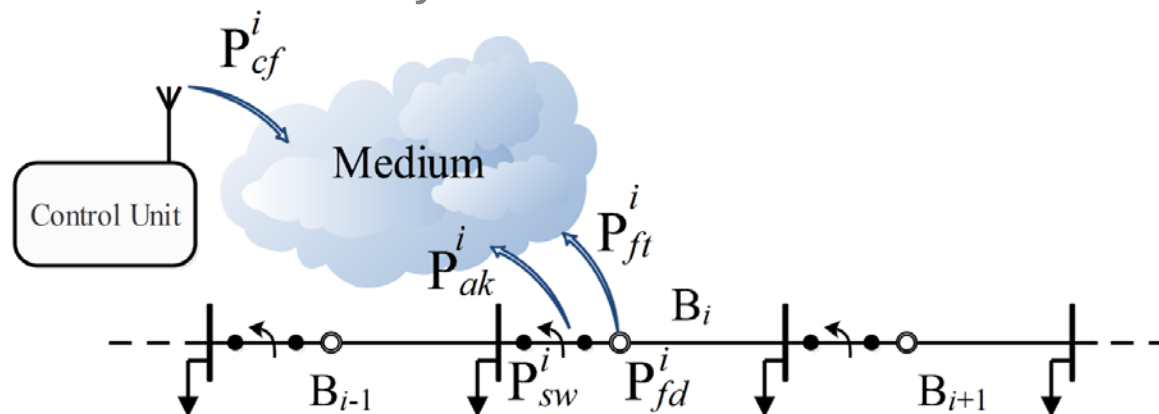
Decision is made based on the information received from fault indicators

- Communication failure can be modeled based on the network behavior



# Cyber System Failure Modeling

- Failure of cyber system
  - Scenario 1:
    - Data unavailability



Fault detector

$$P_{fi} = P_{fd}^i + (1 - P_{fd}^i)P_{ft}^i$$

Remote controlled switch

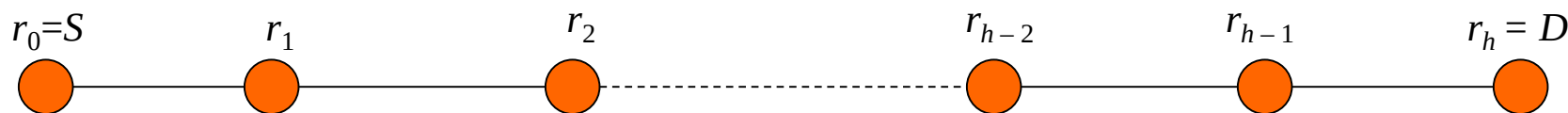
$$P_{si} = P_{cf}^i + (1 - P_{cf}^i)P_{sw}^i + (1 - P_{cf}^i)(1 - P_{sw}^i)P_{ak}^i$$

# Cyber System Failure Modeling

- **Network availability modeling**
  - Cyber network with single path



- Graph



- Probability of transmitted data from  $S$  received at  $D$

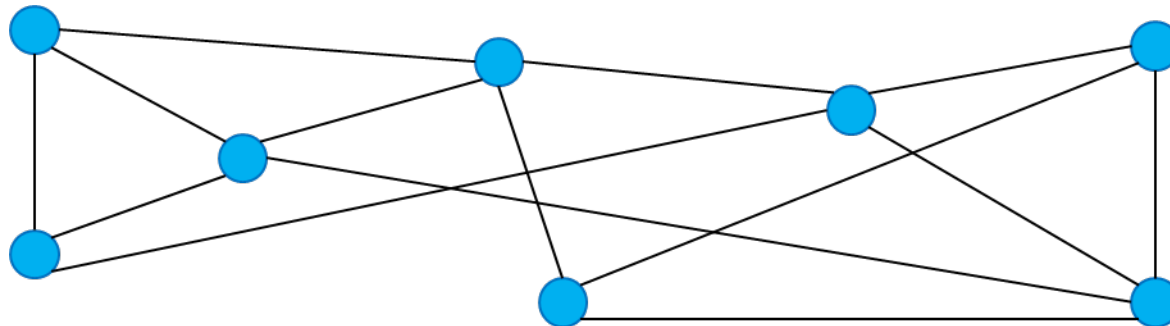
$$P_S = P_S^{(r_0 \rightarrow r_1)} * P_S^{(r_1 \rightarrow r_2)} * \dots * P_S^{(r_{h-1} \rightarrow r_h)}$$

# Cyber System Failure Modeling

- **Network availability modeling**
  - Physical network model with multiple paths

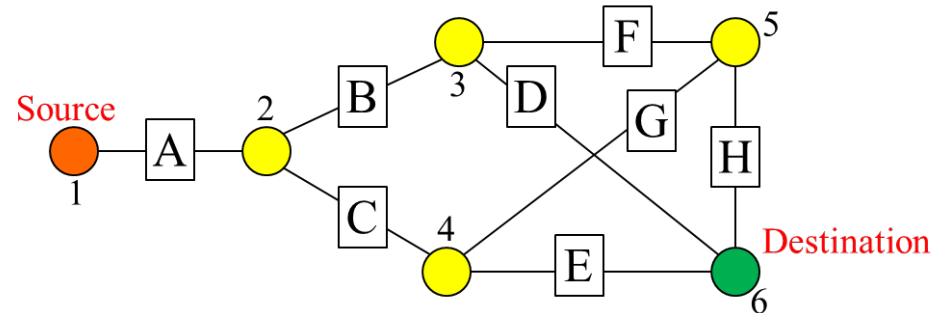


- Graph of the above model



# Cyber System Failure Modeling

- **Network availability modeling**
  - Reliability computation for multipath network



- Multiple paths between source and destination

$$A \rightarrow C \rightarrow E$$

$$A \rightarrow B \rightarrow F \rightarrow H$$

$$A \rightarrow B \rightarrow D$$

$$A \rightarrow C \rightarrow G \rightarrow H$$

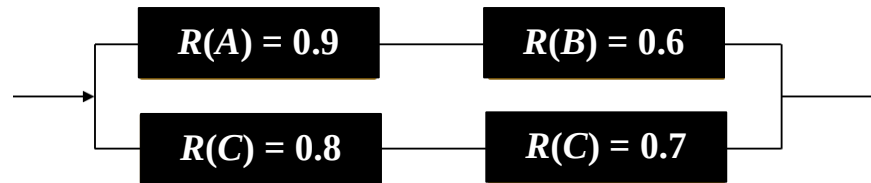
$$A \rightarrow B \rightarrow F \rightarrow G \rightarrow E$$

- Successful data transmission

$$P_S = P(A \rightarrow C \rightarrow E) \cup P(A \rightarrow B \rightarrow F \rightarrow H) \cup P(A \rightarrow B \rightarrow D) \cup P(A \rightarrow C \rightarrow G \rightarrow H) \cup P(A \rightarrow B \rightarrow F \rightarrow G \rightarrow E)$$

# Cyber System Failure Modeling

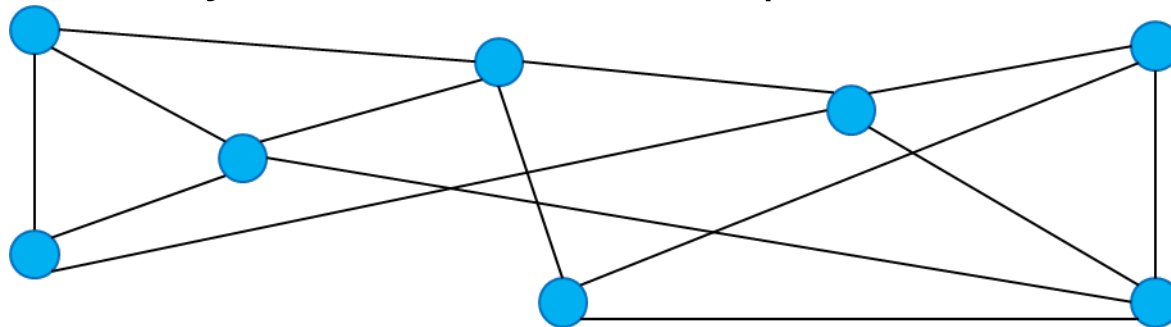
- Reliability computation



- Series parallel approach:

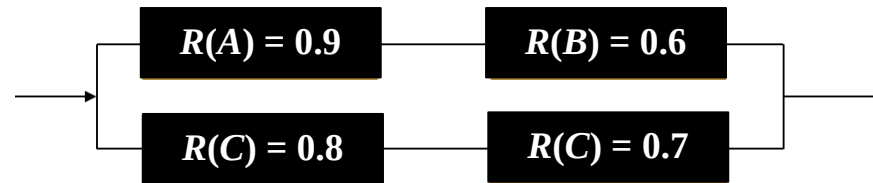
$$R_s = 1 - (1 - R_A R_B)(1 - R_C R_D) = 0.7976$$

- Simple approach but limited to either series or parallel combinations.
- Concern: Cyber network more complicated



# Cyber System Failure Modeling

- Reliability computation



- Minimal cut set approach:

- Minimal cut sets:  $\{AC\}\{AD\}\{BC\}\{BD\}$
- System structure function:

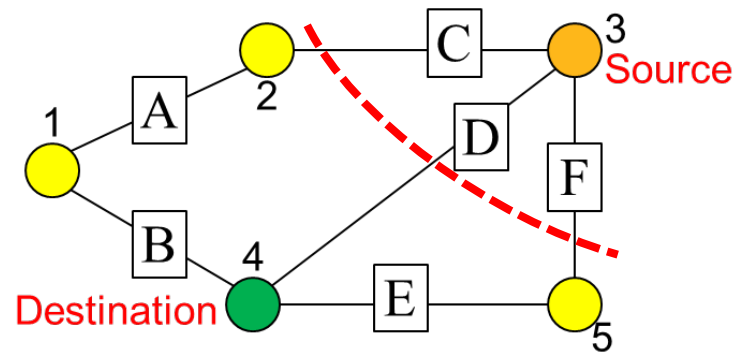
$$\begin{aligned}\psi(X_A, X_B, X_C, X_D) &= [1 - (1 - X_A)(1 - X_C)][1 - (1 - X_A)(1 - X_D)][1 - (1 - X_B)(1 - X_C)] \\ &\quad [1 - (1 - X_B)(1 - X_D)] \\ &= (X_A + X_C - X_A X_C)(X_A + X_D - X_A X_D)(X_B + X_C - X_B X_C)(X_B + X_D - X_B X_D) \\ &= X_A X_B + X_C X_D - X_A X_B X_C X_D\end{aligned}$$

- Reliability of the network

$$\begin{aligned}R_s &= E[\psi(X_A, X_B, X_C, X_D)] = E[X_A X_B] + E[X_C X_D] - E[X_A X_B X_C X_D] \\ &= R_A R_B + R_C R_D - R_A R_B R_C R_D = 0.7976\end{aligned}$$

# Cyber System Failure Modeling

- **Network availability modeling**
  - For the given simple network



- Minimal cut sets  
 $\{CDF\}$
- Structure function is given by

$$\begin{aligned}\psi_{(3,4)} &= 1 - [\{1 - (1 - X_B)(1 - X_D)(1 - X_E)\}\{1 - (1 - X_C)(1 - X_D)(1 - X_F)\}] \\ &\times \{1 - (1 - X_B)(1 - X_D)(1 - X_F)\}\{1 - (1 - X_C)(1 - X_D)(1 - X_E)\} \\ &\times \{1 - (1 - X_A)(1 - X_D)(1 - X_F)\}\{-(1 - X_A)(1 - X_D)(1 - X_E)\}\end{aligned}$$

- **Calculations becomes tedious as network gets larger**

# Cyber System Failure Modeling

- **Network availability modeling**
  - For effective computation
    - Lower bound for the link reliability can be determined
  - Reasonable lower bound
    - Place minimal cut-sets in series

$$R_{link}^{LB} = \prod_{i=1}^c \left[ 1 - \prod_{k \in s_i} (1 - R_k) \right]$$

Diagram illustrating the formula for the lower bound of link reliability ( $R_{link}^{LB}$ ).

The formula is:  $R_{link}^{LB} = \prod_{i=1}^c \left[ 1 - \prod_{k \in s_i} (1 - R_k) \right]$

Annotations:

- Total number of cut sets (points to  $c$ )
- Reliability of element  $i$  (points to  $R_k$ )
- Set of elements in cut set  $i$  (points to  $s_i$ )

# Cyber System Failure Modeling

- **Network availability modeling**

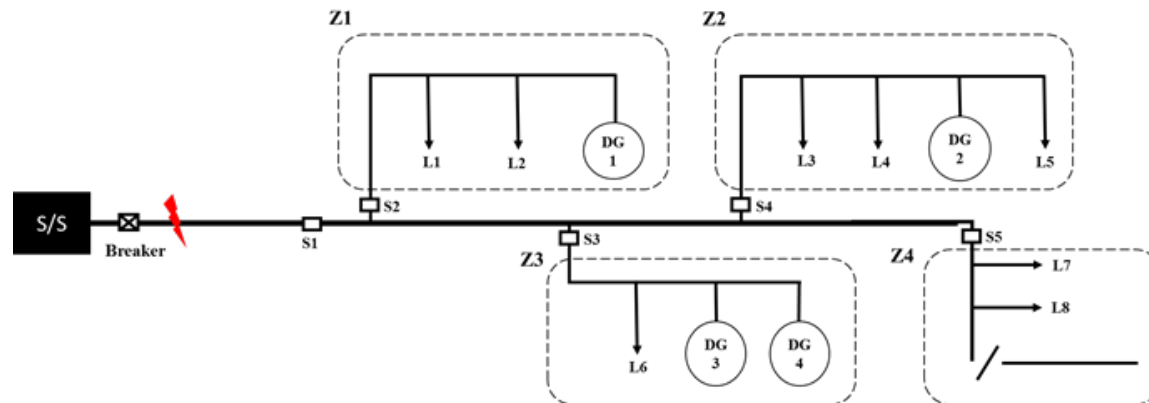
- Example:

- Communication links can be:



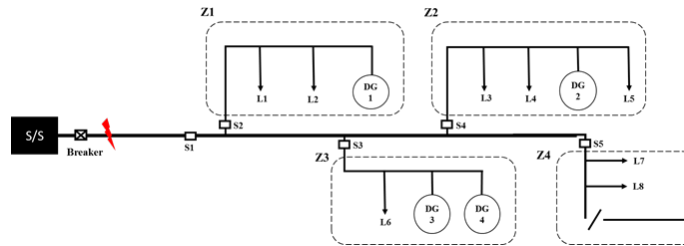
- Decisions can be: centralized or decentralized

- Simple network:

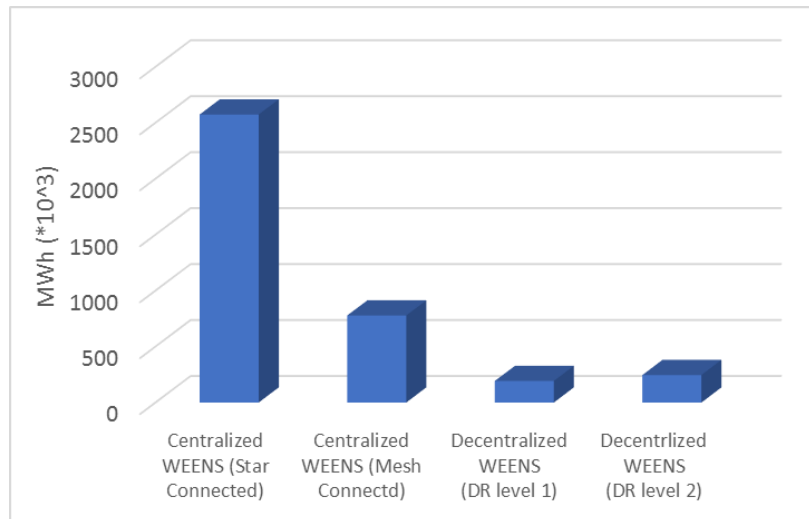


# Cyber System Failure Modeling

- **Network availability modeling**
  - Example:



- **Worst case Expected Energy Not Served (WEENS):**



**DR level 1:** Partial load curtailment  
**DR level 2:** Complete load curtailment

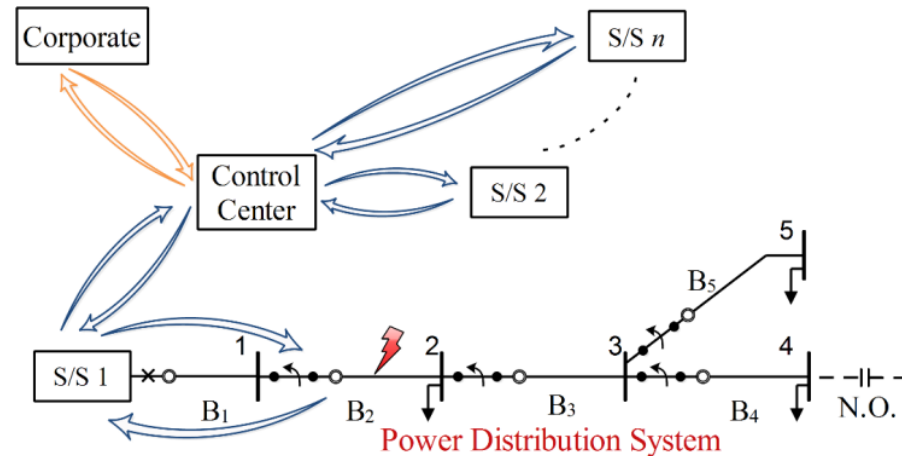


# Presentation Outline

- Background and Motivation
- Monitoring & Preventive Maintenance
- Effect of Communication
- **Cyber System Failure Modeling**
  - Scenario 1: Cyber unavailability
  - Scenario 2: Cyber attack
- Dependent System Modeling Tools: A Need
- Final Remarks and Future Needs

# Cyber System Failure Modeling

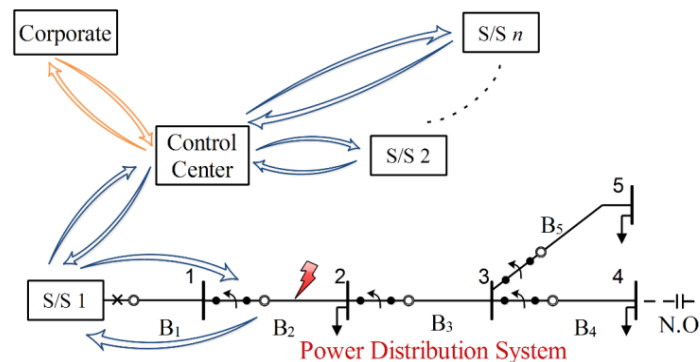
- Failure of cyber system
  - Scenario 2:
    - Information manipulation



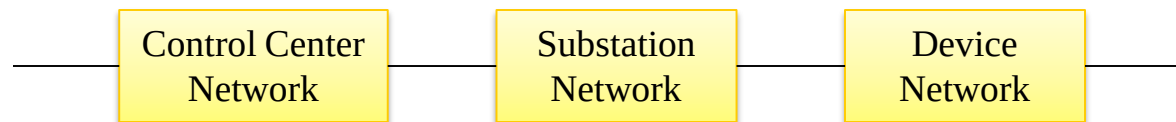
- Any of the following can be compromised
  - Control Center network
  - Corporate network
  - Substation network
  - Device level network

# Cyber System Failure Modeling

- Failure of cyber system
  - Scenario 2:
    - Information manipulation

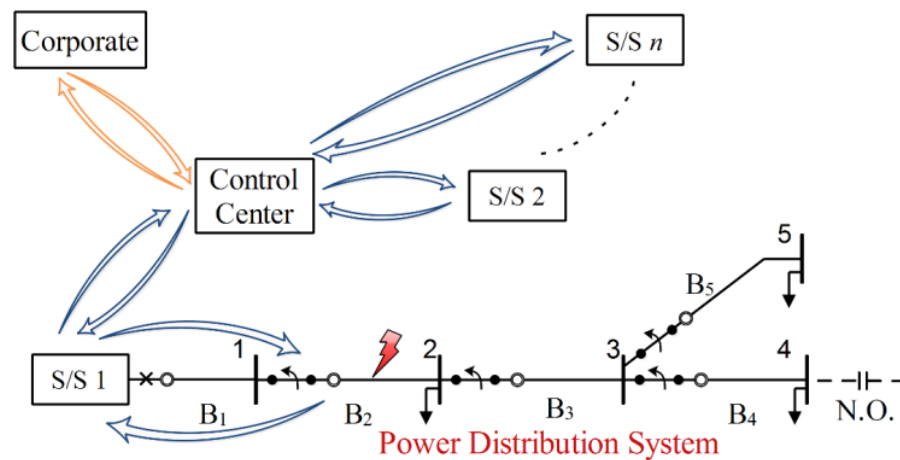


- Compromise of any one network will result in all the associated networks being compromised
  - For reliability analysis – series connected elements (if no firewall)



# Cyber System Failure Modeling

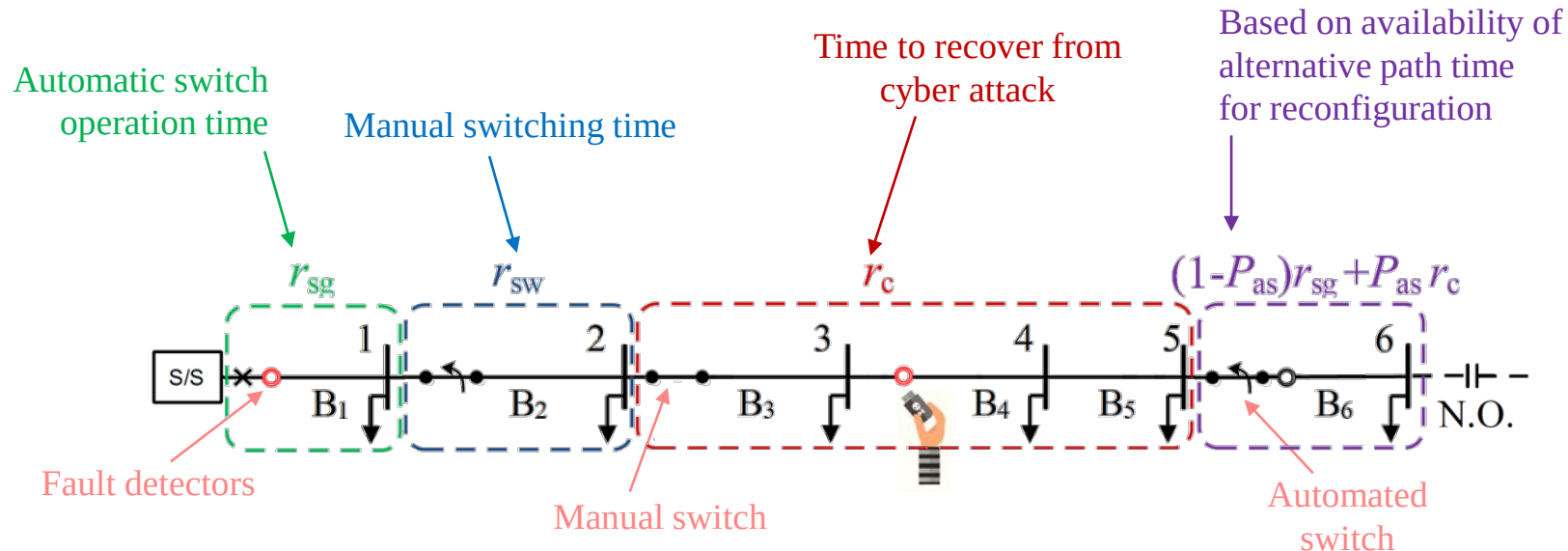
- Failure of cyber system
  - Scenario 2:
    - Effect of cyber attack



- Challenge: Attack and recovery model ...
  - Needs human behavior based modeling
  - If known then could be modeled using common mode failure approach

# Cyber System Failure Modeling

- Failure of cyber system
  - Scenario 2:
    - Effect of cyber attack



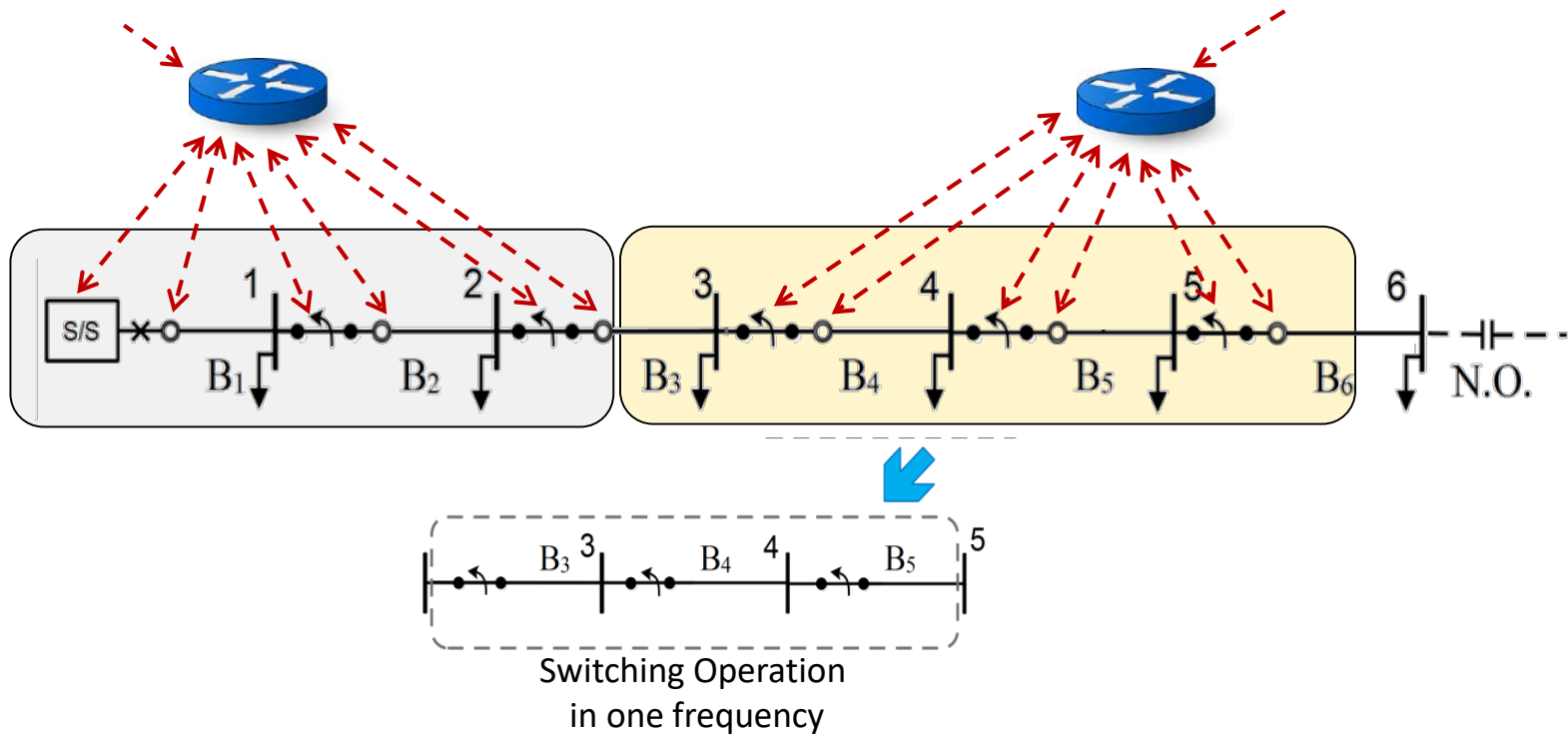


# Cyber System Failure Modeling

- **Failure of cyber system**
  - **A single effect (attack) can affect multiple parts (network)**
  - **Common cause failure (CCF) model:**
    - A group of components fail due to a shared cause
      - The reason behind the failure (root cause)
      - Which parts are affected and why (coupling factor)
    - An event that causes a set of components to fail is known as common cause event (CCE).
    - Components that could fail for the same cause(s) are grouped together; common cause component group (CCCG)

# Cyber System Failure Modeling

- Failure of cyber system
  - Common cause failure (CCF) model:
    - Example:



# Cyber System Failure Modeling

- **Dependent failures**

- **Step 1:** Determine the common cause component group (CCCG)
- **Step 2:** Determine basic event probabilities
  - For example alpha factor method can be used
    - A component can fail due to
      - Independent failure of the given component
      - Dependent failure due to  $k$  out of  $m$  components
      - *Assume equal probability of occurrence*

All possible  
ways

$$\alpha_k = \frac{\binom{m}{k} P_k}{\sum_{j=1}^m \binom{m}{j} P_j}$$

Probability

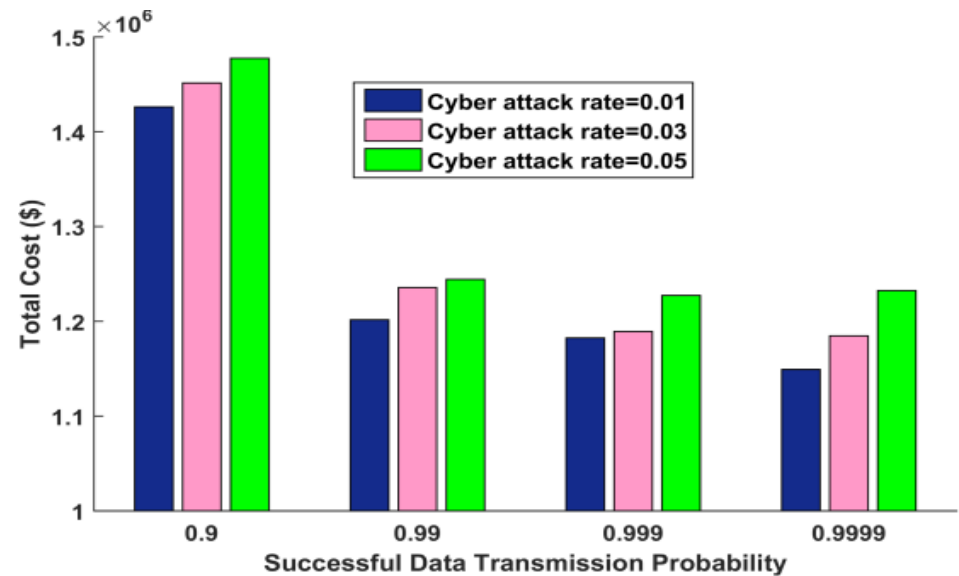
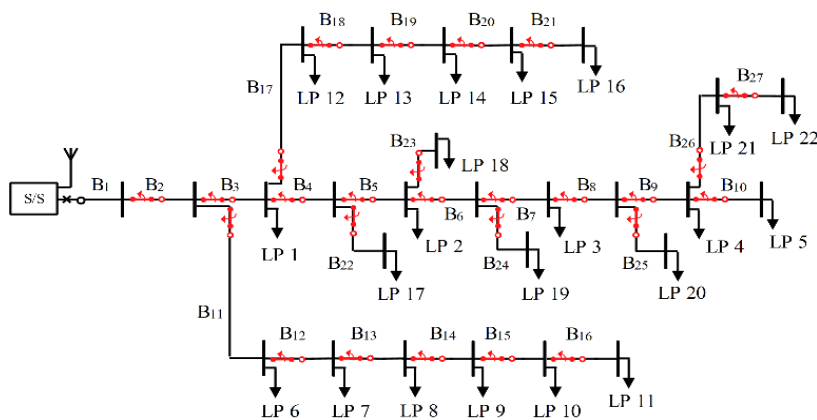
Dependent failure  
probability

$$P_k^{(m)} = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\sum_{j=1}^m j \alpha_j} P_{t(k)}$$

Total failure probability  
of component  $k$

# Cyber System Failure Modeling

- **Fault detector & automatic switch placement based on the cost**
  - **Objective: minimize**
    - Investment cost (switch and fault detectors)
    - Expected interruption cost for customers



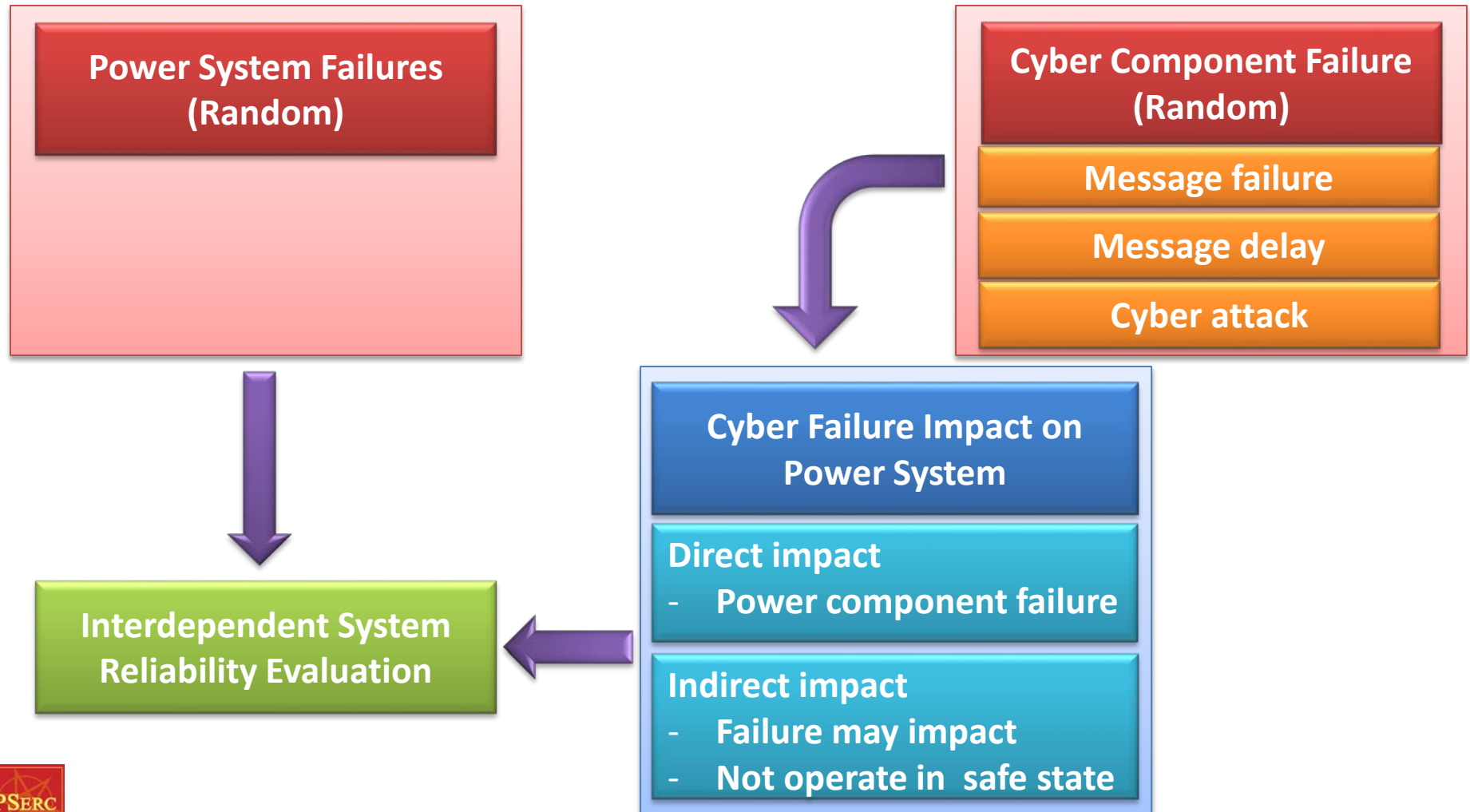


# Presentation Outline

- Background and Motivation
- Monitoring & Preventive Maintenance
- Effect of Communication
- Cyber System Failure Modeling
  - Scenario 1: Cyber unavailability
  - Scenario 2: Cyber attack
- **Dependent System Modeling Tools: A Need**
- Final Remarks and Future Needs

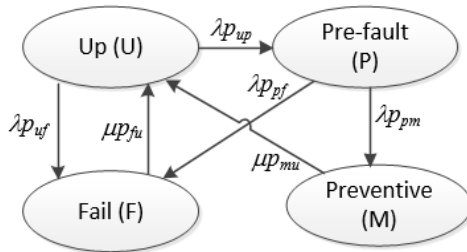
# Dependent System Modeling Tools: A Need

- Required approach

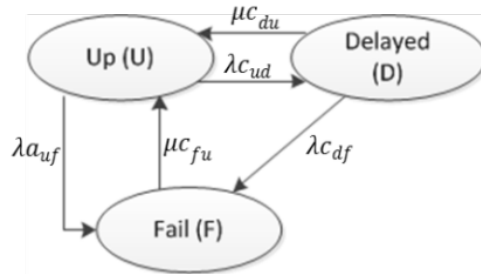


# Dependent System Modeling Tools: A Need

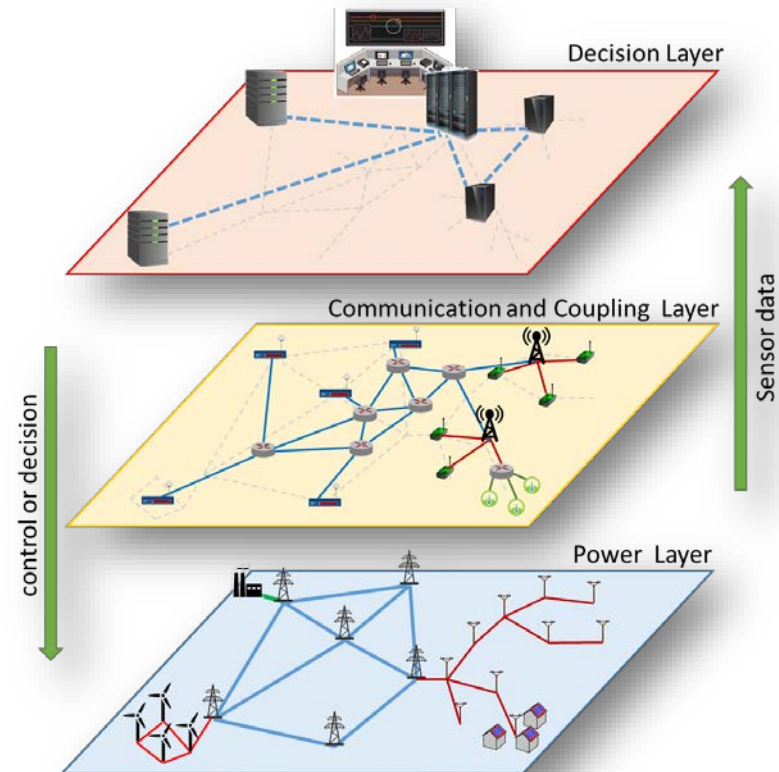
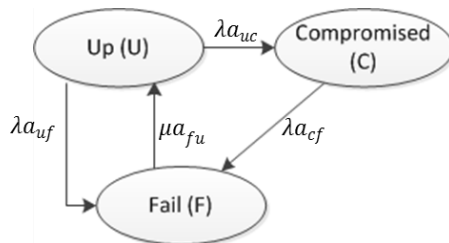
- Failure modes
  - Power component



- Communication and coupling



- Decision





# Presentation Outline

- Background and Motivation
- Monitoring & Preventive Maintenance
- Effect of Communication
- Cyber System Failure Modeling
  - Scenario 1: Cyber unavailability
  - Scenario 2: Cyber attack
- Dependent System Modeling Tools: A Need
- **Final Remarks and Future Needs**



# Final Remarks

- Cyber system benefits are correlated with power system operational needs
- A three layer approach can be utilized by separating
  - Power components
  - Communication and coupling components
  - Decision components
- Dependent system based modeling increases possible states of operations
- Adjustments to reliability analysis is required with
  - Understanding of communication link failure
  - Understanding cyber attack



# Future Needs

- A unified analytical framework for cyber-power system needs to be better established.
- Effective modeling of cyber-unavailability and cyber-manipulation is a prerequisite.
- A human behavior based modeling for cyber attack can provide better insight
- Propagation of cyber failure on power system application (similar to cascading failure) needs to be further studied.



# Final-Final Remarks

- Cyber solutions become more effective if:
  - Power system applications are more identified
  - Dependent effects of cyber and power systems are better understood
  - Solutions utilize the properties of both cyber & power
  - An appropriate performance evaluation tool is used to assess the benefits against the cost and adaptability.

# Questions?

**Visvakumar Aravinthan**

([Visvakumar.aravinthan@wichita.edu](mailto:Visvakumar.aravinthan@wichita.edu))



# Presentation Outline

- Background and Motivation
- Monitoring & Preventive Maintenance
- Effect of Communication
- Cyber System Failure Modeling
  - Scenario 1: Cyber unavailability
  - Scenario 2: Cyber attack
- Dependent System Modeling Tools: A Need
- Final Remarks and Future Needs
- **System Properties Based Communication**

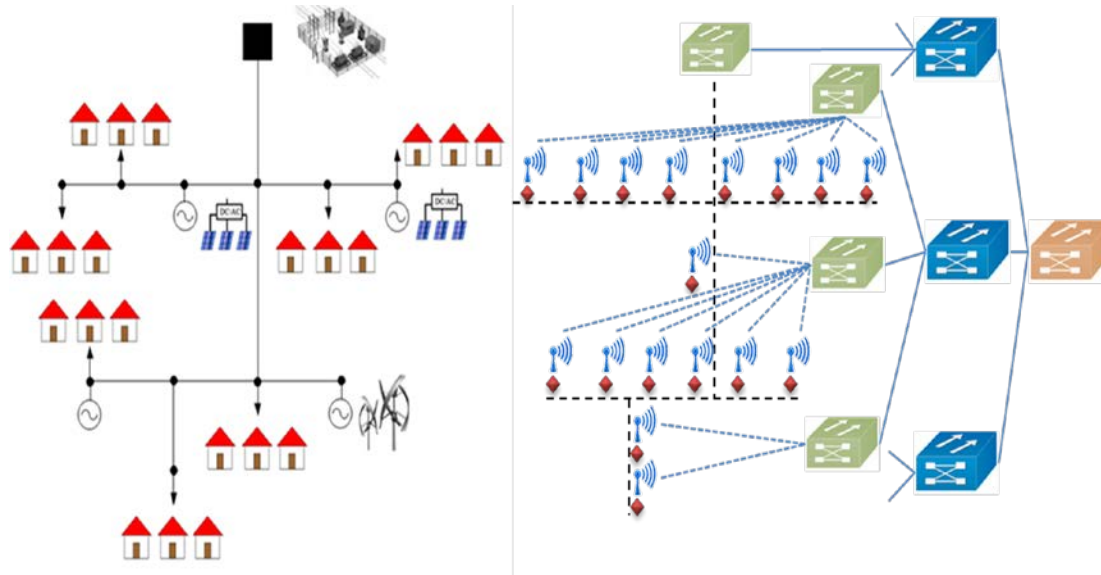


# System Properties Based Communication

- Cyber infrastructure can improve reliability
  - How to enhance the benefits
- One of the options
  - Distributed Sensor Network at feeder level.
  - Event driven communication protocol for distribution
    - Communicate upon an event
    - Not communicate periodically
- One application
  - Use power system properties in communication protocol in anomaly detection applications.

# System Properties Based Communication

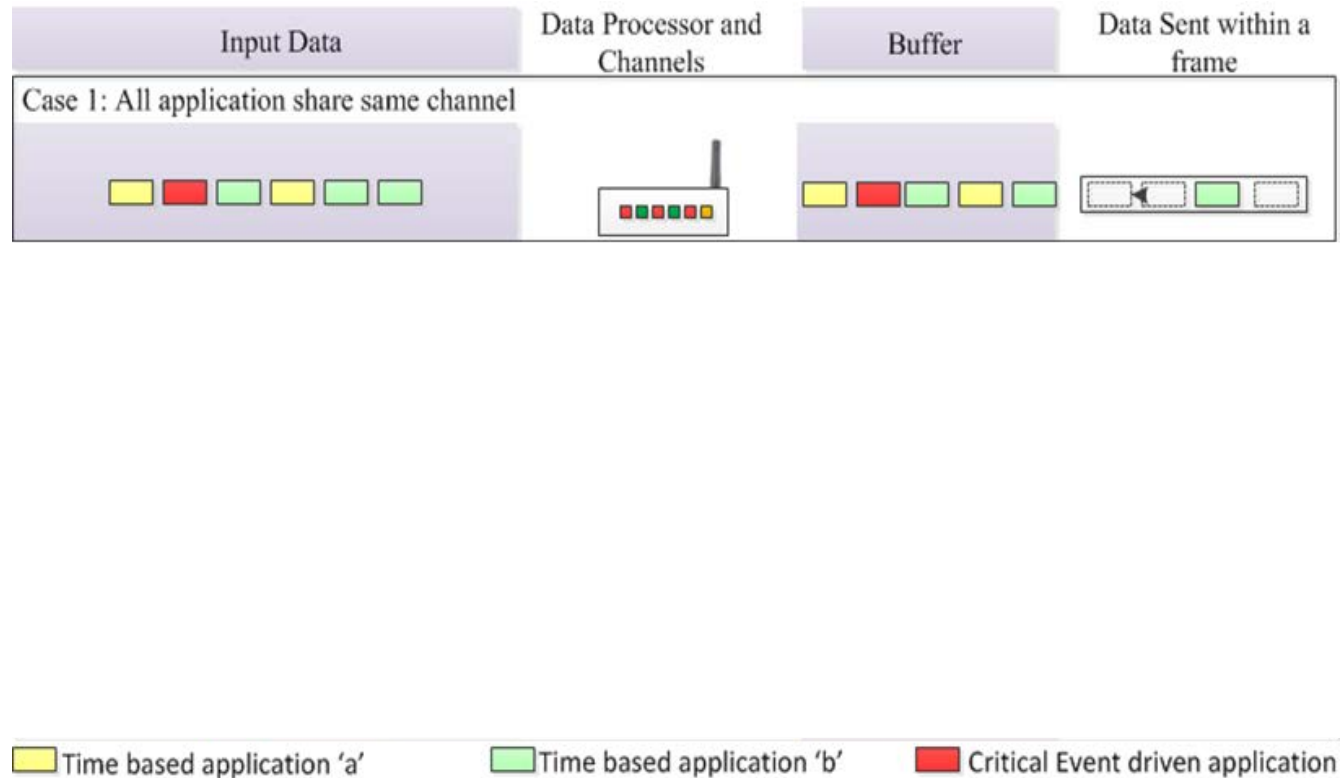
- Distributed sensor network



- Hierarchical communication architecture.
- **Lower level** - WiMax , **Upper Level** – Wired.
- Use mesh network architecture between the control centers and the substation level communication

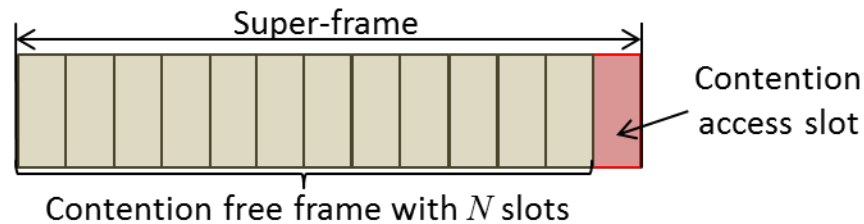
# System Properties Based Communication

- Communication Delay – lost packets
  - Identify a protocol that will prioritize time sensitive data

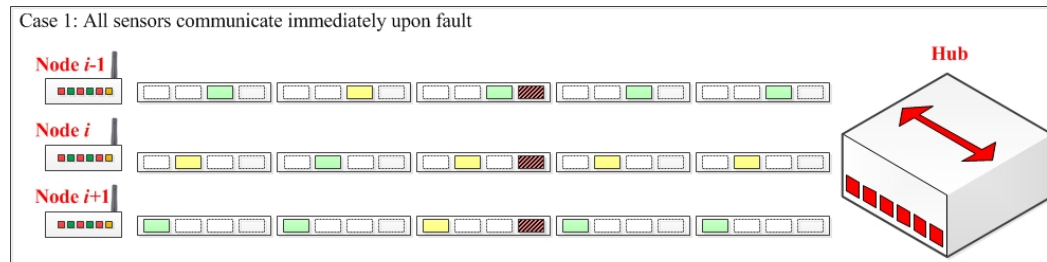


# System Properties Based Communication

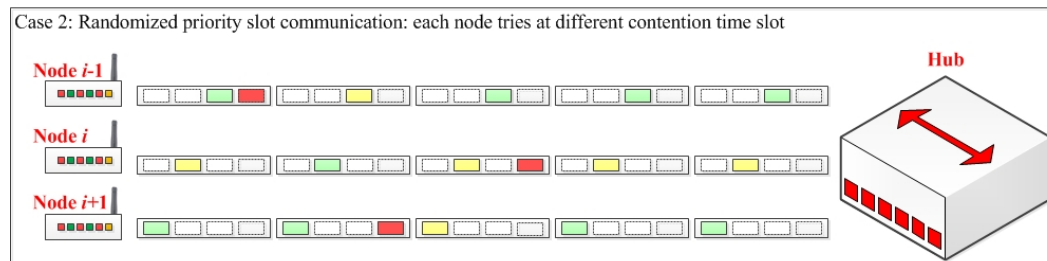
- Communication Delay – lost packets
  - Allocate the first slot for time sensitive data



- Problem:

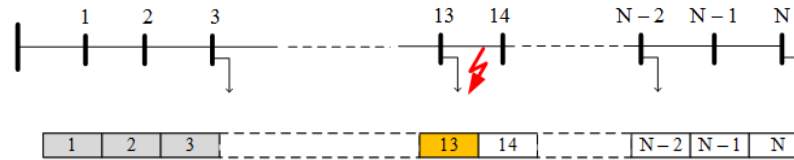


- Solution:

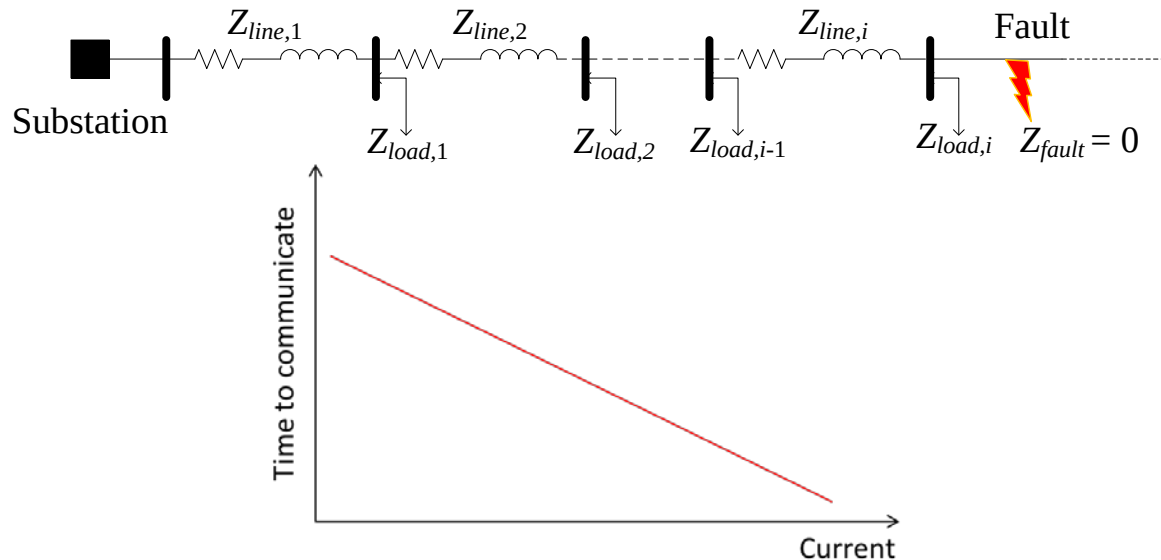


# System Properties Based Communication

- Communication Delay – lost packets
  - Allocate based on the location

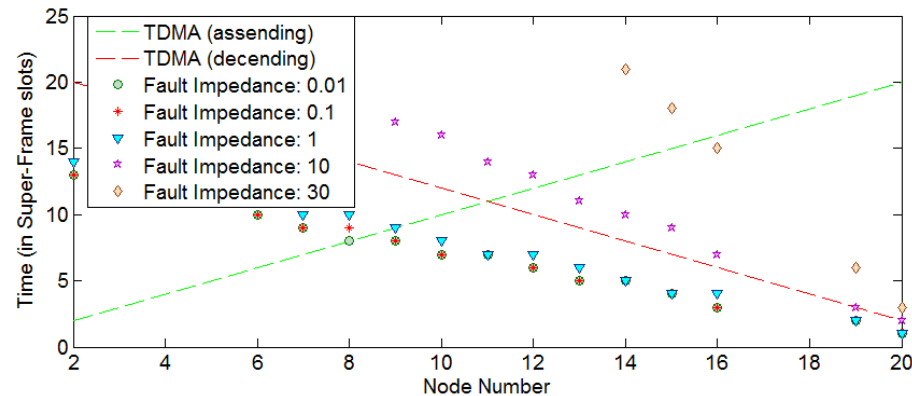


- Or incorporate power system properties



# System Properties Based Communication

- Communication Delay – lost packets
  - Specific node communicating 100% of the time



- Latency

