# *Keeping Future Grid Secure and Smart*

## CHEN-CHING LIU
## PROFESSOR OF POWER SYSTEMS
## UNIVERSITY COLLEGE DUBLIN

*Transforming Ireland – Mobilising Innovation and Enterprise to Become a Prosperous Low Carbon Society*

# Disturbances on Power Grid

## Example Events in Eirgrid

1. June 8, 2009 under frequency event - Nadir 49.29 Hz;
2. Feb 1, 2008 under frequency event - Nadir 49.21 Hz;
3. June 20, 2007 transmission fault-system minutes 2.470;
4. May 20, 2006 under frequency event - Nadir 49.28 Hz;
5. Aug 5, 2005 under frequency event - Nadir 48.41 Hz;
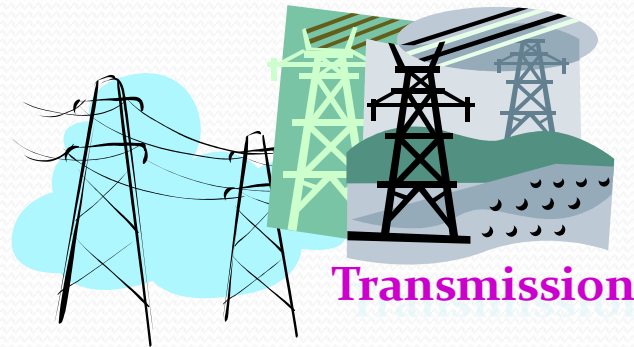
**Reliability Criteria**

**Security**
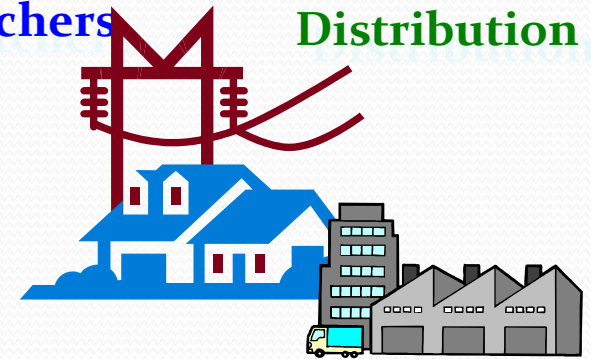
**On-line Security Assessment**

**Supply Planning**

# Power System Security



Transmission

Generation

Control Centre and Dispatchers

Distribution

Reference : Renewable Energy Outlook 2030, www.energywatchgroup.org
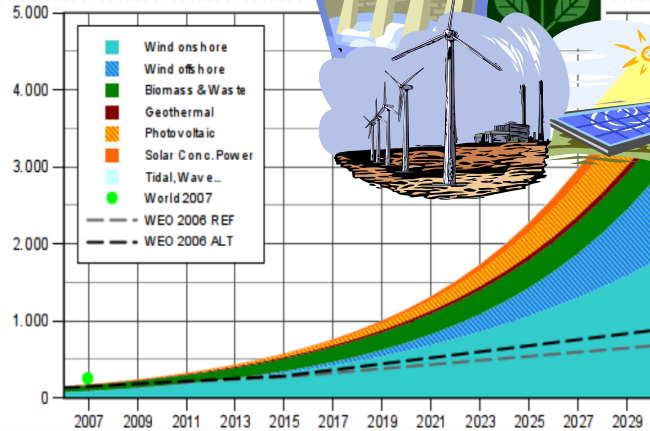
# Offshore Network Security
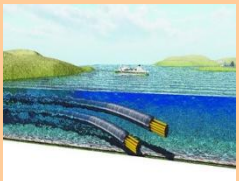
**EU Programme:** Transmission system operation with large penetration of Wind and other renewable Electricity sources in Networks by means of innovative Tools and Integrated Energy Solutions

**Challenges for offshore wind power**

**Intermittent Generation**

**HVDC Connection**
- Long distance
- Large capacity

*Standardized Requirements of Security for Offshore*

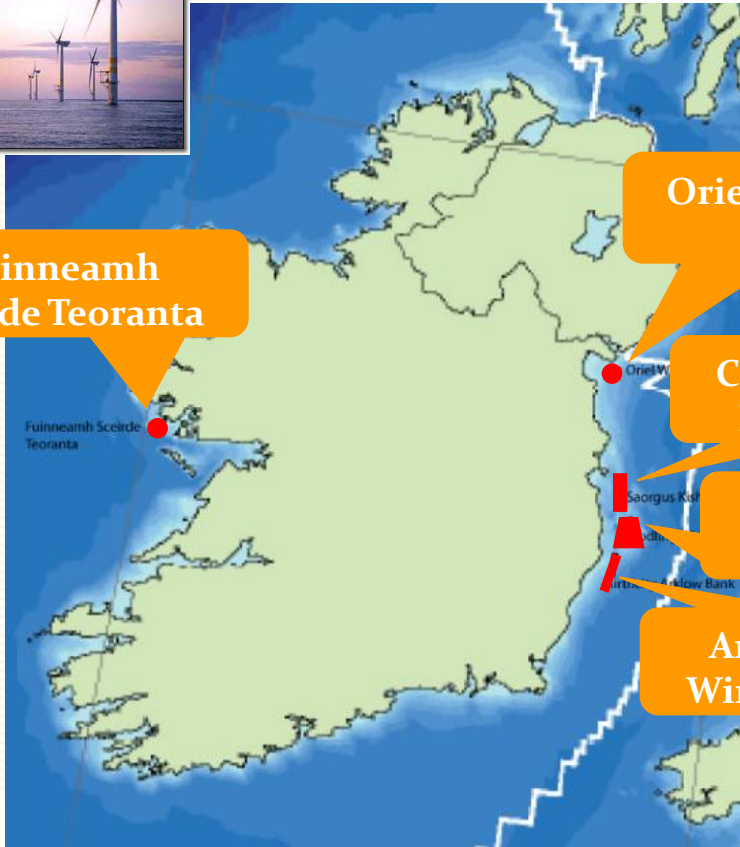✓ **Special Protection Scheme**

✓ **Coordinated Protection**

# Offshore Wind Projects



Offshore Wind Farm Interconnection

Fuinneamh Sceirde Teoranta

Oriel Windfarm 330WM

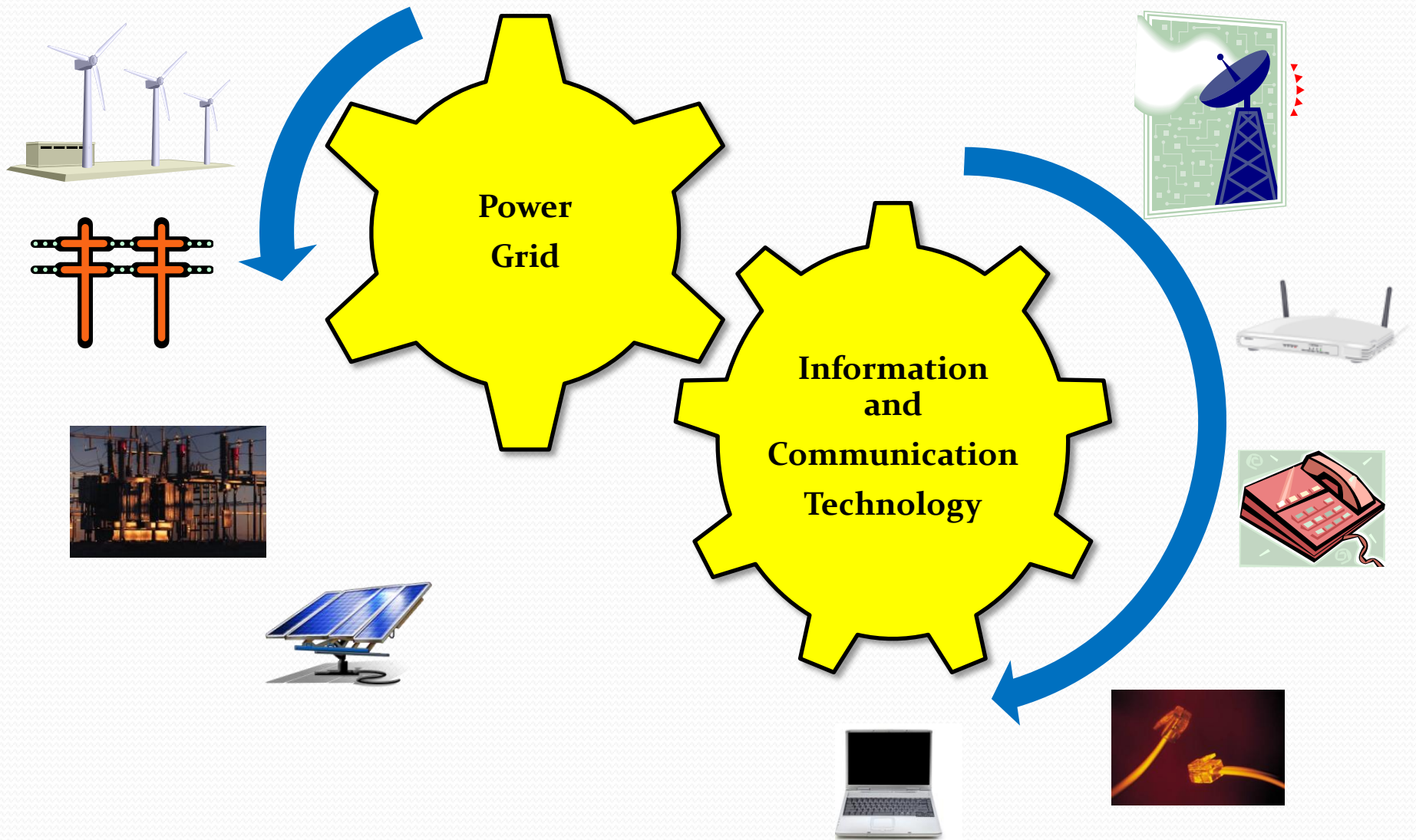Codling Wind Park-1.1GW

Saorgus Kish Bank

Arklow Bank Windfarm-1GW

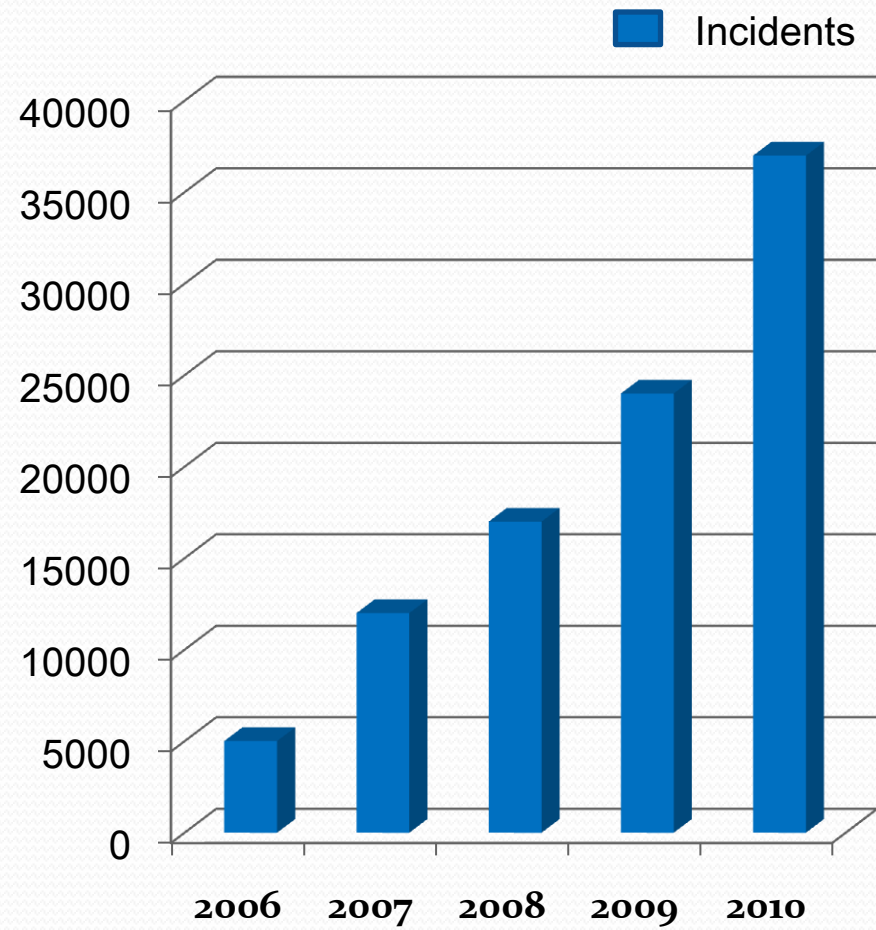Special Protection?

Coordinated Protection?

System Restoration?

......

# Power Grid with ICT
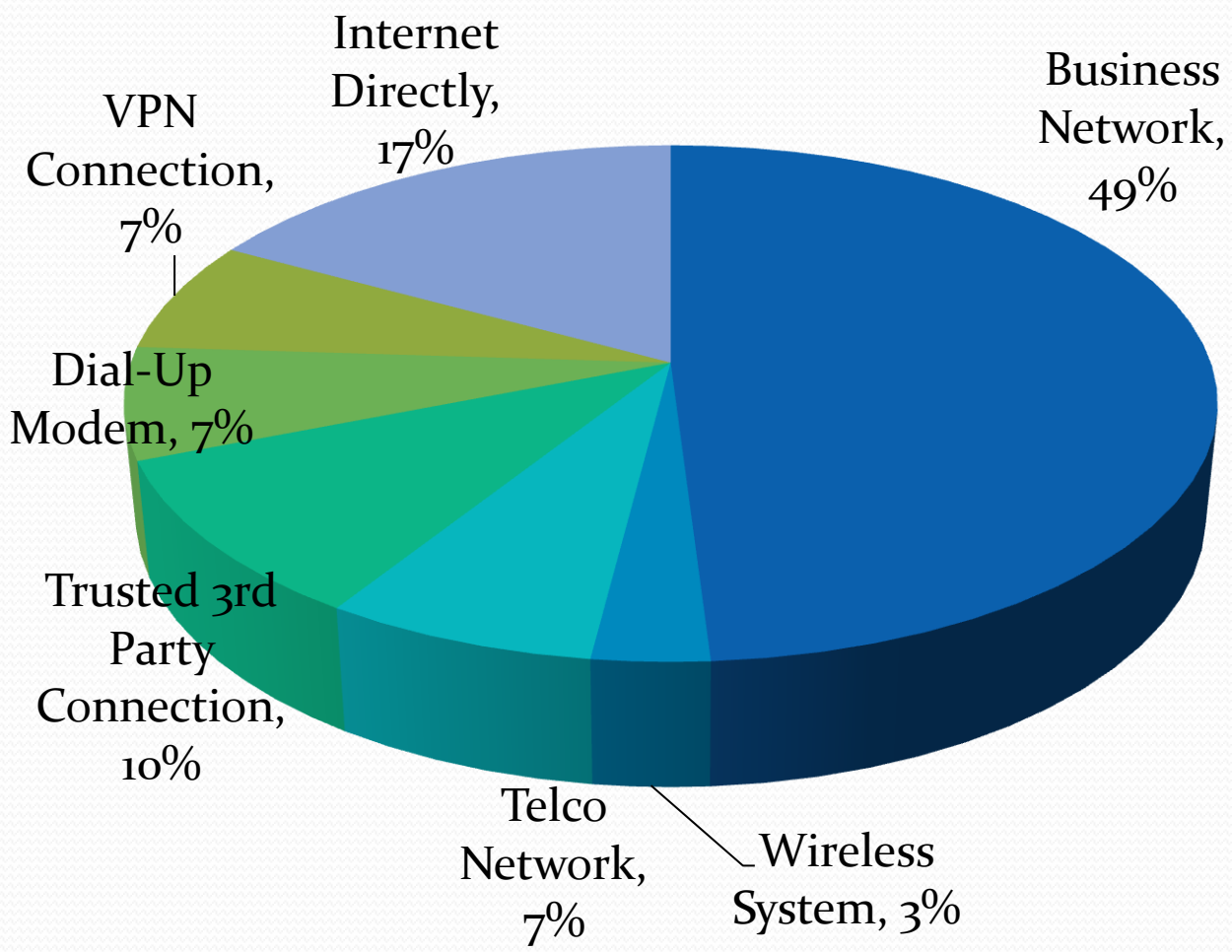
# Cyber Attacks

# Example of Cyber Attack

Source: www.digitaljournal.com

CIA Confirms Cyber Attack Caused Multi-City Power Outage

On Jan 18, 2008, in New Orleans, US CIA senior analyst Tom Donahue told a gathering of 300 US, UK, Swedish, and Dutch government officials and engineers and security managers from electric, water, oil & gas and other critical industry asset owners from all across North America, that "We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. ***We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States....***"

# Attack Points



Pie chart: Attack Points

- Business Network, 49%
- Internet Directly, 17%
- VPN Connection, 7%
- Dial-Up Modem, 7%
- Trusted 3rd Party Connection, 10%
- Telco Network, 7%
- Wireless System, 3%

SFI PI Award: Vulnerability Assessment and Mitigation of ICTs for Critical Infrastructures (Collab: Iowa State Univ., Ind. Advisors: Eirgrid, ERSE, RTE France, INTEL)
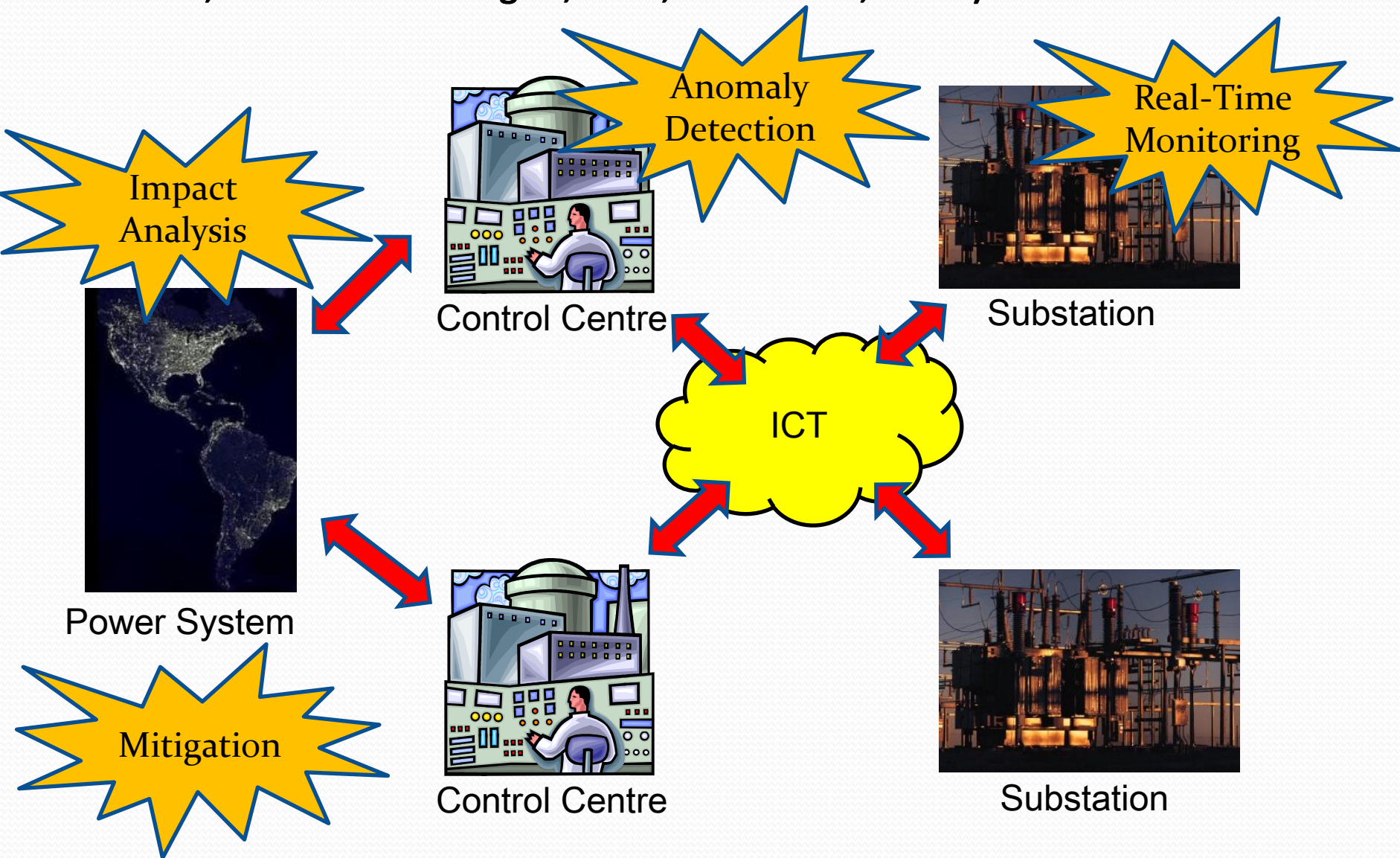
# Detecting Anomaly at Substation



Database

Human Machine Interface

Intelligent Electronic Devices

Anomaly Detection Algorithm
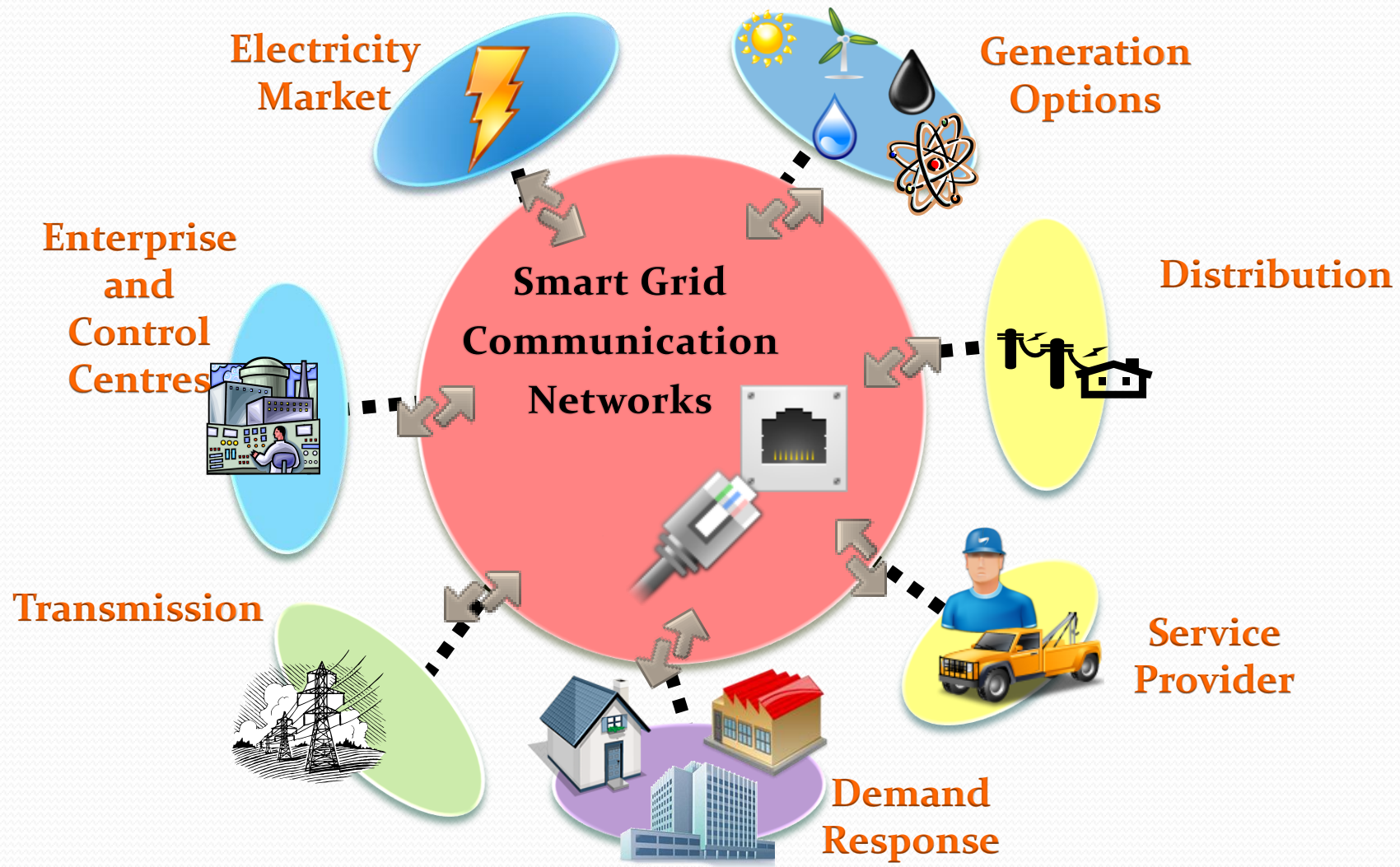
Anomaly Detection

# Smart Grid



Electricity Market

Generation Options

Enterprise and Control Centres

Smart Grid Communication Networks

Distribution

Transmission

Service Provider

Demand Response

# Electricity and Information Flows on Smart Grid



Information Flow

Electricity Flow

Source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0

13
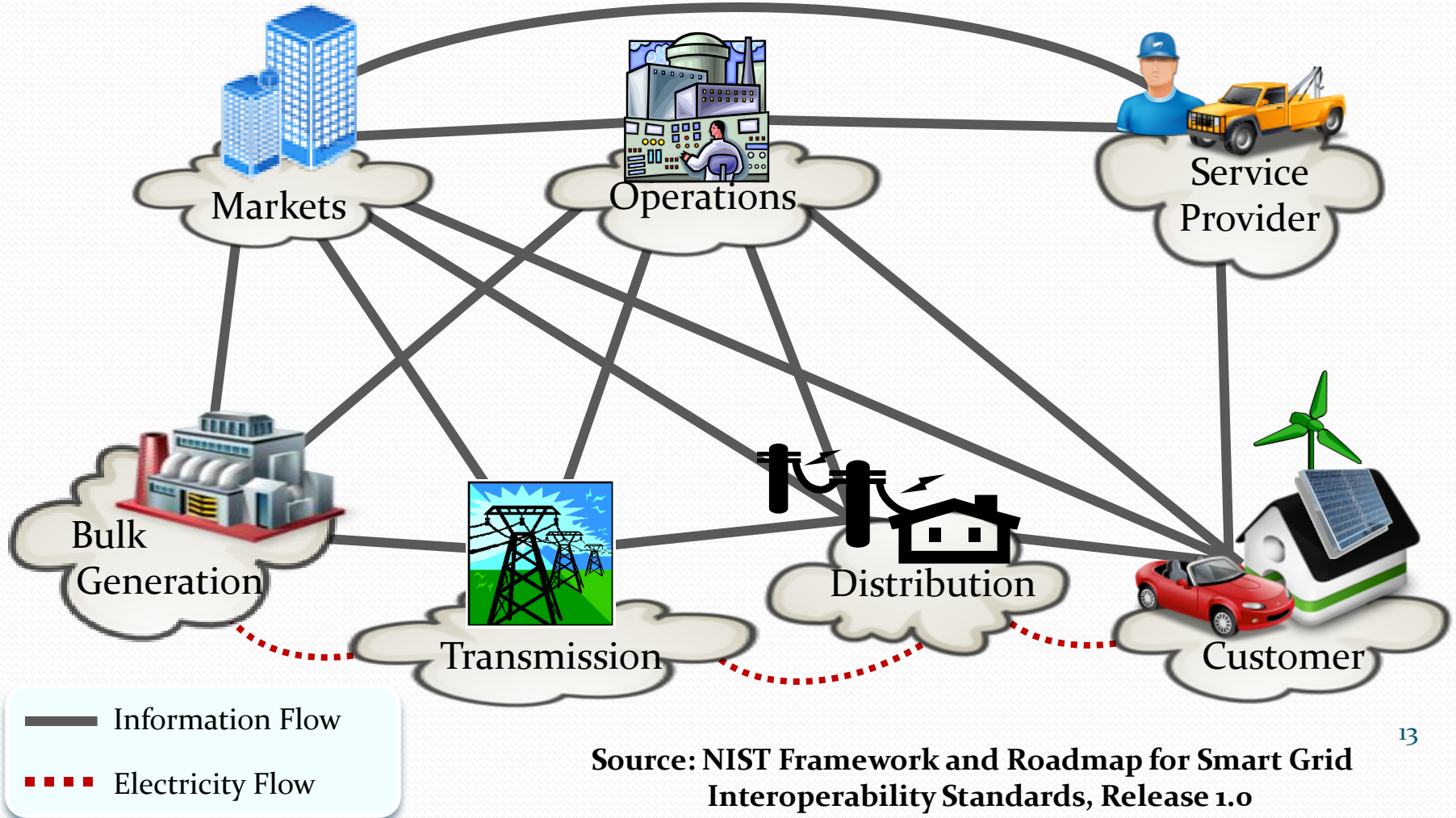
# Security and Privacy

## Personal Information
- Name, Address
- Account Number

## Meter Reading
- Meter IP, Service Provider
- Usage Pattern
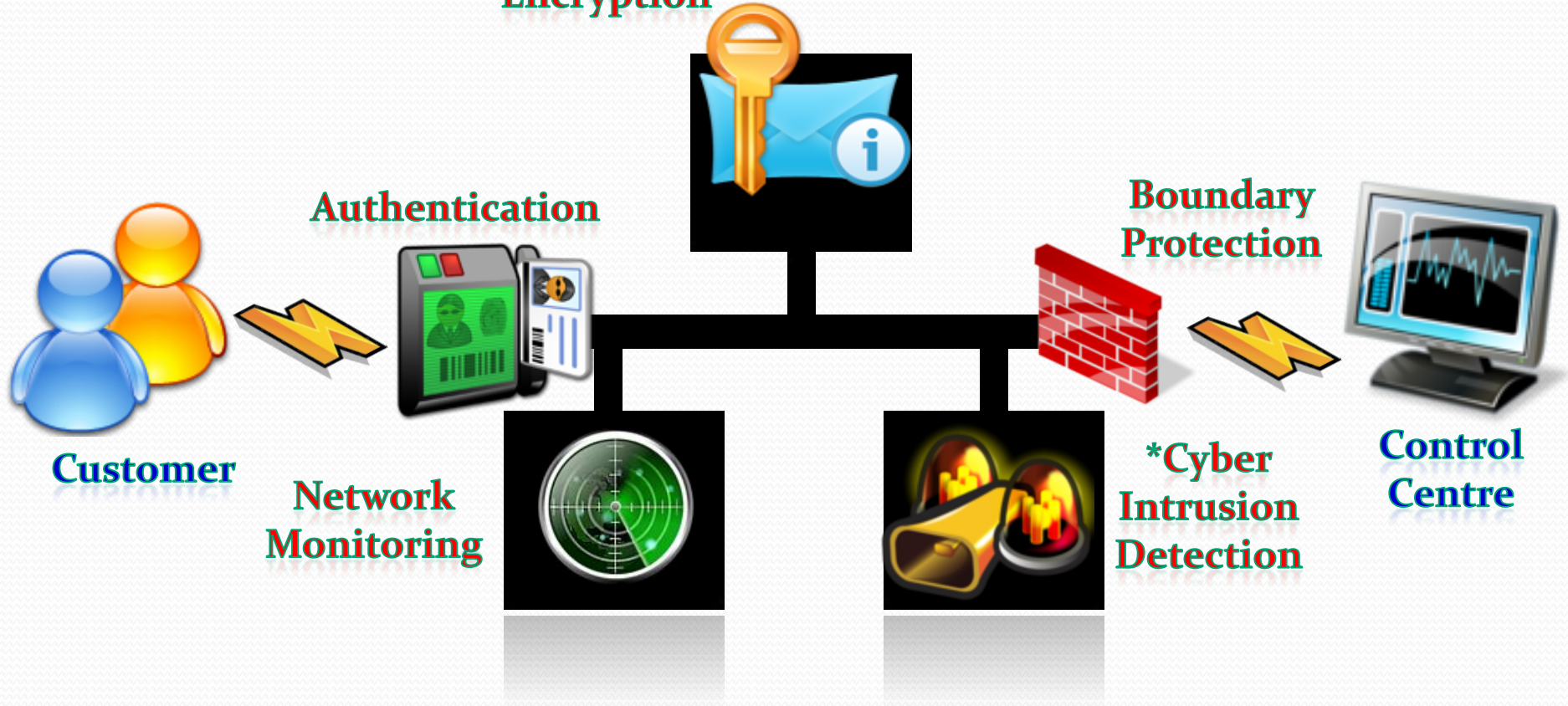
## Billing
- Current Bill
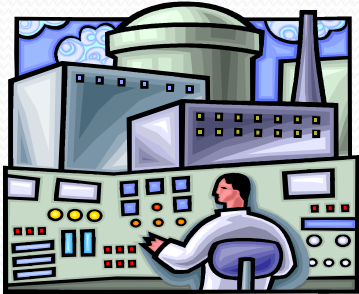- Billing History

## Home Area Network
- Electrical Appliances

# Information Security and Protection

Encryption

Authentication

Boundary
Protection

Customer

Network
Monitoring

*Cyber
Intrusion
Detection

Control
Centre

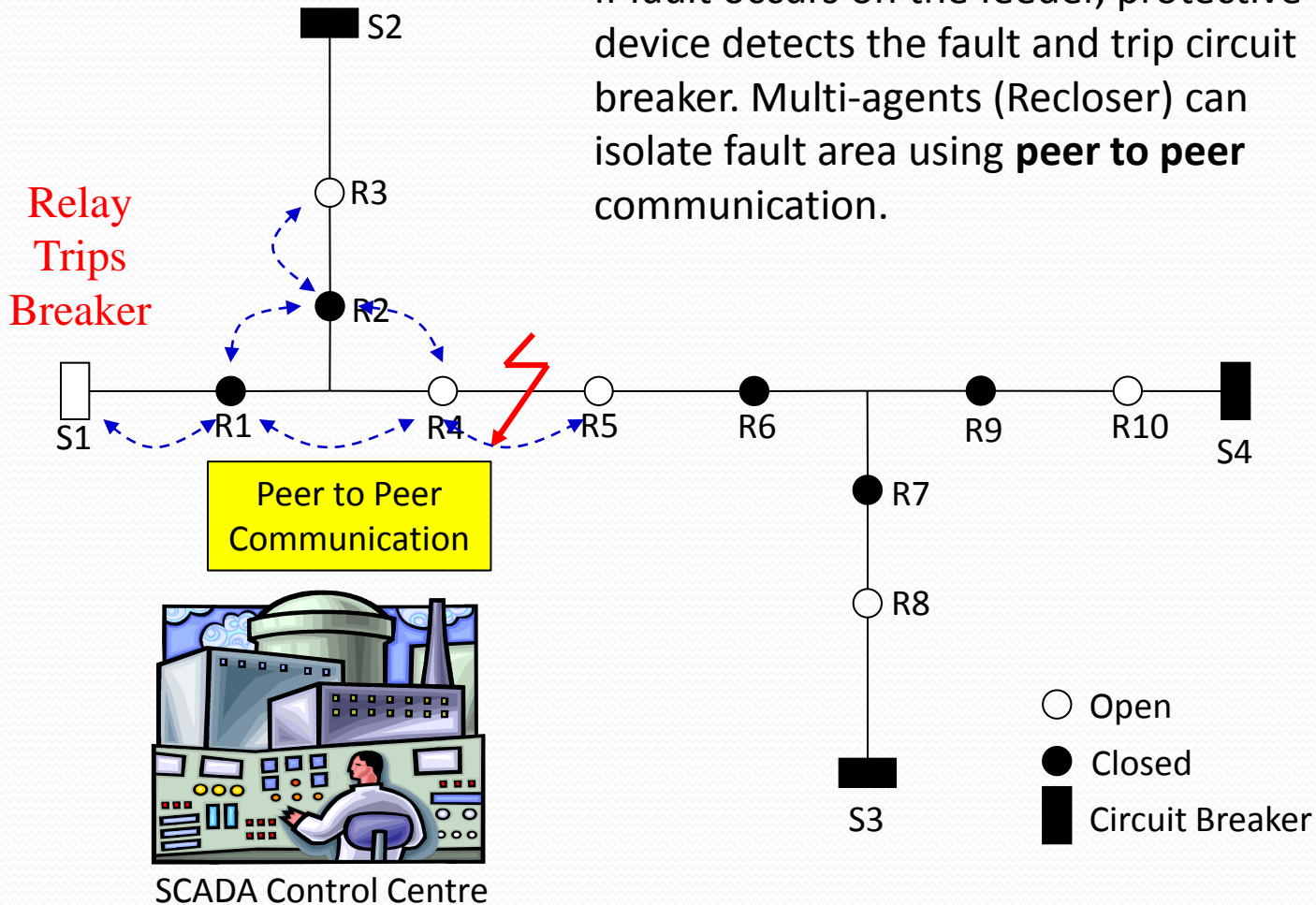# Enhancing System Reliability with ICT

Central Agent : create information, transfer information, status monitoring

Terminal Agent : peer to peer communication, isolate fault area, coordinate protection

SCADA Control Centre

Central Agent

ICT Network

Terminal Agent1

Terminal Agent2

Terminal Agent3

• • •

Recloser1

Recloser2

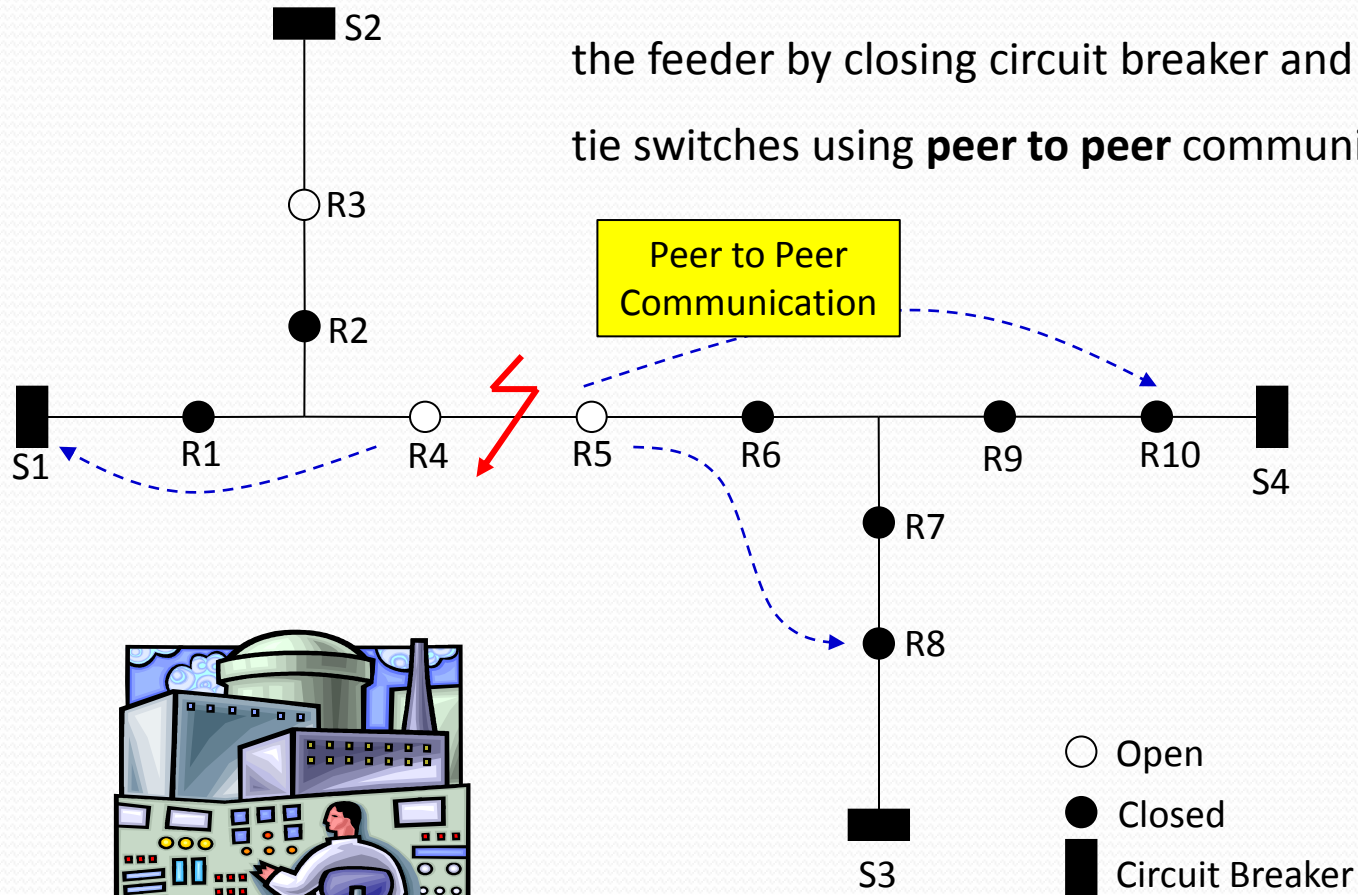Recloser3

Peer to Peer Communication
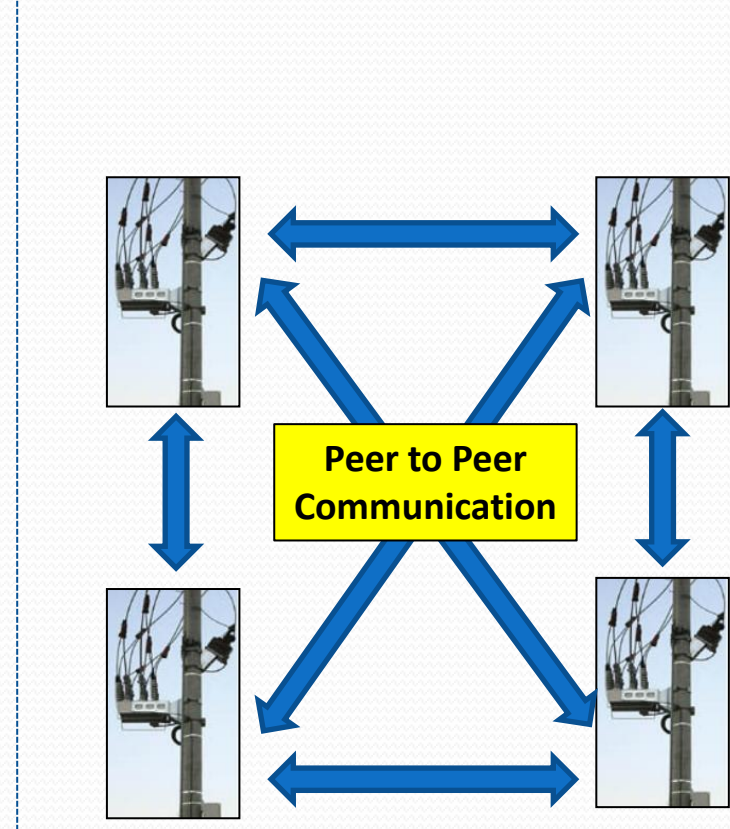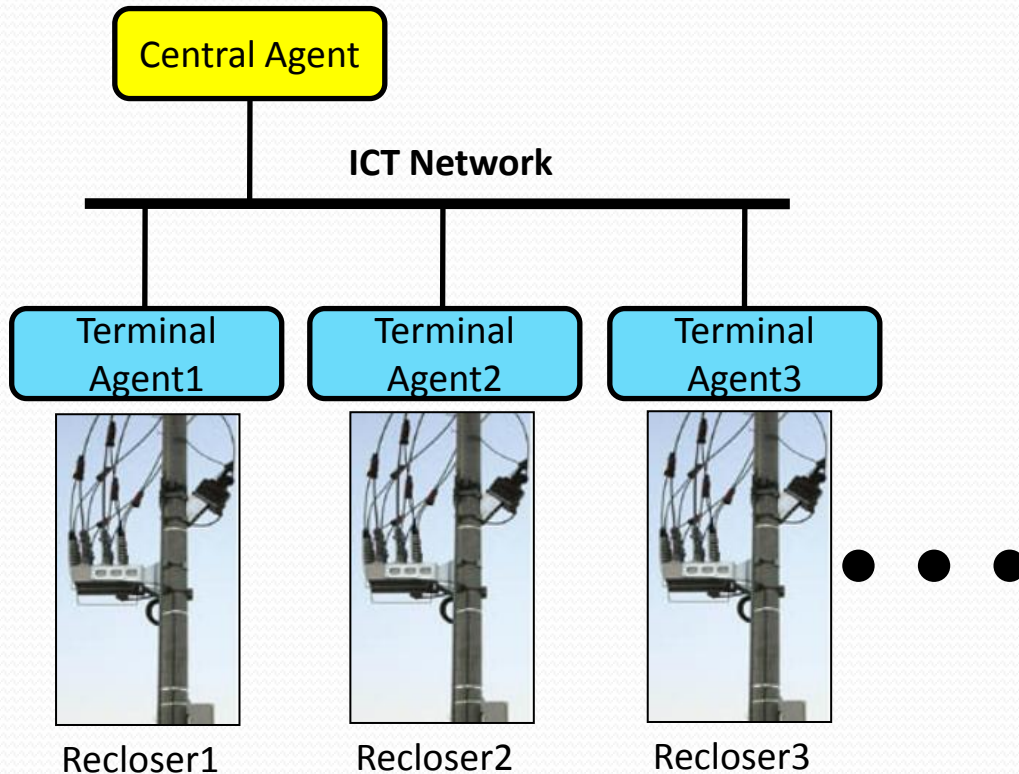
# Smarter Way to Detect Fault

If fault occurs on the feeder, protective device detects the fault and trip circuit breaker. Multi-agents (Recloser) can isolate fault area using **peer to peer** communication.

Relay
Trips
Breaker

S2

R3

R2

S1  R1  R4  R5  R6  R9  R10  S4

Peer to Peer
Communication

R7

R8

SCADA Control Centre

S3

○ Open
● Closed
■ Circuit Breaker

# Efficient Service Restoration

Restore service to unfaulted sections of the feeder by closing circuit breaker and tie switches using **peer to peer** communication.



SCADA Control Centre