TCIPG

TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID | TCIPG.ORG

CONCEPT OVERVIEW

JANUARY 31, 2014

KENTA KIRIHARA & KEVIN LARSON

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

AGENDA

- Poll Results
- 15 min of Power
- 15 min of Security
- Discussion?

POLL RESULTS

What would you like to learn more about this semester?	Are there any fundamental concepts (from either EE or CS) you would like to cover this week?	Would you be interested in having a guest lecturer about Solar Generation?	Would like to have some hands on labs?	Any other suggestions?
Power system fault detection schemes	Fault detection	No	Yes	No more papa del's pizza please
Current state of the grid: how it actually works right now.		Yes	No	The only reason I said no to hands on lab is that I don't want to have to coordinate them with remote sites.
		Yes	Yes	
My EE knowledge is weak in general, but I'd like to know more about the devices that live in the smart grid (synchrophasers, relays, etc.) and what they do (and how quickly they need to do it),	Real-time control - how do operators maintain it?	Maybe	No	
Maybe some basics of power for those of us heavily focused on the computer side. It would be interesting to answer this question: with all this work to make the power grid trusted, etc what are the benefits of the smart grid? Why is it a good idea?	Power distribution	Yes	Yes	Hands on sounds excellent!
More CS topics, but less technical.		Yes	Yes	
I am interested in learning about the many vulnerabilities in the grid and perhaps what the potential solutions and active research are. Also anything related to power systems, protocols and security. So pretty much anything will interest me.		Maybe		
Being an undergrad, I am open to pretty much anything related to the grid.	Alternative Energies	Yes	Yes	

15 MINUTES OF POWER

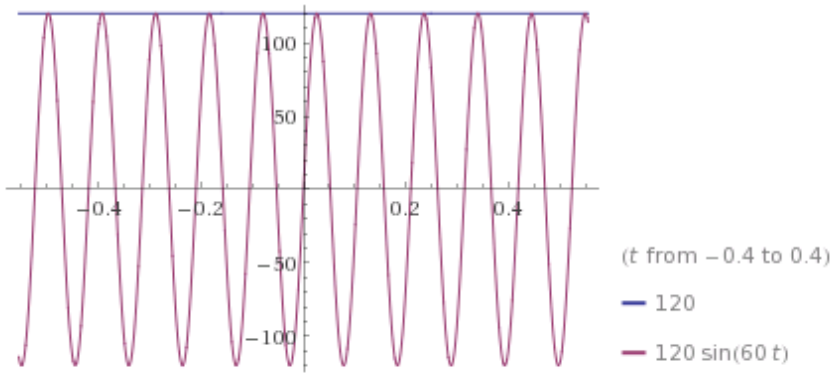
Crash Course in EE topics

BASIC PHYSICS

- Voltage, Current, Resistance, Power…. What are these?
  - Voltage (V): Electrical potential difference.
    - Like a difference between floors in a really tall buildings
  - Current (I): Amount of electric charge moving through per time
  - Resistance (R): Property which opposes the electrons from moving
  - Power (P): Amount of energy used per unit of time.
  - Generally, V=IR & P=VI

DC VOLTAGE VS. AC VOLTAGE

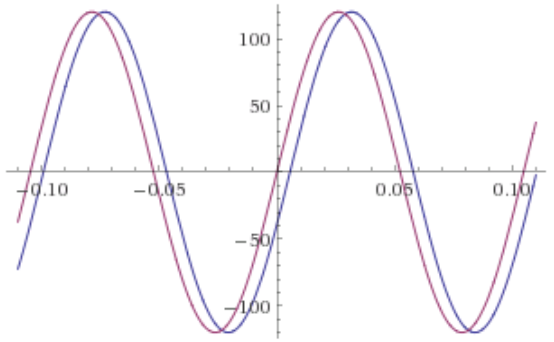
- DC: Direct Current
  - Voltage is constant
  - Household appliances



- AC: Alternating Current
  - Voltage is sinusoidal
  - Pretty much everything in a grid

AC….THE DIFFICULTY

- In DC the current and voltage are always in phase
- In AC, depending on the load, current and the voltage maybe out of phase
  - Resistive : Good. No change
  - Inductive: V leads I
  - Capacitive: V lags I



Both inductor & capacitor take away current that would've been used for a resistive load. This is often called VARS

THREE PHASE

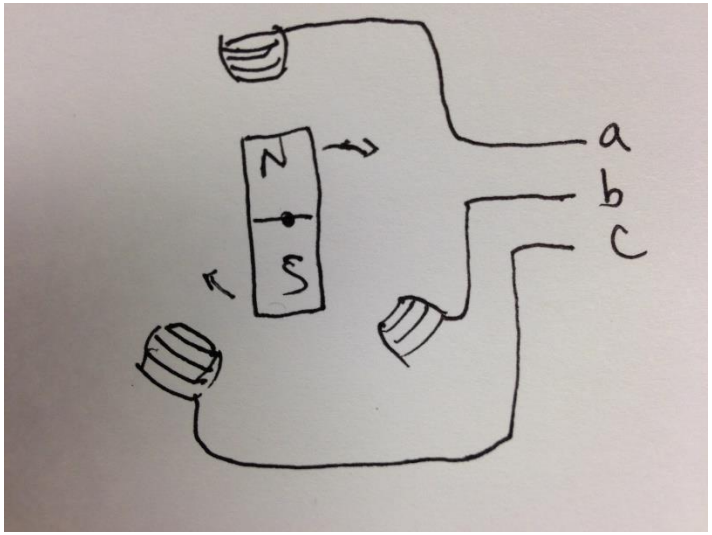
- For infrastructure and resiliency purposes, the grid is compromised in a three phase set up.
- Three phase means that there are three voltage lines that are 120 degrees apart

WHAT IS THE GRID COMPOSED OF?

Grid is comprised of Generation, Transmission, Distribution, and Load.

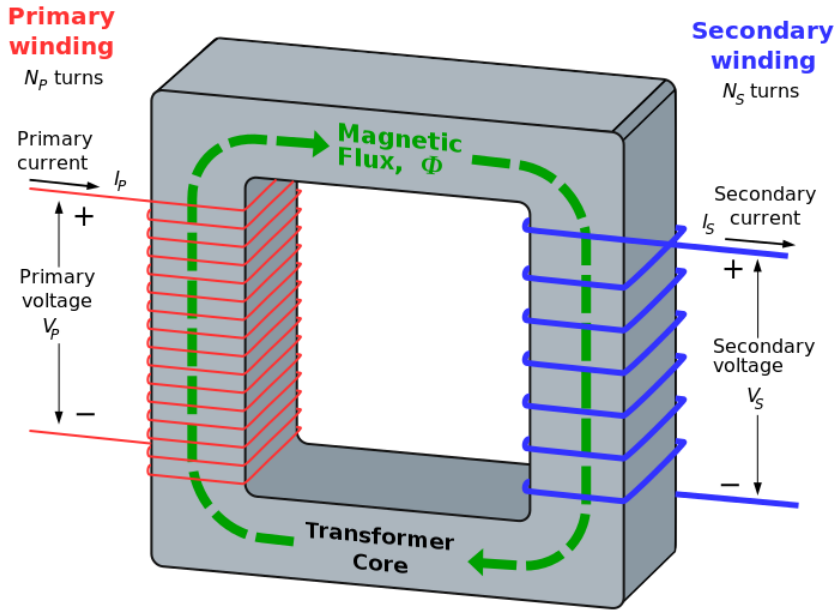
GENERATION

- The most simple way of describing this by visualizing a magnet spinning. Generates magnetic field using Faraday's law.
- Or in terms that I can understand, mechanical energy is converted into electrical energy



TRANSFORMER

- Steps up or down AC voltage for transmission and distribution.



http://upload.wikimedia.org/wikipedia/commons/thumb/6/64/Transformer3d_col3.svg/763px-Transformer3d_col3.svg.png

TRANSMISSION

Transmission: Long distance transmission of electricity usually 115kV, 138kV, 345kV, 765kV.

These are done in high voltages so losses are minimized: V=IR, I=V/R, P=VI=V^2/R

http://retasite.files.wordpress.com/2012/03/power-a2.jpg

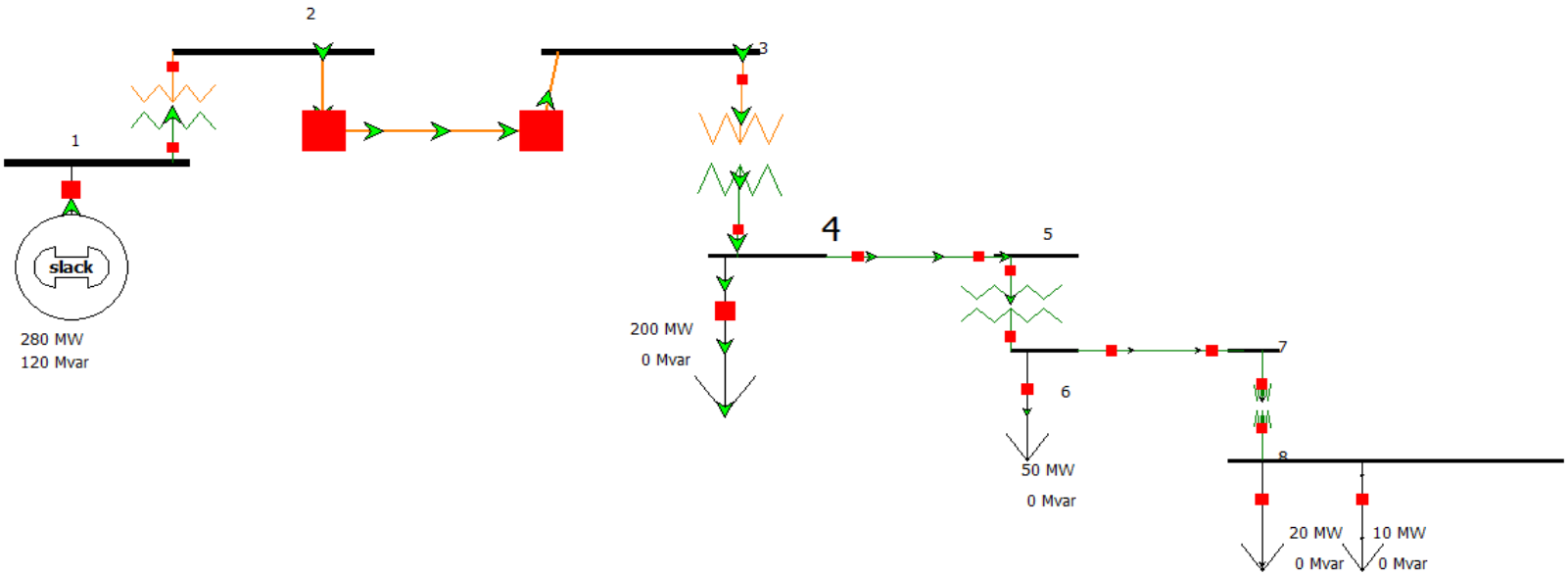
DISTRIBUTION

- TLs with 69kV and below…. but not 120V

LOAD

- Consumes electrical energy
- Can be the following:
  - Transmission/Subtransmission: Industrial
  - Primary: Commercial
  - Secondary: Residential

DEMO


1
2
3
4
5
6
7
8
slack
280 MW
120 Mvar
200 MW
0 Mvar
50 MW
0 Mvar
20 MW
0 Mvar
10 MW
0 Mvar

PROTECTION

- What happens when a line shorts (infinite current)?
- Ways to protect it
  - Fuses: household
  - Relay: detects fault and sends signal to breakers
  - Circuit Breaker: physical device that opens

SO WHY SMART GRID?

- Better situational awareness
  - Less outages, less losses, better control
  - More implementation of renewable energy
  - Optimized grid
- Devices such as:
  - Synchrophasor: heart-rate monitor for the grid
  - Smart meter: load pattern recognition

15 MINUTES OF SECURITY

Crash Course in CS topics

SECURITY MODELS

- What are these?
- Why do we care?

IMPORTANT CONCEPTS

- Tradeoffs
- Users
- Deterrents vs Detection
- Integrity, Authorization, and Availability
- Access Controls

TRADEOFFS

- Security isn't free!
- Passwords & Log-ins
- CPU cycles
- Hardware costs

USERS

A good security model is only as good as its implementation

- Users are one of the most common failing points
  - Ignorance
  - Social engineering
  - Laziness

DETERRENTS VS DETECTION

- Lets think about models again!
- Some physical examples
  - Lock (for a door)
  - Camera
  - Security Guard

CONT.

- Computer examples
  - Firewall
  - Intrusion detection
  - IT personel

INTEGRITY, AUTHORIZATION, AND AVAILABILITY

… and confidentiality, authorization, and non-repudiation

Why do we care about all these words?

Why can't we use shorter words?

Many models span several of these concepts

CONFIDENTIALITY AND INTEGRITY

Confidentiality - related to disclosure of information

Integrity - related to correctness of information

AUTHENTICATION AND AUTHORIZATION

Authentication - confirming identity

Authorization - is one allowed to do something?

AVAILABILITY AND NON-REPUDIATION

Availability - is something running and accessible?

Non-repudiation - confirmation of sending and receiving messages

ACCESS CONTROL

An example of authorization:

Widely used in both physical and computer systems

- Locks
- Log-ins

CRYPTOGRAPHY

Not my strength by a long shot

Basic ideas important though

ENCRYPTION

Simple shifts

- Caesar
- Book

AES/DES/etc

- Bits

Try this: decrypt “uhdglqj jurxs kdv iuhh slccd” with a caeser cipher using a shift of “3”

KEYS AND OTHER CONCEPTS

Keys - pretty close to digital equivalent

Hashes - easy to compute, extremely hard to forge

Signatures - keys tied to identities

Breaking cryptography

- Brute force
- “obsolete” or “broken” standards
- Stealing keys