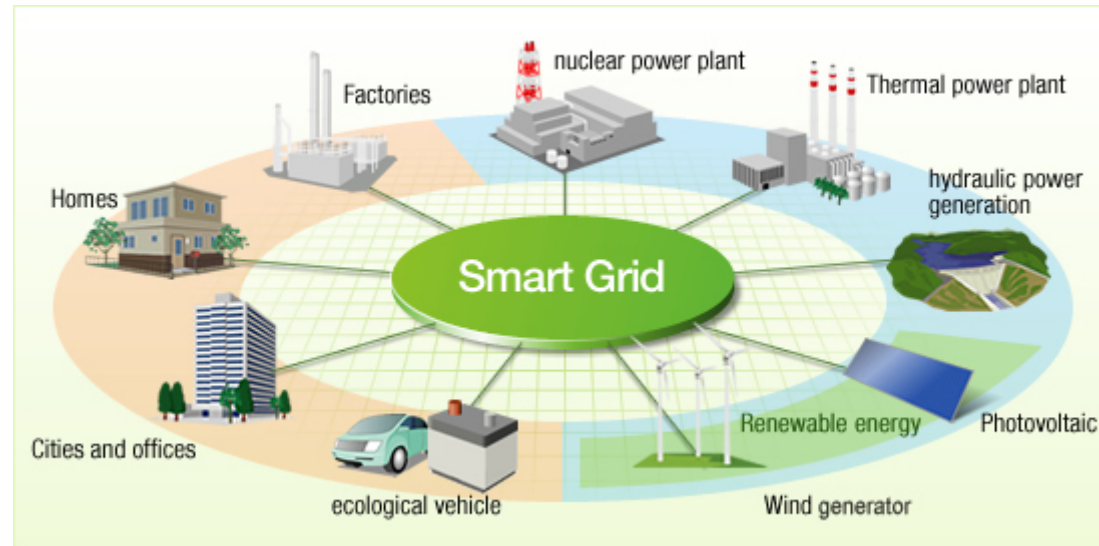


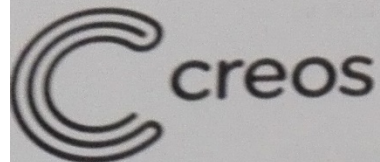
Privacy in the Smart Grid



ISED 2018

Alfredo Rial

alfredo.rial@uni.lu

M. ALFREDO RIAL DURAN
[Redacted]

Strassen, le 27 mars 2018

Concerne: **Remplacement de votre compteur électrique** par le compteur intelligent SMARTY
à l'adresse [Redacted]

Madame, Monsieur,

Soucieux d'assurer un comptage performant de votre consommation d'énergie électrique et de gaz, Creos Luxembourg S.A a engagé la société **CITY ELECTRIC** qui procédera au cours des prochaines semaines au remplacement de votre compteur électrique – conformément à la législation européenne et nationale en vigueur – par le compteur intelligent SMARTY.

En effet, le Grand-Duché du Luxembourg a transposé les directives 2009/72/UE, 2009/73/UE et 2012/27/UE relative à l'efficacité énergétique en droit national en introduisant le concept du comptage intelligent dans les lois du 7 août 2012, et en précisant le régime et les modalités dans les lois du 19 juin 2015, modifiant ainsi la loi modifiée du 1^{er} août 2007 concernant l'organisation du marché de l'électricité et du marché du gaz naturel.

C'est sur cette base que les gestionnaires de réseau ont été mandatés de remplacer jusque fin 2019 tous les compteurs électriques (et jusque fin 2020 les compteurs gaz) par des compteurs de type intelligent. Les compteurs pourront être lus à distance et éviteront ainsi le passage d'un releveur chez vous. Ils permettront également de vous donner plus de détails sur votre profil de consommation.

Les monteurs de notre société partenaire **CITY ELECTRIC** contacteront le syndic ou le responsable de l'immeuble et procéderont au remplacement des compteurs dans les prochaines semaines. L'intervention entraînera éventuellement une coupure de courant de quelques minutes. Pour toute autre question merci de consulter le site smarty.creos.net ou de contacter notre Service Client au numéro 2624-2624 ou par courriel info@creos.net.

Le remplacement et la pose du nouveau compteur sera effectué gratuitement (sous réserve de conformité technique de votre installation). Le compteur faisant partie intégrale de notre réseau, les coûts relatifs au remplacement rentrent dans les coûts de gestion du réseau au même titre que tous nos travaux relatifs à la modernisation de nos infrastructures.

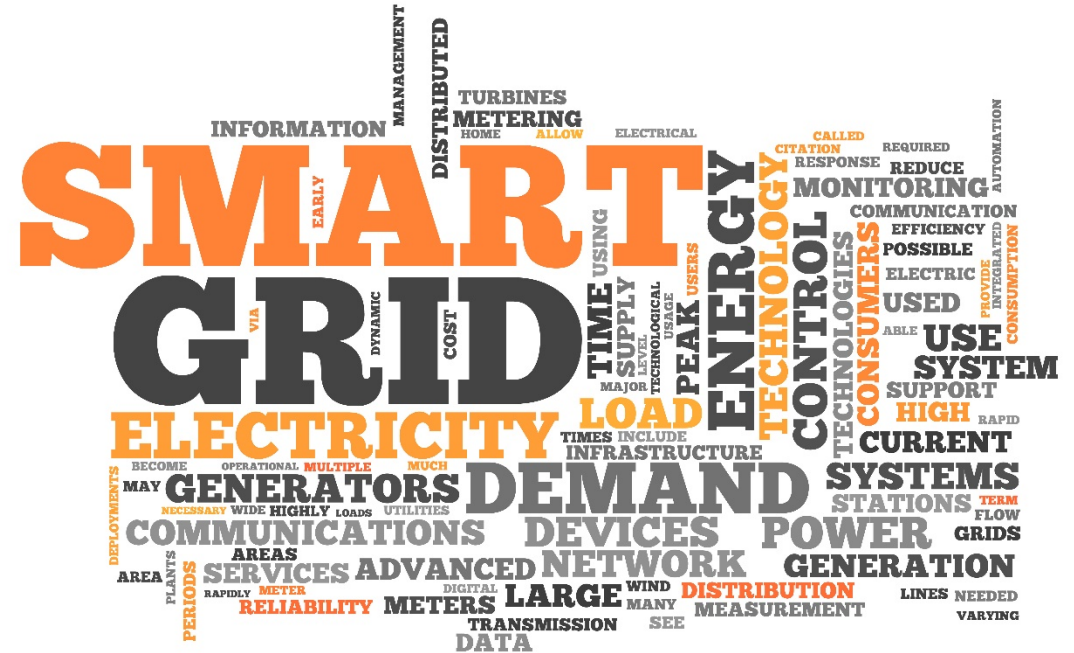
Nous vous remercions d'avance de votre collaboration et vous prions d'agréer, Madame, Monsieur, l'expression de nos sentiments distingués.

[Signature]

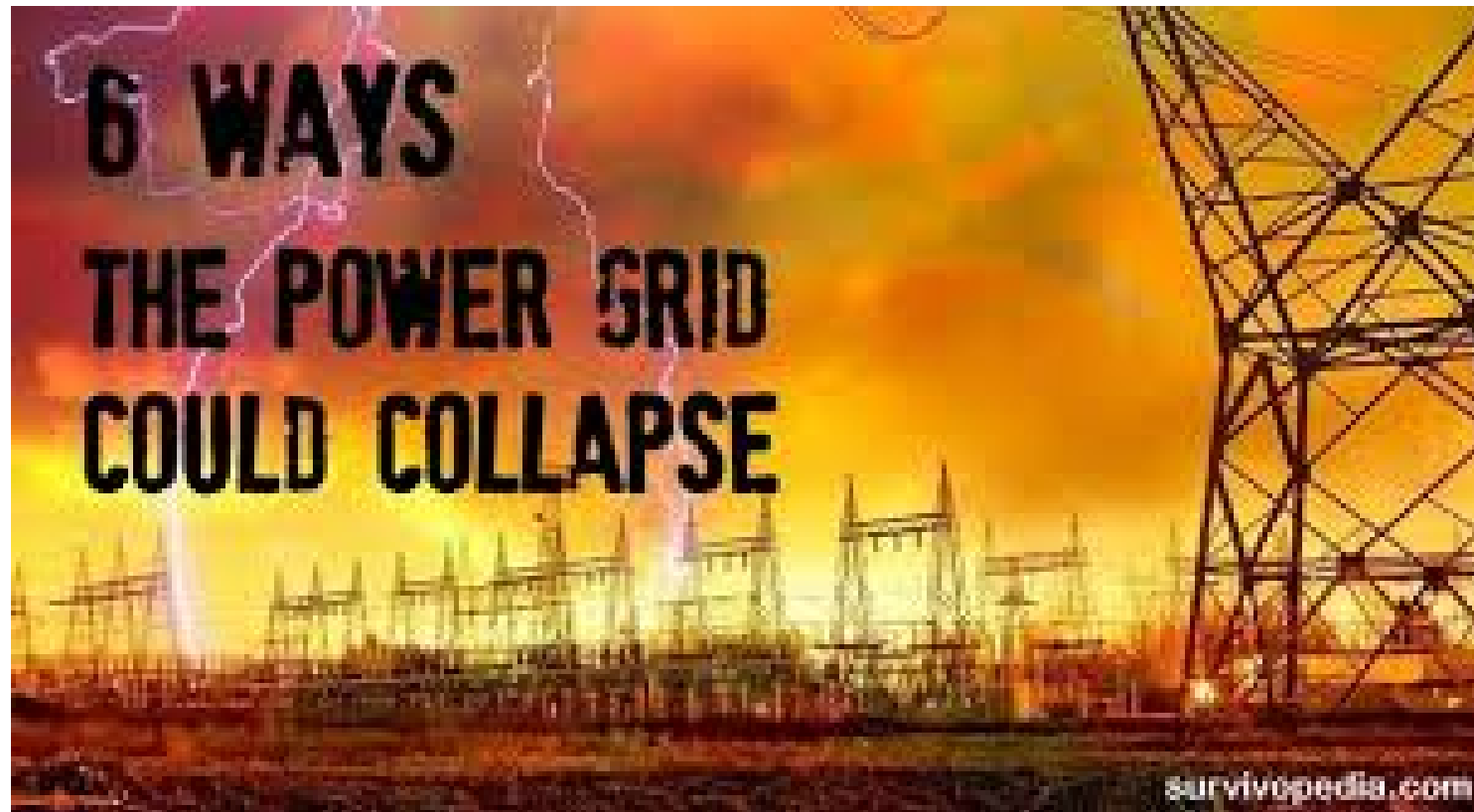
[Signature]

Table of Contents

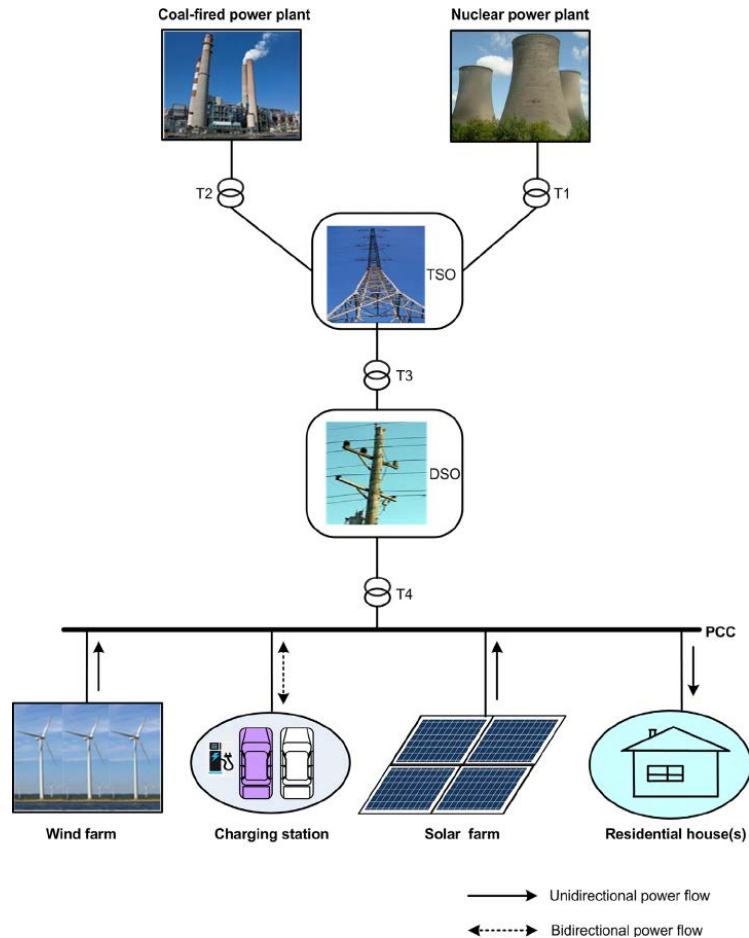
- Challenges of the Current Grid
- The Smart Grid
- Privacy Problems
- Possible Privacy-Friendly Solutions



Current Challenges in the Grid



Integration of renewable sources of energy



Integration of renewable sources of energy:

- Solar panels
- Wind mills

From centralized to distributed power generation:

- Transmission and distribution borders blur
 - Requires bidirectional energy flows
- More resilience to attacks against plants
- Help meeting demand grow

Improving the load factor

- Short peaks caused, e.g., by heating and air conditioning
- Costly gas turbines employed to match peak loads
 - They can be started and shut down fast
- Peak power plants only on several hours a day
- Electricity prices are incremented



Incorporation of Demand Response

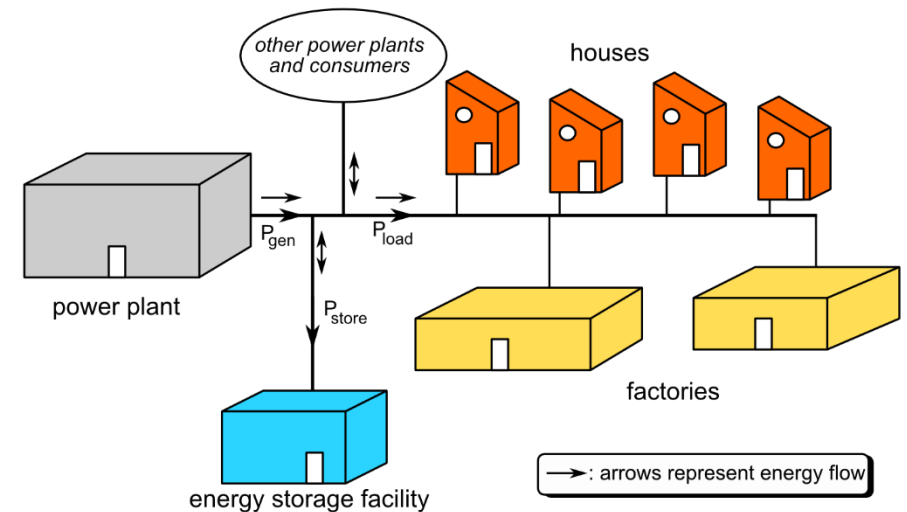


Load Control Switch

To reduce the load, customers are requested to reduce their load. Currently, this is mainly done with large industrial customers.

Integration of Advance Electricity Storage

- Renewable sources are variable, so electricity generation can be higher than demand.
- Electricity is stored to be used during peak demand periods
- Different methods (not cheap):
 - Batteries.
 - Pumped water
 - Electric vehicles
 - Hydrogen
 - Compressed air

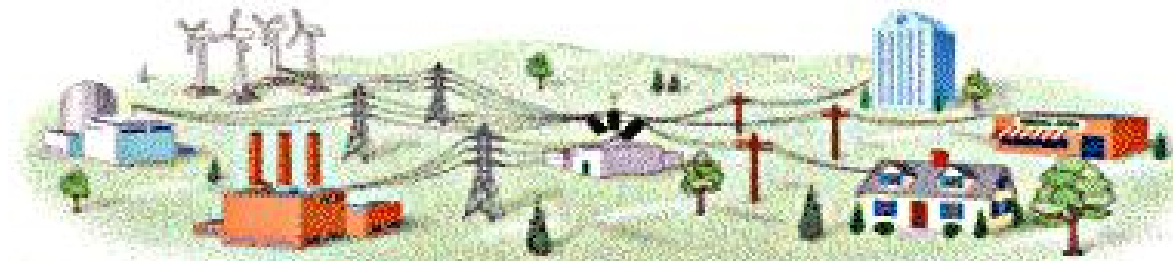


Obsolescence

- Aging Equipment
- Obsolete layout – insufficient facilities
- Outdated Engineering



Deregulation of the Electricity Market



Generation

- no longer utility only
- no longer regulated
- suppliers compete

Transmission

- remains utility only
- lines open to all suppliers

Distribution

- remains utility responsibility
- service remains the same
- rates remain regulated

Customers

- choose generation suppliers

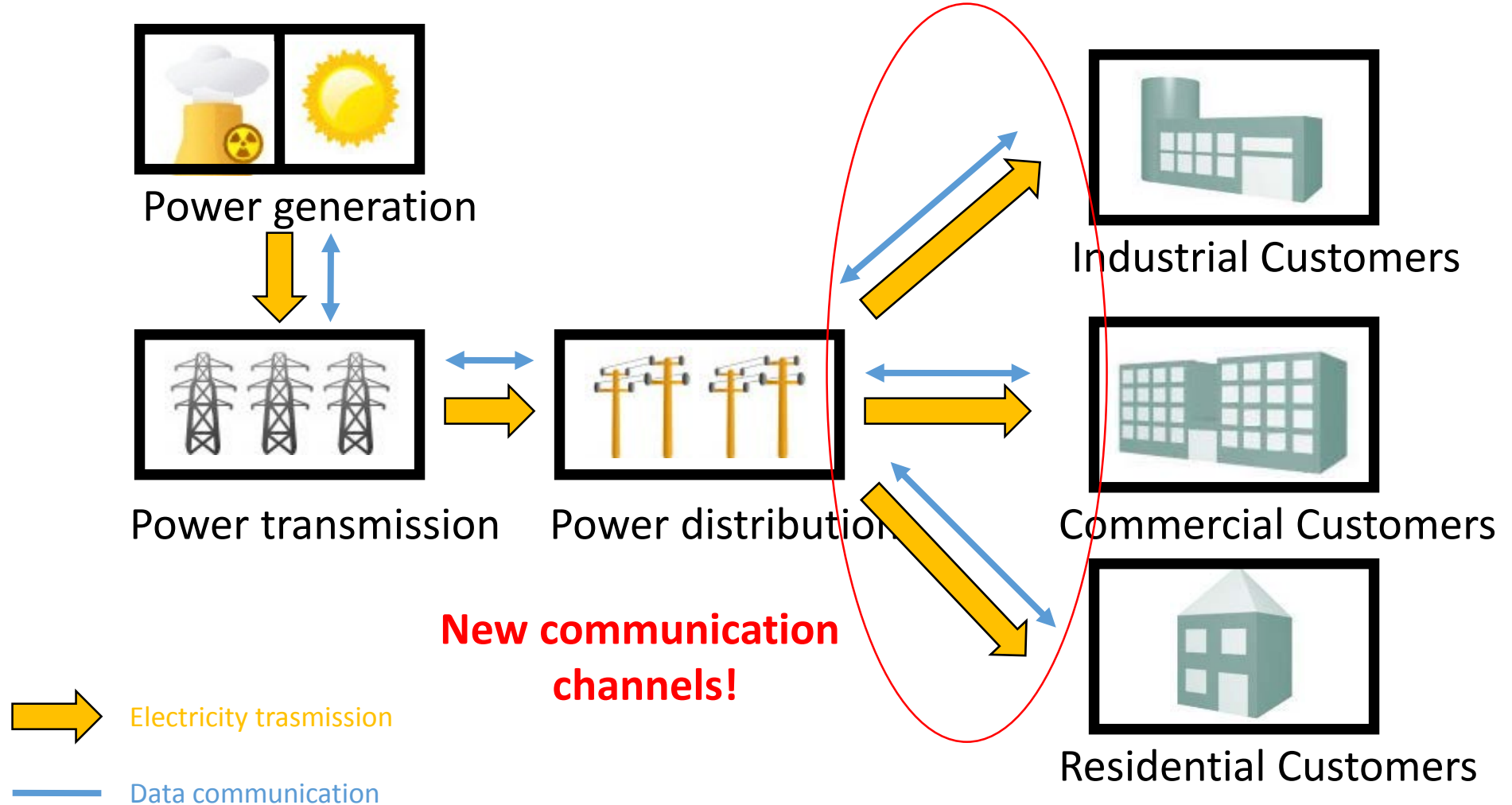
Illustration used with permission of Nexus Energy Software.
Copyright ©2002 ENERGYguide.com. All Rights Reserved.

Operating a system using concepts and procedures that worked in vertically integrated industry exacerbate the problem under a deregulated industry.

The Smart Grid



New Data Communication Channels



New Data Communication Channels

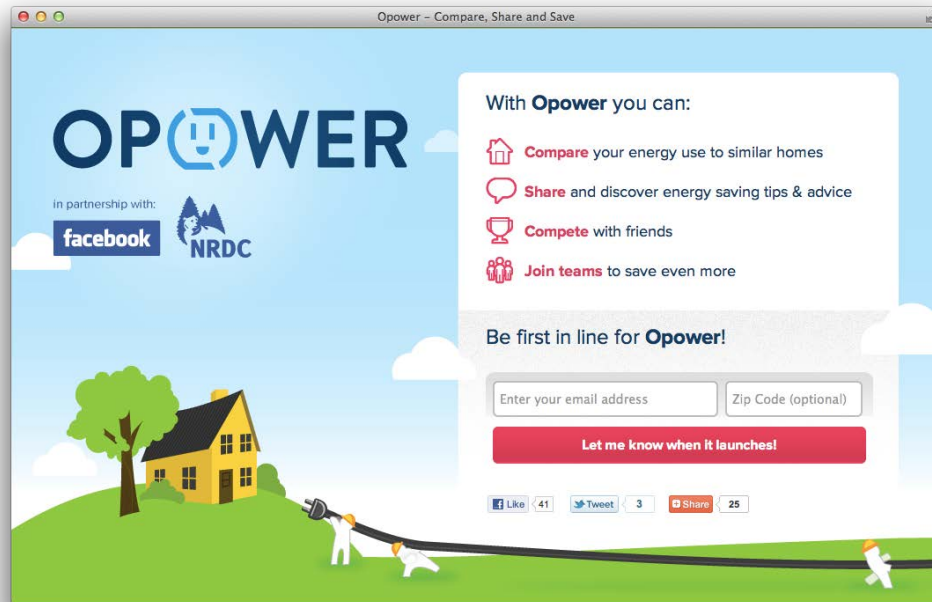
- Communicate customer consumption to the utilities
- Communicate demand dependent prices to the meters
- Control information for dynamic optimization of grid operation and reconfiguration
- Control systems to facilitated the integration of:
 - Solar panels
 - Windmills

Smart Meter

- Reports fine-grained consumption data in real time
- Detects service outages
- Receives commands: switch-off, demand response, change to prepaid mode, etc.
- Interacts via a user-friendly interface



<http://legalplanet.wordpress.com/2010/08/20/smart-meters-and-smart-regulation/>

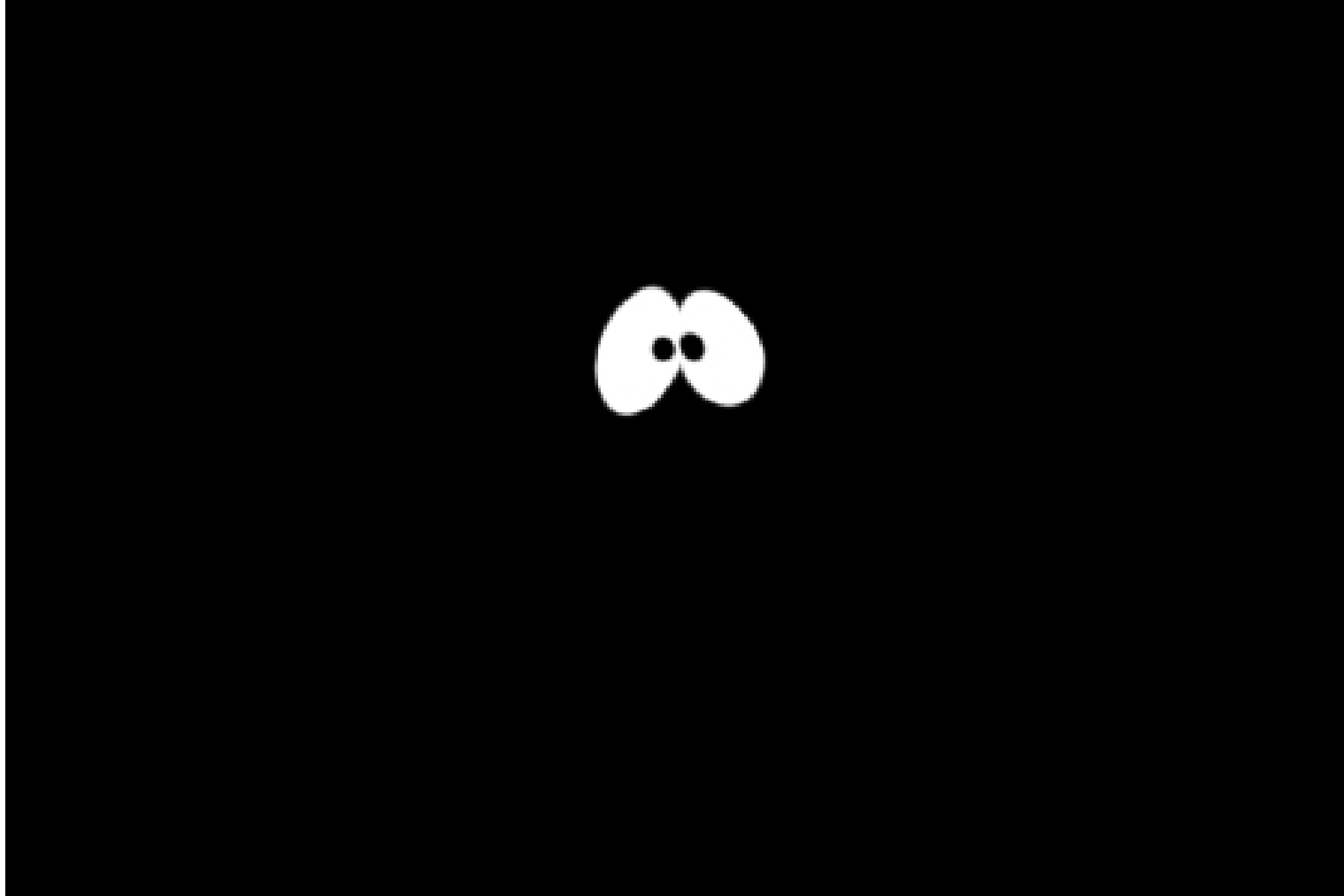


<http://cdn1.tnwn.com/wp-content/blogs.dir/1/files/2011/10/Screen-Shot-2011-10-17-at-10.37.53-AM.png>

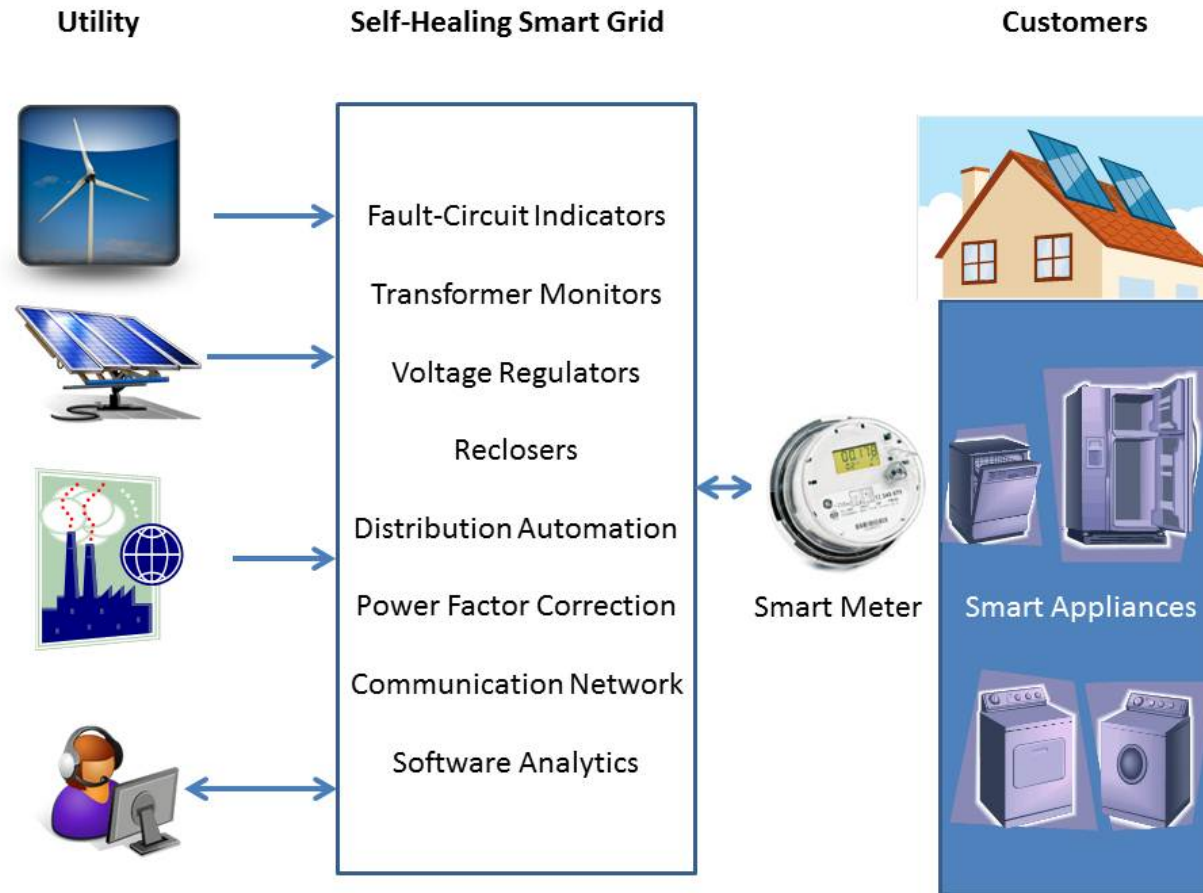
Advantages: Efficient Delivery



Advantages: Prevention of outages



Advantages: Self-Healing grid



<http://www.engineering.com/ElectronicsDesign/ElectronicsDesignArticles/ArticleID/6041/Grid-Heal-Thyself.aspx>

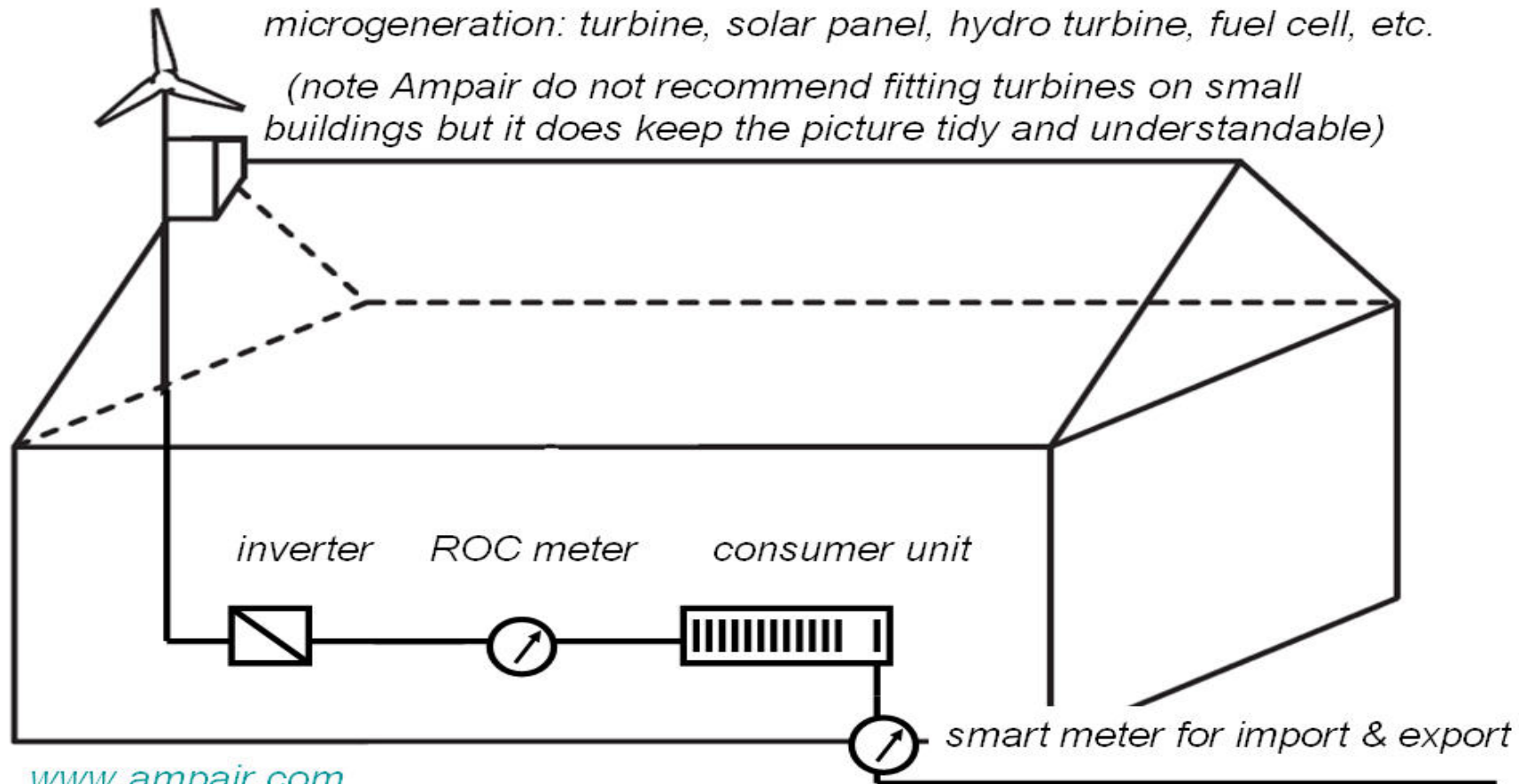
Advantages: End of Estimated Bills



<http://www.fresnobee.com/2010/02/26/1838492/editorial-cartoon-pges-smart-meters.html>

Advantages: Integration of microgenerators

Microgeneration meter locations



Advantages: Energy Saving

ELECTRICITY
SAVING VIA
MATCHING
GENERATION
AND DEMAND



http://blog.news-record.com/opinion/letters/archives/2007/10/cartoon_took_cheap_shot_at_ove.shtml

Advantages: User's energy savings

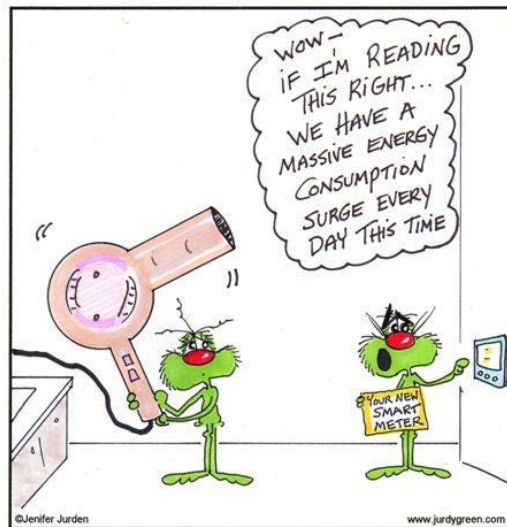
Helps users save energy

- Time of day tariff policies
- User-friendly interface



http://www.citizensutilityboard.org/ciLiveWire_RI_FactsOnEnergyReports.html#

Jurdy Green™



<http://www.birminghammail.net/birmingham-videos-pictures/colin-whittock-cartoons/2009/12/03/smart-meters-must-be-fitted-97319-25314443/>

Deployment: USA

- USA: Energy Independence and Security Act of 2007
- American Recovery and Reinvestment Act (2009, \$4.5bn)



<http://www.ci.royal-oak.mi.us/portal/book/export/html/1751>

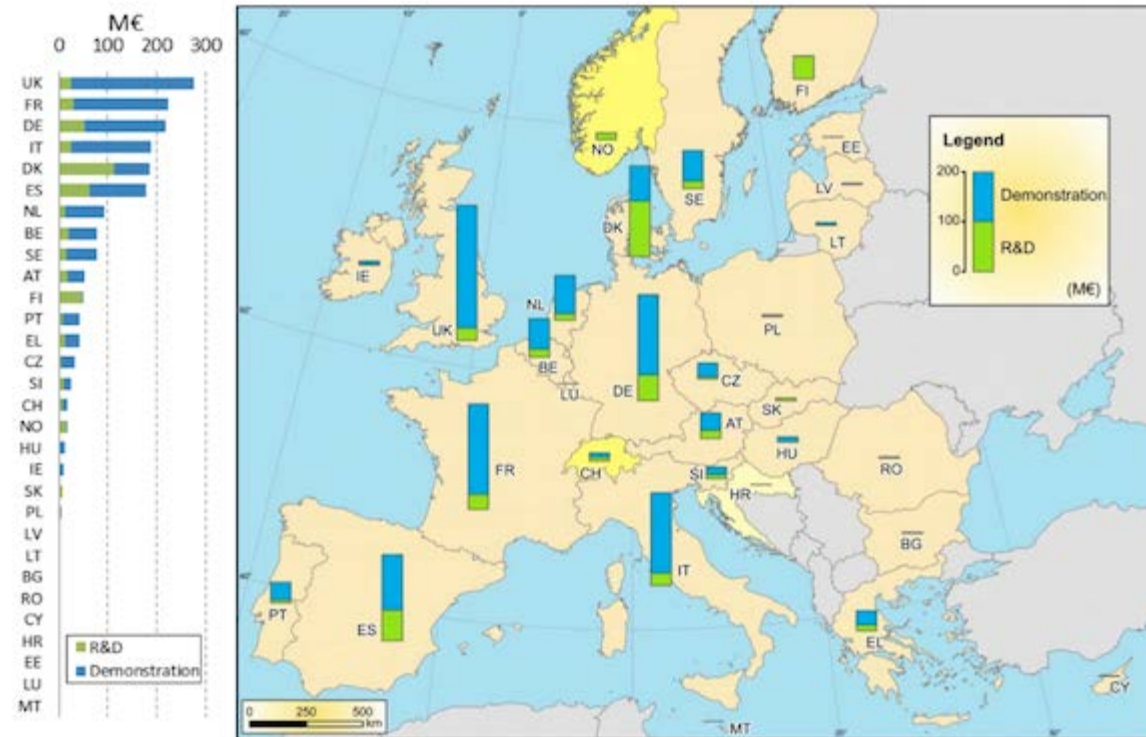


<http://blogs.wsj.com/venturecapital/2013/12/13/opower-shapes-its-software-story/> <http://www.treehugger.com/files/2010/05/obama-finally-starts-talking-clean-energy-wake-gulf-spill.php>

Deployment: EU

EU: Directive 2009/72/EC (80 % meters replaced by 2020)

- UK: 56 million smart meters by 2019
- France: 35 million smart meters by 2017
- Spain: 28 million by 2018

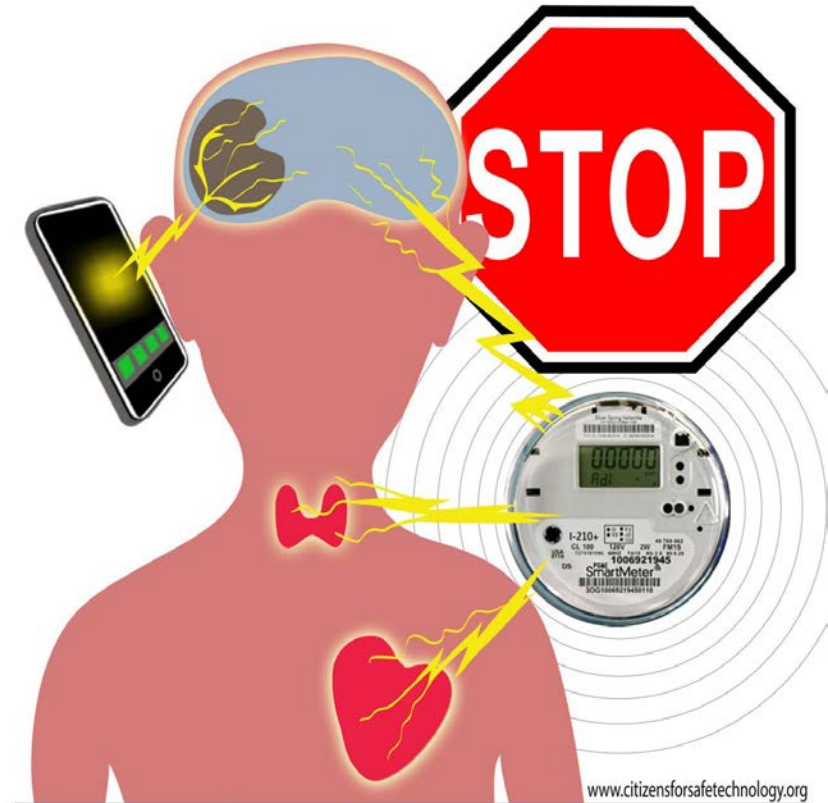


Deployment: Growth Prediction



<http://www.greentechmedia.com/articles/read/smart-grid-market-to-surpass-400-billion-worldwide-by-2020>

Privacy Threats



How Smart is Smart?
Think first about "SmartMeters". It's your life.
STOPSMARTMETERS.ORG

Fine-Grained Consumption Data



Privacy Threats: Concerns

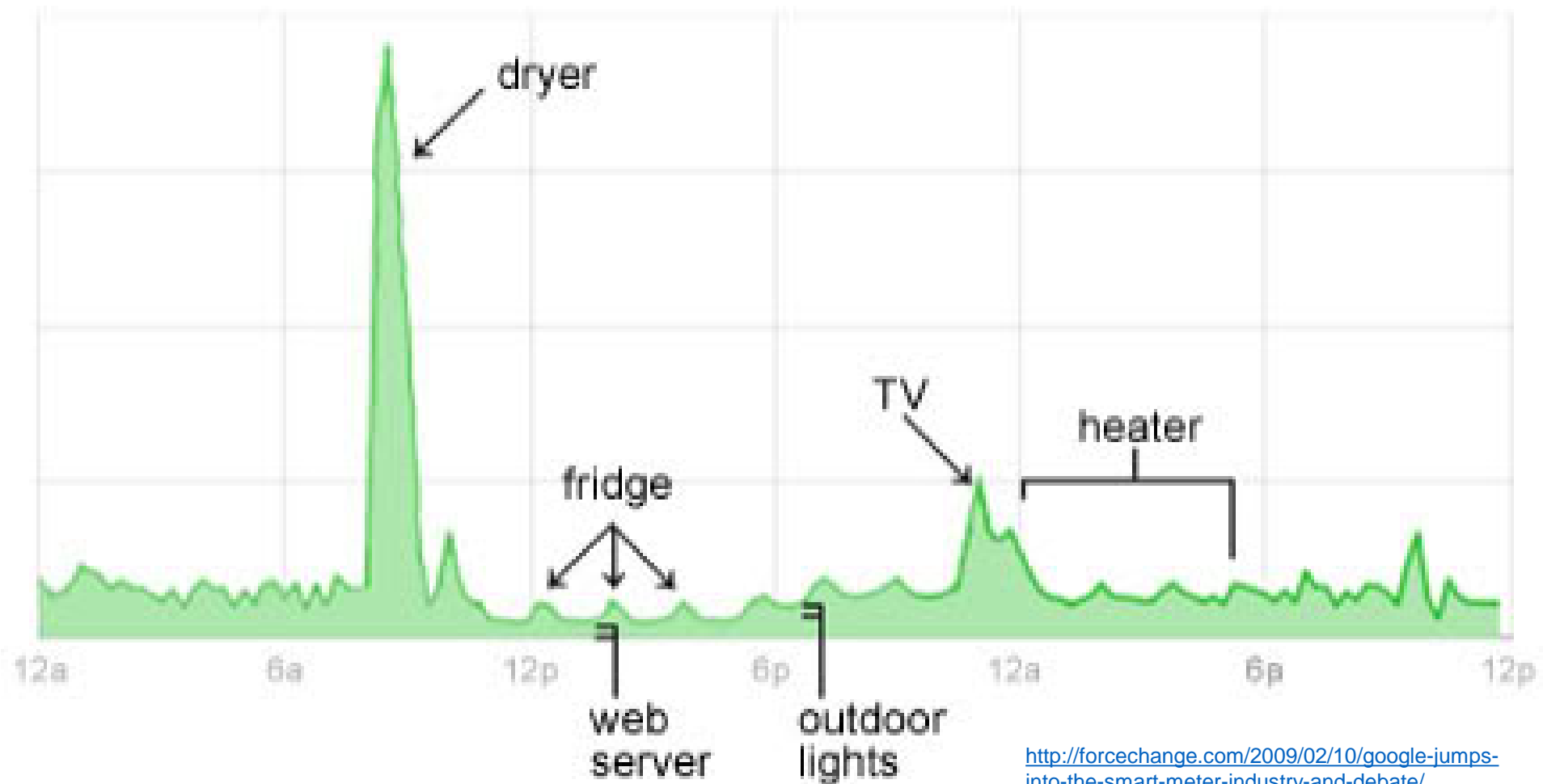
Personal Information can be inferred:

- When you are at home
- Which appliances you use
- When you eat
- Whether you arrive late to work



Privacy Threats: Concerns

Home Electricity Use

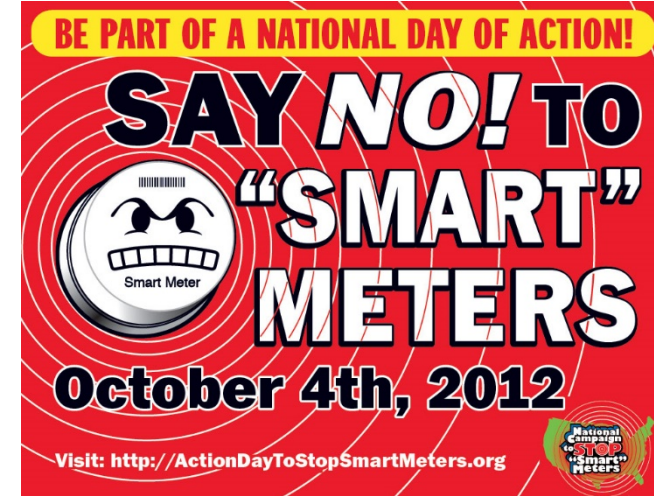


<http://forcechange.com/2009/02/10/google-jumps-into-the-smart-meter-industry-and-debate/>

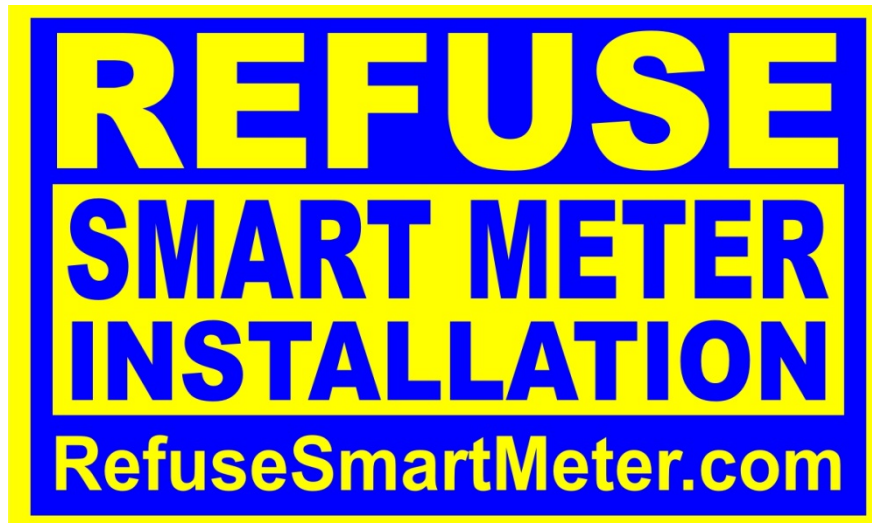
Privacy Threats: Social Pressure



<http://www.indybay.org/newsitems/2010/08/26/18656872.php>



<http://stopsmartmeters.org/2012/09/21/national-day-of-action-to-stop-smart-meters-october-4th/>



Privacy Threats: Consequences

“The Dutch First Chamber considers the mandatory nature of smart metering as an unacceptable infringement of citizens’ privacy and security”



The Account Holder hereby REMOVES IMPLIED CONSENT for the installation of any Smart Meters, or other data transmission equipment, at this property. This is a formally recorded

LAWFUL NOTICE

If you are in any doubt, consult the account holder directly before taking any further action. The meter's number(s) and placing of this Notice have been **RECORDED.**

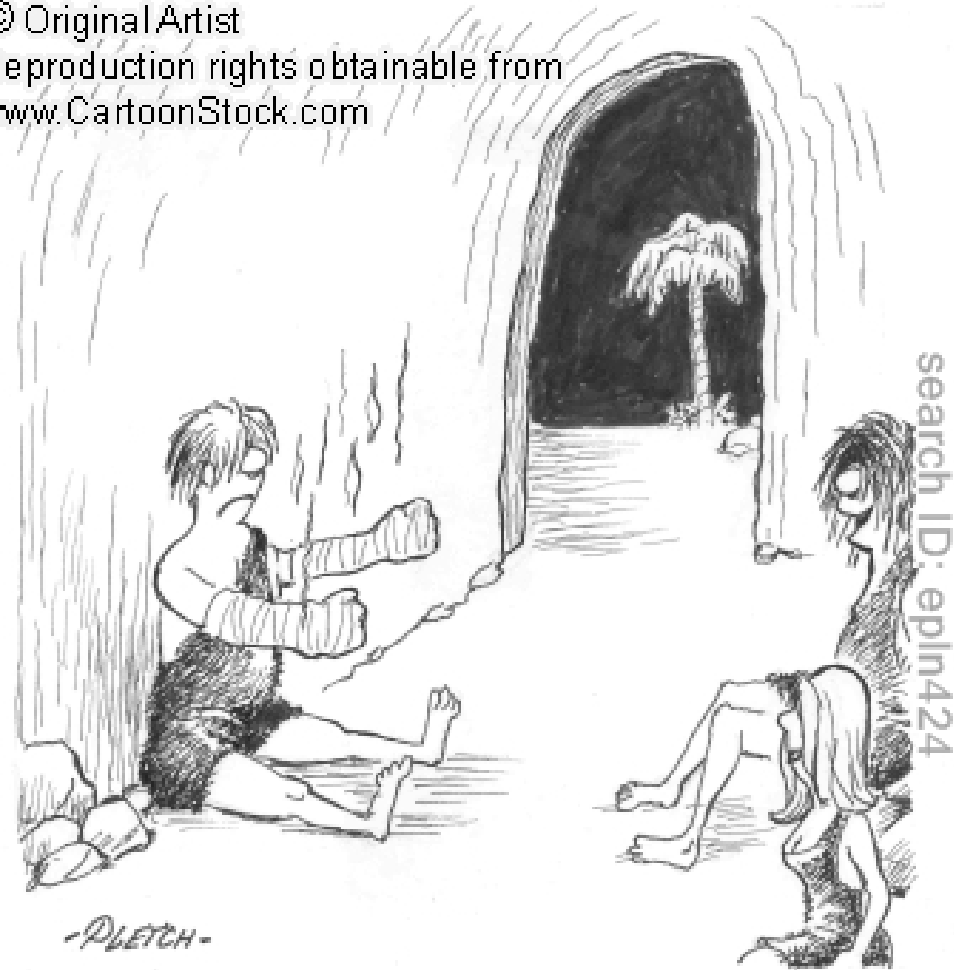
**Do Not Install
Smart Meter**

http://www.stetzerizer-us.com/Smart-Meters_bc_6.html

Possible Solutions

© Original Artist

Reproduction rights obtainable from
www.CartoonStock.com



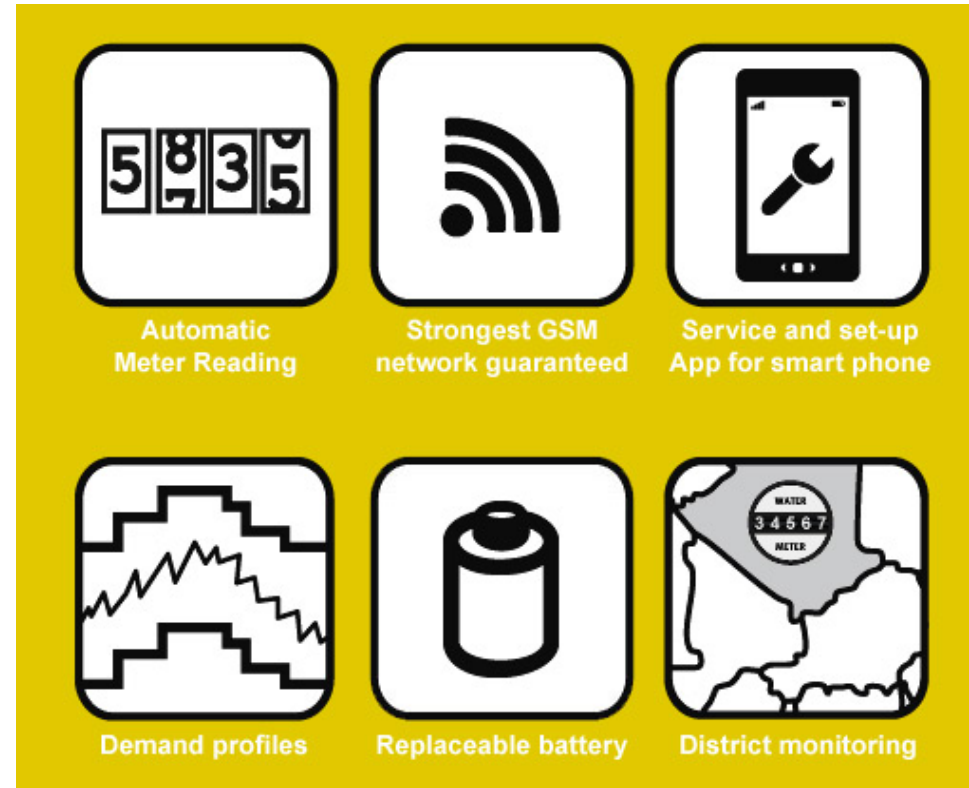
-PETCH-

"OG'S SO MODEST...HE WON'T MENTION IT
BUT HE WAS THE VERY FIRST TO DISCOVER FIRE!"

http://www.cartoonstock.com/directory/d/discovering_fire.asp

Applications of Fine-Grained Consumption Data

- Billing customers
- Fraud Detection
- Demand Forecasting
- Customer Profiling
- Leak Detection
- Flow monitoring



Existing Protocols and Standards

- Ansi C12.18
- IEC 61107 / IEC 62056
- Open Smart Grid Protocol (ETSI)



Utility learns consumption data

Solutions: Regulations and Codes of Conduct



<http://members.iinet.net.au/~greenleaf/plpr/>

- Cavoukian, A., Polonetsky, J., Wolf, C.: “SmartPrivacy for the smart grid: embedding privacy into the design of electricity conservation”
- Quinn, E.L.: “Privacy and the new energy infrastructure”
- Lisovich, M., Wicker, S.: “Privacy concerns in upcoming residential and commercial demand-response systems”
- McDaniel, P., McLaughlin, S.: “Security and privacy challenges in the smart grid”

Solutions: Rechargeable battery



Disadvantages:

- Cost of battery
 - Not suitable when consumption surpasses capacity
-
- Kalogridis, Georgios, et al. "Privacy for smart meters: Towards undetectable appliance load signatures." *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010.
 - Varodayan, David, and Ashish Khisti. "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage." *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*. IEEE, 2011.

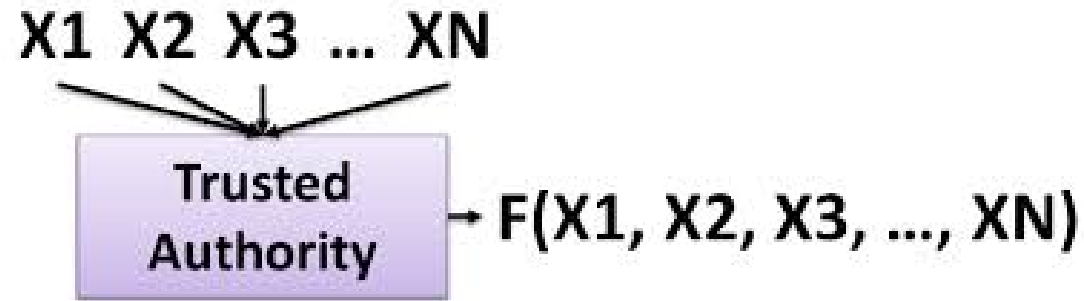
Solutions: Anonymization



Disadvantages:

- Billing needs authentication. Not suitable for time of use billing
 - Deanonymization possible sometimes with side information
-
- Efthymiou, Costas, and Georgios Kalogridis. "Smart grid privacy via anonymization of smart metering data." *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010.
 - Wang, Shuang, et al. "A randomized response model for privacy preserving smart metering." *Smart Grid, IEEE Transactions on* 3.3 (2012): 1317-1324.

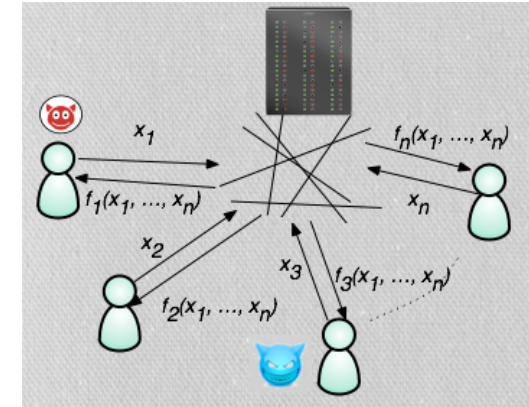
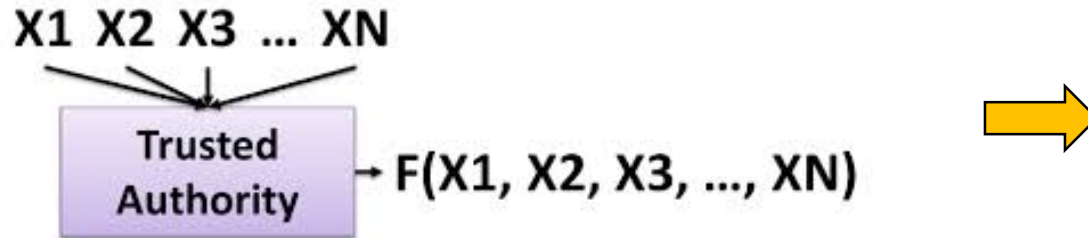
Solutions: Trusted party



The scheme relies on a central uncorruptible party

- Bohli, J-M., Christoph Sorge, and Osman Ugus. "A privacy model for smart metering." *Communications Workshops (ICC), 2010 IEEE International Conference on*. IEEE, 2010.

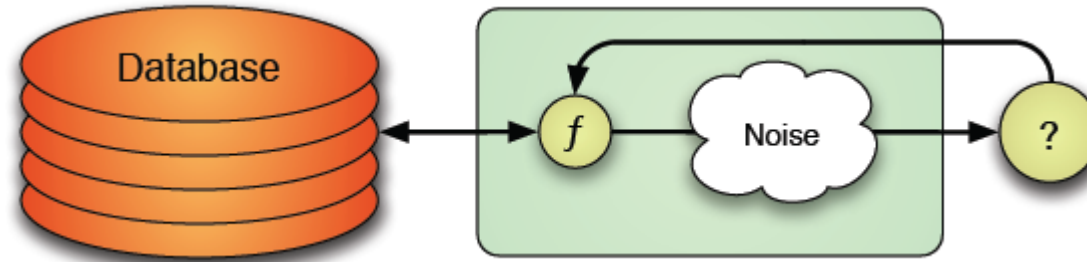
Solutions: Secure Multiparty Computation



Disadvantages:

- Inefficient for complex functions
- Requires communication between meters
- High computation and communication cost
- Some schemes require majority of honest parties
- Kursawe, Klaus, George Danezis, and Markulf Kohlweiss. "Privacy-friendly aggregation for the smart-grid." *Privacy Enhancing Technologies*. 2011.
- Garcia, Flavio D., and Bart Jacobs. "Privacy-friendly energy-metering via homomorphic encryption." *Security and Trust Management*. Springer Berlin Heidelberg, 2011. 226-238.
- Marmol, Felix Gomez, et al. "Do not snoop my habits: preserving privacy in the smart grid." *Communications Magazine, IEEE* 50.5 (2012): 166-172.
- Rottondi, Cristina, Giacomo Verticale, and Antonio Capone. "Privacy-preserving smart metering with multiple data consumers." *Computer Networks* 57.7 (2013): 1699-1713.

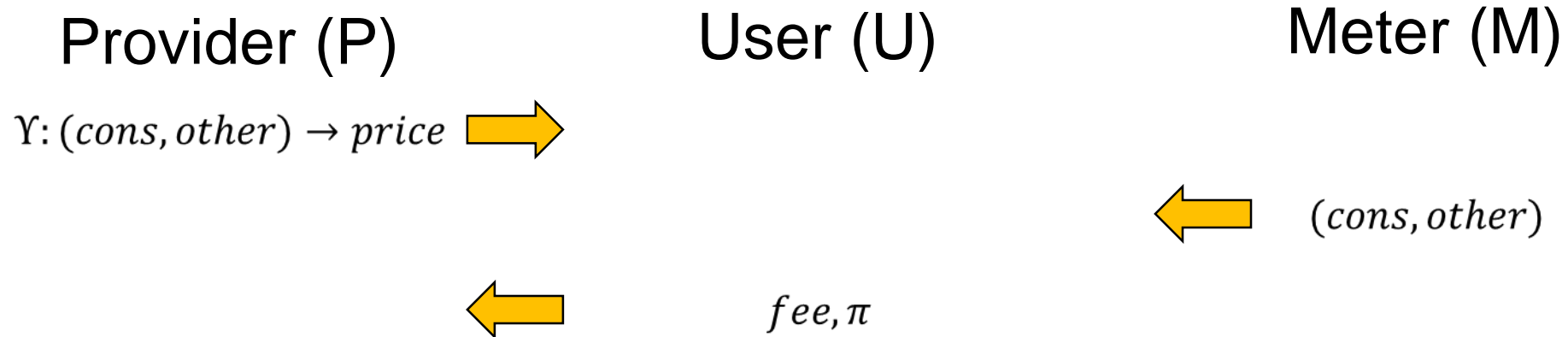
Solutions: Differential Privacy



Disadvantages:

- Amount of noise required usually too big
 - Inaccurate aggregated result
-
- Acs, Gergely, and Claude Castelluccia. "I have a DREAM!(Differentially private smArt Metering)." *Information Hiding*. Springer Berlin Heidelberg, 2011.
 - Barthe, Gilles, et al. "Verified computational differential privacy with applications to smart metering." *Computer Security Foundations Symposium (CSF), 2013 IEEE 26th*.

User-Side Verifiable Computation

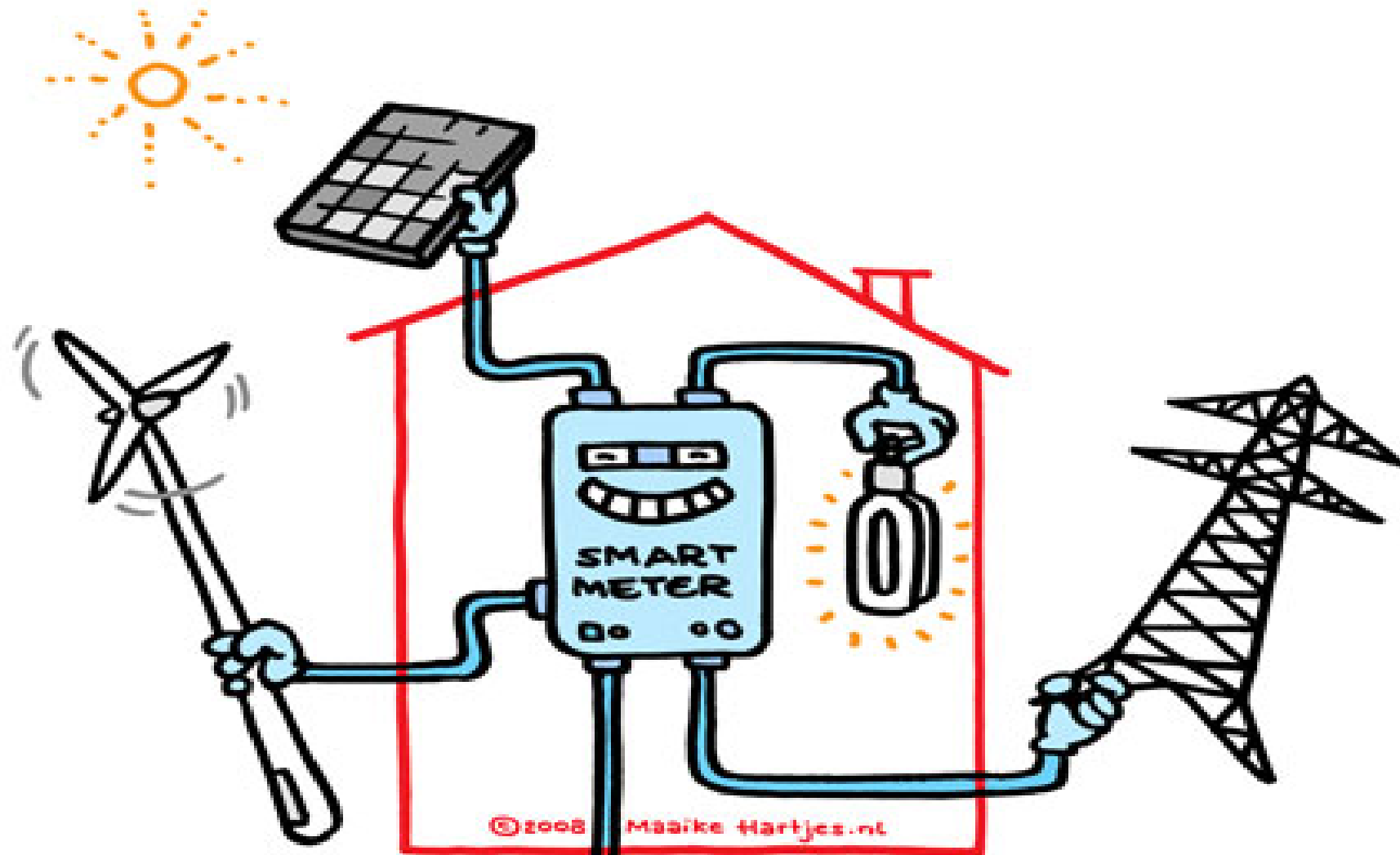


Disadvantage: Not suitable for multiparty computations

Example: Billing

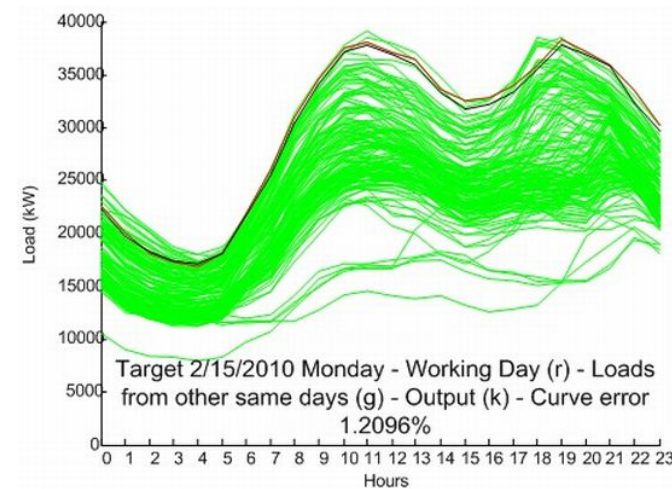
- Users compute bill locally and prove correctness to the utility
- Differential privacy can be used to obfuscate the result
- Jawurek, Marek, Martin Johns, and Florian Kerschbaum. "Plug-in privacy for smart metering billing." *Privacy Enhancing Technologies*. Springer Berlin Heidelberg, 2011.
- Rial, Alfredo, and George Danezis. "Privacy-preserving smart metering." *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*. ACM, 2011.
- Danezis, George, Markulf Kohlweiss, and Alfredo Rial. "Differentially private billing with rebates." *Information Hiding*. Springer Berlin Heidelberg, 2011.

Open Problems



Open Problem: Power Demand Forecasting

- Multiple Regression
- Exponential Smoothing
- Iterated Reweighted Least-Squares
- Stochastic Time Series
- Genetic Algorithms
- Neuronal Networks
- Expert Systems



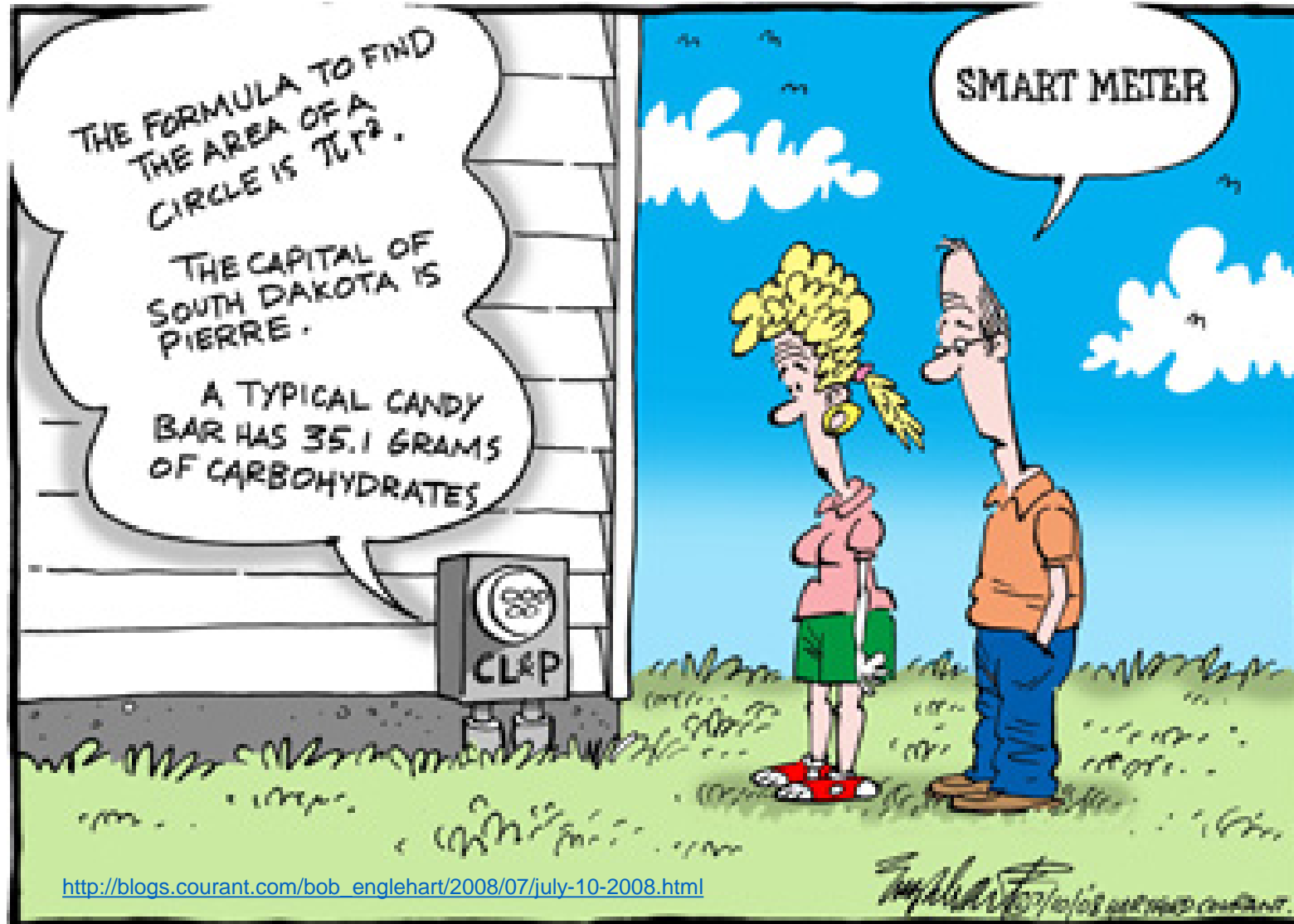
Difficulties:

- Multiparty: Users-Side Verifiable Computing not suitable
- Complex Functions: Secure Multiparty Computation inefficient
- Combine multiple data sources:
 - Weather
 - Location
 - ...

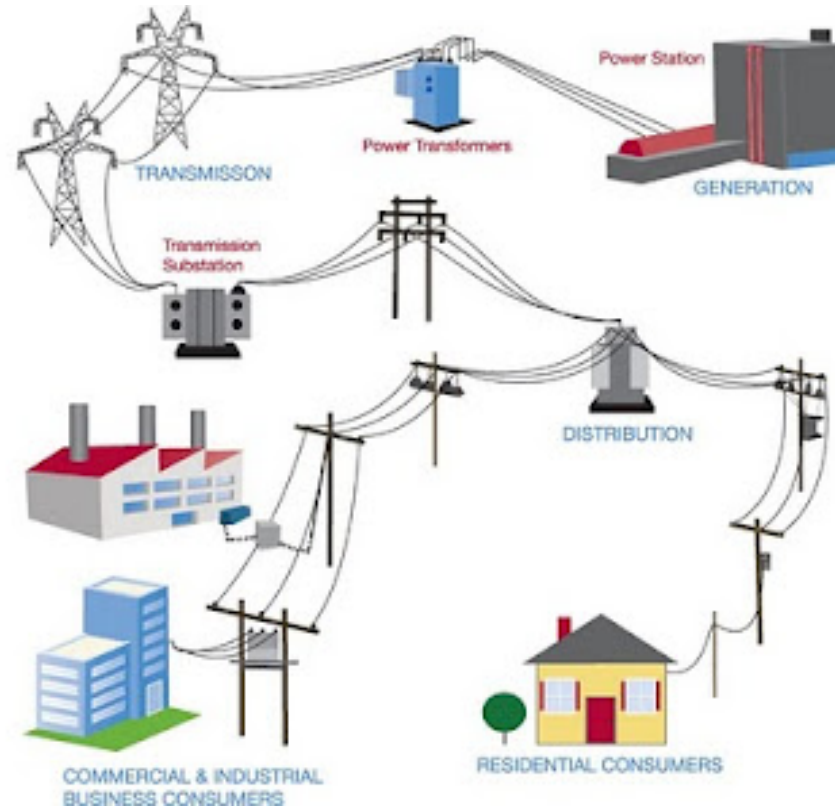
Open Problem: Customer Profiling

- Bottom-up approach:
 - Gather data of individual electrical appliances
 - Aggregate those data to compute the total for the household
- Top-down approach:
 - Gather the total for the household
 - Use data mining to identify individual electrical appliances
- Clustering algorithms:
 - Decision trees

Questions



The Electrical Grid



<https://xenogyre.com/2012/05/24/introduction-to-grid-energy-storage/>

Before 1880's



Industry:

- Line Shaft and Belt Drive
- Power Generation normally on-site
- Long distance transmission also possible (e.g., pneumatic or hydraulic)



Gas Street Lighting



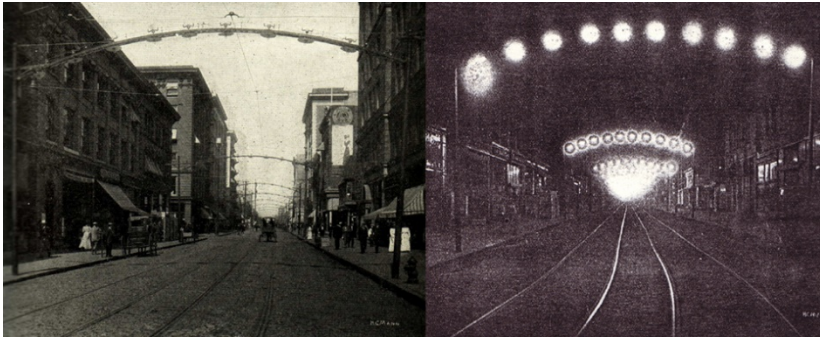
Telegraph:

- Main Deployment that used electricity

1880: Electric Lighting

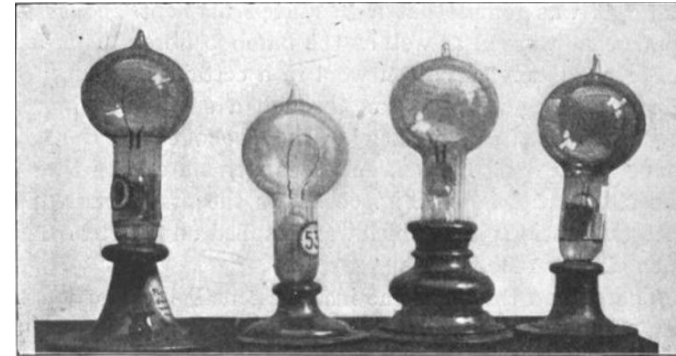
Arc lighting:

- High voltages (around 3000 v)
- Very brilliant (for outdoors, not indoors)
- Disadvantages: fire hazard, costly maintenance



Incandescent lamps:

- Low voltages (110v)
- Good for indoor lighting



1880's: Beginning of Electrification

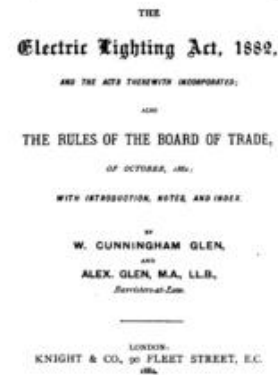
First central power plants:

- From 1879: plants for arc lights (10 km)
- 1882 DC 110v in London (2 km)
- 1882 DC 110v in New York (2 km)
- 1884 First long distance transmission of AC in Turin
- 1889 First long distance transmission of DC in Genoa
- 1890: More than 1000 plants



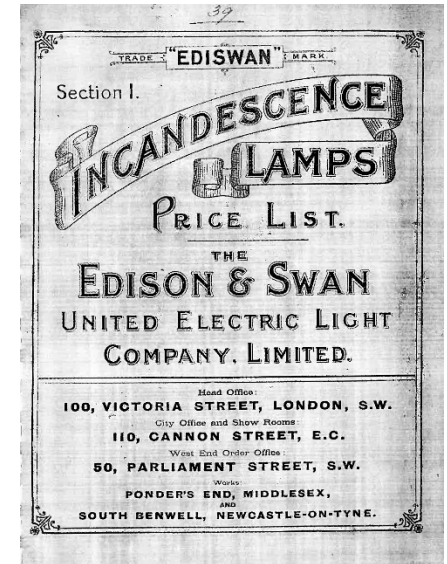
First production and distribution companies

- Crompton & Co and Swan Electric Light Company (UK)
- Thomson-Houston and Westinghouse (US)
- Siemens (Germany)



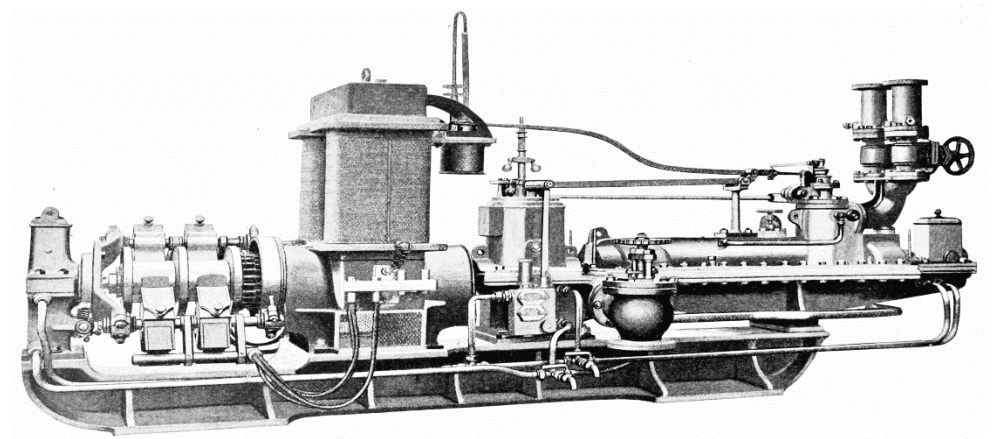
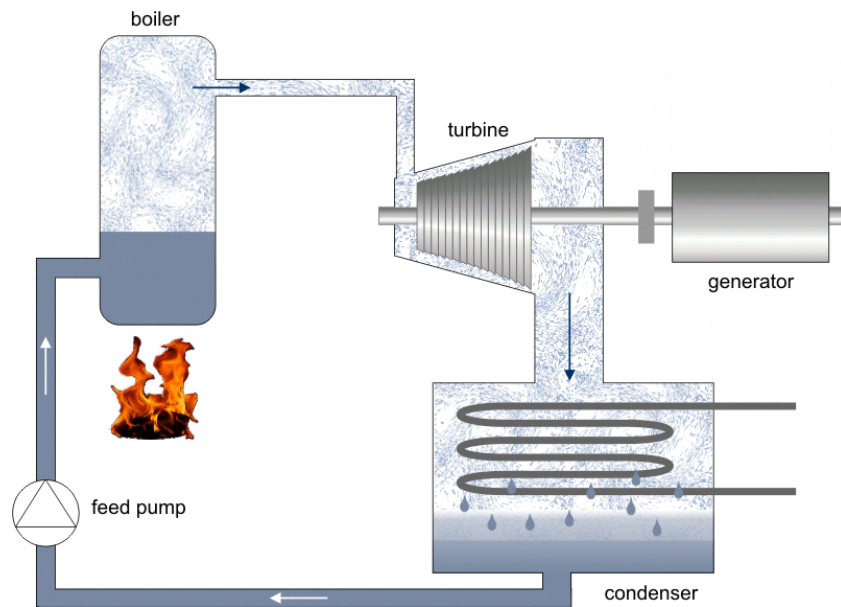
First laws regulating electricity:

- 1882 Electric Lighting Act (UK)

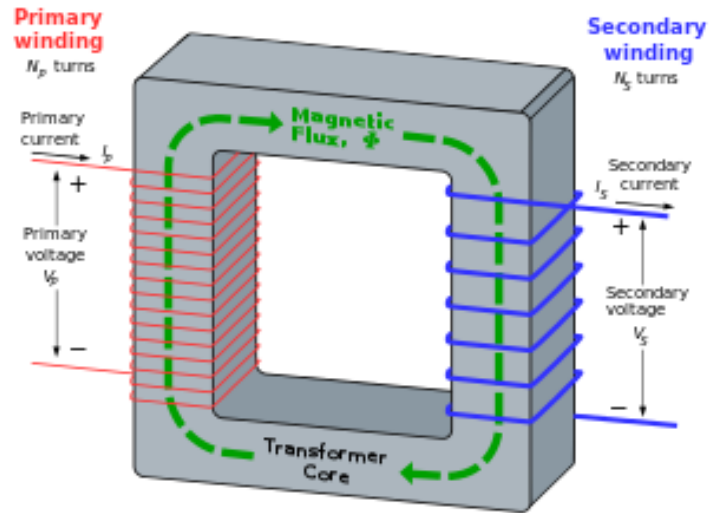


1884: Invention of Modern Steam Turbines

Steam turbines convert heat energy into mechanical energy more efficiently than previous reciprocating engines.



1884: Invention of Efficient Transformers



$$\frac{\text{Voltage in Secondary Coil}}{\text{Voltage in Primary Coil}} = \frac{\text{Turns on Secondary Coil}}{\text{Turns on Primary Coil}}$$

OR

$$\frac{V_S}{V_P} = \frac{N_S}{N_P}$$



ZBD Transformer (more efficient than 1881 Gaulard-Gibbs)



Károly Zipernowsky, Ottó Bláthy and Miksa Déri

1888-1892: The War of Currents

- Joule Effect: Power loss proportional to square of current. $P = I^2 \times R$.
- $P = V \times I$. Therefore, a high voltage is desirable to decrease current and thus minimize power loss, or to reduce the size of the conductor for the same relative loss.

Direct Current (DC):

- No efficient and reliable voltage conversion.
- Separate lines required to deliver different voltages.
- Inefficient long distance transmission on low voltage (Expensive wires)
- Requires many small distributed power plants



Thomas Edison

Alternating Current (AC):

- Efficient voltage conversion thanks to the transformer
- Efficient long distance transmission because it uses high voltage (cheap wires)
- Allows for a central large power plant



George Westinghouse



William Stanley

1888-1890: The War of Currents

Direct current propaganda:

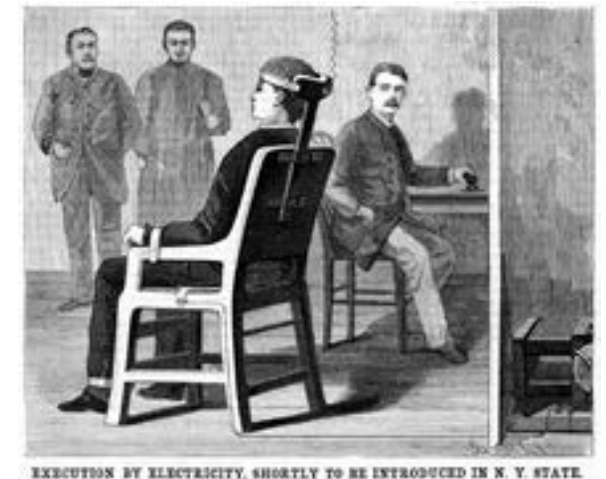
- Safer
- No deaths
- Efficient

Alternating current propaganda:

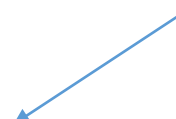
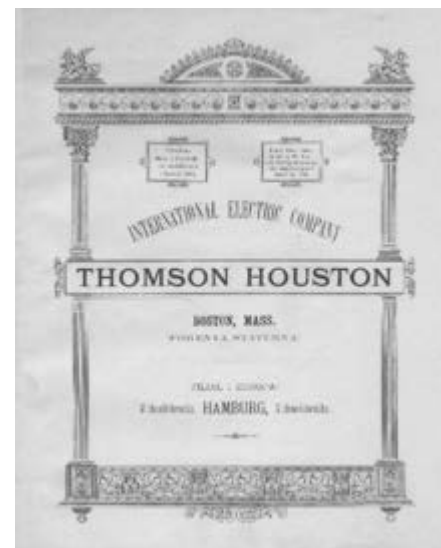
- Dangerous
- Reports of several people killed
- Building large plants would kill the transmission savings
- AC systems employ patents hold by Edison
- AC was better suited for the electric chair
- Voltage should be limited to 300 v -> AC transmission useless



Harold Brown



1892: End of War



1891: Three-Phase Alternating Current

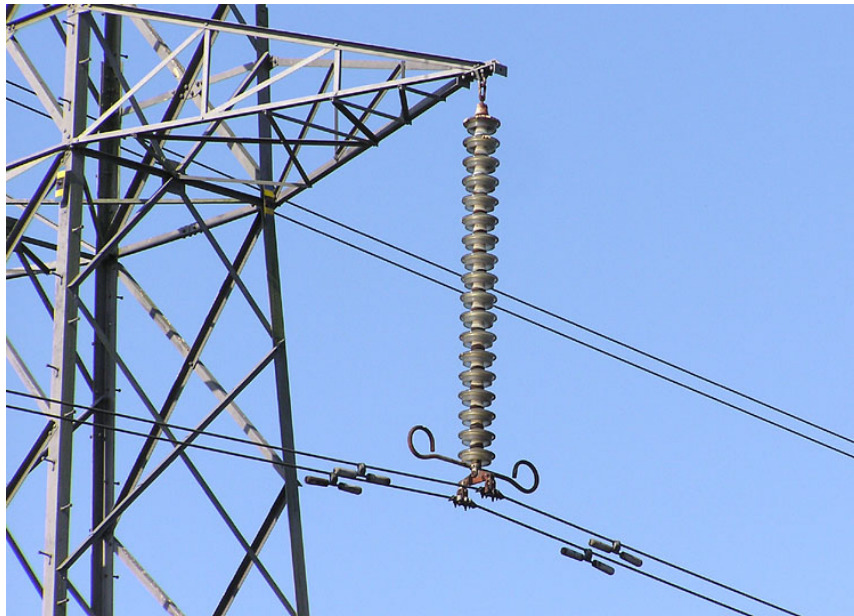


Efficiency of 75 %



1907: Invention of Suspension-Type Insulators

They allow voltages > 40kv



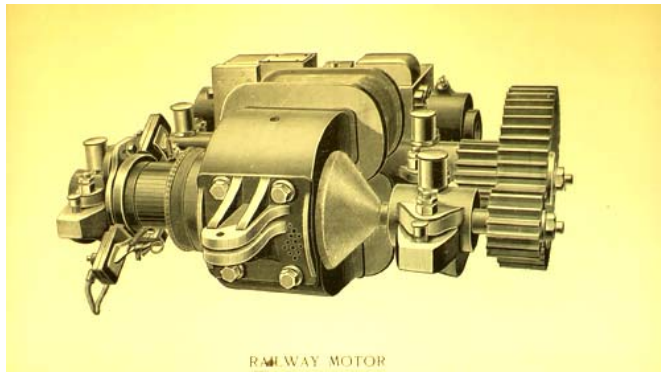
Problem: Load Balancing

- Demand at night much higher than during the day.
- Load Factor: ration of the average load with respect to the peak load.
- Most power plants did not provide service during the day.

Improve the load factor through electricity use during the day:

- DC motor (used, e.g., for electric street railways)
- AC induction motor

Electric motors were more efficient than steam engines.



1900-1950: Creation of the Electrical Grids

Interconnect central power stations for reliability, and for load balancing and improving the load factor.

- By 1914, 55 transmission lines were operating in the US at more than 70 kv
- In 1912, first European line at more than 100kv in Germany
- In 1920's, first lines over 200 kv
- In 1952, first line of 380 kv in Sweden

Problem: AC requires synchronization of the lines to be interconnected

Regulations for the electrical grid:

- 1919 Electricity Supply Bill and 1926 Electricity Supply Act (UK) -> (standard of 132 kv, 50 Hz)
- 1934 Public Utility Holding Company Act (US)

This problem can also be solved using AC to DC conversion and HVDC transmission.

AC/DC is possible thanks to rectifiers and DC/AC conversion is possible thanks to inverters.

- Early: rotary converters
- 1940s: mercury arc valves
- 1970s: thyristors, etc

After 1950: The Electrical Grid Today

Generation

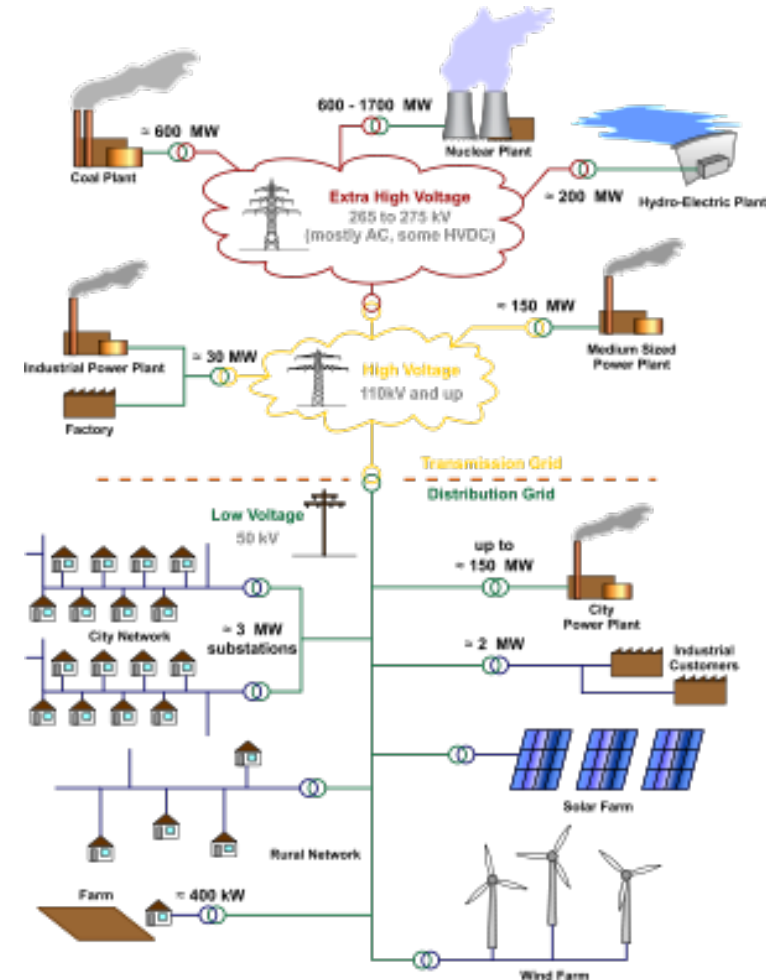
- Power Plants
- Step up transformer

Transmission Grid:

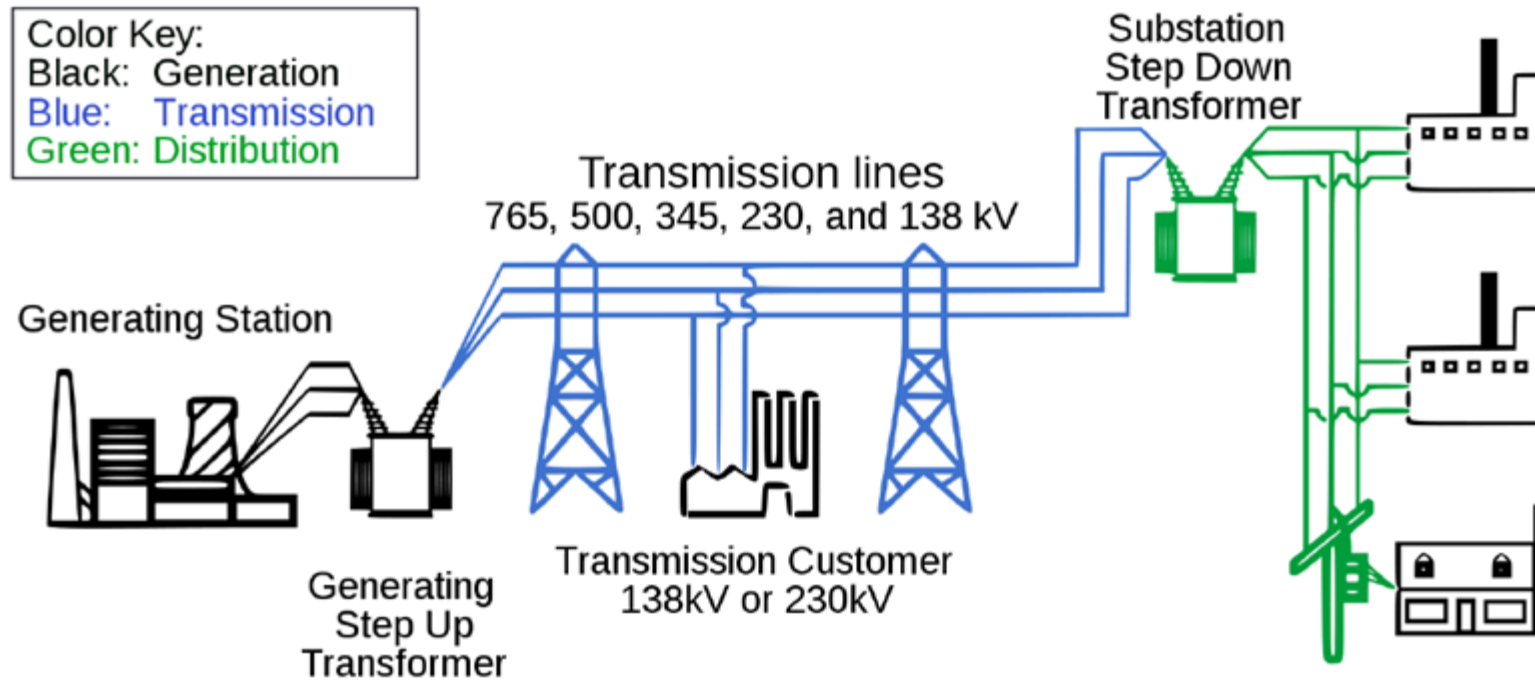
- Extra High Voltage
- High Voltage

Distribution Grid

- Substations: Step down transformer
- Customers:
 - Residential
 - Commercial
 - Industries

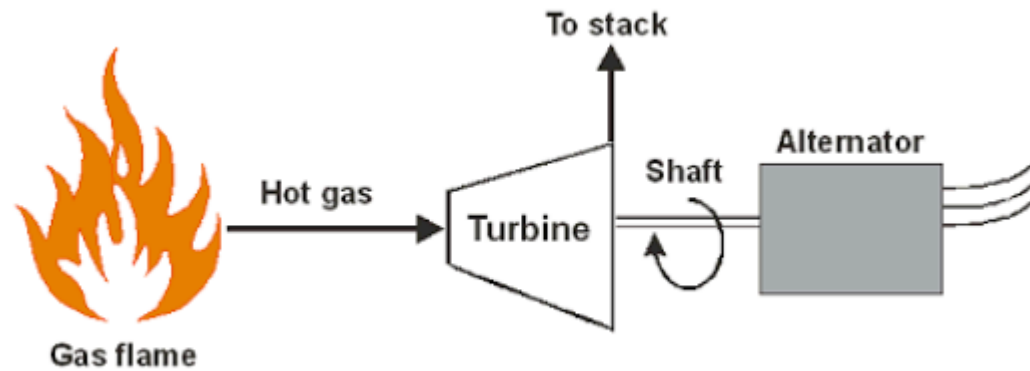


Components

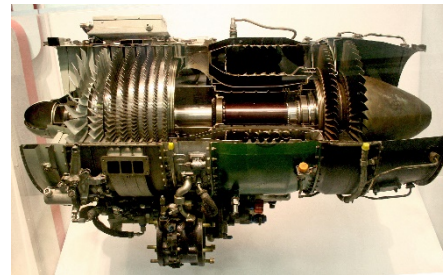


Generation: Basic Process

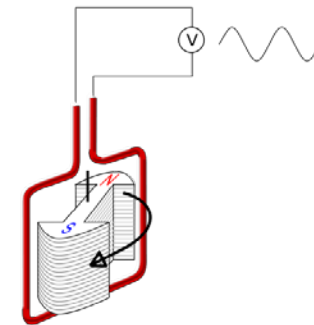
Energy Source -> Mechanical Power -> Electrical Power



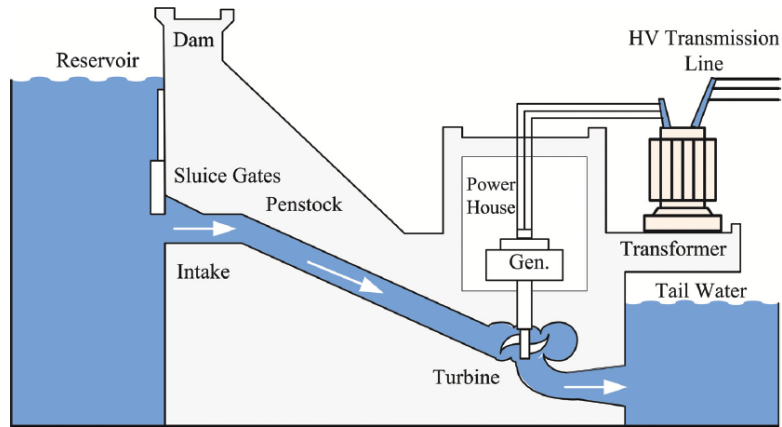
->



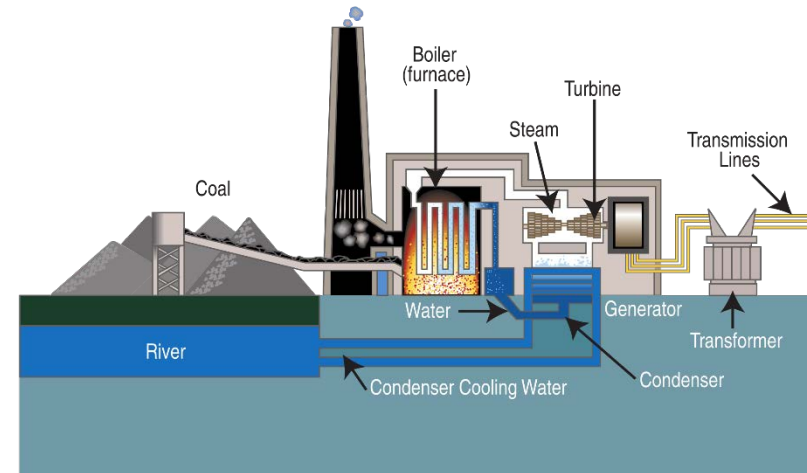
->



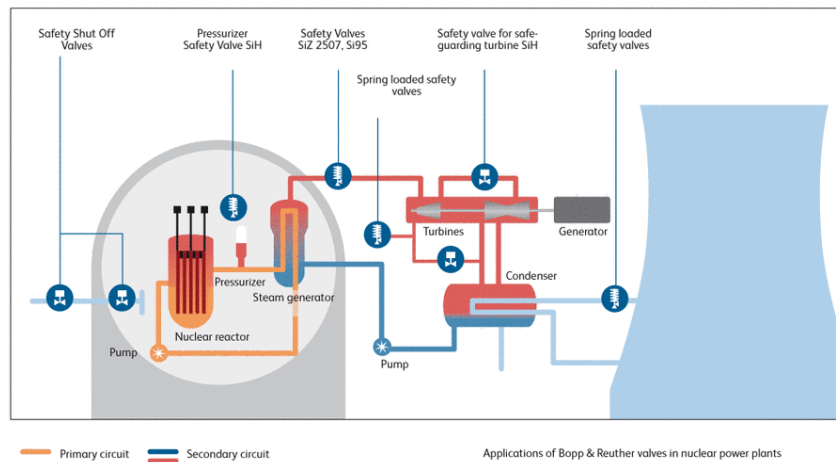
Power Plants by Energy Source



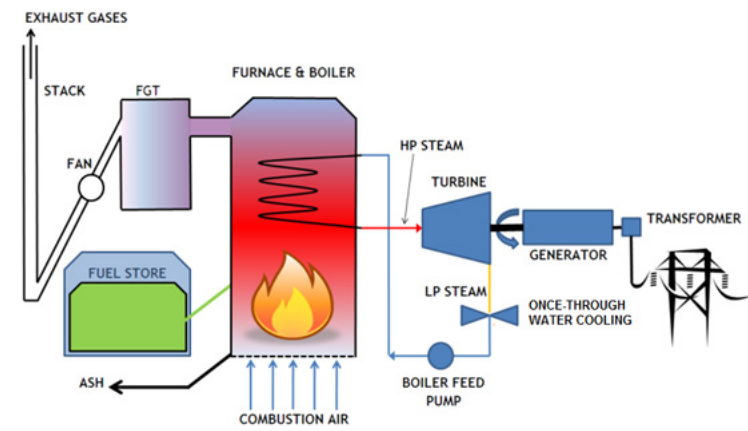
Hydroelectric Plant



Coal Plant

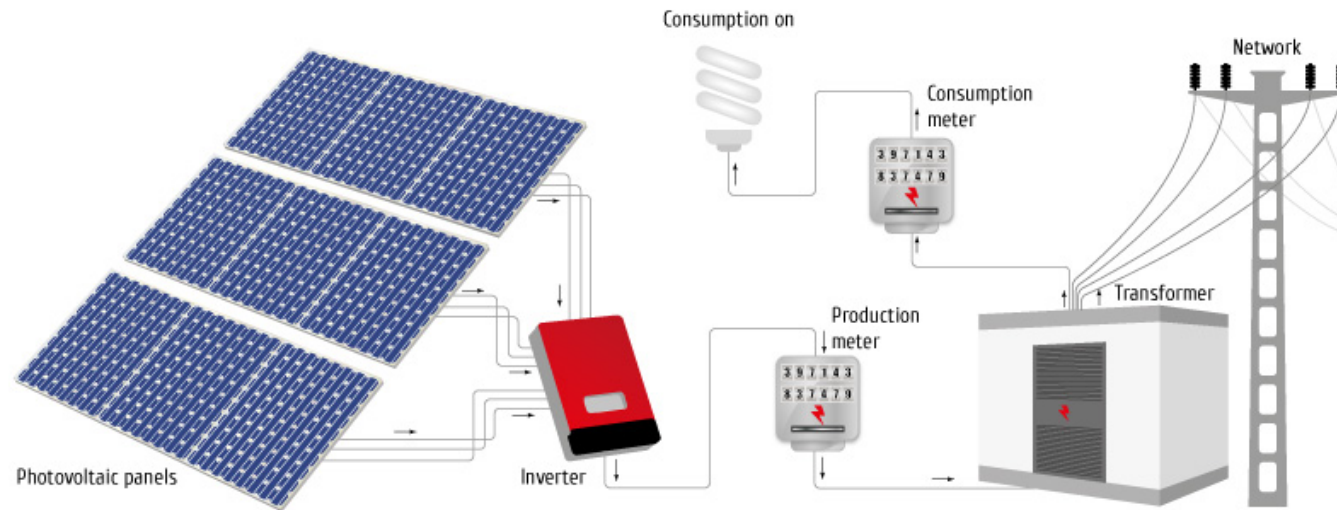


Nuclear Plant

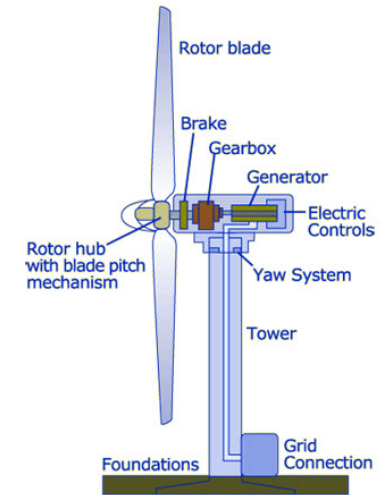


Biomass Plant

Power Plants by Energy Source

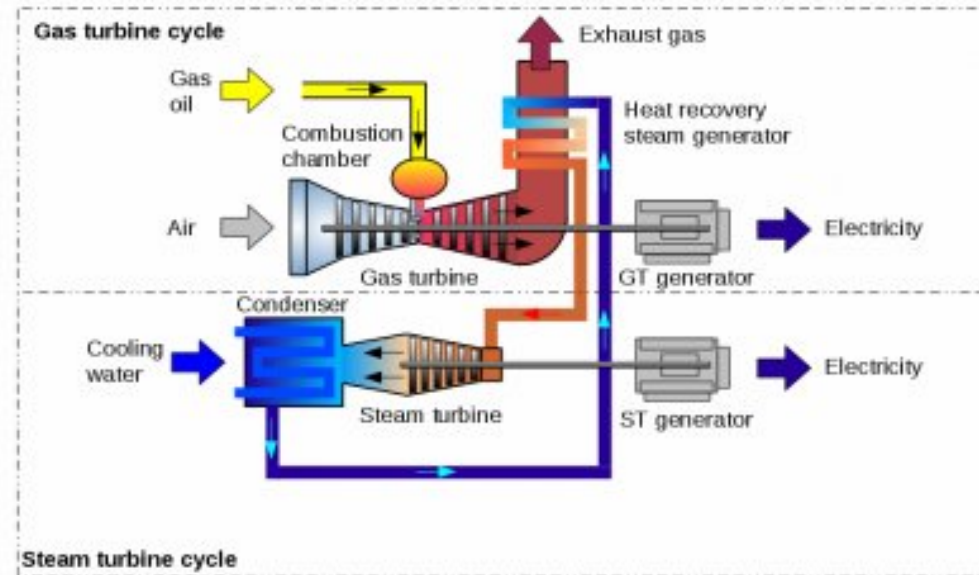


Photovoltaic Plant



Wind Plant

Power Plants



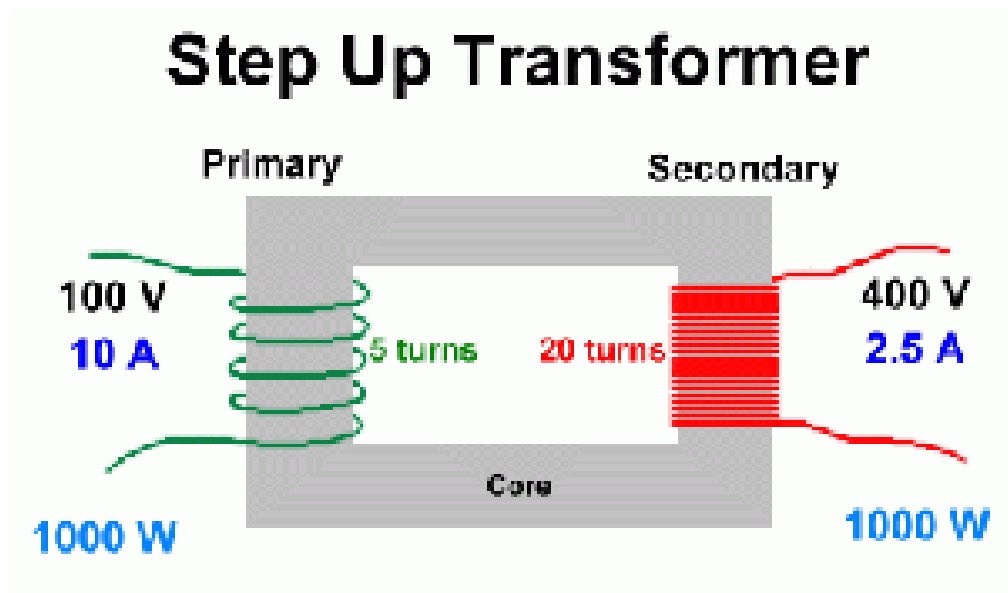
CCPP : Combined cycle power plant

Copyright 2012 © energythic.com

Gas Turbine and Combined Cycle

Gas Turbine can start rapidly -> Ideal for peak demand periods

Step up Transformer



$$\frac{\text{Voltage in Secondary Coil}}{\text{Voltage in Primary Coil}} = \frac{\text{Turns on Secondary Coil}}{\text{Turns on Primary Coil}}$$

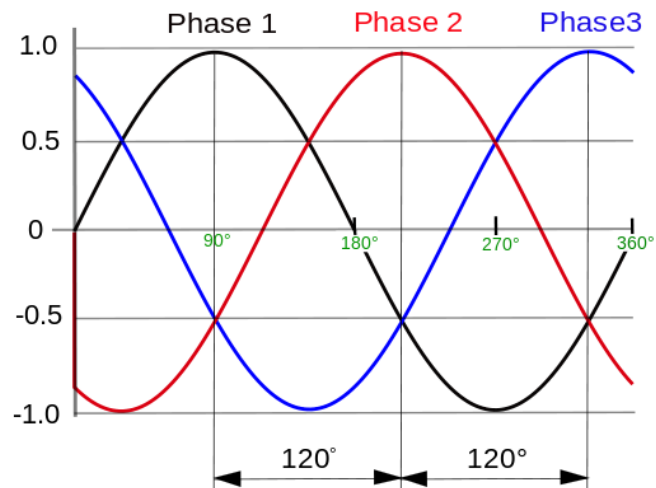
OR

$$\frac{V_s}{V_p} = \frac{N_s}{N_p}$$

Typically the voltage is stepped up to > 100 kv for transmission

Transmission lines: Three Phase AC

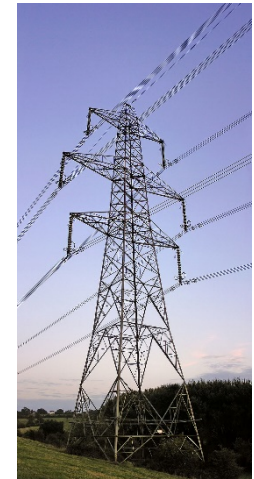
Mostly use Three Phase Alternating Current.
High Voltages are used to minimize energy loss.



In comparison to single-phase alternating current, it uses less conductor material and transmits constant power.



Single circuit transmission tower



Two circuit transmission tower



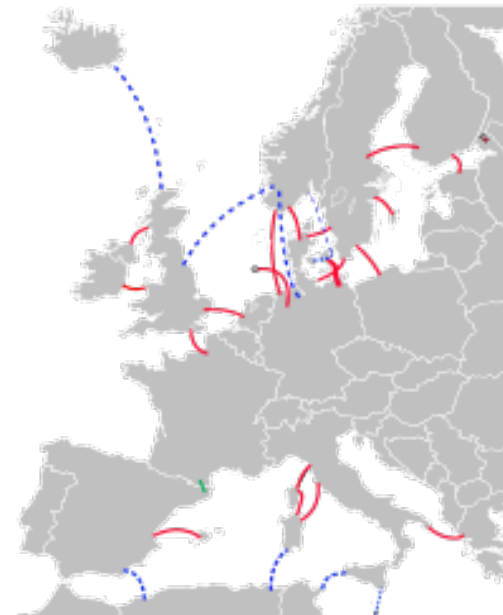
Four circuit transmission tower

Transmission lines: HVDC

From the 1960's, thyristors made possible the efficient conversion AC-DC and DC-AC.

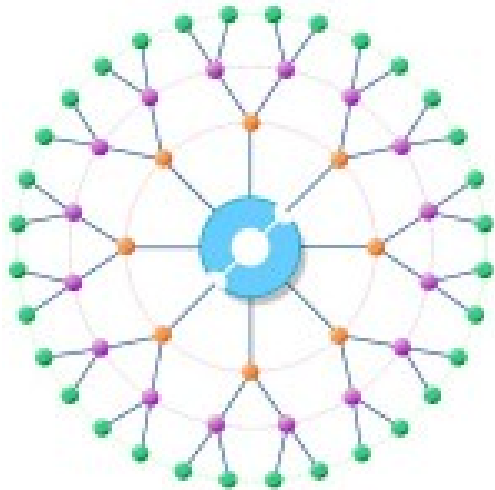
High Voltage Direct Current used for:

- To allow transmission between unsynchronized AC systems.
- Long distances (submarine cables).

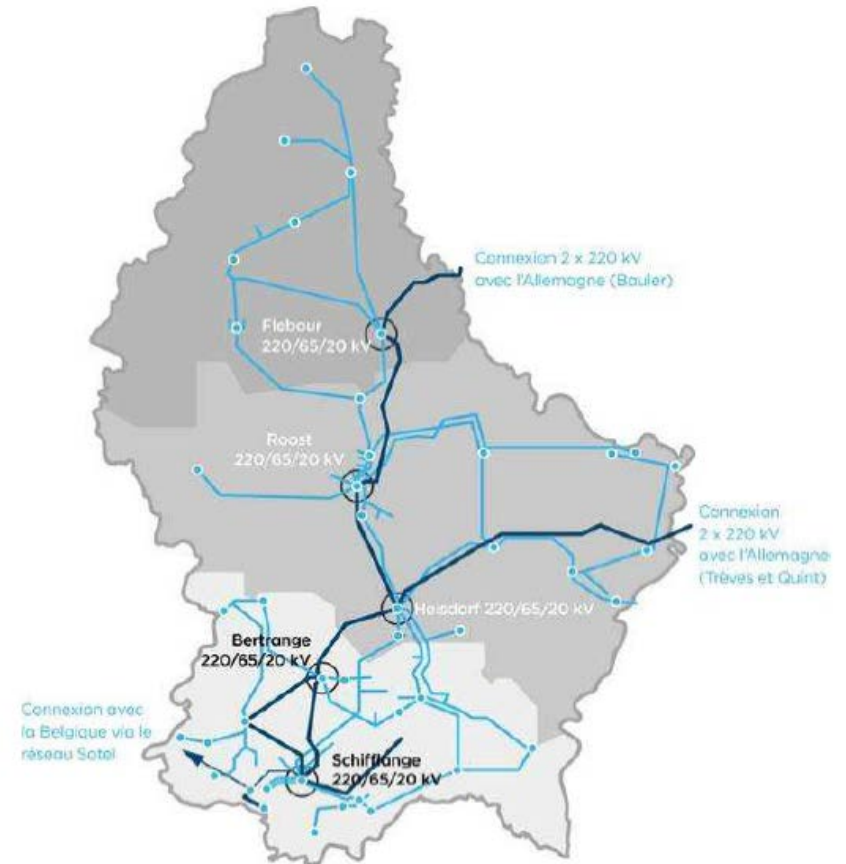


Structure of the Grid

Cheapest is a radial structure from power plant to customers



Mesh networks add redundancy to account for failures



Load Balancing

Load Balancing Problem:

- The transmission system can provide between a minimum load and a maximum load, defined by safe and fault-tolerance margins.
- Load typically varies a lot:
 - Industry mix
 - Weather conditions
- The transmission system does not have a big storage capacity => generation should match demand.

Control of generation and load:

- Power plants receive load control signals to adjust generation to the varying load.
 - Voltage signaling
 - Frequency signaling
- Transmission of the signal is done over the power lines or on separate lines

Failures

Under excess load (generation is lower than demand) the system fails:

- Brownout: graceful degradation (voltage drops)
- Blackout
- Rolling blackout: intentional blackout

Overloading can cause components to fail:

- One component shutting down affects neighboring components => cascade failure
- Protective relays and fuses protect components at risk of damage.
- Circuit breakers and switches allow to disconnect part of the network.
- Communication of failures to control operators from fault-sensing protective relays.
 - Microwaves
 - Power line communication
 - Optical fiber

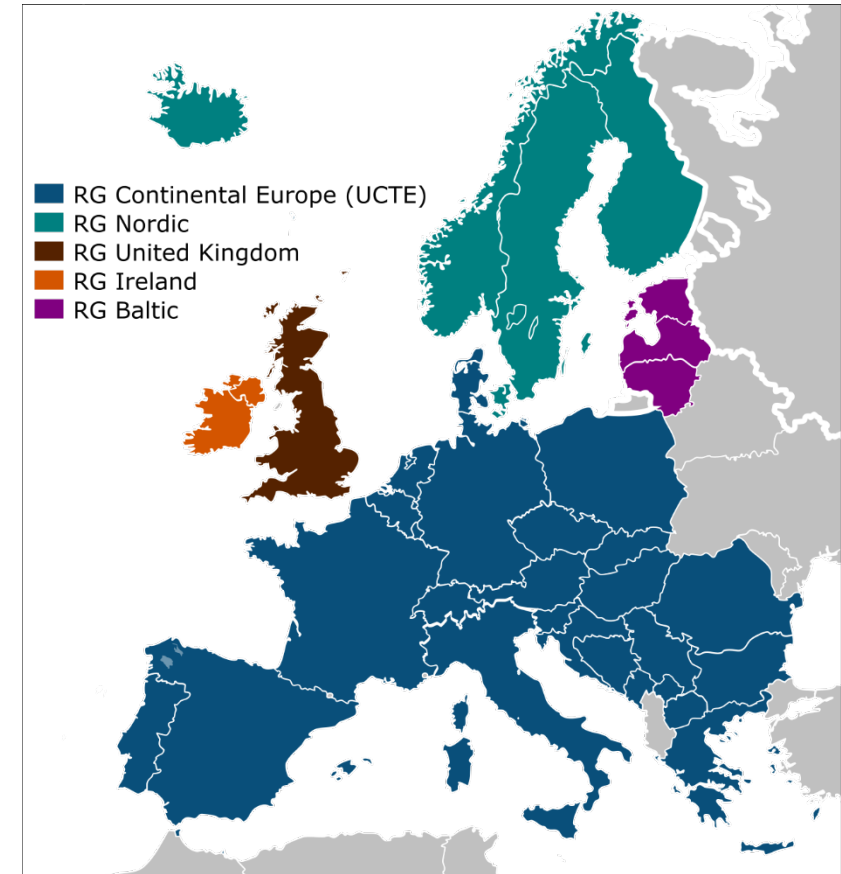
The Electrical Grids in the Europe

Synchronous Grid of Continental Europe

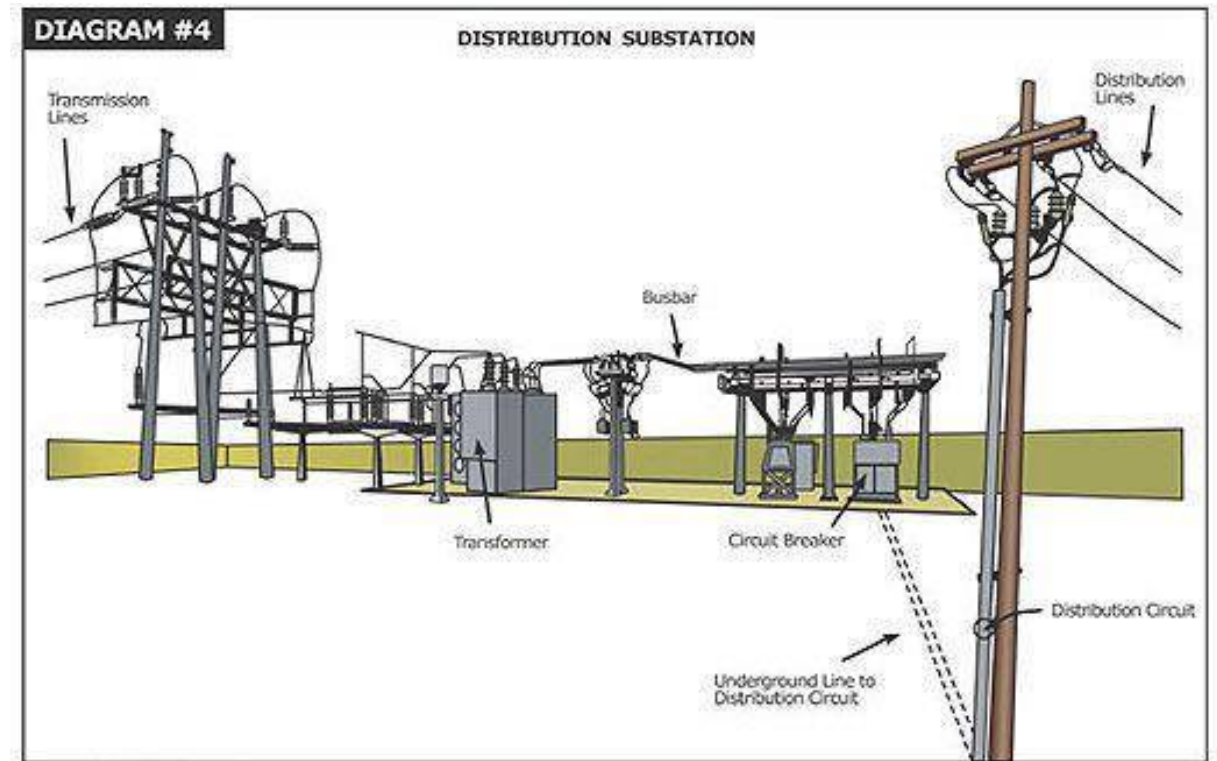
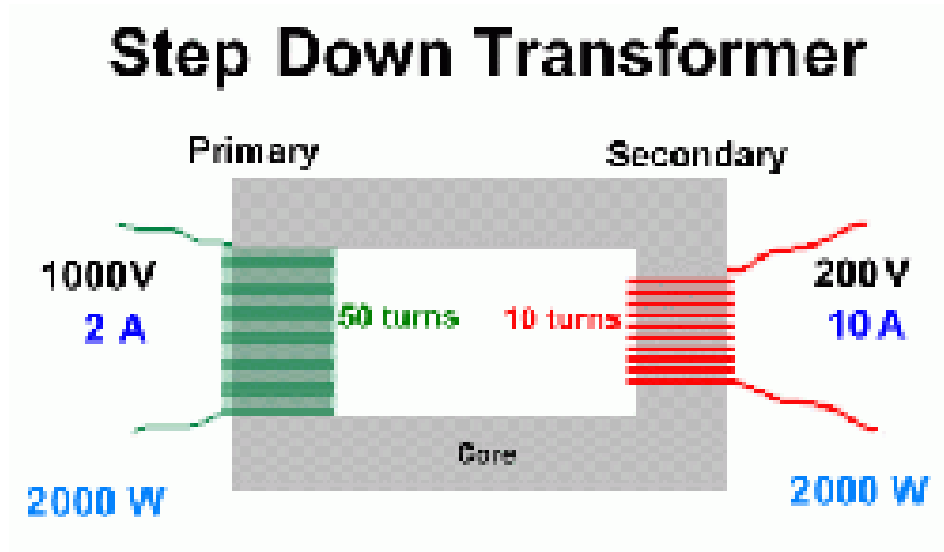
- 50 Hz
- 400 million customers
- 667 MW (Excess of 80 MW)

Long distance transmission is cheap and efficient
(cheaper than distribution)

Interconnection allows for load balancing and
Improved load factors



Substation: Step Down Transformer



Typically the voltage is stepped down to 600-35000 v (typically 11 kv or 22 kv)

Distribution Lines



Underground lines in urban areas



Utility Poles in rural areas

Topology can be:

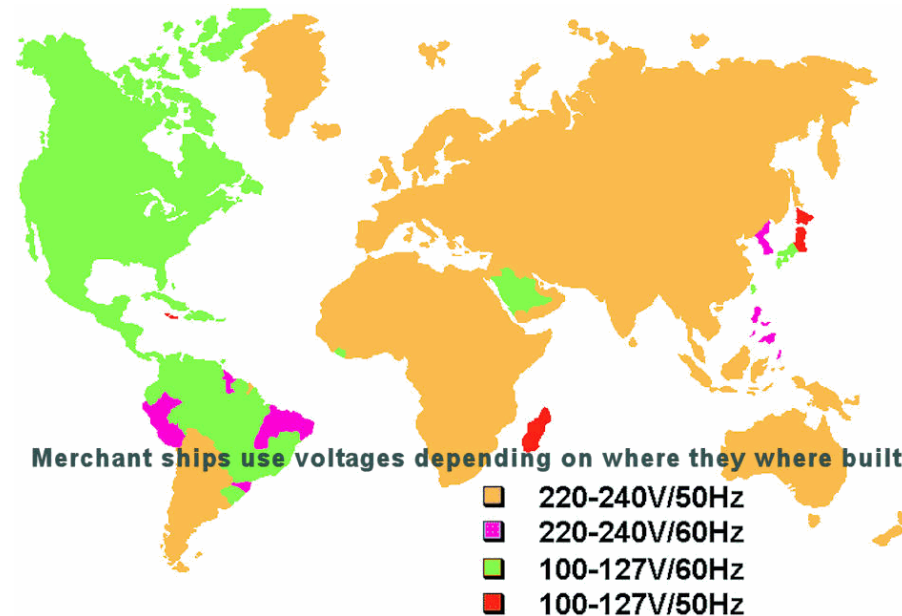
- Radial: Each customer has one supply source.
- Network: Parallel supply with multiple sources is available.

Distribution transformer



Distribution Transformers deliver (typically) single phase alternating current to commercial and residential customers.

The output voltage is 220-240 v in most of the world



Electricity Meter



Traditional meter:

- Limited metering capability
- Fix tariff or dual tariff (day and night) arrangements
- Communication of consumption not possible

1980's: Automatic Meter reading

- Monitor loads from large customers

1990's: Advanced Metering Infrastructure

- Store load at different times of the day

ENTITIES

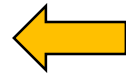
Provider (P)

User (U)

Meter (M)

$\gamma: (cons, other) \rightarrow price$ →

← $(cons, other)$



fee, π



SECURITY REQUIREMENTS

- P is assured that U reports correct fee
- P does not learn (cons, other)
- P cannot claim U must pay fee'



<http://www.inkity.com/catalog/product/2/2077/Shaking-On-Money-Deal.html>



<http://apcit.blogspot.com/>



<http://www.billboardmama.com/recording-connection-scam-p-1017.html>

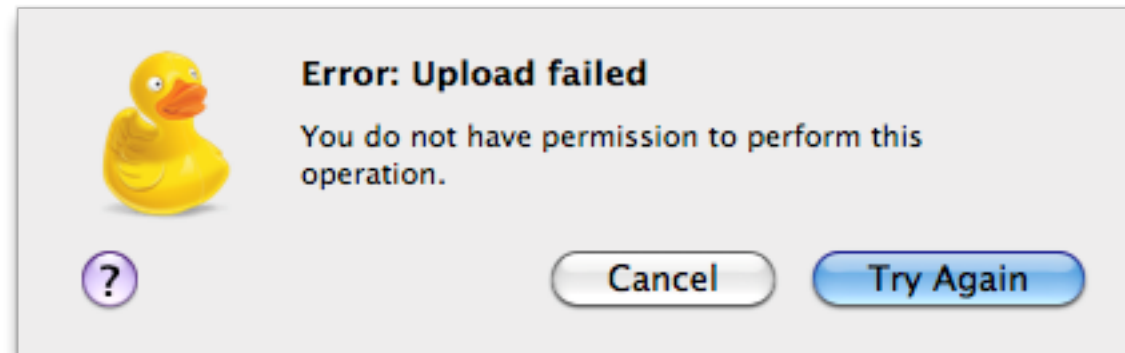
ASSUMPTIONS

- M should be tamper-resistant



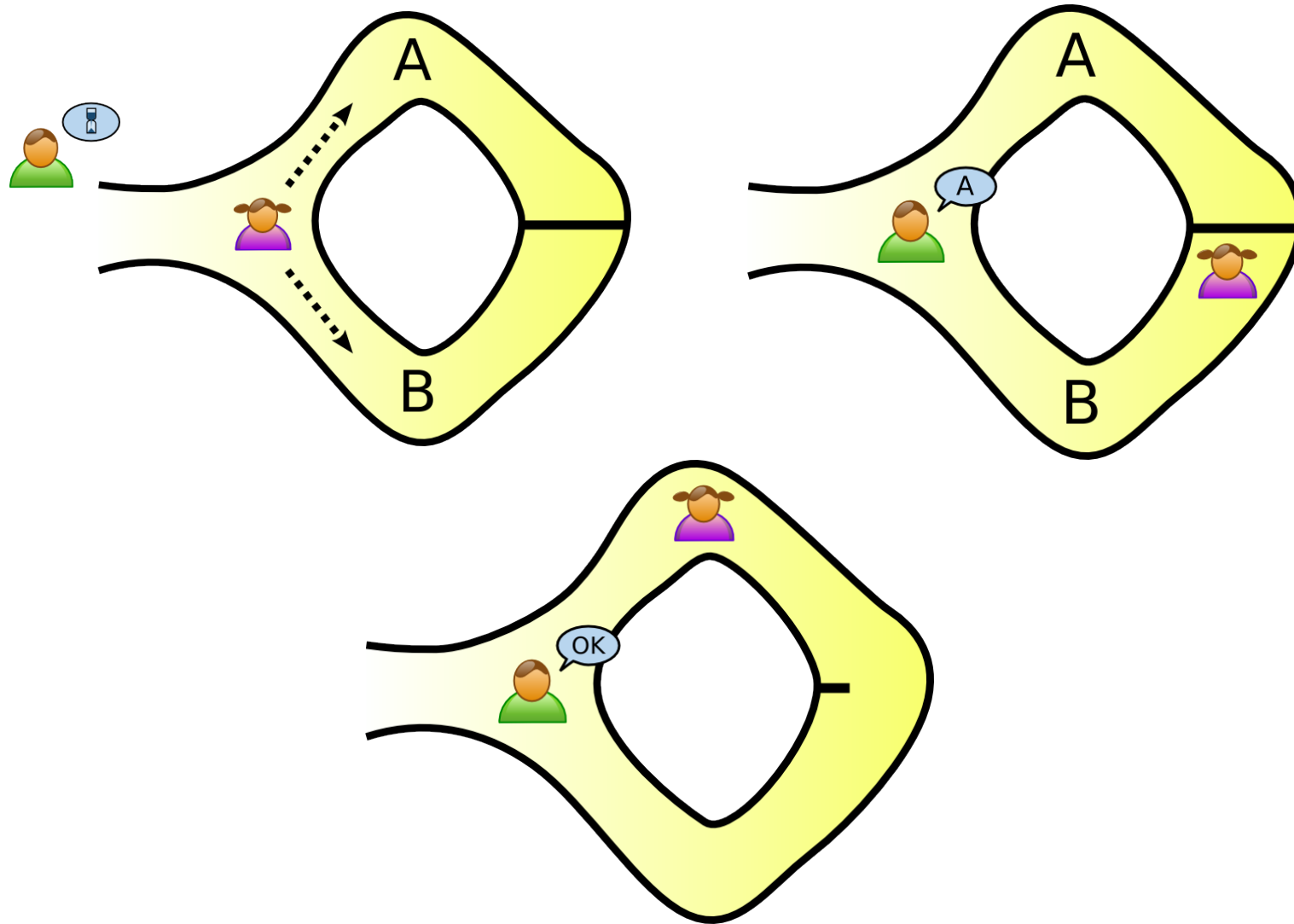
<http://www.smartplanet.com/business/blog/smart-takes/report-smart-meters-have-security-holes-that-could-allow-hackers-access-to-grid/5532/>

- No direct uplink from M to P

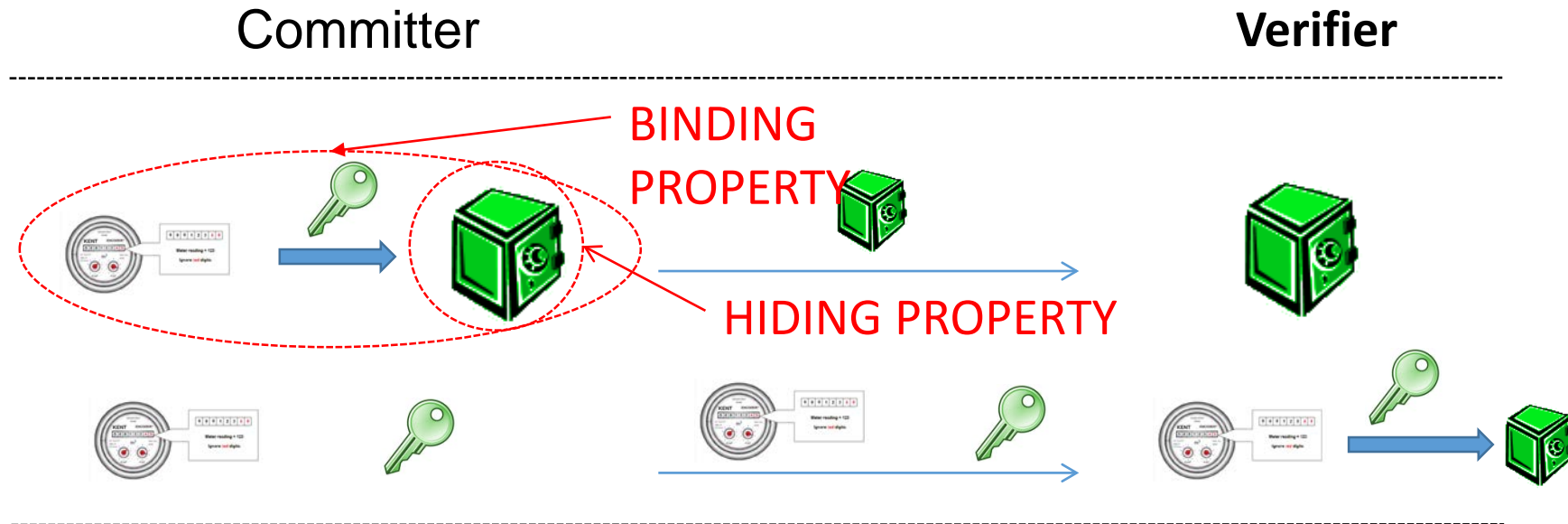


<http://trac.cyberduck.ch/wiki/help/en/howto/googledocs>

Our Protocol: Preliminaries



Commitment Schemes

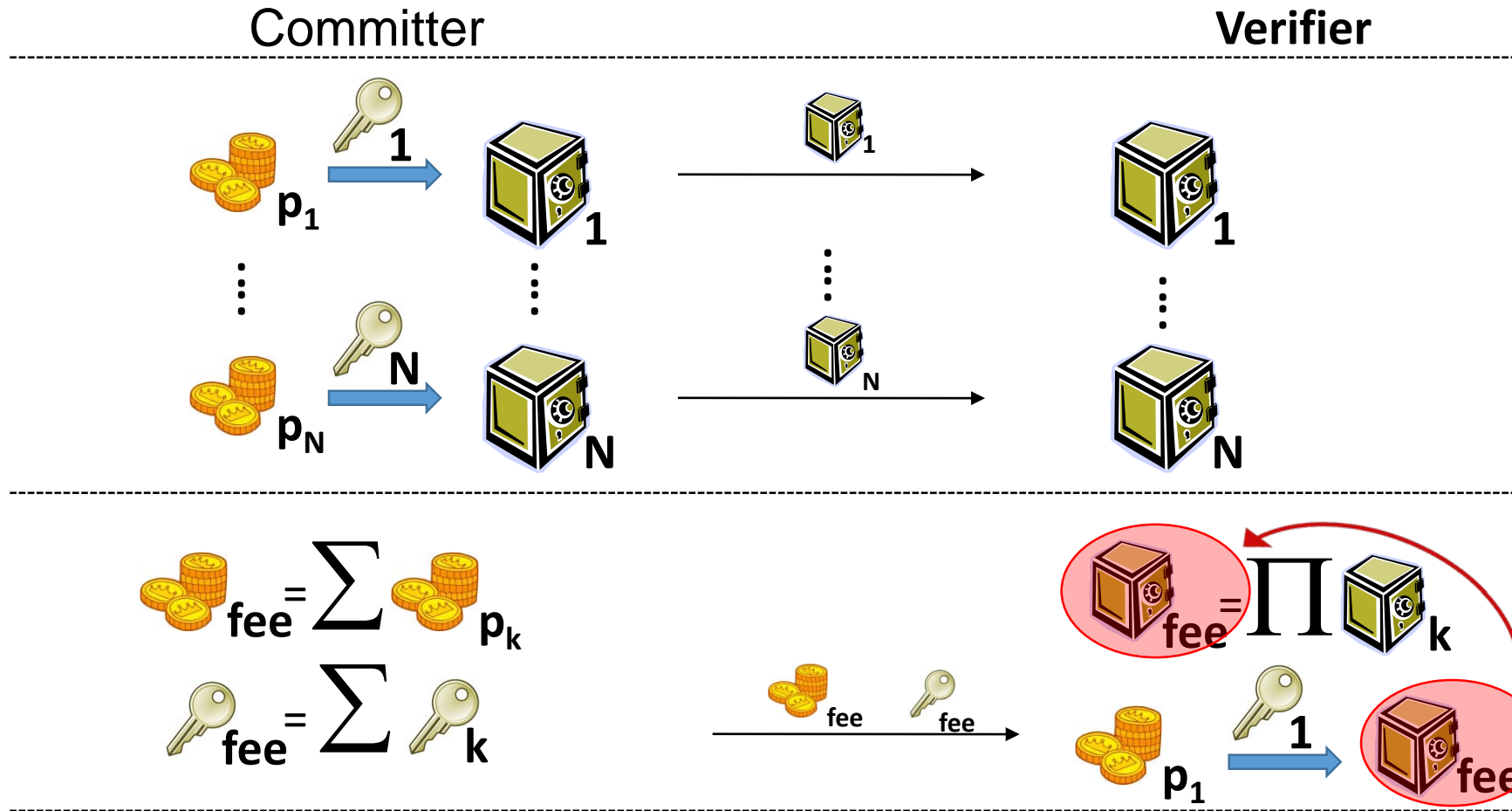


Compute parameters $par \leftarrow ComSetup(1^k)$

Compute commitment $(C_m, open_m) \leftarrow Commit(par, m)$

Open commitment $\{0,1\} \leftarrow Open(par, C_m, m, open_m)$

Homomorphic Commitments



$$(C_{m_1}, \text{open}_{m_1}) \leftarrow \text{Commit}(\text{par}, m_1)$$

$$(C_{m_2}, \text{open}_{m_2}) \leftarrow \text{Commit}(\text{par}, m_2)$$

$$C = C_{m_1} \times C_{m_2}$$

$$1 \leftarrow \text{Open}(\text{par}, C, m_1 + m_2, \text{open}_{m_1} + \text{open}_{m_2})$$

Zero-Knowledge Proofs of Knowledge

- Protocol between a prover and a verifier where the prover proves knowledge of a witness w that satisfies a statement s . Two properties:
 - Proof of knowledge (PK): a prover without knowledge of w succeeds with negligible probability.
 - Zero-knowledge (ZK): The verifier does not get any information on w .

- Notation: $NIPK\{(w): 1 \leftarrow s(w)\}$



http://www.cafepress.com/+i_love_zk_womens_tshirt,129534271

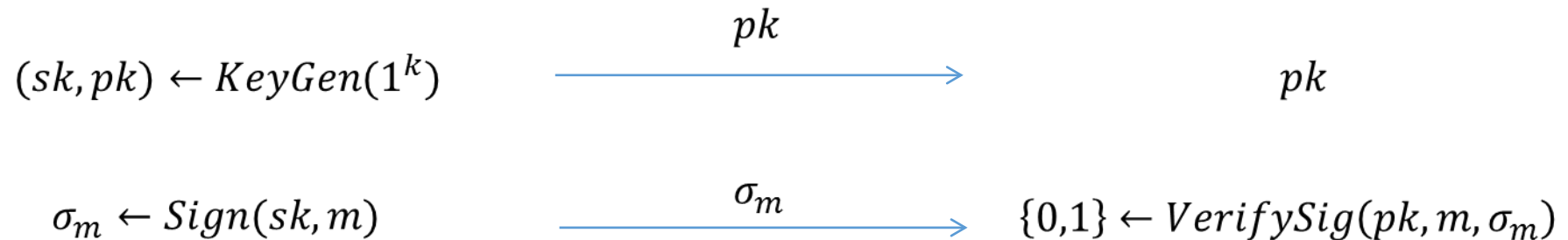
Signature Schemes



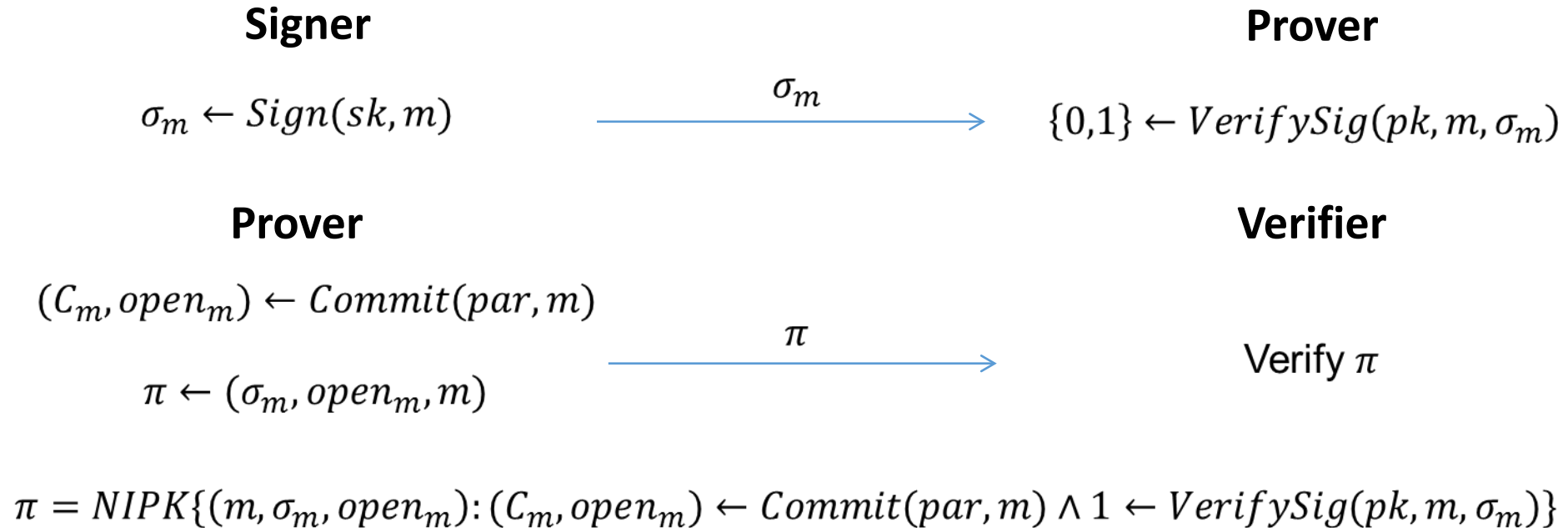
<http://www.nobleco.org/surveyor/index.php?q=node/64>

Signer

Verifier



Proof of possession of a signature



<http://self-issued.info/?p=272>



<http://www.obron.ch/?p=253>

Our Protocol: Construction

M, U, P interact in five phases:

- Setup & Initialization
- Consumption Phase
- Payment Phase
- Reveal Phase
- Policies

A complete smart meter
solution

<http://www.imetertechnology.com/>

Setup Phase



Compute key pair
 $(sk_U, pk_U) \leftarrow UKeyGen(1^k)$



Compute key pair
 $(sk_M, pk_M) \leftarrow MKeyGen(1^k)$



Compute key pair
 $(sk_P, pk_P) \leftarrow PKeyGen(1^k)$

Compute commitment params
 $par \leftarrow ComSetup(1^k)$

Initialization Phase



Choose pricing policy $\Upsilon: (cons, other) \rightarrow price$

Signs pricing policy

$$\{\sigma \leftarrow PSign(sk_p, \langle cons, other, price \rangle)\}$$

Υ_s

$\xleftarrow{\Upsilon_s}$

$$\Upsilon_s = \{\sigma\}$$

Verify signed policy

$$\{0,1\} \leftarrow PVerifySig(pk_p, \sigma, \langle cons, other, price \rangle)$$

Consumption Phase



Read ($cons, other$)

Commits to consumption and other

$(C_{cons}, open_{cons}) \leftarrow Commit(par, cons)$

$(C_{other}, open_{other}) \leftarrow Commit(par, other)$

Signs commitments

$\sigma \leftarrow MSign(sk_m, \langle d_M, C_{cons}, C_{other} \rangle)$

$(\sigma, d_M, cons, open_{cons}, other, open_{other})$

Verifies commitment openings

$\{0,1\} \leftarrow Open(par, C_{cons}, cons, open_{cons})$

$\{0,1\} \leftarrow Open(par, C_{other}, other, open_{other})$

Verifies signature

$\{0,1\} \leftarrow MVerifySig(pk_m, \sigma, \langle d_U, C_{cons}, C_{other} \rangle)$

Payment Phase (I)



For all tuples $(cons, other)$ output by M

Compute price $Y: (cons, other) \rightarrow price$

Commit to price $(C_{price}, open_{price}) \leftarrow Commit(par, price)$

Proof knowledge of signature that bind consumption and price

$\pi \leftarrow NIPK\{(\sigma, price, open_{price}, cons, open_{cons}, other, open_{other})\}:$

$(C_{price}, open_{price}) \leftarrow Commit(price) \wedge$

$(C_{cons}, open_{cons}) \leftarrow Commit(cons) \wedge$

$(C_{other}, open_{other}) \leftarrow Commit(other) \wedge$

$1 \leftarrow PVerifySig(pk_p, \sigma, \langle cons, other, price \rangle)\}$

Payment Phase (II)



Aggregate prices and openings

$$fee = \sum_{k=1}^N price_k \quad open_{fee} = \sum_{k=1}^N open_{price}$$

Compose a payment message

$$m = (fee, open_{fee}, \{\sigma, \langle d_U, C_{cons}, C_{other} \rangle, C_{price}, \pi\})$$

Sign payment message

$$s_m \leftarrow USign(sk_U, m)$$

(m, s_m)

Verify Signature

$$1 \leftarrow UVerifySig(pk_U, s_m, m)$$

Verify proofs π

Aggregate commitments to price

$$C_{fee} = \prod_{k=1}^N C_{price_k}$$

Verify Opening of C_{fee}

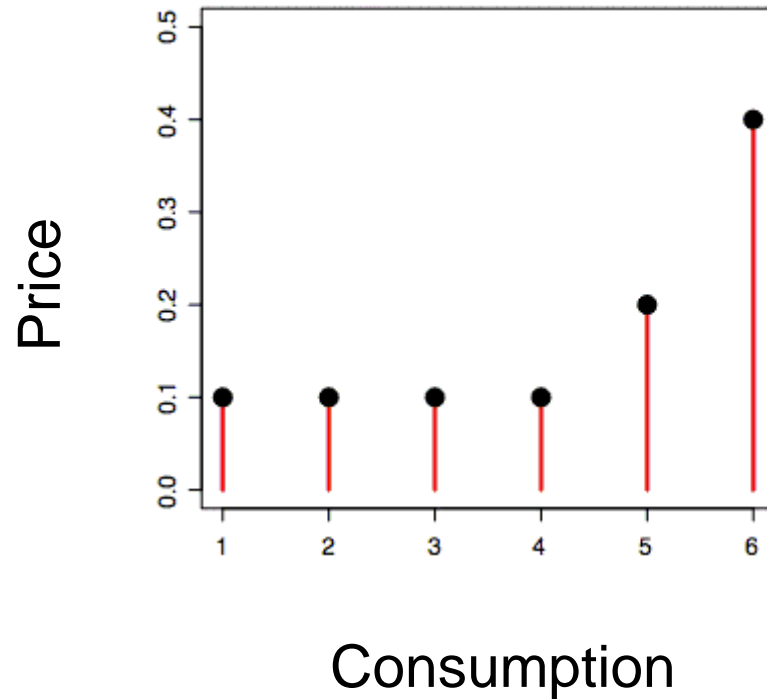
$$1 \leftarrow Open(C_{fee}, fee, open_{fee})$$

Remarks

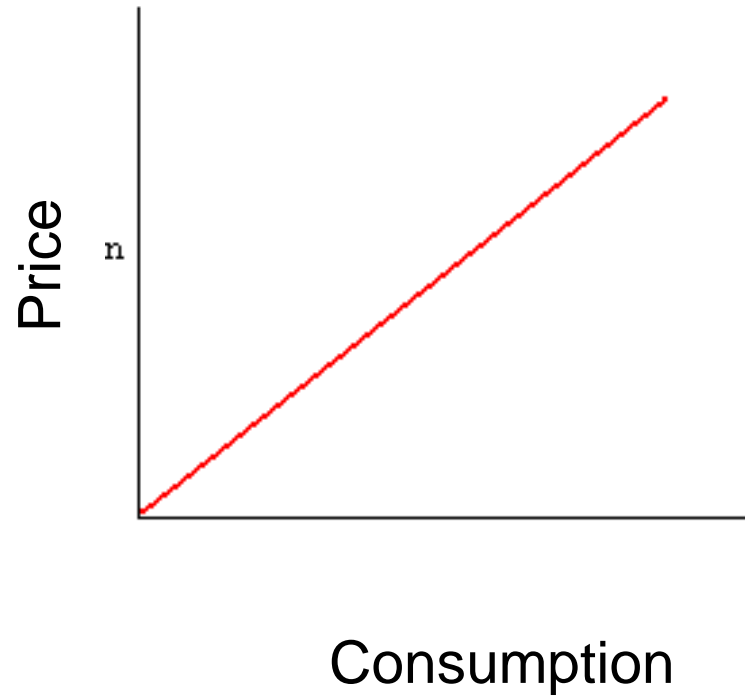
- Reveal Phase (optional):
 - P asks U to open one or more commitments to *cons* or *other*.
 - U discloses only the openings of those commitments
- Secure when M and P do not collude.
 - Modification possible to ensure security when they collude, albeit efficiency decreases by a factor of ≈ 2
- Very Efficient construction when choice of signature in the policy does not depend on *cons* and Υ is linear.
 - NIPK are not needed.
 - Ideal for electricity metering

Pricing Policies

Discrete Policy

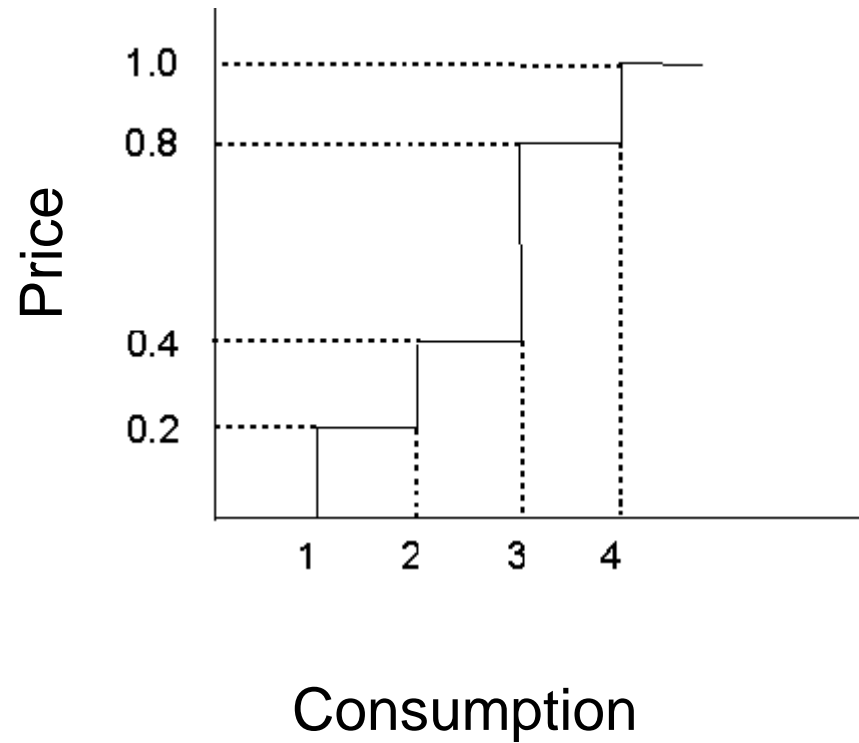


Linear Policy

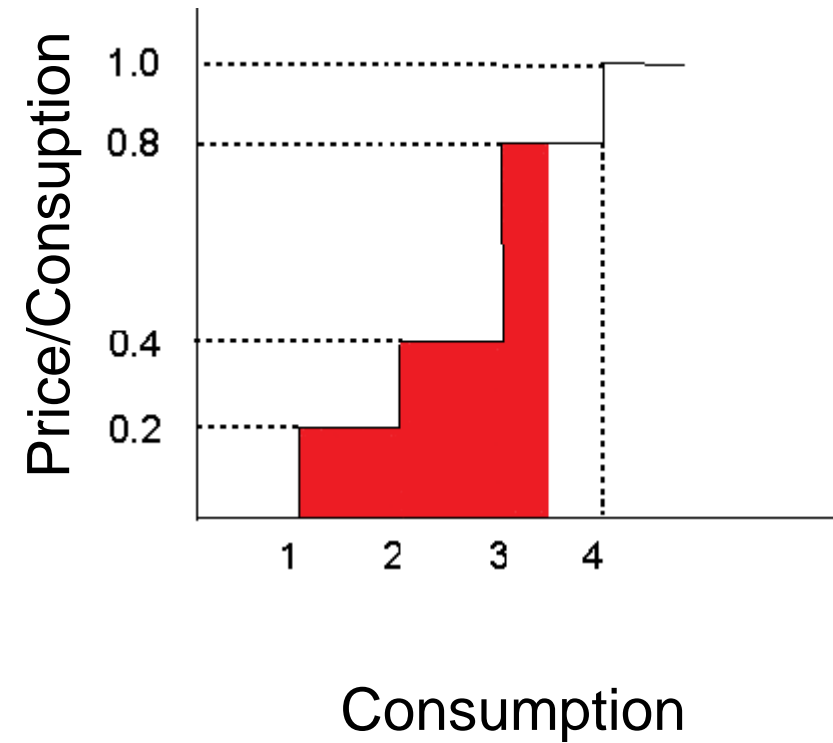


Pricing Policies

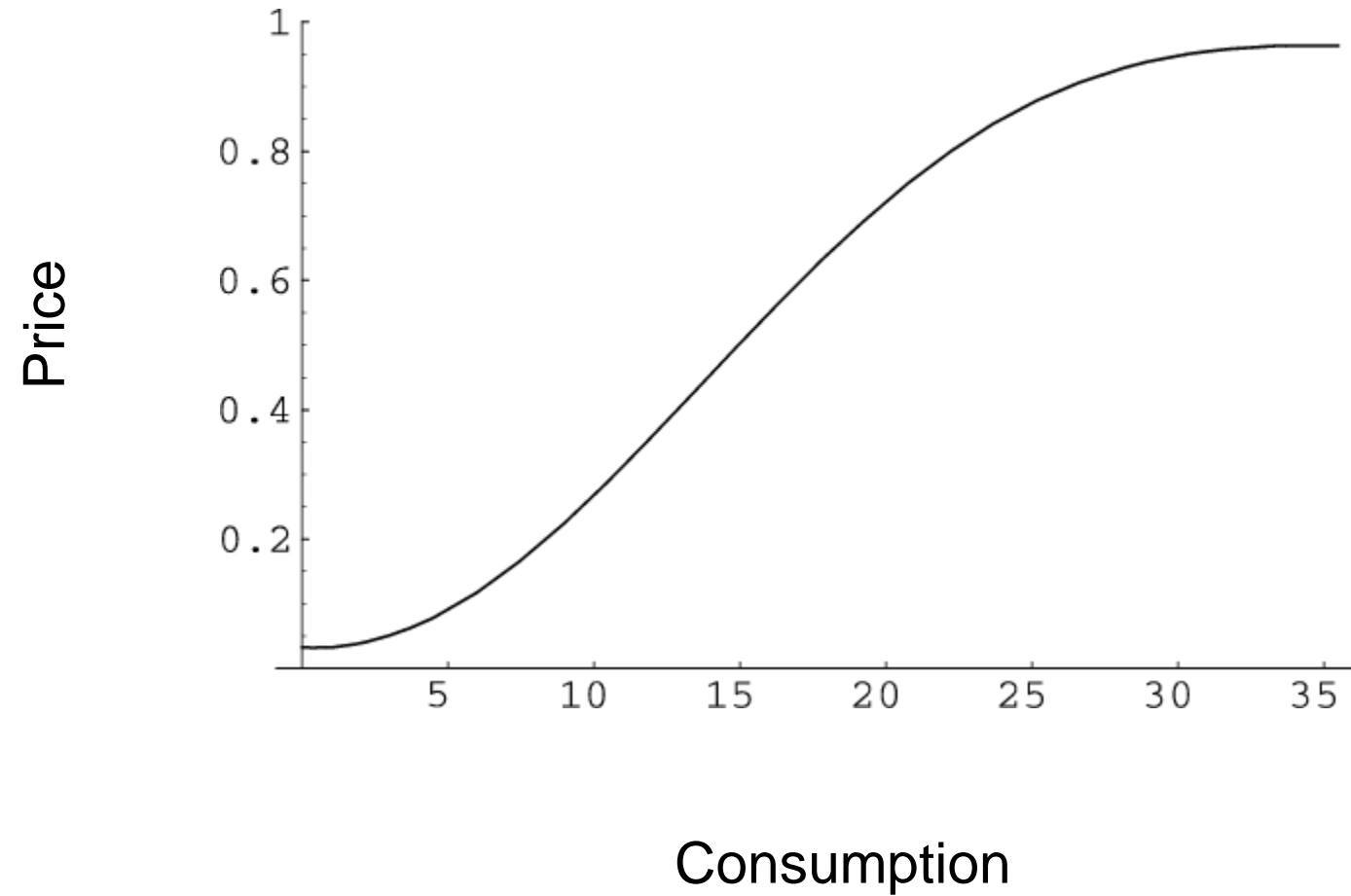
Interval Policy



Cumulative Policy



Pricing Policies



Advantages



<http://www.frikipedia.es/friki/n%C3%B3nimo>

- It does not require anonymous channels or anonymized databases
- It does not require interaction among users
- Minimises Trusted Computing Base
- It does not require trusted parties
- It is efficient enough for practical applications
- It supports a wide variety of pricing policies
- It permits selective disclosure of private data

Implementation & Evaluation



Efficient Instantiation

- M's and U's signature schemes can be instantiated by any existentially unforgeable signature scheme.
- Camenisch-Lysysanskaya signatures for P's signature scheme (strong RSA assumption)
- Commitments scheme due to Groth
- NIPK implemented via Fiat-Shamir heuristic:
 - PK of the opening of a Groth commitment
 - PK of CL signature possession
 - PK that a value lies in an interval (3 squares)

Implementation Tools

- Programing language: C & C++
- MS Bignum Library (not optimized with assembler)
- HW
 - 32 Bit Win 7 – Intel Core2 DUO P9600 @ 2.66GHz (1 core) / 4GB Ram (3.49GB Usable)
 - 64 Bit Win Server Enterprise – Intel Xeon E5440 @ 2.83GHz (1 core / 2 processors) / 32GB Ram
- Security level: RSA 1024.



Evaluation

	32 Bit		64 Bit	
	Full-fledged Construction	Efficient Construction	Full-fledged Construction	Efficient Construction
Consumption Phase	31.4/s	31.4/s	171.209/s	171.209/s
Compute Payment	1.5/s	26780.6/s	20.1444/s	298295/s
Verify Payment	2.2/s	3711.02/s	91.3977/s	16345/s