Review of "High-Assurance Smart Grid: A Three-Part Model for Smart Grid Control Systems"

Thomas M. Overman, Ronald W. Sackman,
Terry L. Davis, Brad S. Cohen
Proceedings of the IEEE, Vol. 99, No. 6, June 2011

Francesco Mucci

Corso di Laurea Magistrale in Informatica

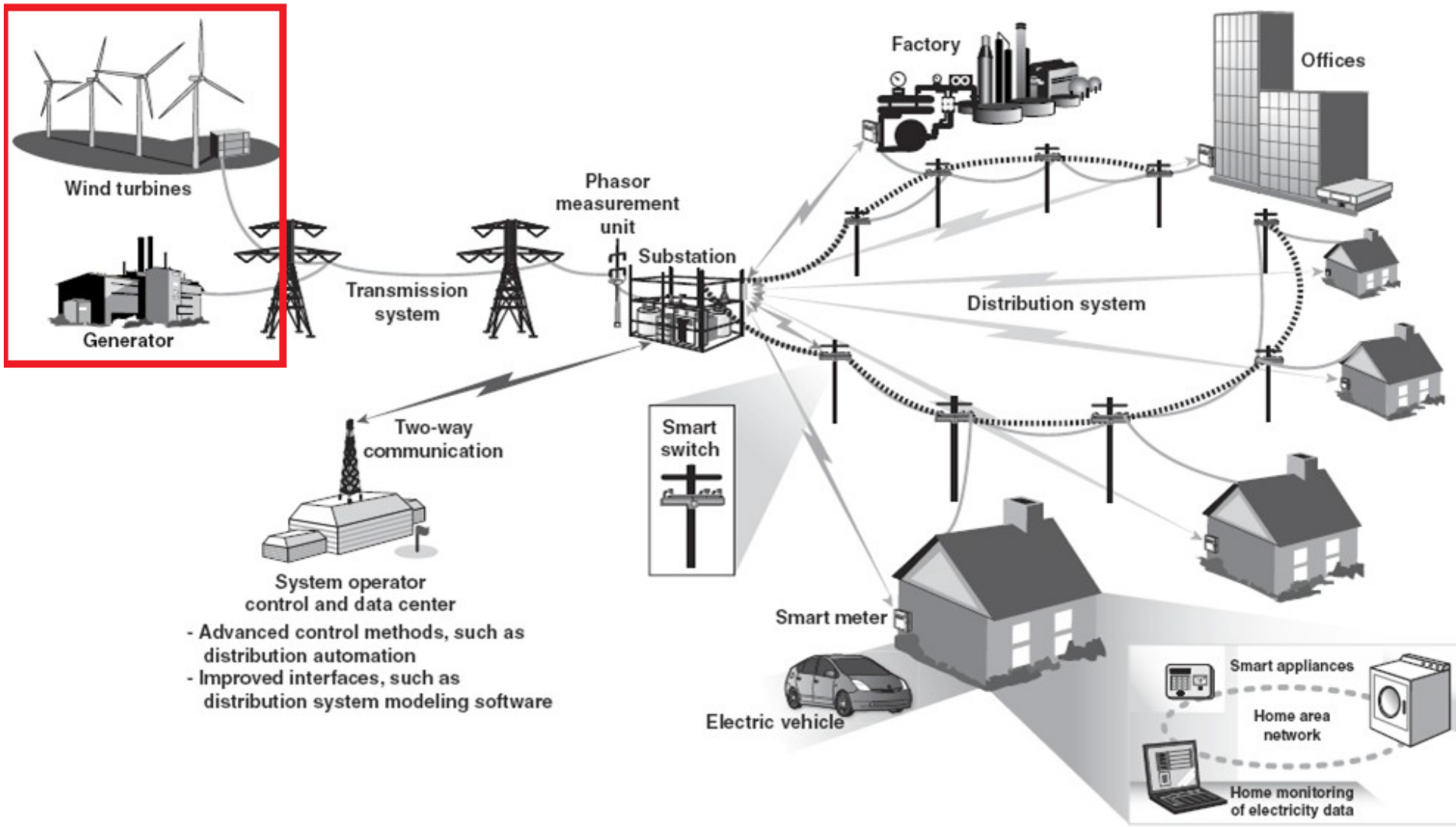
Sistemi Critici e Real Time

UNIVERSITÀ
DEGLI STUDI
FIRENZE

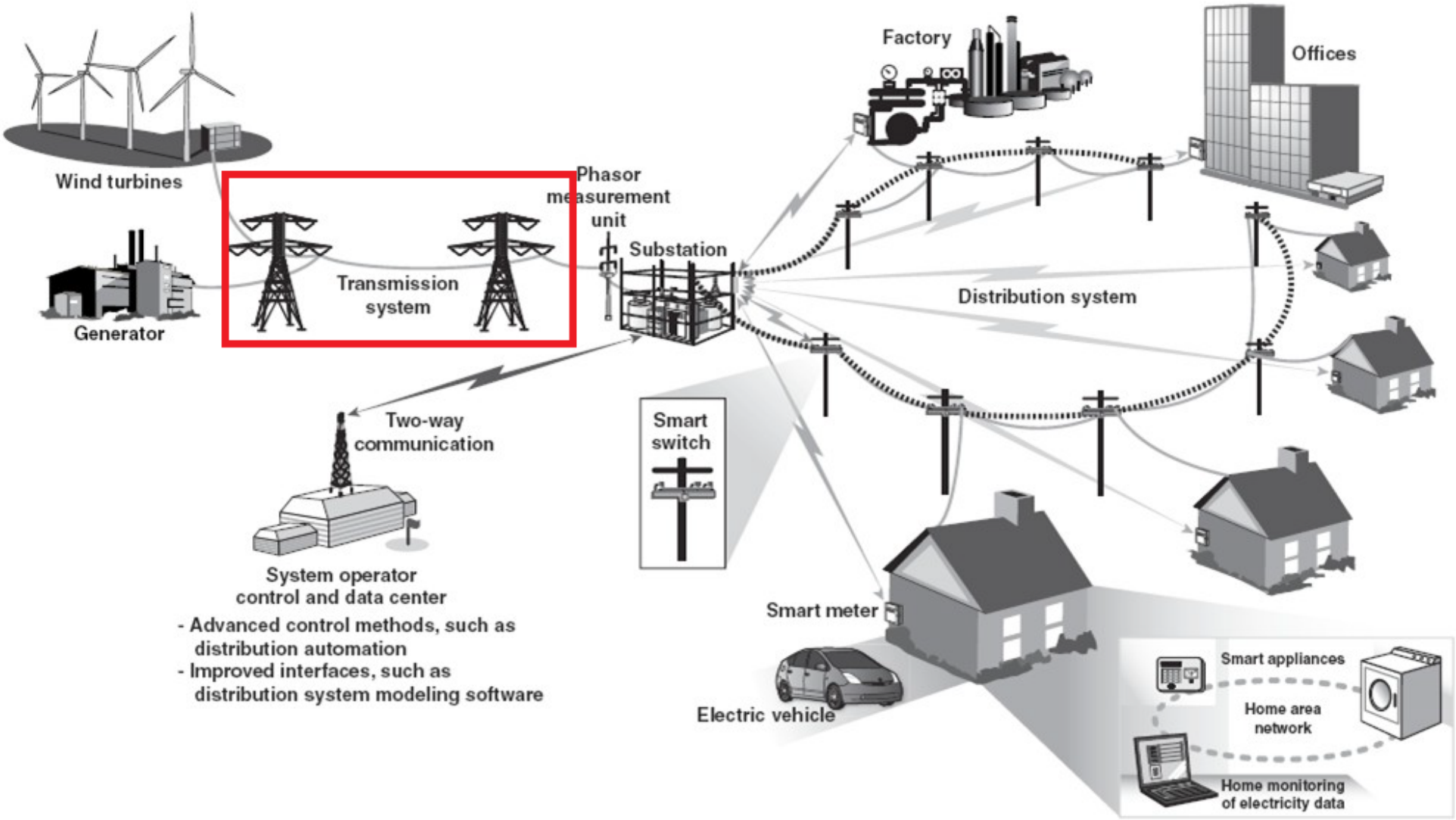
Outline

1. Introduction to smart grid and work motivation.
2. Impact of failure in the electrical grid.
3. Defense-in-depth cybersecurity architecture.
4. High-Assurance Smart Grid (HASG) control system architecture:
   - grid control architecture;
   - HASG trust model;
   - autoresponsive load as a cybersecurity countermeasure.
5. Conclusions.

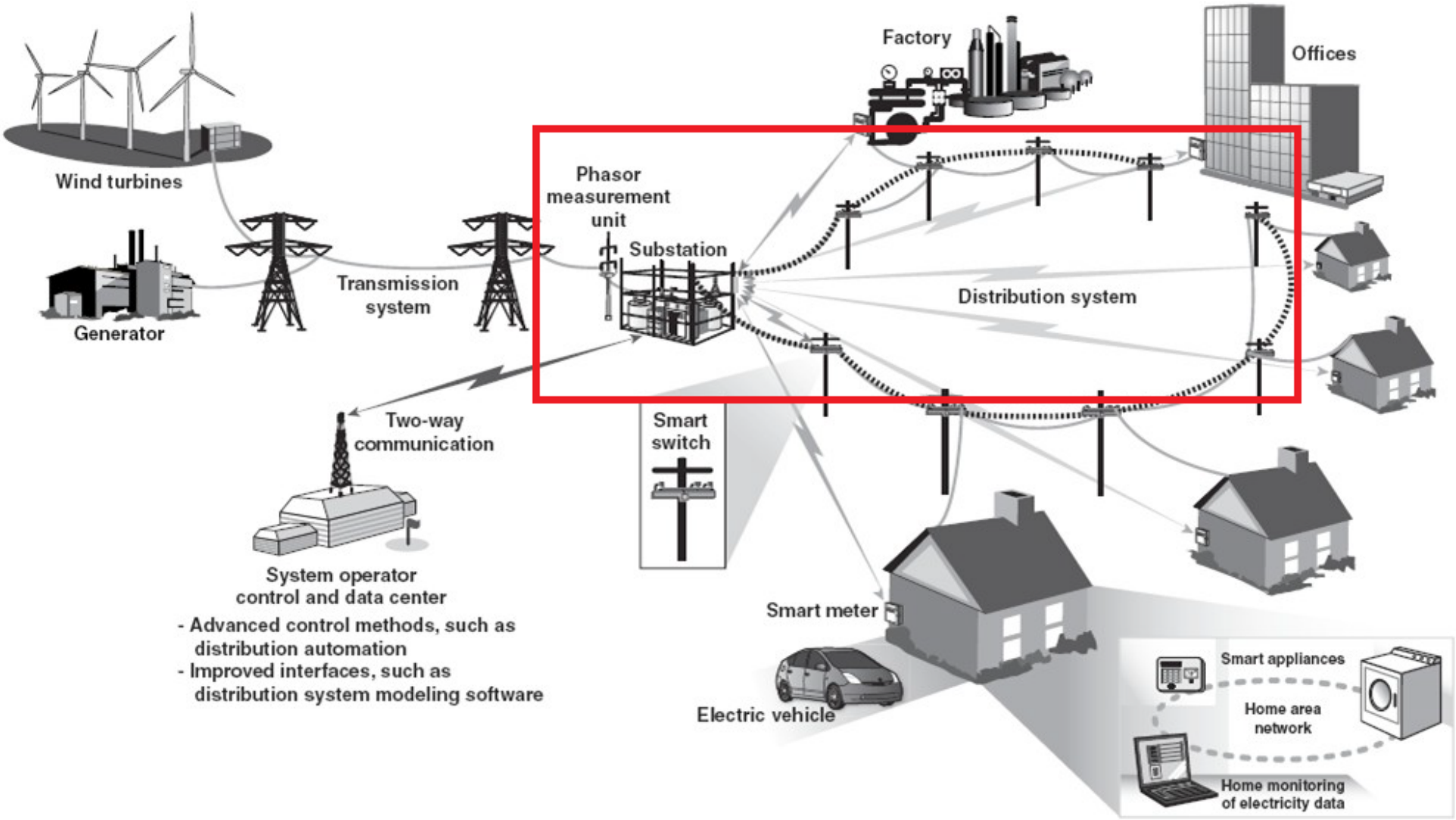
Smart grid


Wind turbines
Generator
Transmission system
Phasor measurement unit
Substation
Factory
Offices
Distribution system
Two-way communication
System operator control and data center
- Advanced control methods, such as distribution automation
- Improved interfaces, such as distribution system modeling software
Smart switch
Smart meter
Electric vehicle
Smart appliances
Home area network
Home monitoring of electricity data

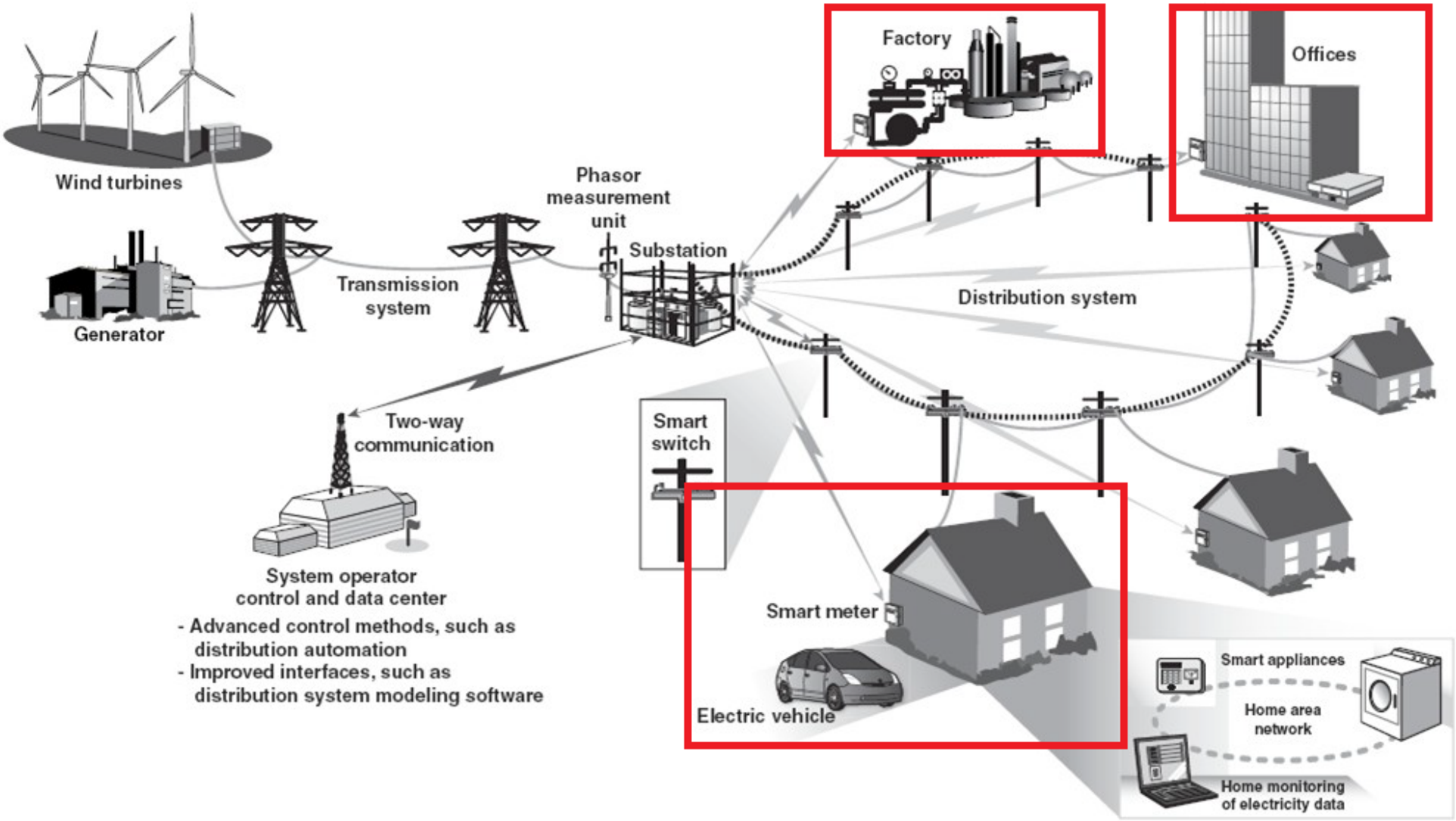
Smart grid


Wind turbines
Generator
Transmission system
Phasor measurement unit
Substation
Factory
Offices
Distribution system
Two-way communication
System operator control and data center
- Advanced control methods, such as distribution automation
- Improved interfaces, such as distribution system modeling software
Smart switch
Smart meter
Electric vehicle
Smart appliances
Home area network
Home monitoring of electricity data

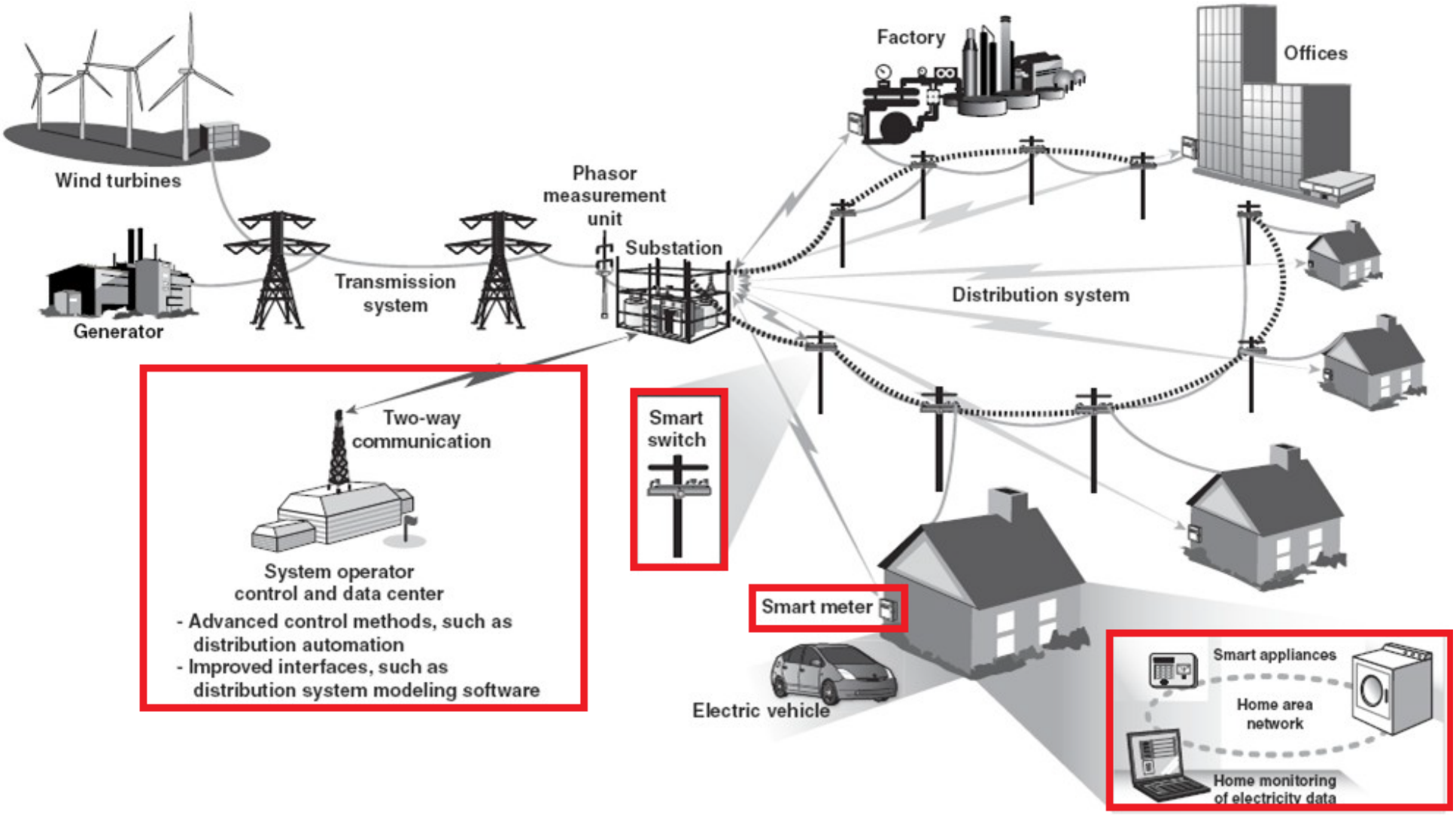
Smart grid


Wind turbines
Generator
Transmission system
Factory
Offices
Phasor measurement unit
Substation
Distribution system
Two-way communication
Smart switch
System operator control and data center
- Advanced control methods, such as distribution automation
- Improved interfaces, such as distribution system modeling software
Smart meter
Electric vehicle
Smart appliances
Home area network
Home monitoring of electricity data

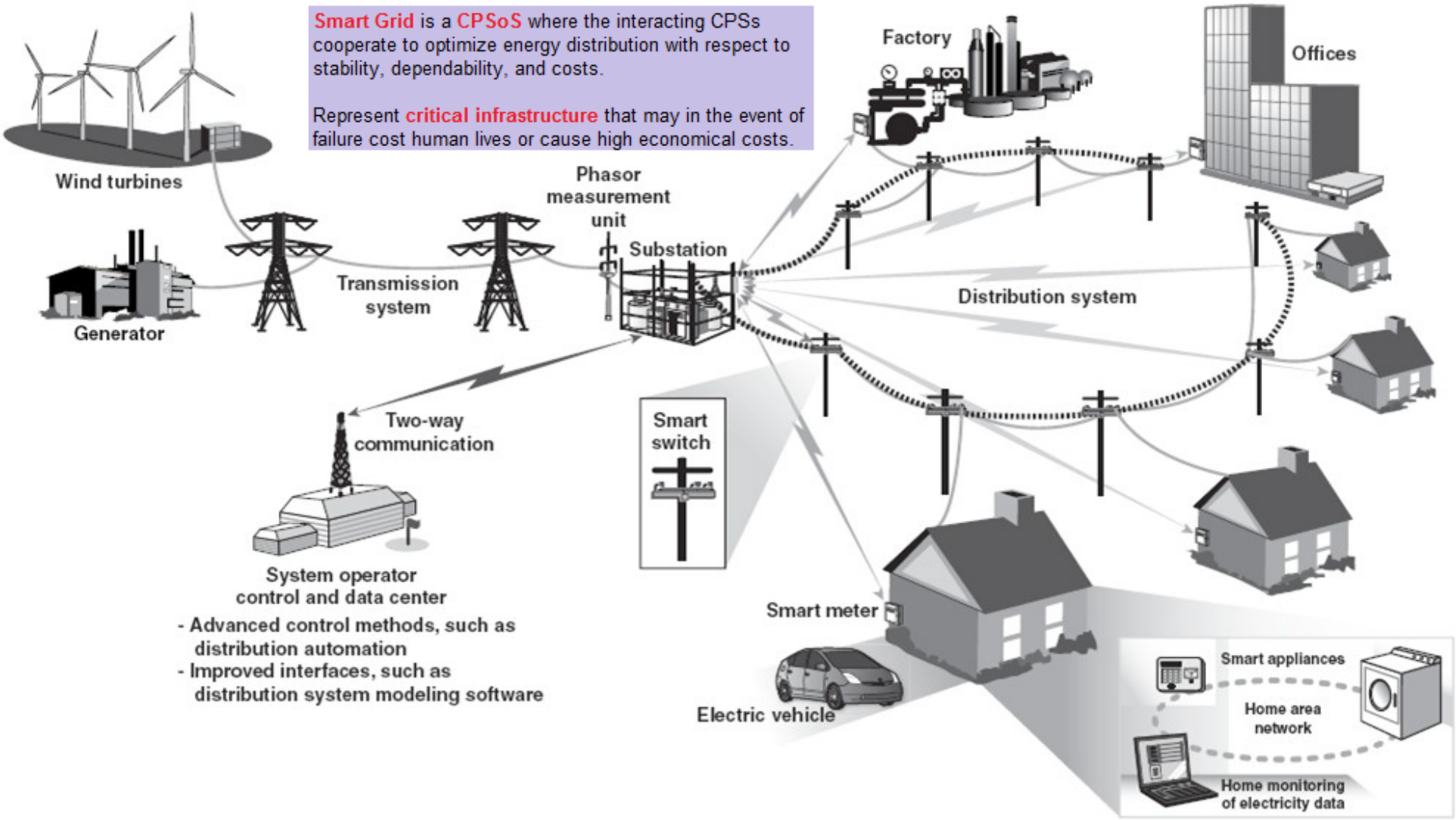
Smart grid


Wind turbines
Generator
Transmission system
Phasor measurement unit
Substation
Factory
Offices
Distribution system
Two-way communication
System operator control and data center
- Advanced control methods, such as distribution automation
- Improved interfaces, such as distribution system modeling software
Smart switch
Smart meter
Electric vehicle
Smart appliances
Home area network
Home monitoring of electricity data

Smart grid


Wind turbines
Generator
Transmission system
Phasor measurement unit
Substation
Factory
Offices
Distribution system
Two-way communication
System operator control and data center
- Advanced control methods, such as distribution automation
- Improved interfaces, such as distribution system modeling software
Smart switch
Smart meter
Electric vehicle
Smart appliances
Home area network
Home monitoring of electricity data

Smart grid


Smart Grid is a CPSoS where the interacting CPSs cooperate to optimize energy distribution with respect to stability, dependability, and costs.
Represent critical infrastructure that may in the event of failure cost human lives or cause high economical costs.
Wind turbines
Generator
Transmission system
Phasor measurement unit
Substation
Factory
Offices
Distribution system
Two-way communication
System operator control and data center
- Advanced control methods, such as distribution automation
- Improved interfaces, such as distribution system modeling software
Smart switch
Smart meter
Electric vehicle
Smart appliances
Home area network
Home monitoring of electricity data

Smart grid: pros and cons

IT technologies can make the grid smart:

- advanced information analysis (big data);
- real time monitoring (smart meters);
- automated control (self-healing, smart actuators).

IT technologies also make the grid vulnerable:

Possible attacks to:

- confidentiality (analysis of the load profile can reveal your life style);
- integrity (smart meter data can be alterd);
- availability (hackers can take control of automation system).

$\Rightarrow$ Cybersecurity controls, combination of security systems.

Smart grid: reliability challanges increased

The likelihood of unplanned outages to the control system components is increased:

- $\Leftarrow$ fragility of the new grid devices;
- $\Leftarrow$ cyberattack;
- $\Leftarrow$ inadvertent action of untrained/distracted employees;

$+$ well known grid vulnerabilities:

- unplanned line outages;
- higher than expected loads;
- loss of generation capacity;

$\Rightarrow$ rethink the underlying architecture of the grid control system:

- High-Assurance Smart Grid: reliable, available, safe, secure, and timely.

Multi-tier model for impact of failure in the electrical grid

Multi-tier model for criticality:

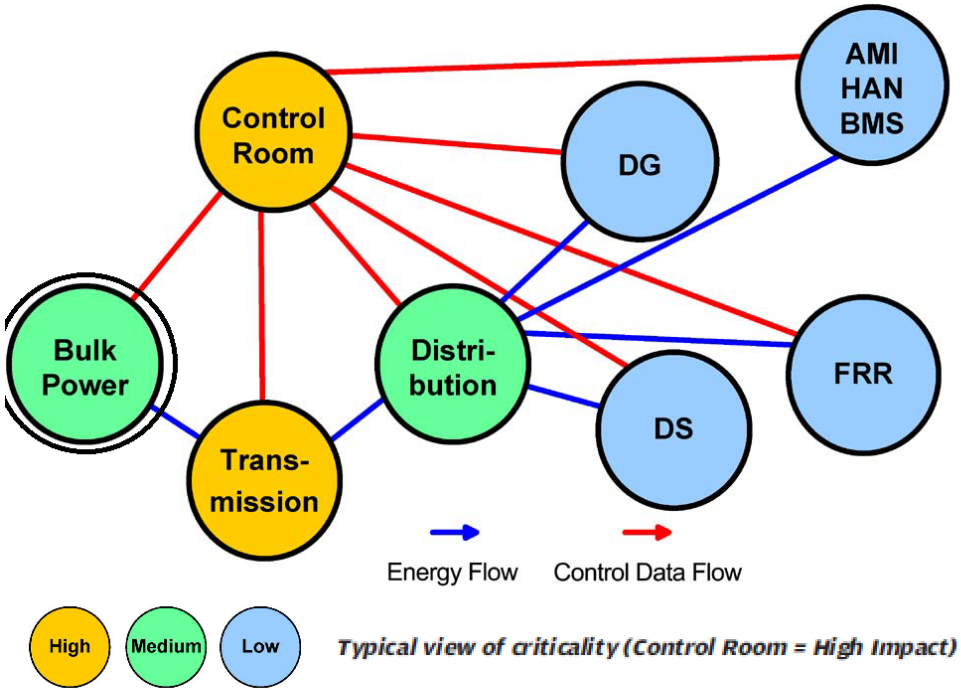
- defines three categories based on the impact of a subsystem failure (catastrophic, major, and minor impact) to the grid.

Legend for impact of failure.

Failure of these systems are likely to cause:

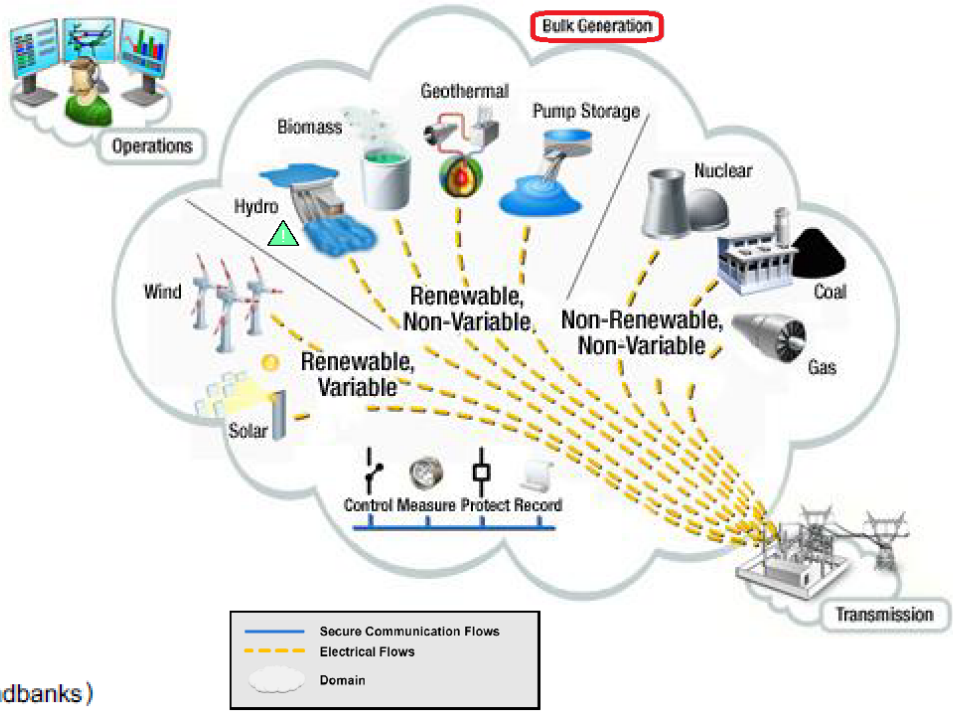
- Level A (or High): failure across tens of thousands of nodes;
- Level B (or Medium): loss of power to hundreds or thousands of nodes in a smaller geographic area;
- Level C (or Low): localized failure.

Typical criticality analysis of the power grid

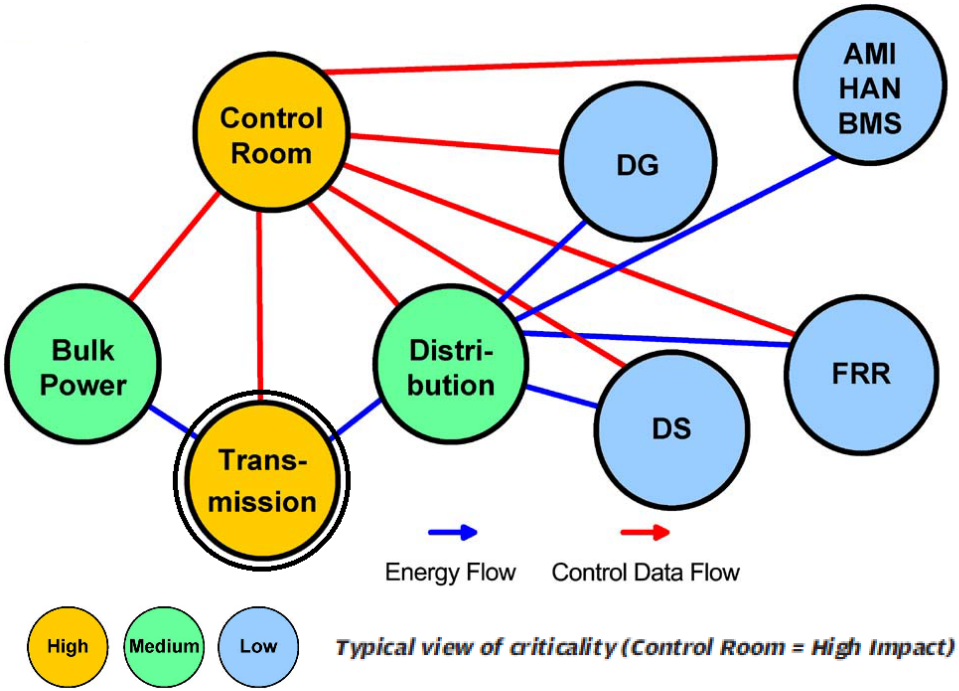


BMS = Building Management System
AMI = Advanced Metering Infrastructure
HAN = Home Area Network

DG = Distributed Generation
DS = Distributed Storage
FRR = Frequency Responsive Reserve (Loadbanks)

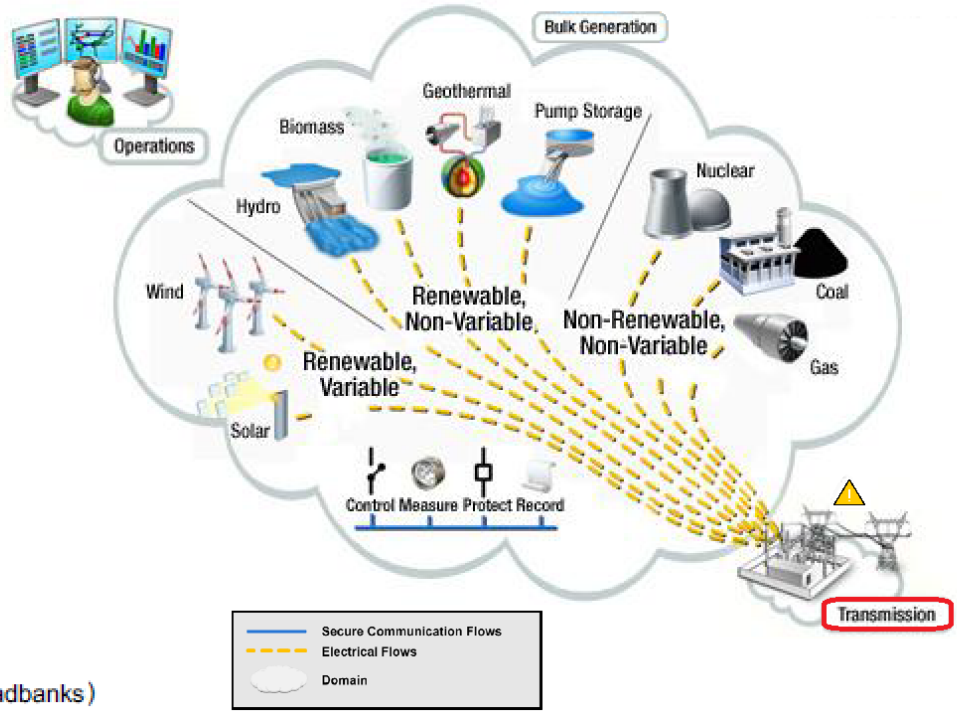


Typical criticality analysis of the power grid

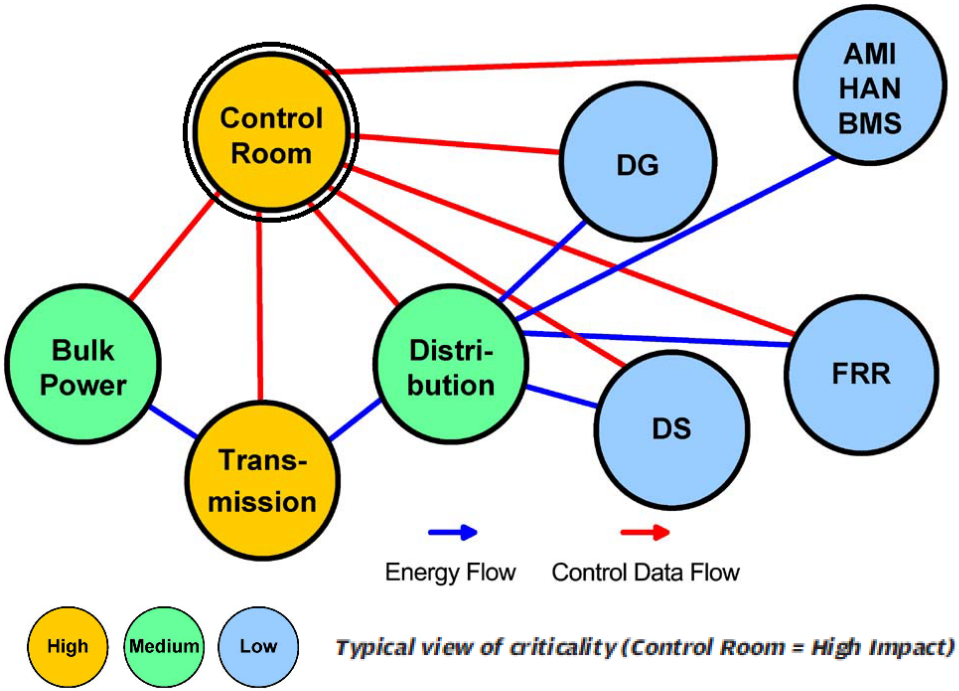


Typical view of criticality (Control Room = High Impact)

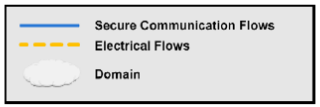
BMS = Building Management System
AMI = Advanced Metering Infrastructure
HAN = Home Area Network
DG = Distributed Generation
DS = Distributed Storage
FRR = Frequency Responsive Reserve (Loadbanks)



Typical criticality analysis of the power grid

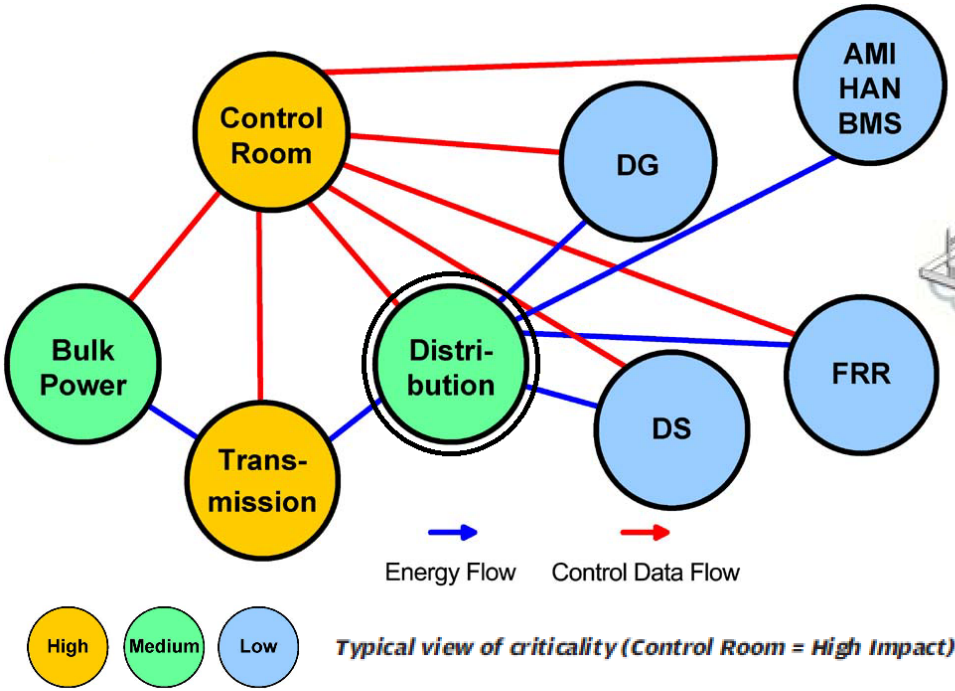


Typical view of criticality (Control Room = High Impact)

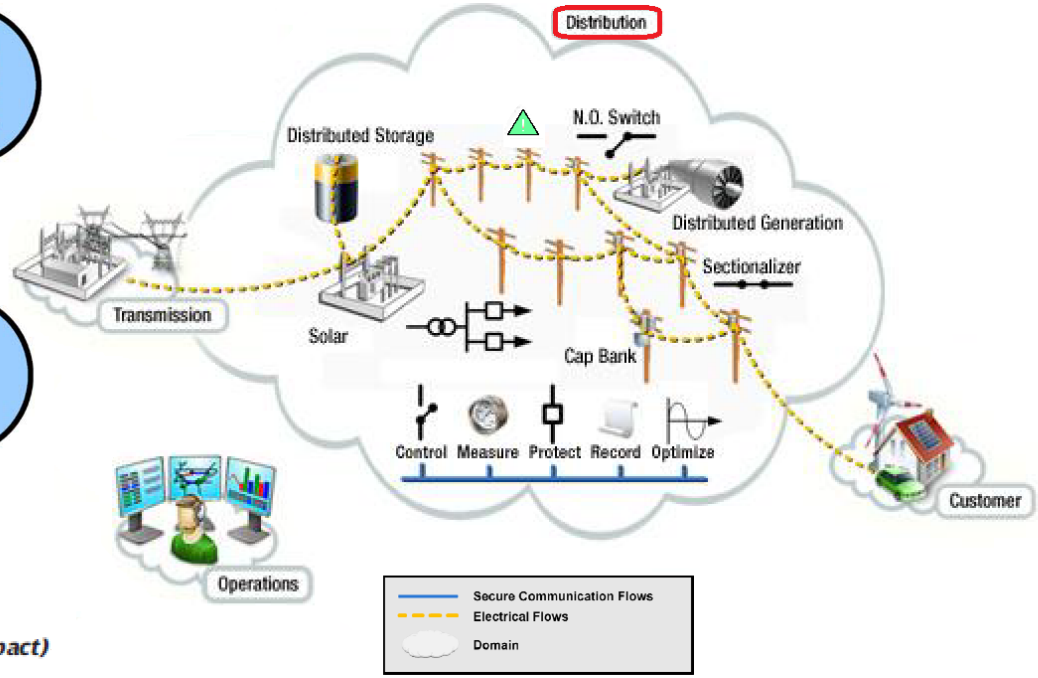


BMS = Building Management System
AMI = Advanced Metering Infrastructure
HAN = Home Area Network
DG = Distributed Generation
DS = Distributed Storage
FRR = Frequency Responsive Reserve (Loadbanks)

Typical criticality analysis of the power grid



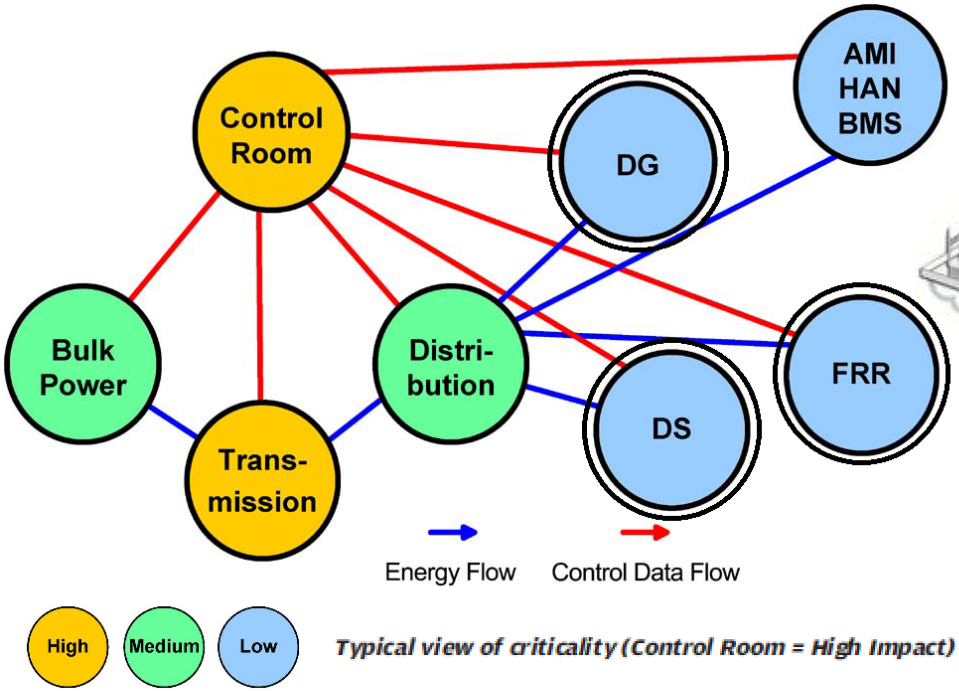
Typical view of criticality (Control Room = High Impact)

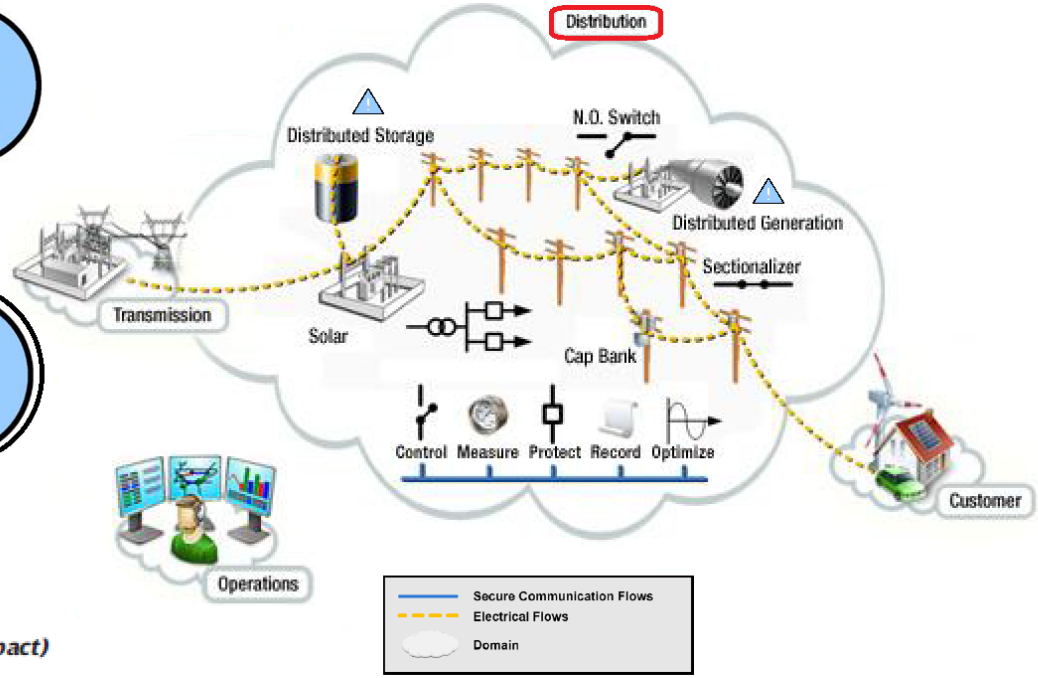


BMS = Building Management System
AMI = Advanced Metering Infrastructure
HAN = Home Area Network

DG = Distributed Generation
DS = Distributed Storage
FRR = Frequency Responsive Reserve (Loadbanks)

Typical criticality analysis of the power grid

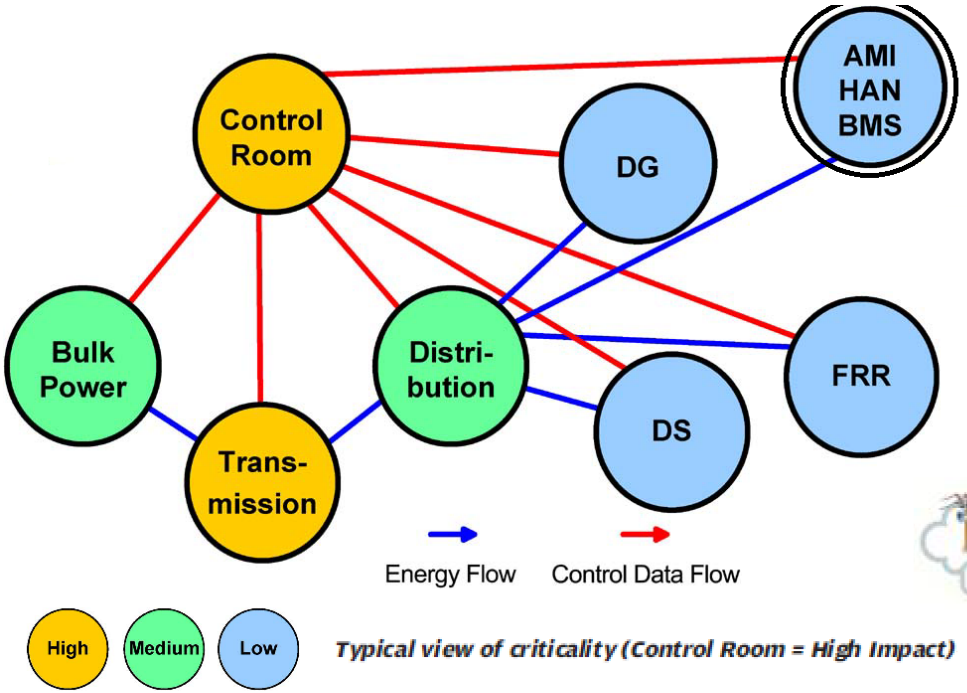


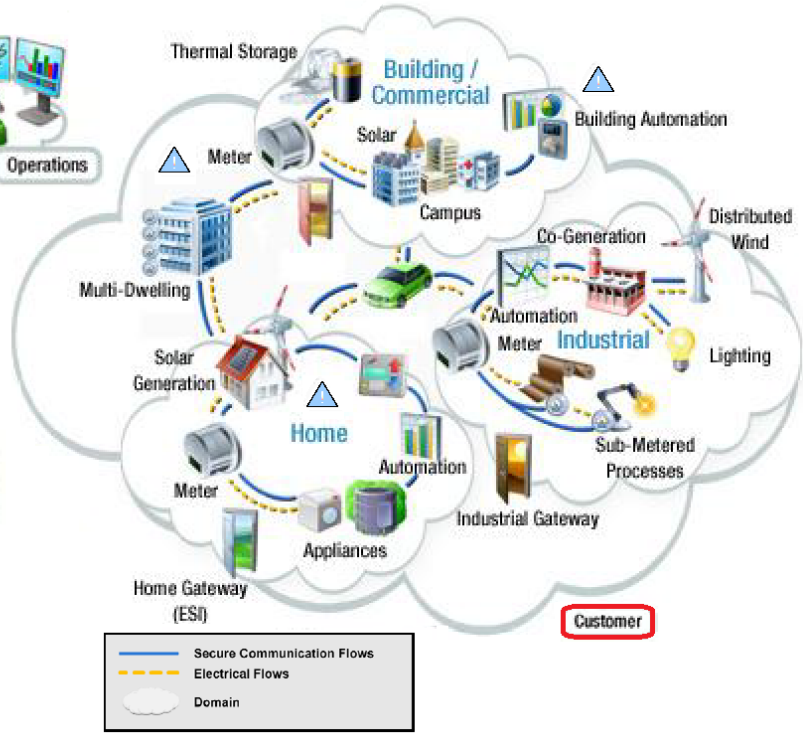


BMS = Building Management System
AMI = Advanced Metering Infrastructure
HAN = Home Area Network

DG = Distributed Generation
DS = Distributed Storage
FRR = Frequency Responsive Reserve (Loadbanks)

Typical criticality analysis of the power grid

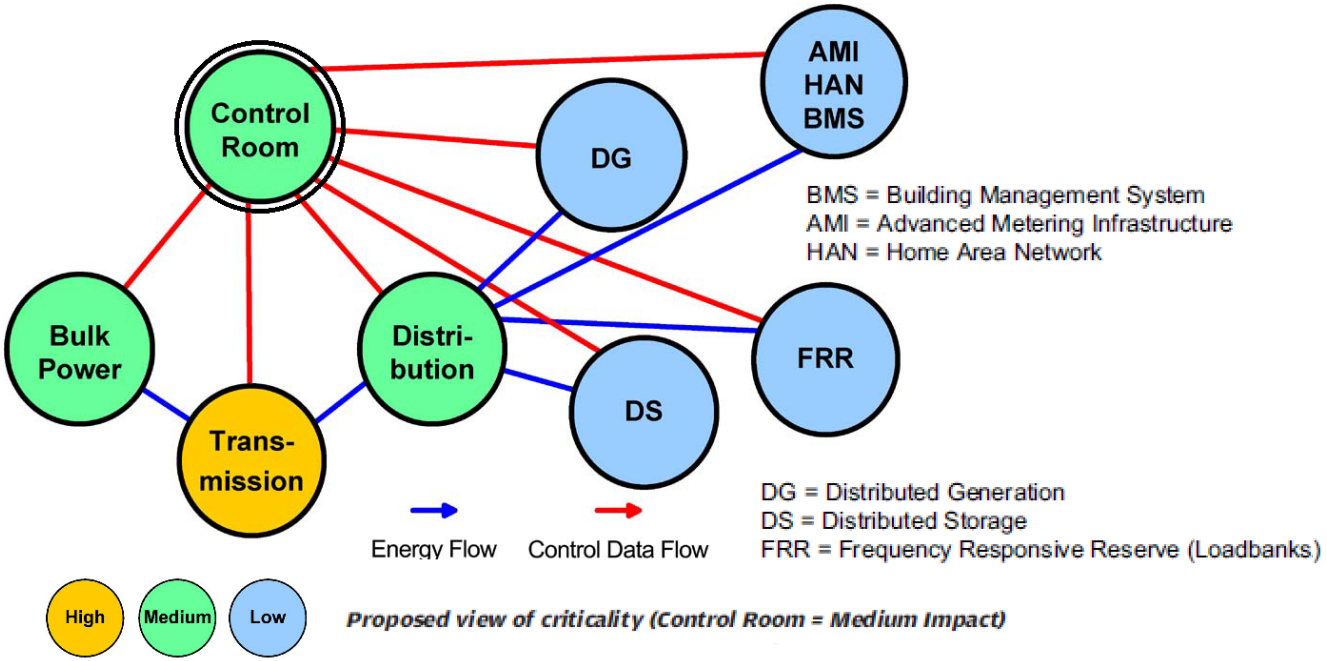




BMS = Building Management System
AMI = Advanced Metering Infrastructure
HAN = Home Area Network

DG = Distributed Generation
DS = Distributed Storage
FRR = Frequency Responsive Reserve (Loadbanks

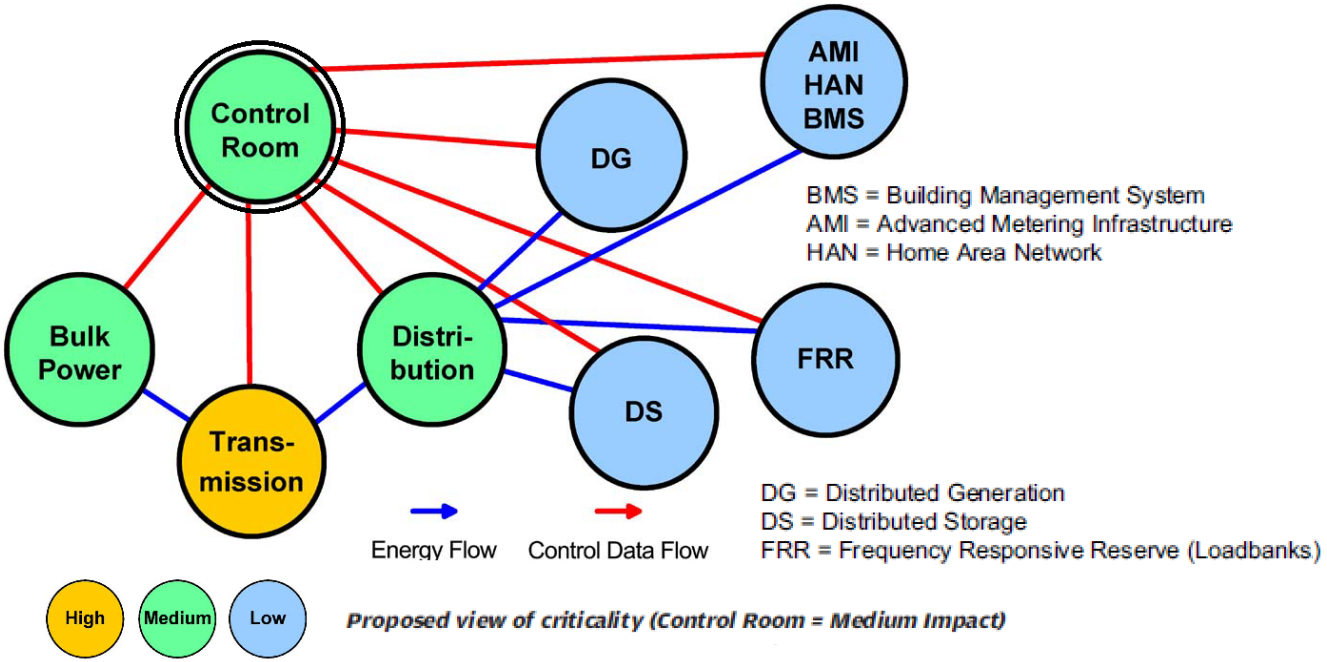
Proposed criticality anlysis of the power grid



Control room criticality level decreased:

- grid operators use tools to determine what-if scenario responses;
- results of the what-if analysis preloaded onto distributed sensors, actuators, and controllers.

Proposed criticality anlysis of the power grid



Ideal condition:

- substation and field devices do their own what-if analysis based on direct communications with a number of adjacent sensors.

Defense-in-depth cybersecurity architecture

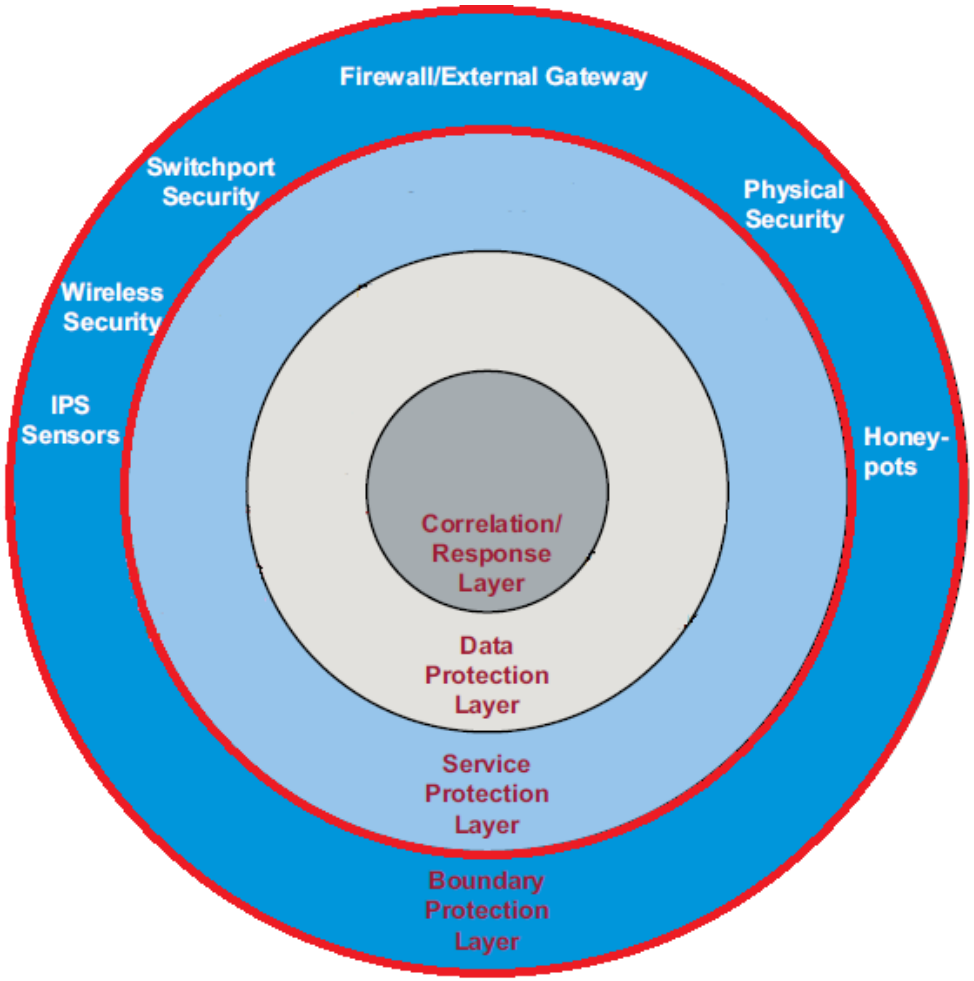
- Layered security controls to protect critical elements in electrical utility control networks.

Defense-in-depth principle:

- is more than a ploy to "keep out" threats;
- it assumes the threat may already exist within the environment, whether through malicious intent or the mistaken actions of untrained or distracted personnel.

Defense-in-depth cybersecurity architecture

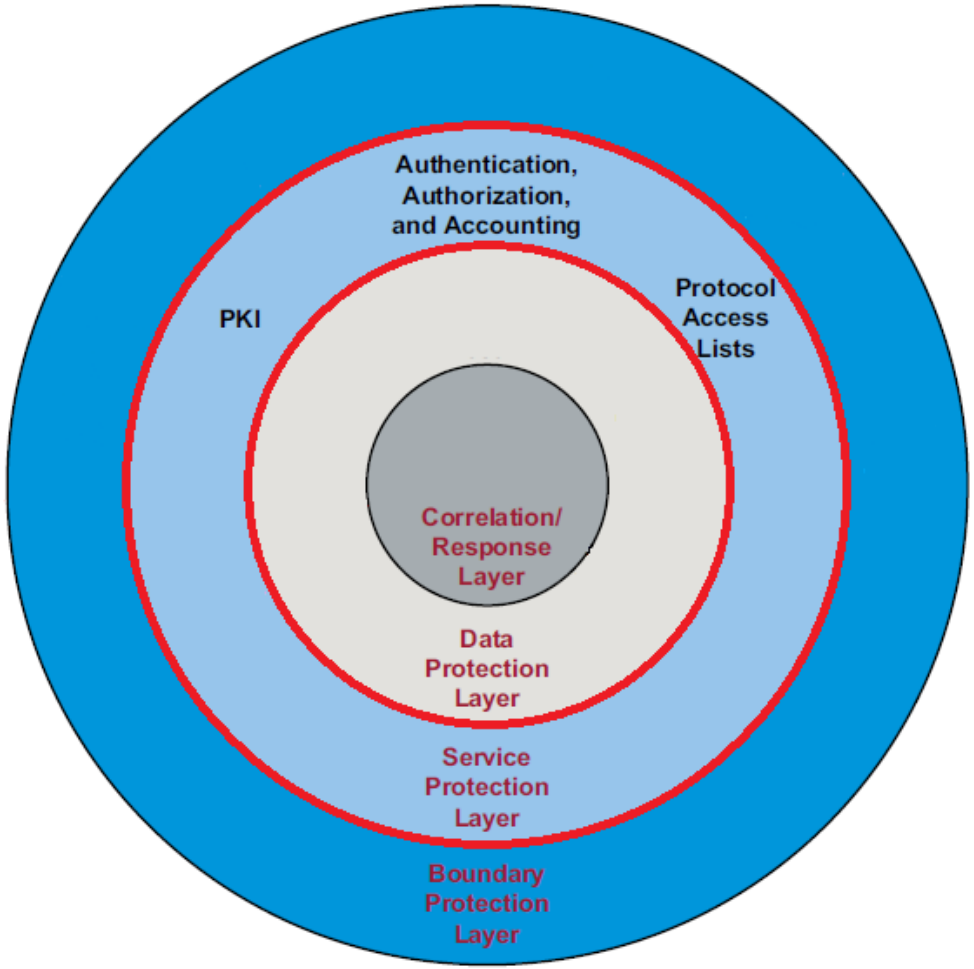
- Boundary protection layer: contains controls for the cyber and physical perimeter of the control center



Utility control center defense in depth model

Defense-in-depth cybersecurity architecture

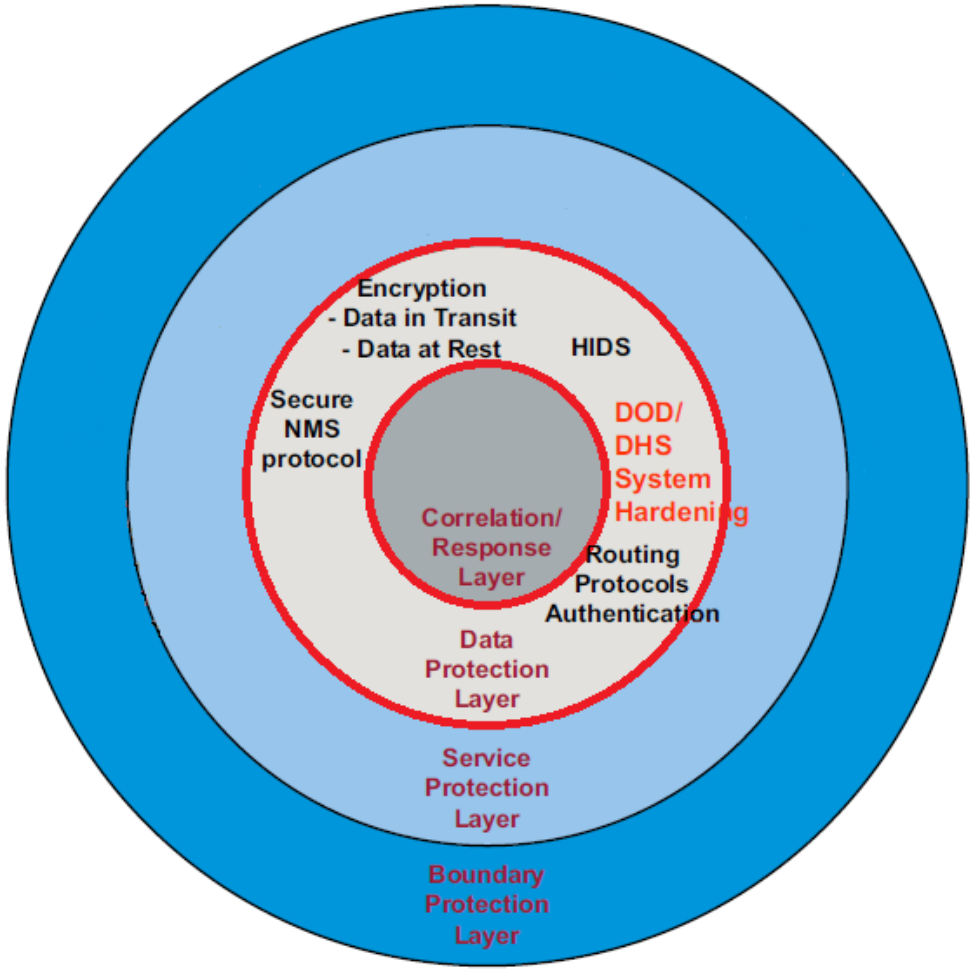
- Service protection layer: contains controls for access to services and applications for users inside of the HASG cyber/physical perimeter.



Utility control center defense in depth model

Defense-in-depth cybersecurity architecture

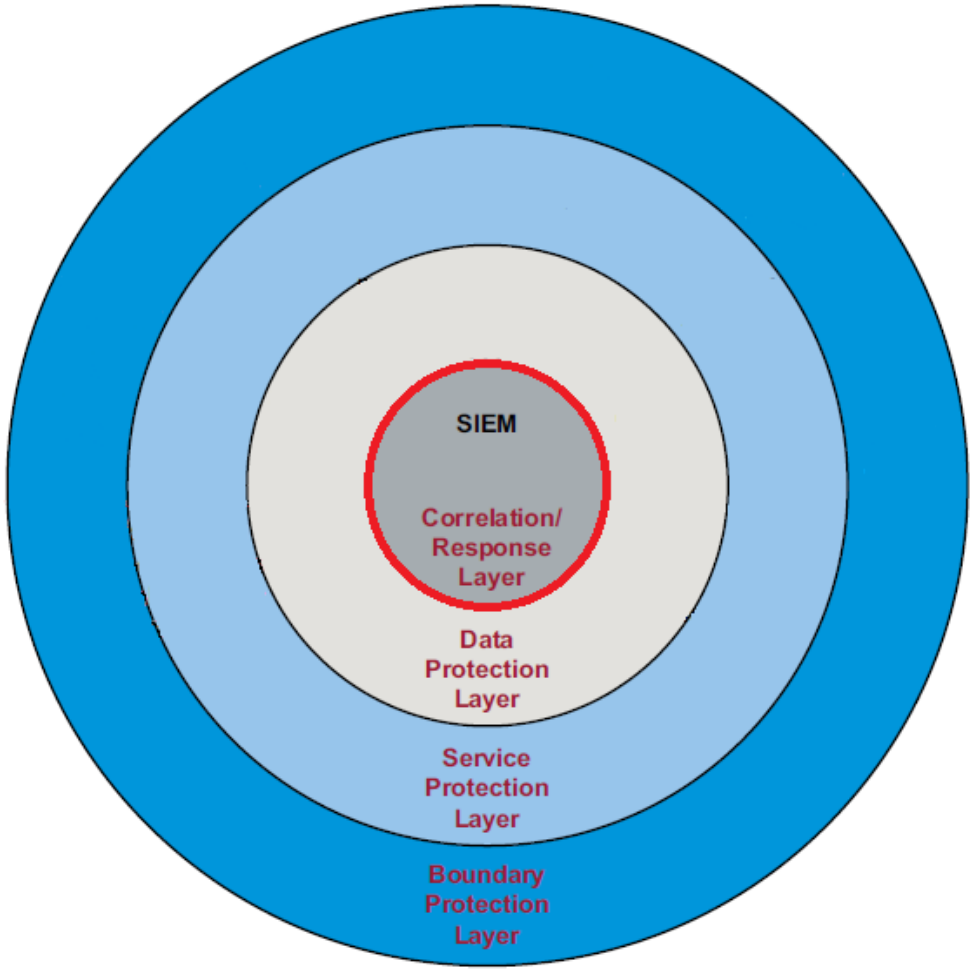
- Data protection layer: contains controls to protect data within the HASG perimeter.



Utility control center defense in depth model

Defense-in-depth cybersecurity architecture

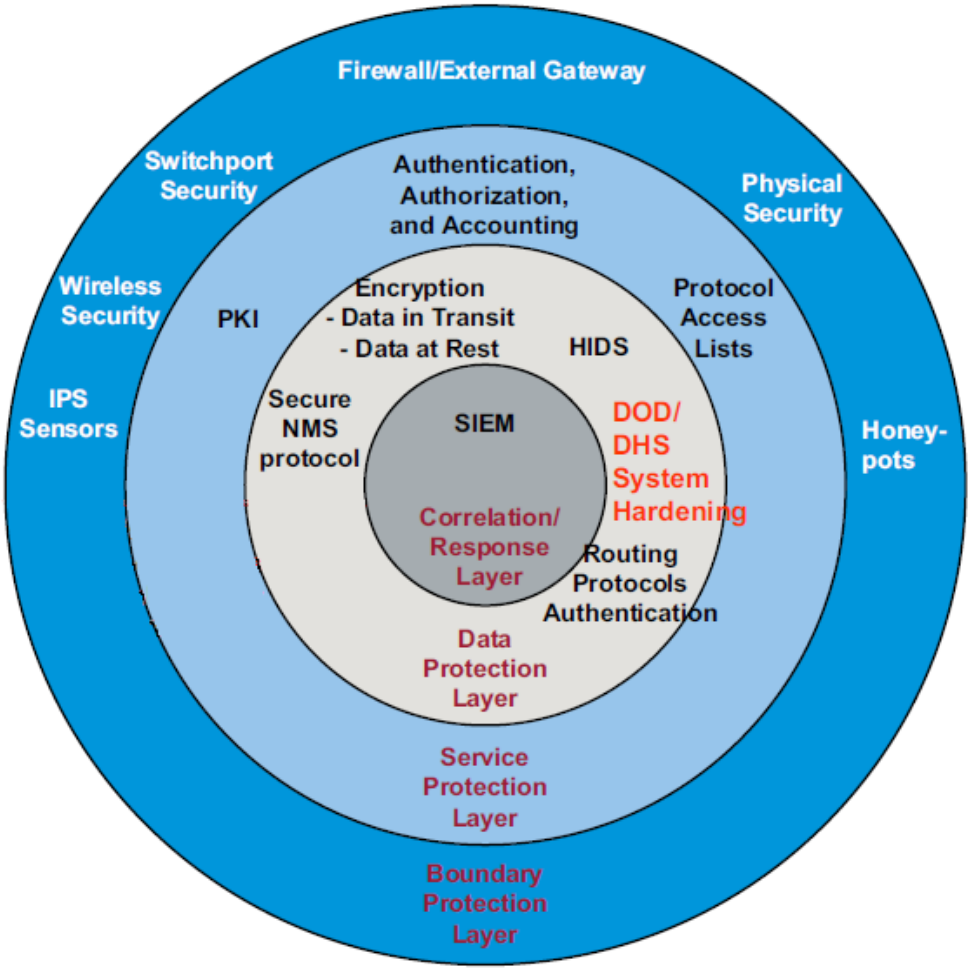
- Correlation/response layer: contains controls to perform correlation of event and response to security incidents.



Utility control center defense in depth model

Defense-in-depth cybersecurity architecture

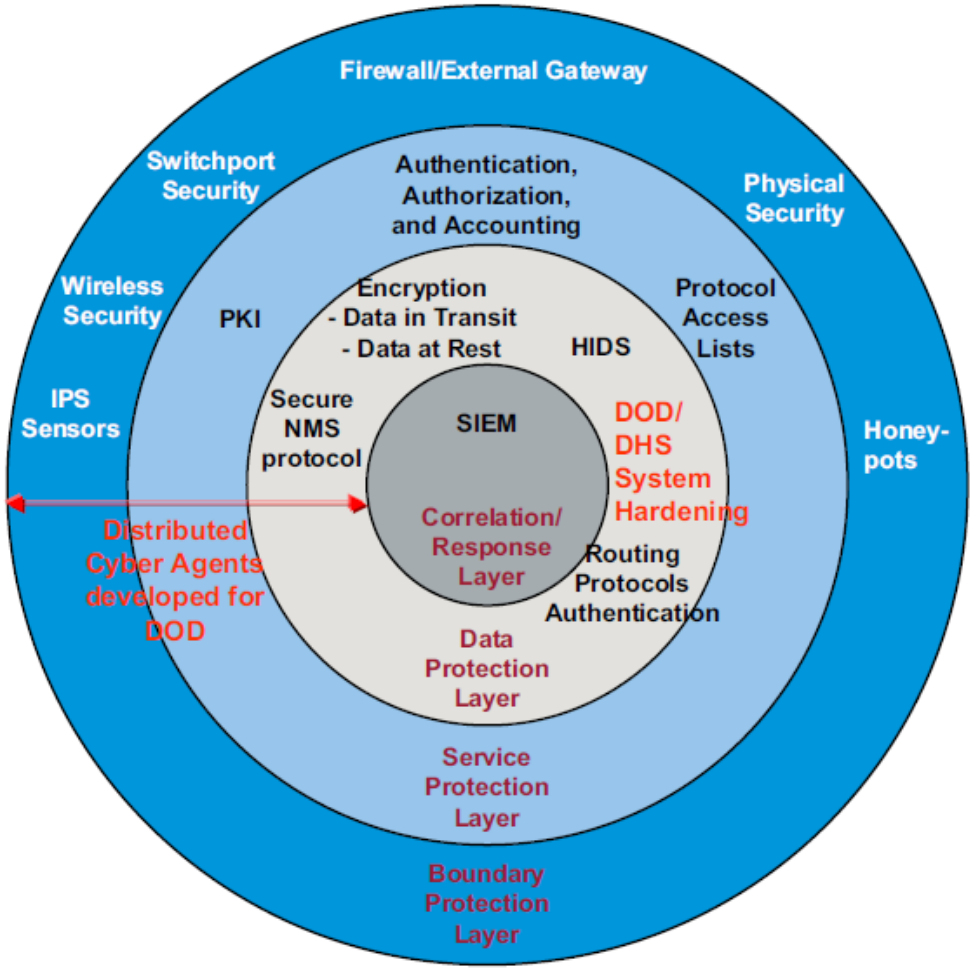
- Layered security controls to protect critical elements in electrical utility control networks.



Utility control center defense in depth model

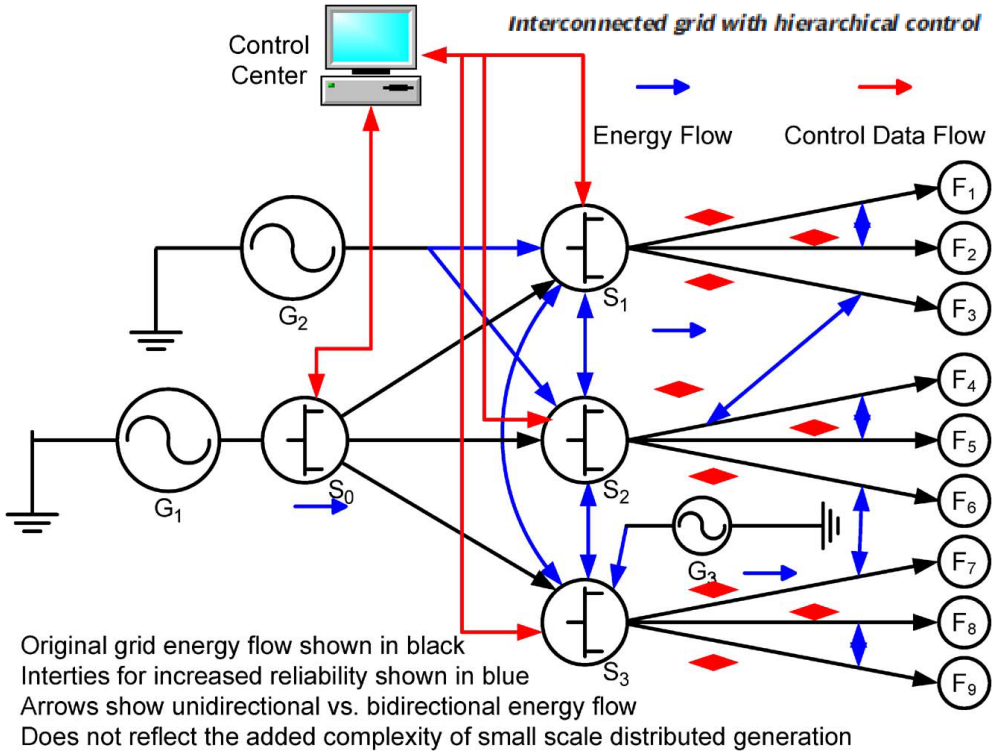
Defense-in-depth cybersecurity architecture

- Distributed cyberagents performing intrusion detection, log scanning, and event correlation.



Utility control center defense in depth model

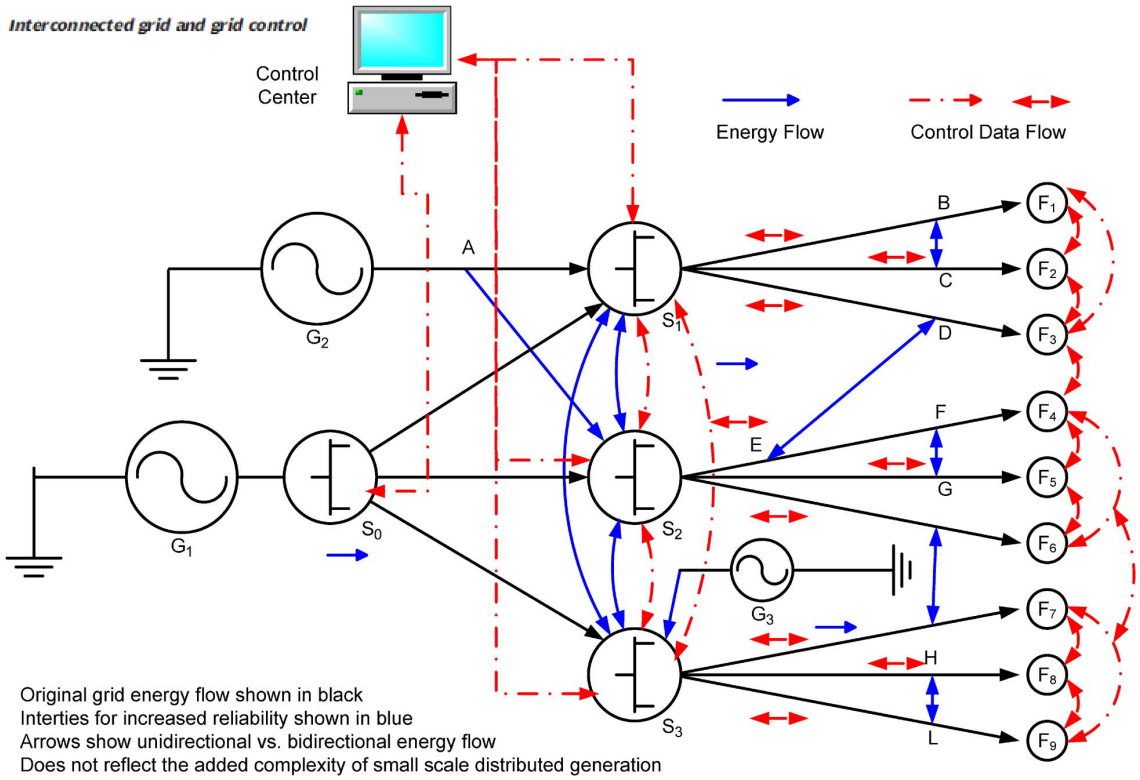
Grid control architecture: hierarchical control data flow



Field device and substation:

- automatic modes: local sensors state $\Rightarrow$ binary decisions;
  e.g (circuit breakers, automatic reclosers);
- for complex decisions rely on commands from control rooms.

Grid control architecture: distributed control data flow

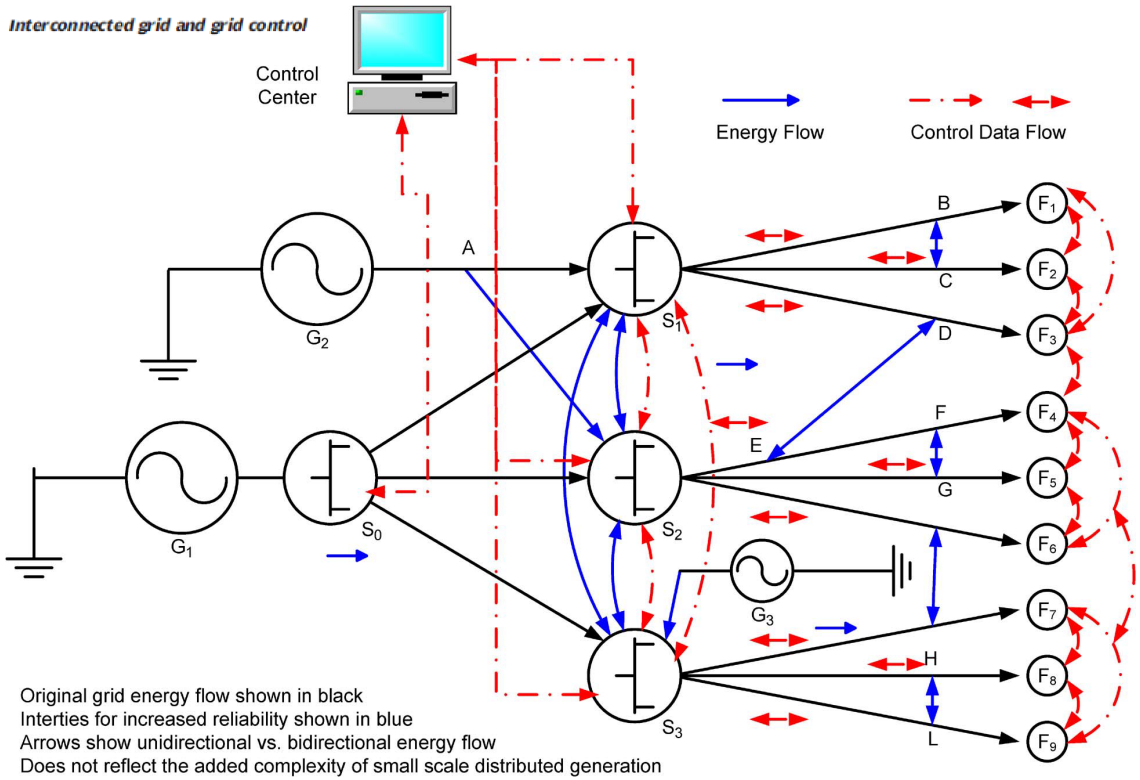


Distributed control signaling between intelligent electronic devices:

- field device sense peer devices;
- substations can collaborate.

$\Rightarrow$ losses of control capability from control system $\not\Rightarrow$ losses of communication and device collaboration.

Grid control architecture: distributed control data flow



Distributed grid sensors and actuators:

- with more autonomous capability;
- or preloaded with next-step instructions in case of (electric/control) system failures.

$\Rightarrow$ toward a self-healing grid.

Cybersecurity in the distributed grid control architecture

- *"Focusing cybersecurity efforts just on preventing external attack is not sufficient"*.

Loss of reliable control capability:

- $\Leftarrow$ communications link failure;
- $\Leftarrow$ sensor/controller/actuator failure;
- $\Leftarrow$ control center system failure;
- $\Leftarrow$ improper commands from control room;

caused by: hw/sw failures and/or malicious activity (employees / external attackers).

Distributed grid control $\Rightarrow$ limited damage from loss of reliable control capability;

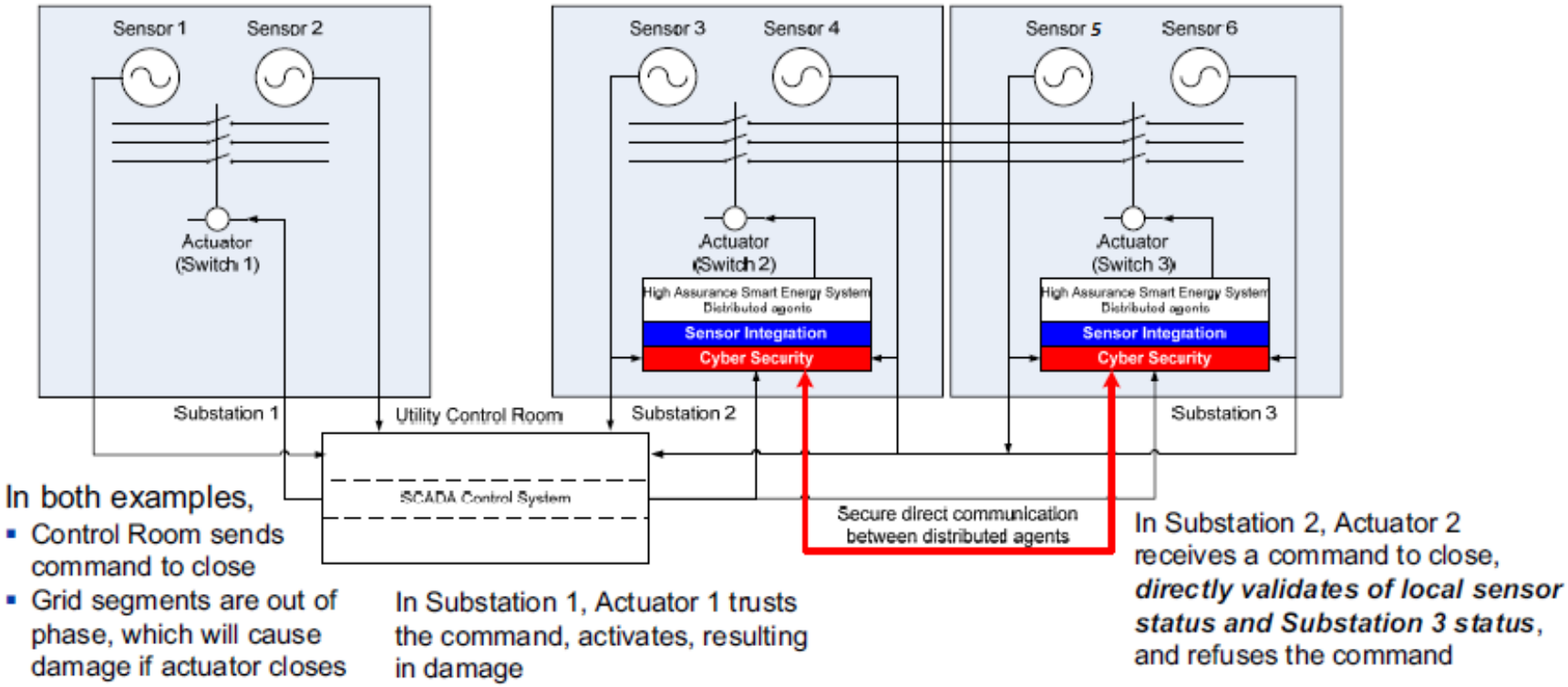
$\Rightarrow$ more resilient and reliable against attack by malicious actors.

High-Assurance Smart Grid (HASG) trust model

- *"Systems should be designed with the expectation that adjacent systems will be compromised (whether through system failure, user error, or malicious activity)."*
  - $\Rightarrow$ control room/substation/field devices must sense when to trust received sensor and command inputs.
- Intrusion prevention systems (IPSs) and intrusion detection systems (IDSs):
  - often ineffective at preventing intrusions;
  - fails to account for insider threats (malicious/untrained/distracted).

$\Rightarrow$ make the grid an Intrusion-tolerant systems (ITSs).

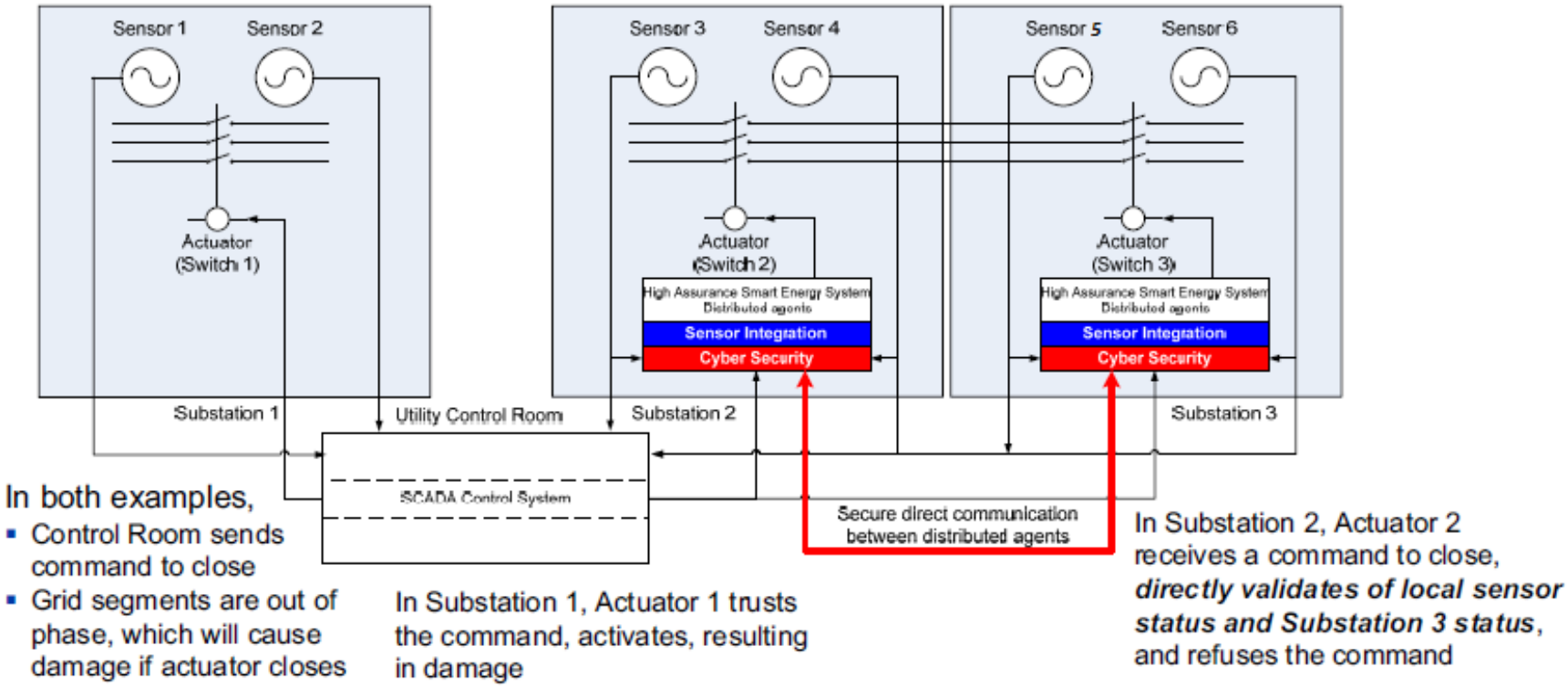
HASG intrusion tolerace example



Distributed intelligence for remote devices:

1. synthesize information from distributed sensors and control room;
2. do what-if analysis $\Rightarrow$ determine impact of received commands;
3. determine if trust them (validate integrity and reasonableness).

HASG intrusion tolerace example



Distributed intelligence for remote devices:

1. synthesize information from distributed sensors and control room;
2. do what-if analysis $\Rightarrow$ determine impact of received commands;
3. determine if trust them (validate integrity and reasonableness).

Risk/benefit analysis of Two-Way Communication and Control (2W-C2) for Demand-Response (DR)

Home-Area-Network:

- 2W-C2 from the Utility to individual consumer-owned appliances;
- to obtain DR functions: enable operating utilities to reduce loads in response to grid overload conditions or price.

2W-C2 benefits:

- more refined consumer information $\Rightarrow$ better power planning;
- better load control available to utilities.

2W-C2 risks (cybersecurity concerns):

- insecure communications path from the consumer into the Utility control room $\Rightarrow$ false load control ack to a Utility (realize cost benefits while not actually reducing the load).

Risk/benefit analysis of Two-Way Communication and Control (2W-C2) for Demand-Response (DR)

2W-C2 risks (cybersecurity concerns):

- insecure communications path from the consumer into the Utility control room $\Rightarrow$ false load control ack to a Utility (realize cost benefits while not actually reducing the load).

Solution:

- two-way communications between a distribution utility and its home meters;
- one-way communications from a meter to consumer-owned devices;
  $\Rightarrow$ reduces the attack surface.

Autoresponsive load as a cybersecurity countermeasure

Alternative/complimentary approach to explicit utility control over consumer appliances:

Autoresponsive load:

appliances can be given the ability to directly sense and respond to grid instability;

- under-frequency conditions ($< 59.95\ Hz$): devices programmed to automatically reducing load (load shedding);
- frequency exceeding a limit ($> 60.05\ Hz$): loads automatically serve as distributed load banks (load increases);
- could also based on voltage sensing.

Conclusions: paper achievements

Integrated Energy Management, Cyber Security and Physical Security with Defense in Depth to achieve an High-Assurance Smart Grid architecture that:

1. categorizes cybersecurity requirements based on a multi-tier determination of a subsystem's potential impact on the overall system;
2. implements a robust defense-in-depth cybersecurity architecture;
3. implements a distributed control system architecture based on an assumed compromise (untrusted condition) of system control components and subsystems using autoresponsive load control wherever possible to achieve demand-response without the vulnerabilities inherent in all command and control systems.

Conclusions: areas for further research

- Autonomous robotics and multi-agent coordination: provide examples for how grid devices can work with limited individual capability and yet manage, together, more complex operations than any individual device could do on its own.
- Intrusion-tolerant systems in the electrical or other control systems environments.
- Evolution of grid controls and grid security: methods of increasing the inherent security capabilities of many installed grid devices should be explored.
- AR load control.

Bibliography

- Thomas M. Overman, Ronald W. Sackman, Terry L. Davis, Brad S. Cohen, "High-Assurance Smart Grid: A Three-Part Model for Smart Grid Control Systems", *Proceedings of the IEEE, Vol. 99, No. 6*, 2011.
- Thomas M. Overman, Ronald W. Sackman, "High assurance smart grid: Smart grid control systems communications architecture", *Smart Grid Communications (SmartGridComm), First IEEE International Conference*, 2010.

Grazie per l'attenzione.

Smart grid glossary

- Electrical grid: is an interconnected network for delivering electricity from suppliers to consumers. It consists of generating stations that produce electrical power, high-voltage transmission lines that carry power from distant sources to demand centers, and distribution lines that connect individual customers.
- Substation: is a part of an electrical generation, transmission, and distribution system. Substations transform voltage from high to low, or the reverse, or perform any of several other important functions. Between the generating station and consumer, electric power may flow through several substations at different voltage levels. A substation may include transformers to change voltage levels between high transmission voltages and lower distribution voltages, or at the interconnection of two different transmission voltages. Substations may be owned and operated by an electrical utility, or may be owned by a large industrial or commercial customer. Generally substations are unattended, relying on SCADA for remote supervision and control.

Smart grid glossary

- Electrical load: is an electrical component or portion of a circuit that consumes electric power. This is opposed to a power source, such as a battery or generator, which produces power.In electric power circuits examples of loads are appliances and lights. The term may also refer to the power consumed by a circuit.
- Field device: controls local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.
- Intelligent electronic device (IED): is a term used in the electric power industry to describe microprocessor-based controllers of power system equipment, such as circuit breakers, transformers and capacitor banks.

Smart grid glossary

- Circuit breaker: is an automatically operated electrical switch designed to protect an electrical circuit from damage caused by overcurrent or overload or short circuit. Its basic function is to interrupt current flow after protective relays detect a fault.
- Demand-response: mechanisms to manage domestic and industrial consumption of electricity in response to supply conditions, for example, having electricity customers reduce their consumption at critical times or in response to prices. Requests for energy coming from electronic appliances are forwarded towards the subsystems in charge of granting or denying each request while achieving the Smart Grid goal, i.e., keeping the production and consumption rates for connected households balanced.

Smart grid glossary

- Load control switch: A load control switch is a remotely controlled relay that is placed on home appliances which consume large amounts of electricity, such as air conditioner units and electric water heaters. Consist of a communication module and the relay switch and can be used as part of a demand response energy efficiency system such as a smart grid. Receiving signals from the power company or electrical frequency shift to turn off or reduce power to the appliance during times of peak electrical demand. Most load control switches have only one-way communication, receiving signals from the power company. Some are now two-way, which helps the power company locate faulty load control switches. In a dynamic demand mode the switches are stand alone at the appliance and turn off independently by monitoring the grid without receiving signals. Can be a powerful tool to prevent black-outs when electricity storage, transmission, or generation resources are insufficient. It allows the electric companies to respond to emergencies without shutting off all power to customers.

Smart grid glossary

- Dynamic demand: is the name of a semi-passive technology for adjusting load demands on an electrical power grid. The concept is that by monitoring the frequency of the power grid, as well as their own controls, intermittent domestic and industrial loads switch themselves on/off at optimal moments to balance the overall grid load with generation, reducing critical power mismatches. As this switching would only advance or delay the appliance operating cycle by a few seconds, it would be unnoticeable to the end user. This is the foundation of dynamic demand control. Dynamic demand devices passively shut off when stress in the grid is sensed, whereas demand response mechanisms respond to transmitted requests to shut off.

Smart grid glossary

- Smart meter is an electronic device that records consumption of electric energy in intervals of an hour or less and communicates that information at least daily back to the utility for monitoring and billing. Smart meters enable two-way communication between the meter and the central system. Smart meters can gather data for remote reporting. Such an advanced metering infrastructure (AMI) differs from traditional automatic meter reading (AMR) in that it enables two-way communications with the meter.

Smart grid glossary

- Advanced metering infrastructure (AMI): is an integrated system of smart meters, communications networks, and data management systems that enables two-way communication between utilities and customers. The goal of an AMI is to provides utility companies with real-time data about power consumption and allow customers to make informed choices about energy usage based on the price at the time of use.
- Building management system (BMS): is a computer-based control system installed in buildings that controls and monitors the building's mechanical and electrical equipment such as ventilation, lighting, power systems, fire systems, and security systems.

Cyber security glossary

- Demilitarized zone (DMZ): is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a usually larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled. Any service that is being provided to users on the external network can be placed in the DMZ. The most common of these services are: Web servers, Mail servers, FTP servers and VoIP servers.

Cyber security glossary

- Honeypot: is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, which are then blocked.
- Switchport security: offers the ability to configure a switchport so that traffic can be limited to only a specific configured MAC address or list of MAC addresses.
- Key management: is the management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.

Cyber security glossary

- Routing protocol authentication: Authentication of routers for a given routing protocol. One of the ways that a network can be exploited is by an attacker gaining access to a directly connected network line and directly influencing the route traffic takes to reach a destination. For example, a route for traffic could be changed to route through a device that is able to capture the traffic and resend it leaving few footprints of attack. One of the methods that can be used to prevent these types of attack is the use of routing protocol authentication. The integrity of routing information inside a network is of the utmost importance as it can influence how traffic reaches specific destinations. Configuring the use of routing protocol authentication is an easy option that ensures that the device on the other side of a connection is who they say they are.

Cyber security glossary

- Simple network management protocol (SNMP): is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more. SNMPv3, feature improvements in performance, flexibility and security.
- Hardening: hardening is usually the process of securing a system by reducing its surface of vulnerability. Reducing available ways of attack typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, and the disabling or removal of unnecessary services.
- Host-based intrusion detection system (HIDS): is an intrusion detection system that monitors and analyzes the internals of a computing system as well as (in some cases) the network packets on its network interface.

Cyber security glossary

- Access-list: is a record that identifies and manages traffic. IP ACLs are the most popular type of access lists because IP is the most common type of traffic. There are two types of IP ACLs: standard and extended. Standard IP ACLs can only control traffic based on the source IP address. Extended IP ACLs are far more powerful; they can identify traffic based on source IP, source port, destination IP, and destination port. You can use ACLs to filter traffic according to the "three P's"—per protocol, per interface, and per direction. You can only have one ACL per protocol (e.g., IP or IPX), one ACL per interface (e.g., FastEthernet0/0), and one ACL per direction (i.e., IN or OUT).

Cyber security glossary

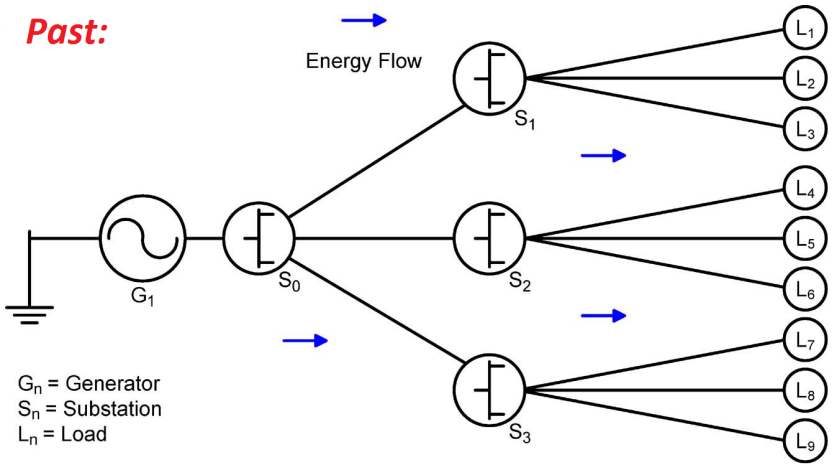
- Security information and event management (SIEM): software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by network hardware and applications. Used to log security data and generate reports for compliance purposes. The segment of security management that deals with real-time monitoring, correlation of events, notifications and console views is commonly known as security event management (SEM). The second area provides long-term storage as well as analysis and reporting of log data, and is known as security information management (SIM).

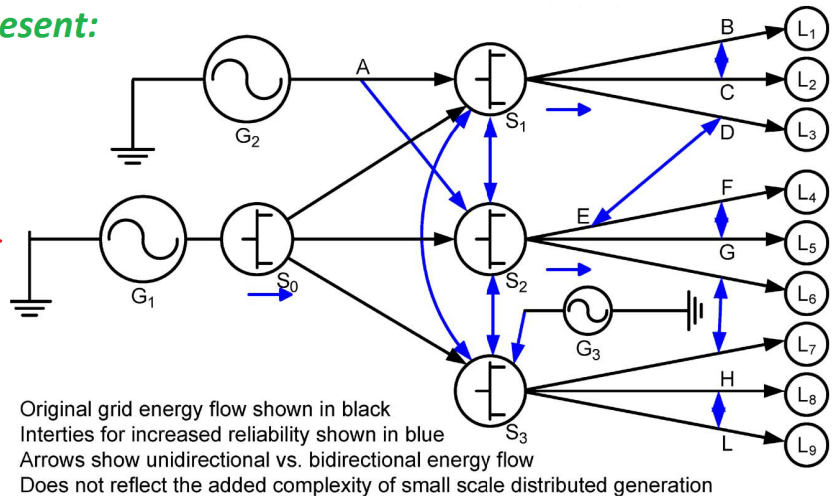
Paper aim

Framework for an High-Assurance Smart Grid architecture
that incorporates three core attributes:

1. categorizes cybersecurity requirements based on a multi-tier determination of a subsystem's potential impact on the overall system;
2. implements a robust defense-in-depth cybersecurity architecture;
3. implements a distributed control system architecture based on an assumed compromise (untrusted condition) of system control components and subsystems using autoresponsive load control wherever possible.

Grid control architecture: hierarchical vs distributed energy flow





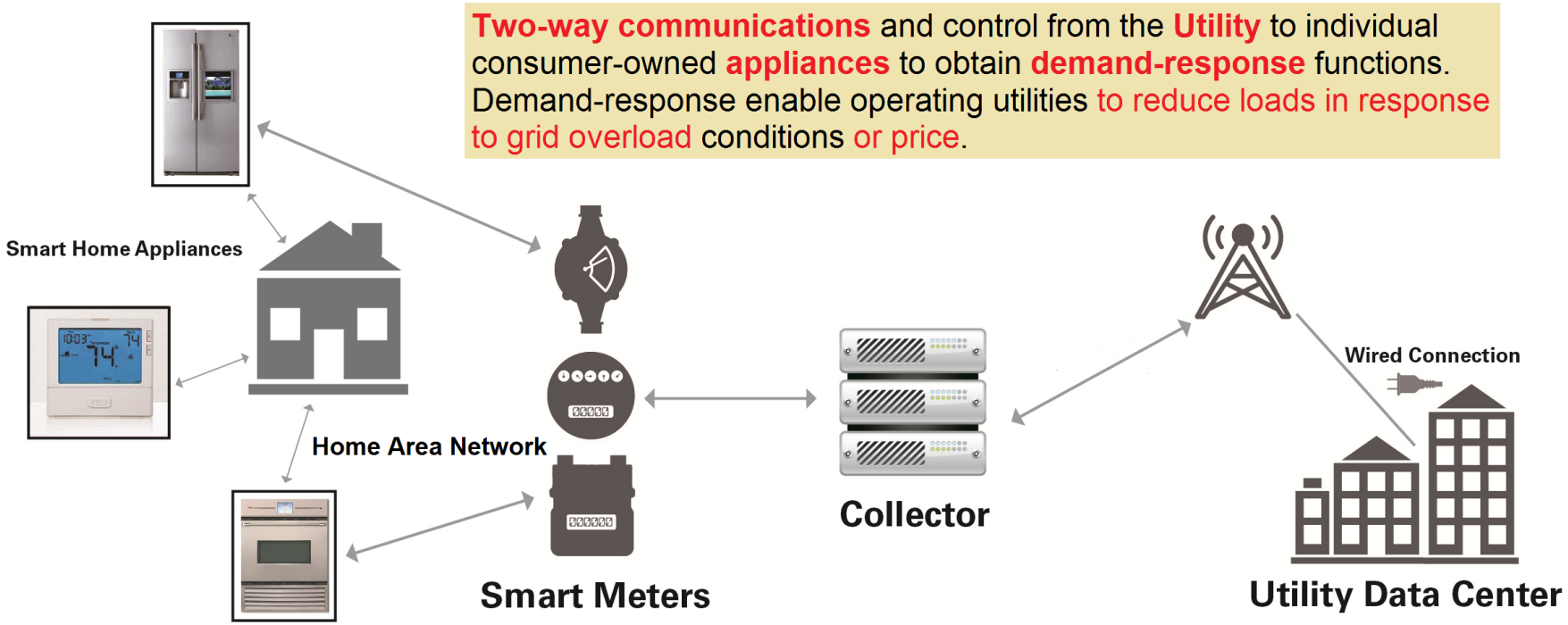
Simple tree graph of energy flow:

- hierarchical.

Interconnected energy distribution:

- distributed generation;
- more reliability: alternate path.

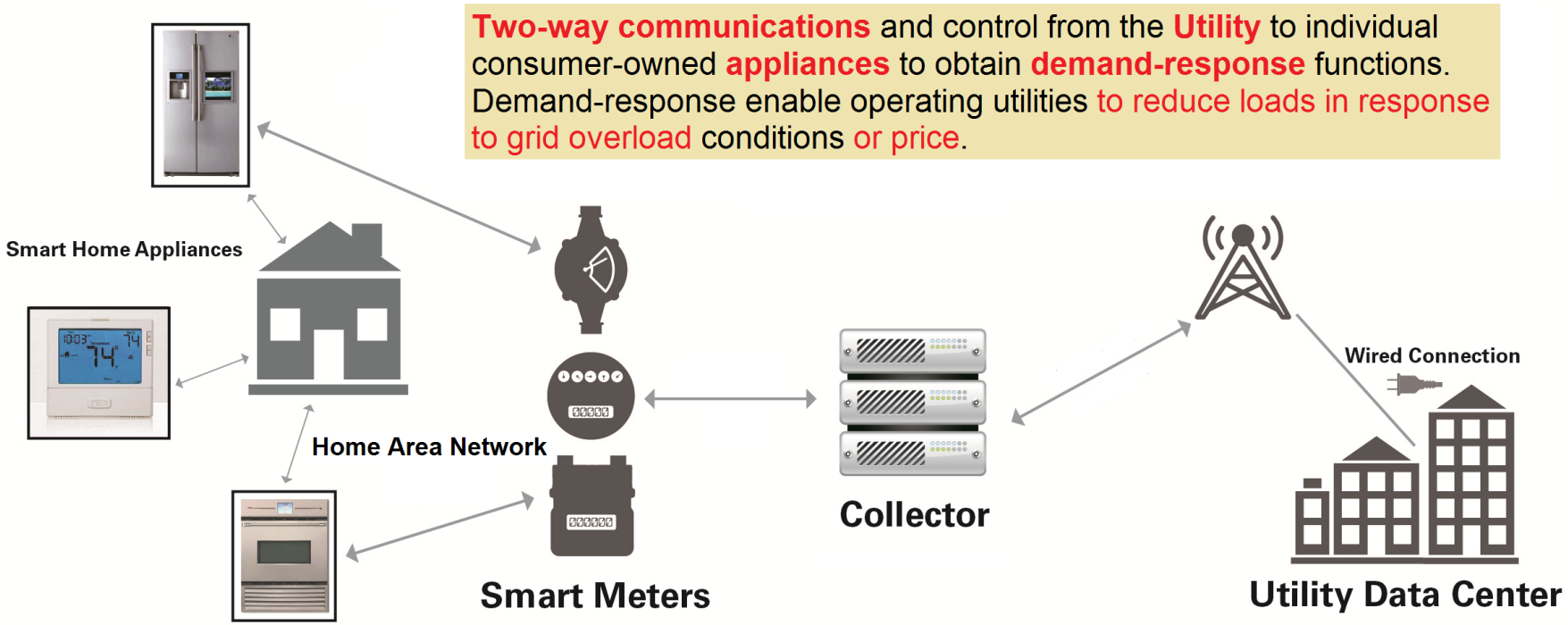
Risk/benefit analysis of Two-Way Communication and Control (2W-C2) for Demand-Response (DR)



2W-C2 benefits:

- more refined consumer information $\Rightarrow$ better power planning;
- better load control available to utilities.

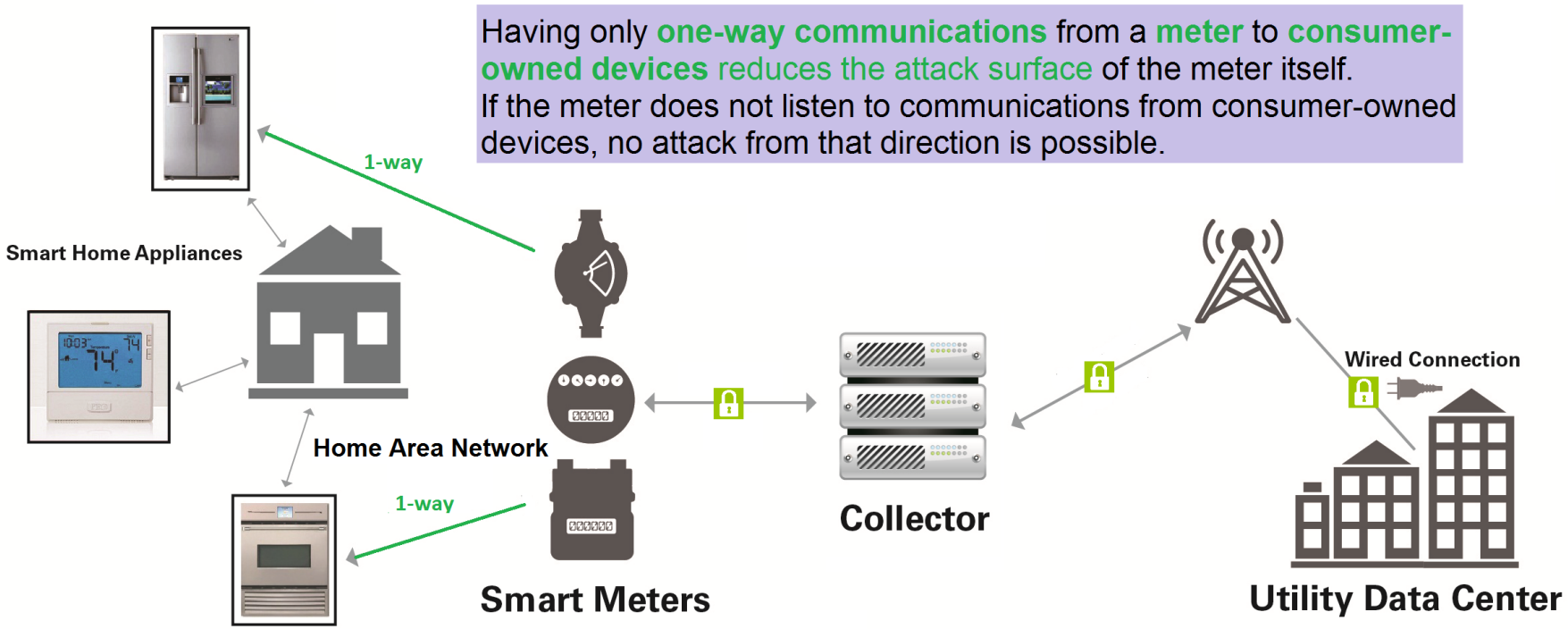
Risk/benefit analysis of Two-Way Communication and Control (2W-C2) for Demand-Response (DR)



2W-C2 risks (cybersecurity concerns):

- insecure communications path from the consumer into the Utility control room $\Rightarrow$ false load control ack to a Utility (realize cost benefits while not actually reducing the load).

Risk/benefit analysis of Two-Way Communication and Control (2W-C2) for Demand-Response (DR)



2W-C2 risks (cybersecurity concerns):

- insecure communications path from the consumer into the Utility control room $\Rightarrow$ false load control ack to a Utility (realize cost benefits while not actually reducing the load).