Critical Infrastructure Security

Lecture 6

Dr. Naveed Anwar Bhatti

Webpage: naveedanwarbhatti.github.io

SMART GRID

- Increase grid resilience

SMART GRID

- Increase grid resilience

- Improve environmental performance

SMART GRID

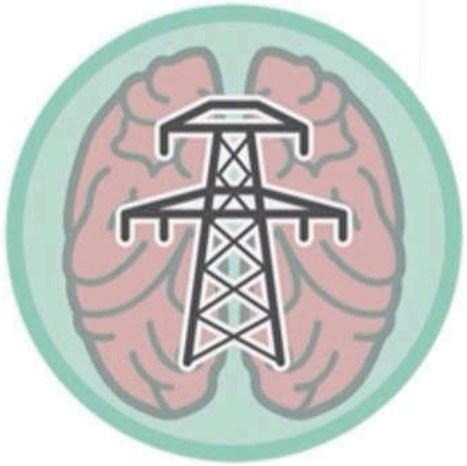
- Increase grid resilience

- Improve environmental performance

- Deliver operational efficiencies

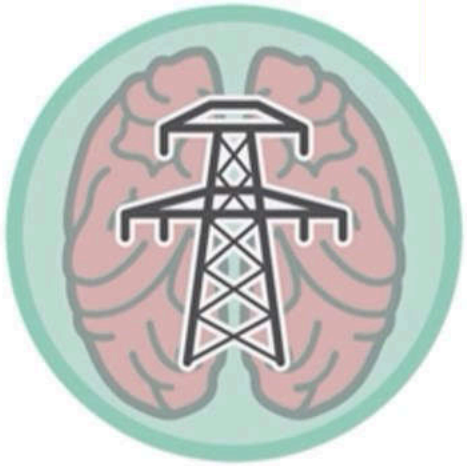
SMART GRID

Smart Grid



Smart Grid

Many different systems



Smart Grid

Many different systems

Common, open, and specialized protocols

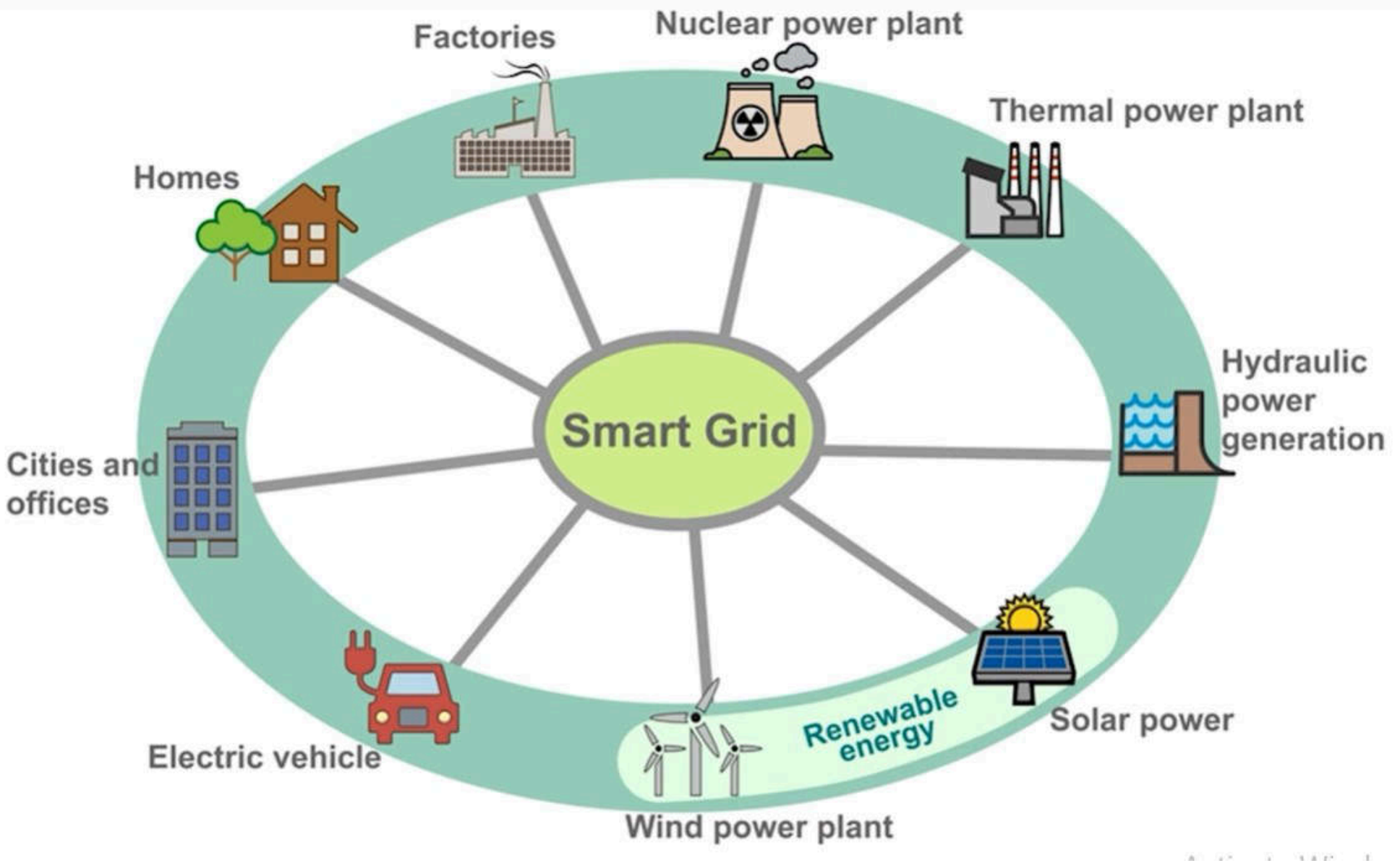
Smart Grid

Many different systems

Common, open, and specialized protocols

Blend of open and proprietary networks

Smart Grid


Factories
Nuclear power plant
Thermal power plant
Homes
Hydraulic power generation
Smart Grid
Cities and offices
Renewable energy
Solar power
Electric vehicle
Wind power plant

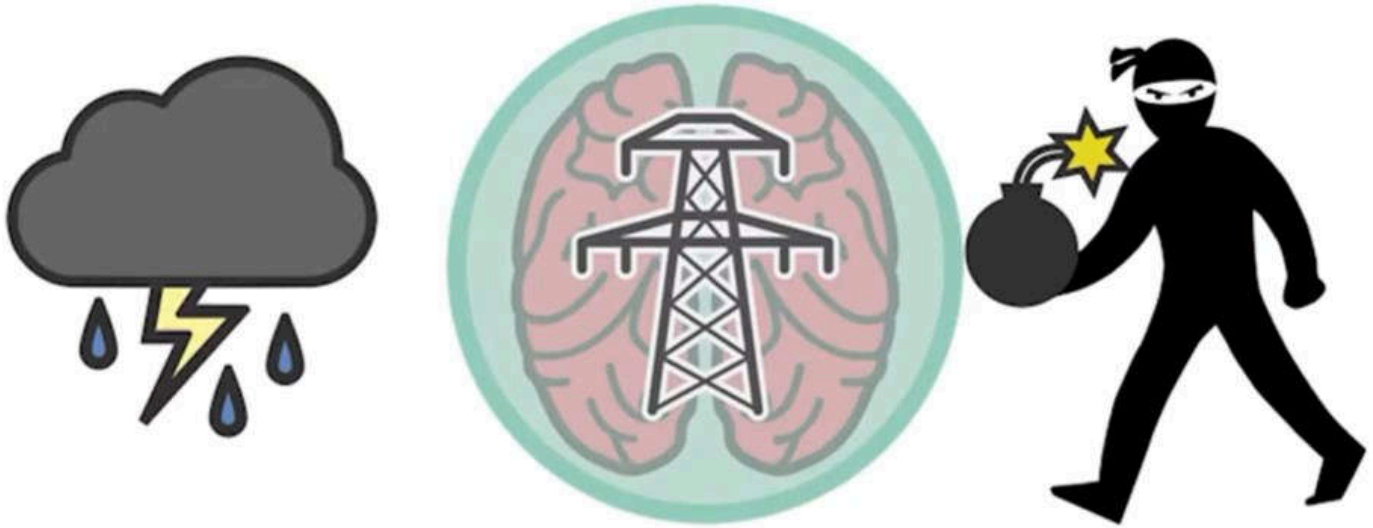
GRID RESILIENCE

Resilience: the capability of a given entity to withstand from unexpected actions, and recover very quickly thereafter.

GRID RESILIENCE

In the case of the electricity network, a Smart Grid should be able to withstand such environmental threats (both intentional or unintentional), and recover in a timely fashion.

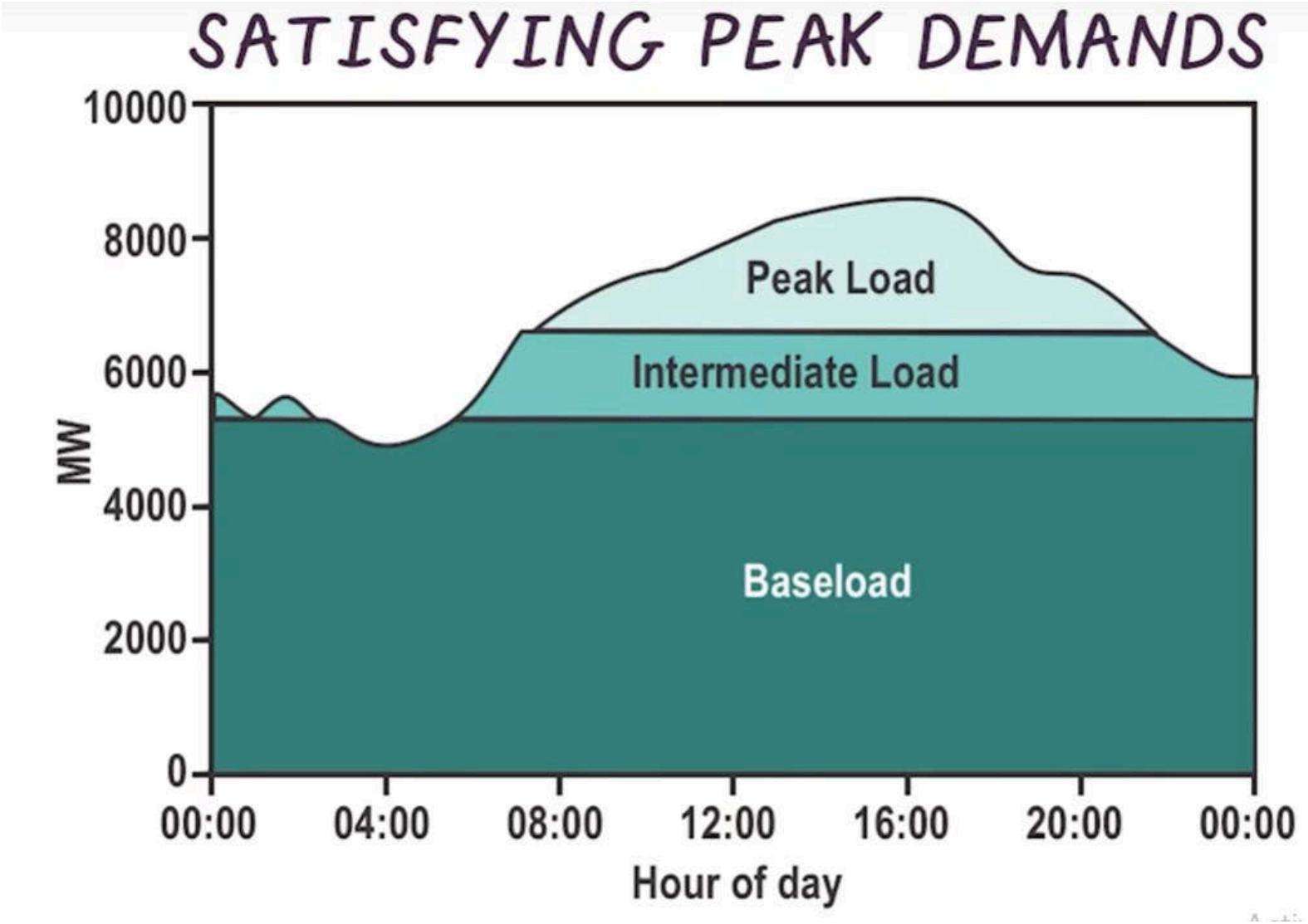
GRID RESILIENCE



In the case of the electricity network, a Smart Grid should be able to withstand such environmental threats (both intentional or unintentional), and recover in a timely fashion.

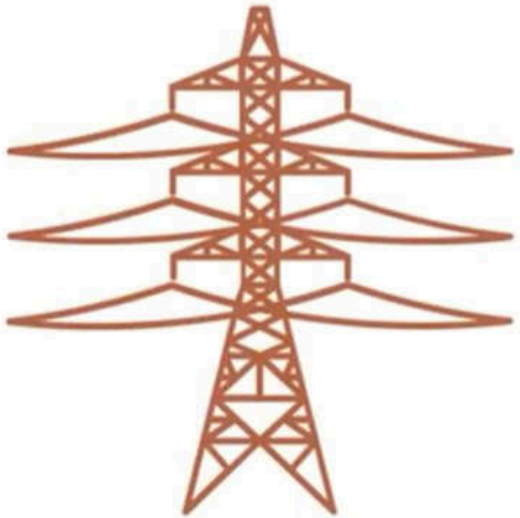
GRID RESILIENCE

One of the biggest threats to resilience is peak load demands.


SATISFYING PEAK DEMANDS
10000
8000
6000
4000
2000
0
MW
Peak Load
Intermediate Load
Baseload
00:00
04:00
08:00
12:00
16:00
20:00
00:00
Hour of day

GRID RESILIENCE

Other threats include old equipment and cyber attacks.



ENVIRONMENTAL PERFORMANCE

Improving efficiency of the US power grid reduce CO_2 emissions

ENVIRONMENTAL PERFORMANCE

Improving efficiency of the US power grid reduce CO_2 emissions

Greater efficiency

ENVIRONMENTAL PERFORMANCE

Improving efficiency of the US power grid reduce CO_2 emissions

Greater efficiency

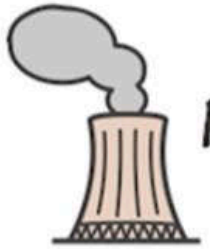
Integration of renewable technologies

ENVIRONMENTAL PERFORMANCE

Improving efficiency of the US power grid reduce CO_2 emissions

Greater efficiency

Integration of renewable technologies



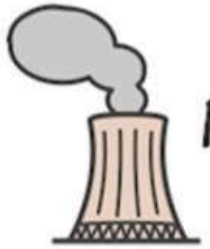
Reduction in the need for new power plants

ENVIRONMENTAL PERFORMANCE

Improving efficiency of the US power grid reduce CO_2 emissions

Greater efficiency

Integration of renewable technologies



Reduction in the need for new power plants

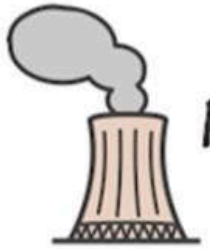
Support for electric vehicles

ENVIRONMENTAL PERFORMANCE

Improving efficiency of the US power grid reduce CO_2 emissions

Greater efficiency

Integration of renewable technologies

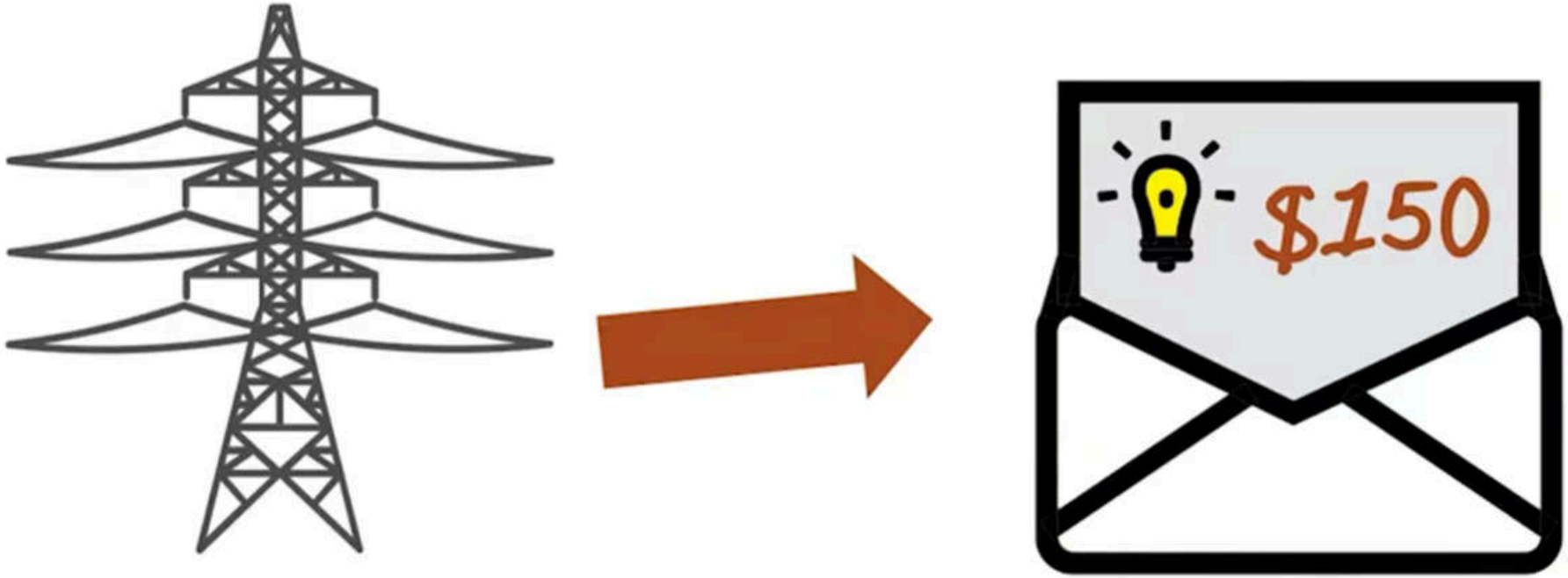


Reduction in the need for new power plants

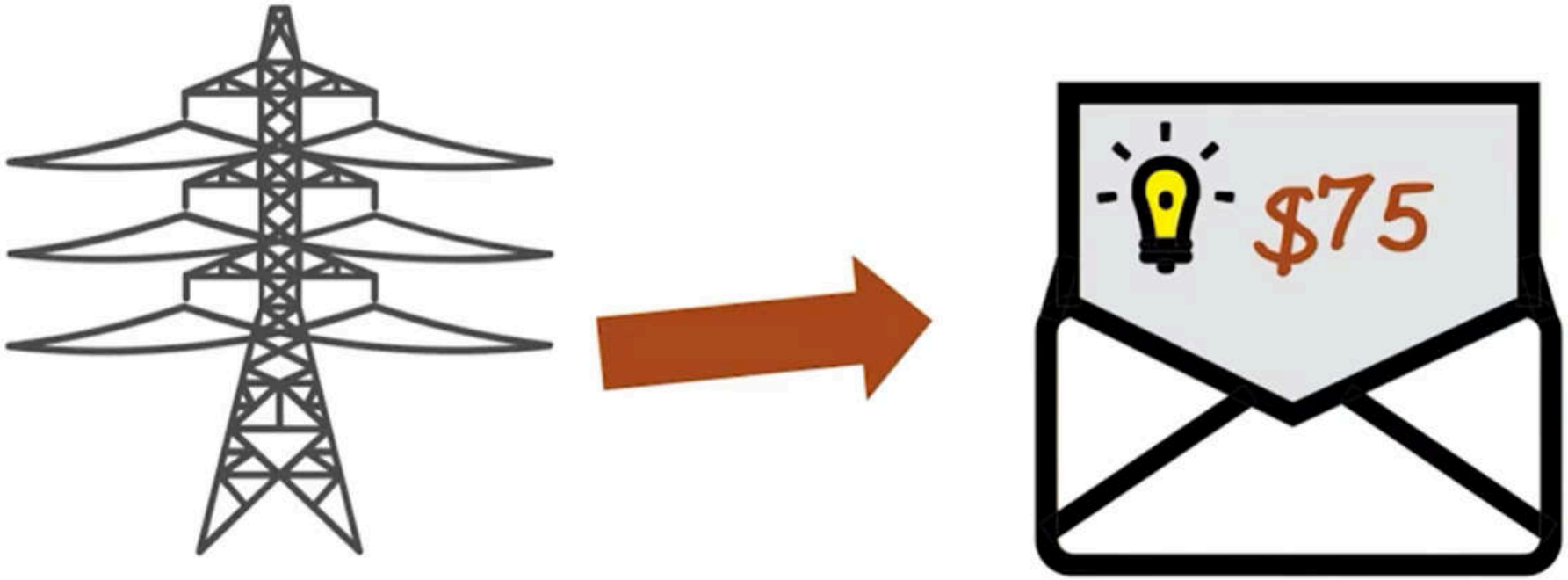
Support for electric vehicles

Smarter appliances

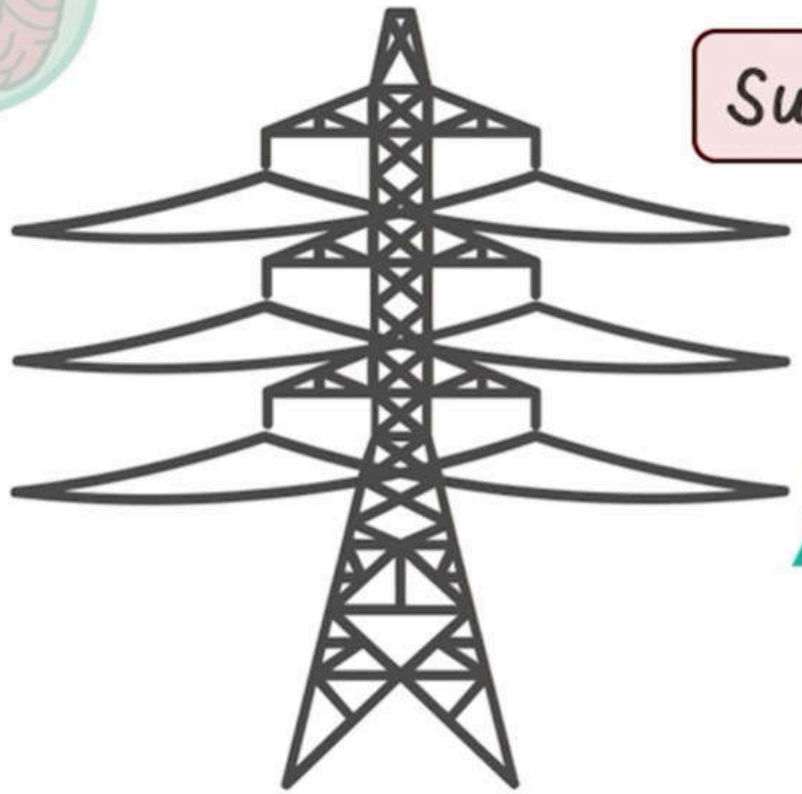
OPERATIONAL EFFICIENCIES



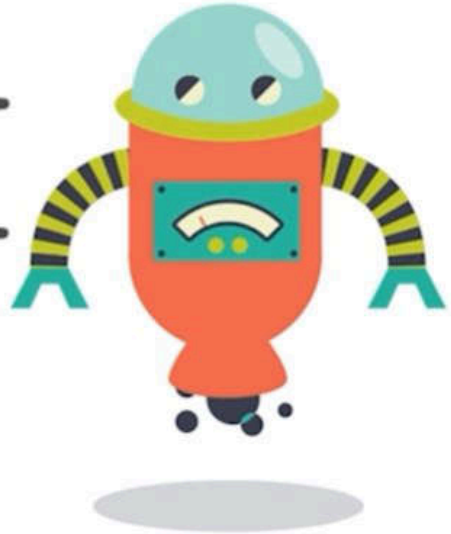
OPERATIONAL EFFICIENCIES

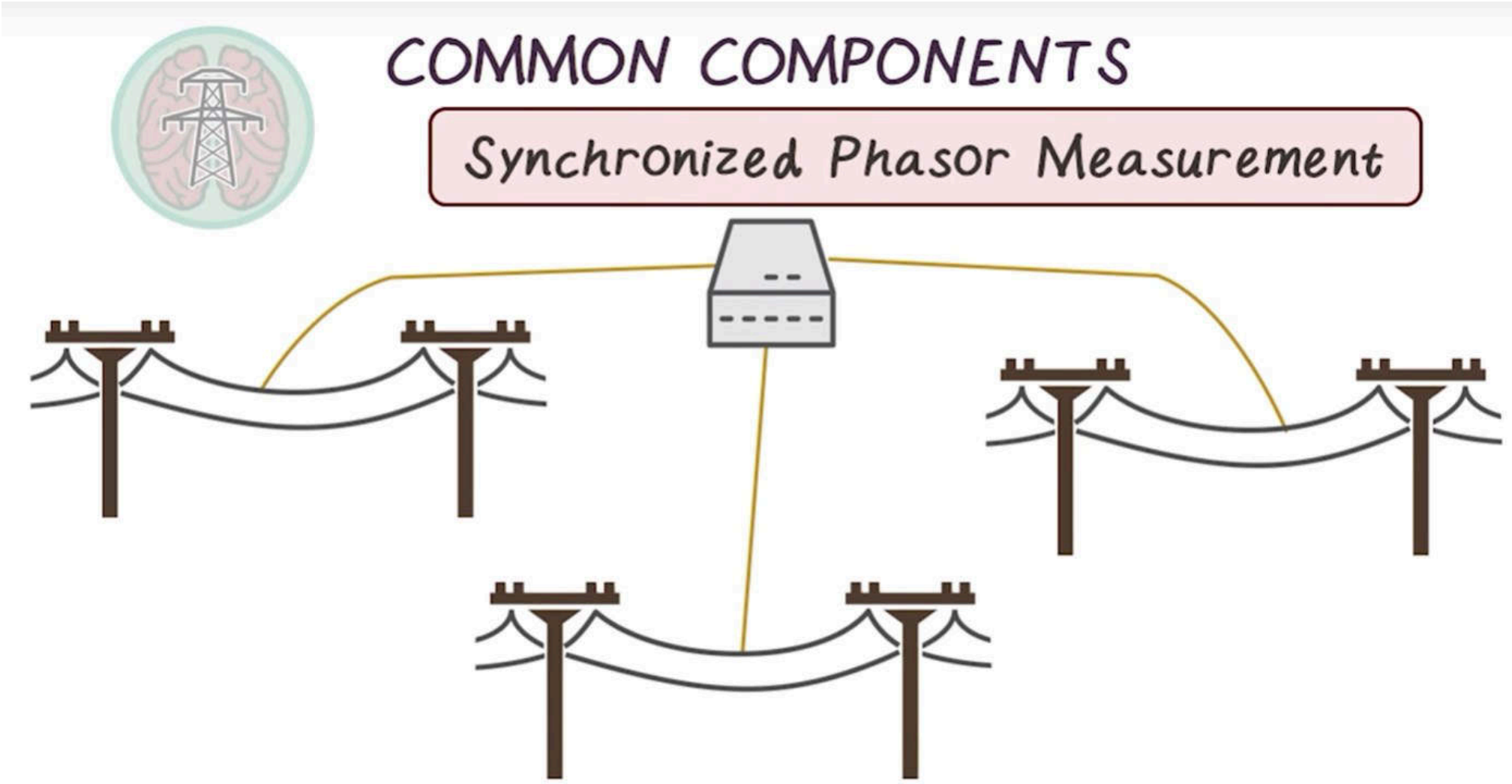


COMMON COMPONENTS



Substation Automation




COMMON COMPONENTS
Synchronized Phasor Measurement

COMMON COMPONENTS

Advanced Metering Infrastructure

SOCIAL PITFALLS OF THE SMART GRID

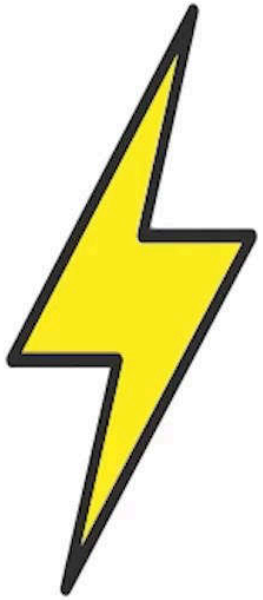
Communities based at home all day

Individuals unable to grasp the information overload presented to them

Individuals who can't afford smart appliances

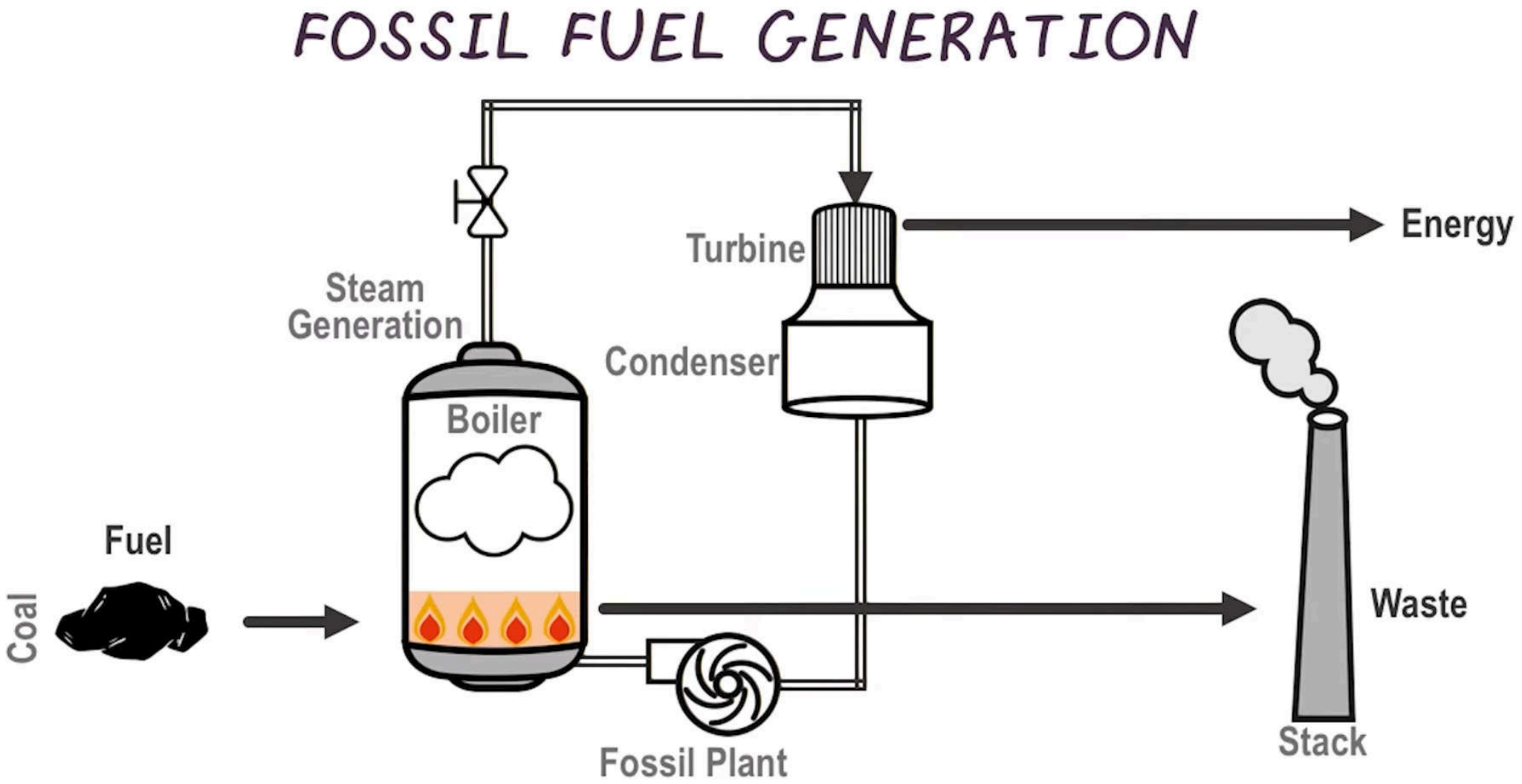
Renters whose landlord don't embrace smart devices

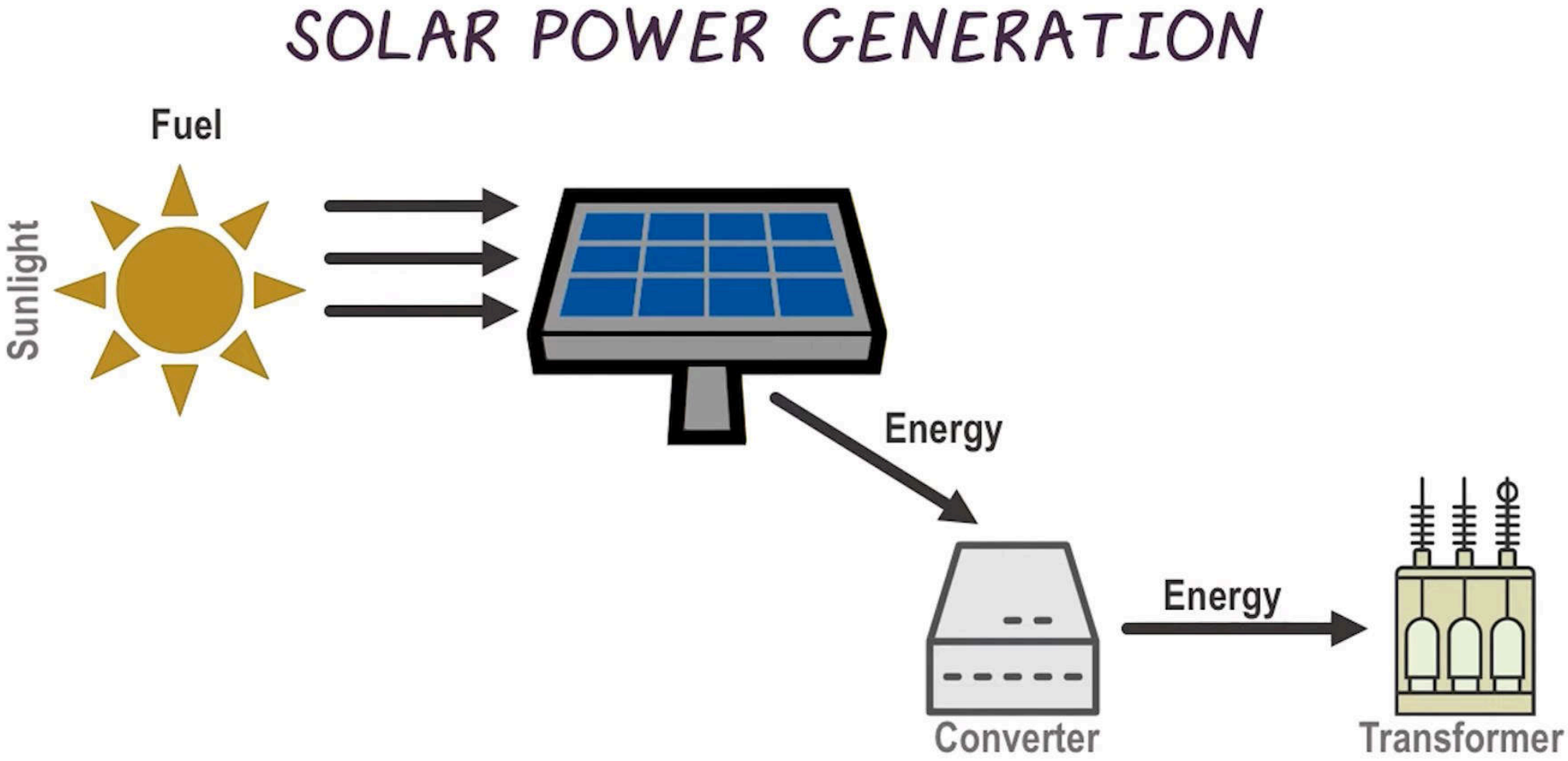
TYPES OF ELECTRICAL GENERATION



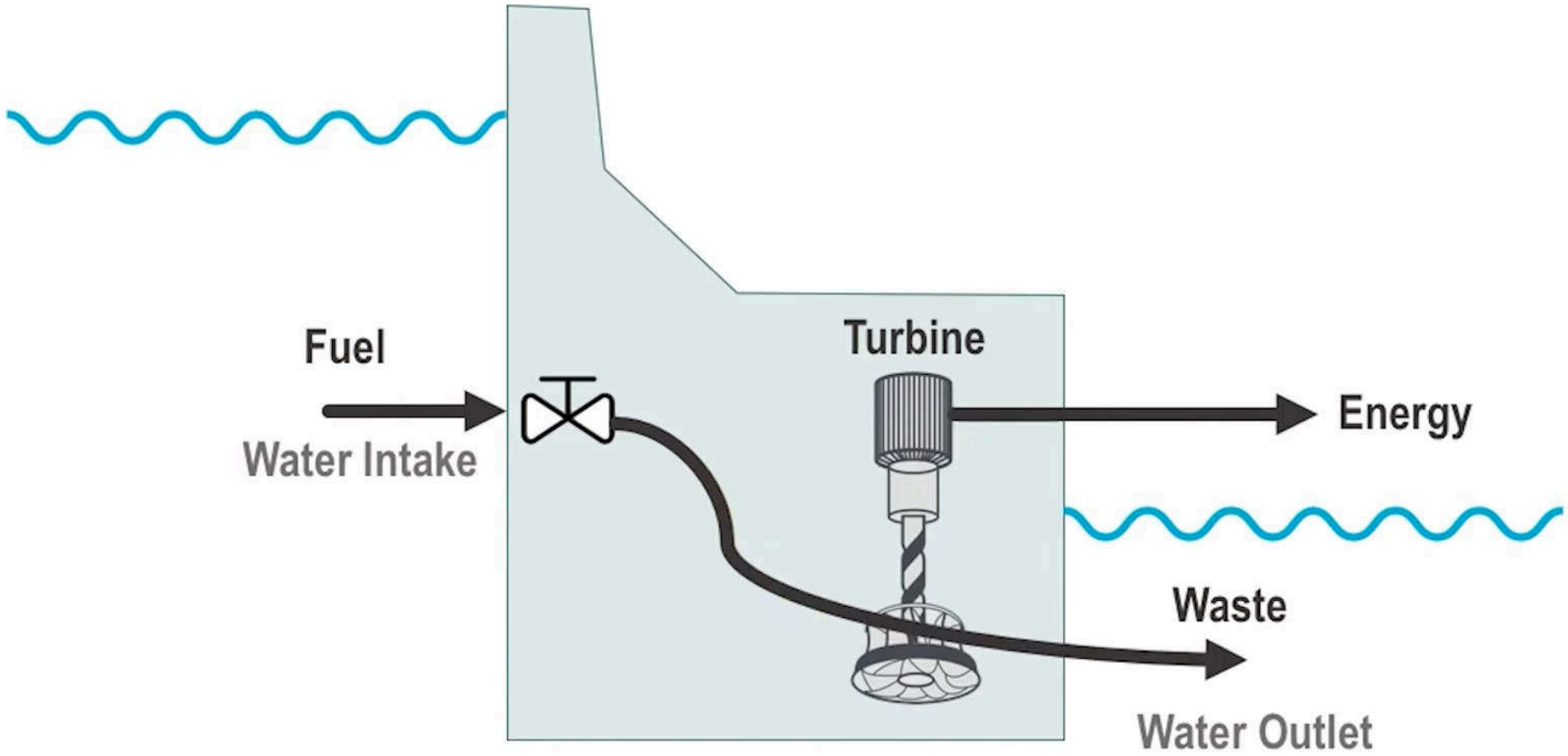
Electric generation sources include several distinct mechanisms, built around the specific fuel used to create electricity.

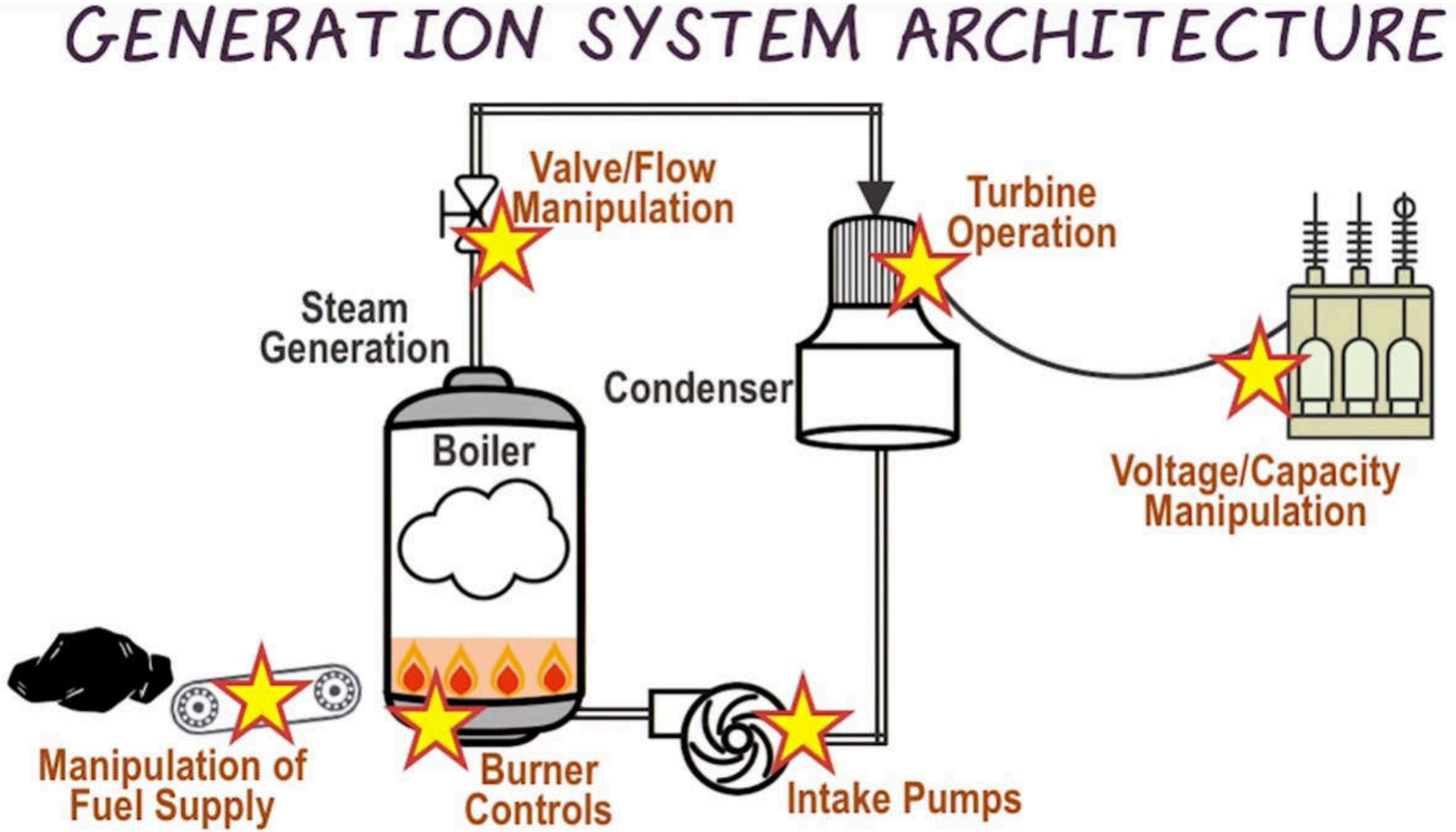
Each system represents its own vulnerabilities that are inherent in their designs.


FOSSIL FUEL GENERATION
Steam Generation
Turbine
Energy
Condenser
Boiler
Fuel
Coal
Waste
Stack
Fossil Plant

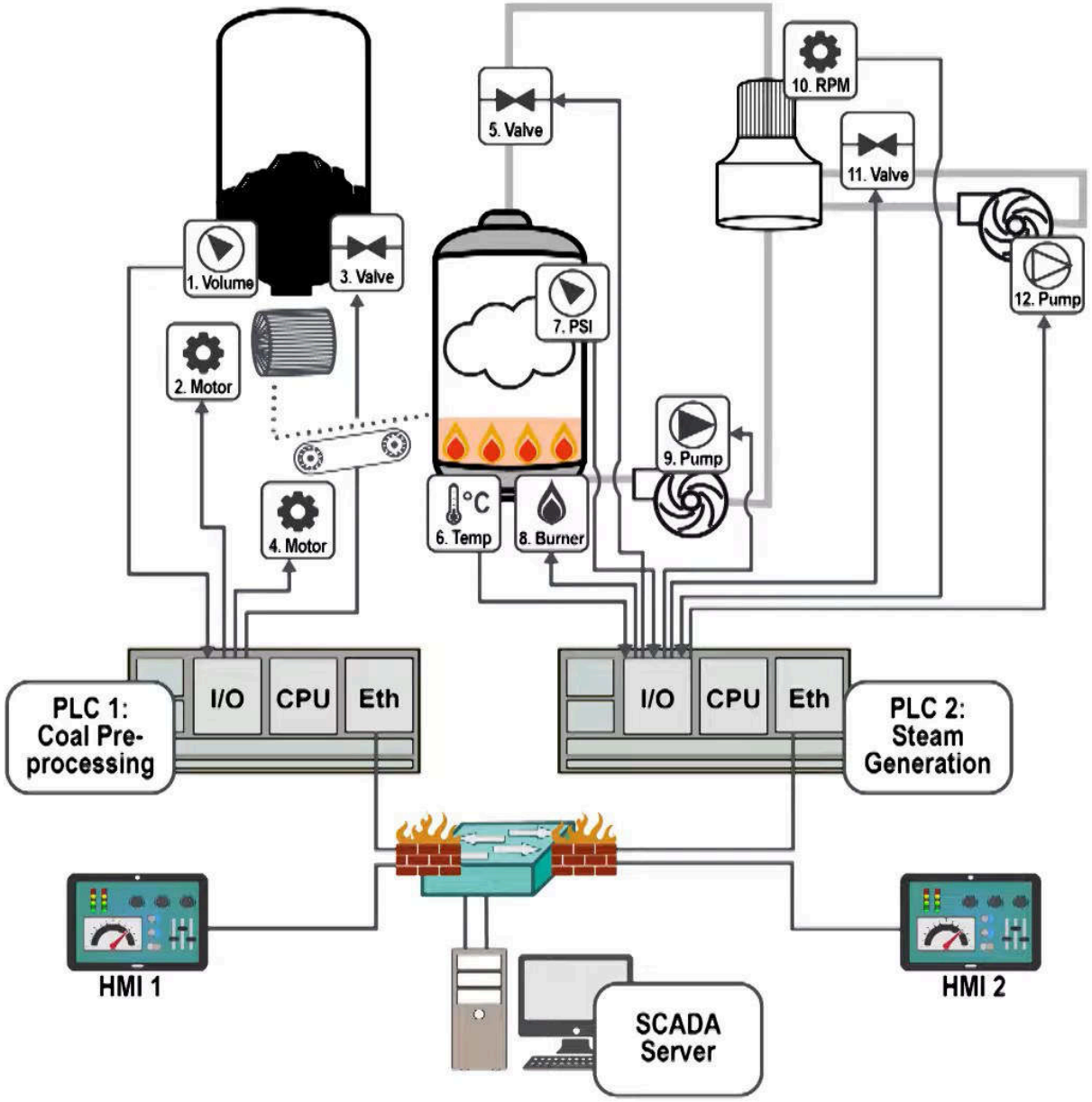

SOLAR POWER GENERATION
Fuel
Sunlight
Energy
Converter
Energy
Transformer

HYDRO-ELECTRIC GENERATION

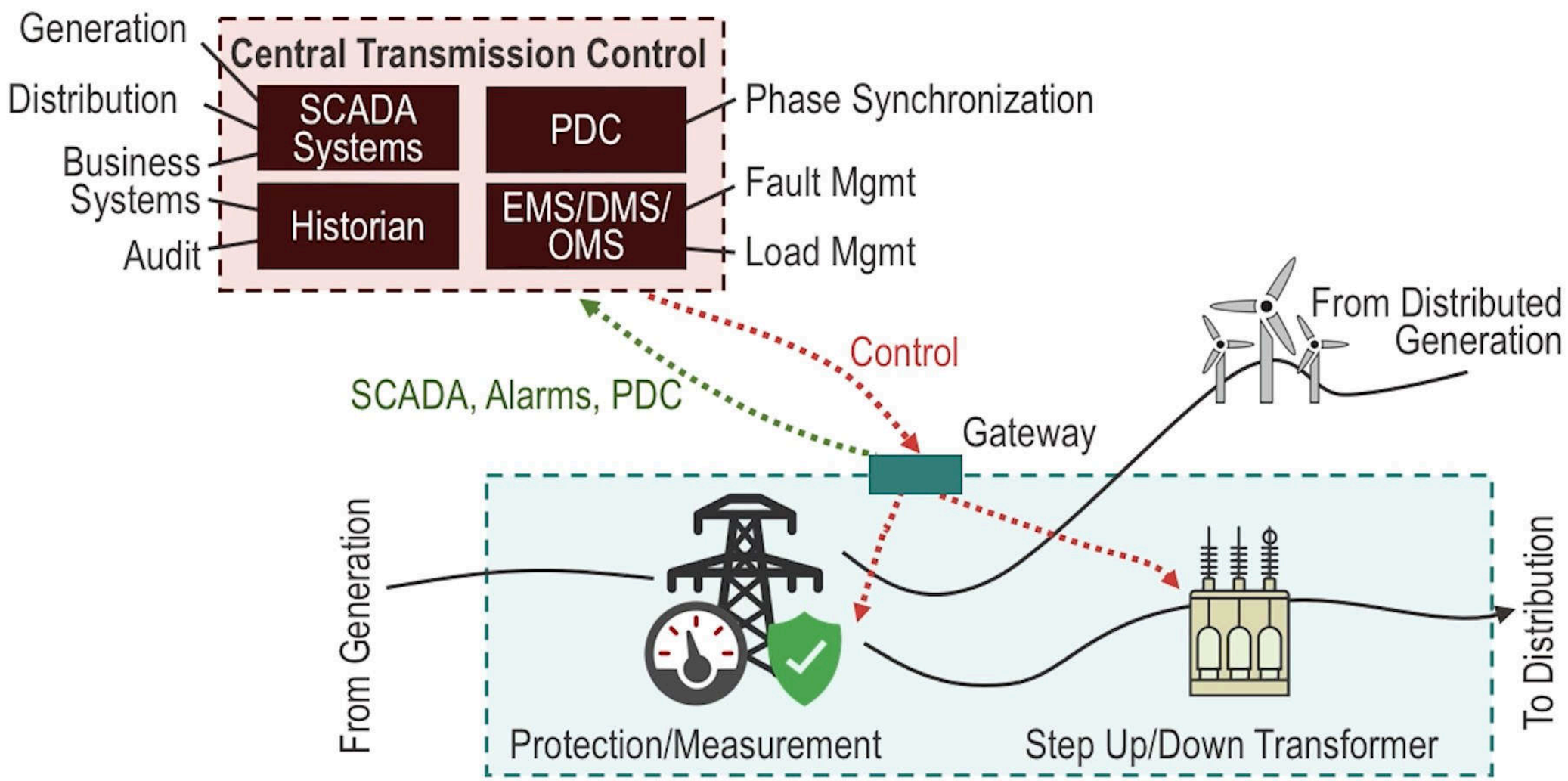



GENERATION SYSTEM ARCHITECTURE
Valve/Flow Manipulation
Turbine Operation
Steam Generation
Condenser
Boiler
Voltage/Capacity Manipulation
Manipulation of Fuel Supply
Burner Controls
Intake Pumps

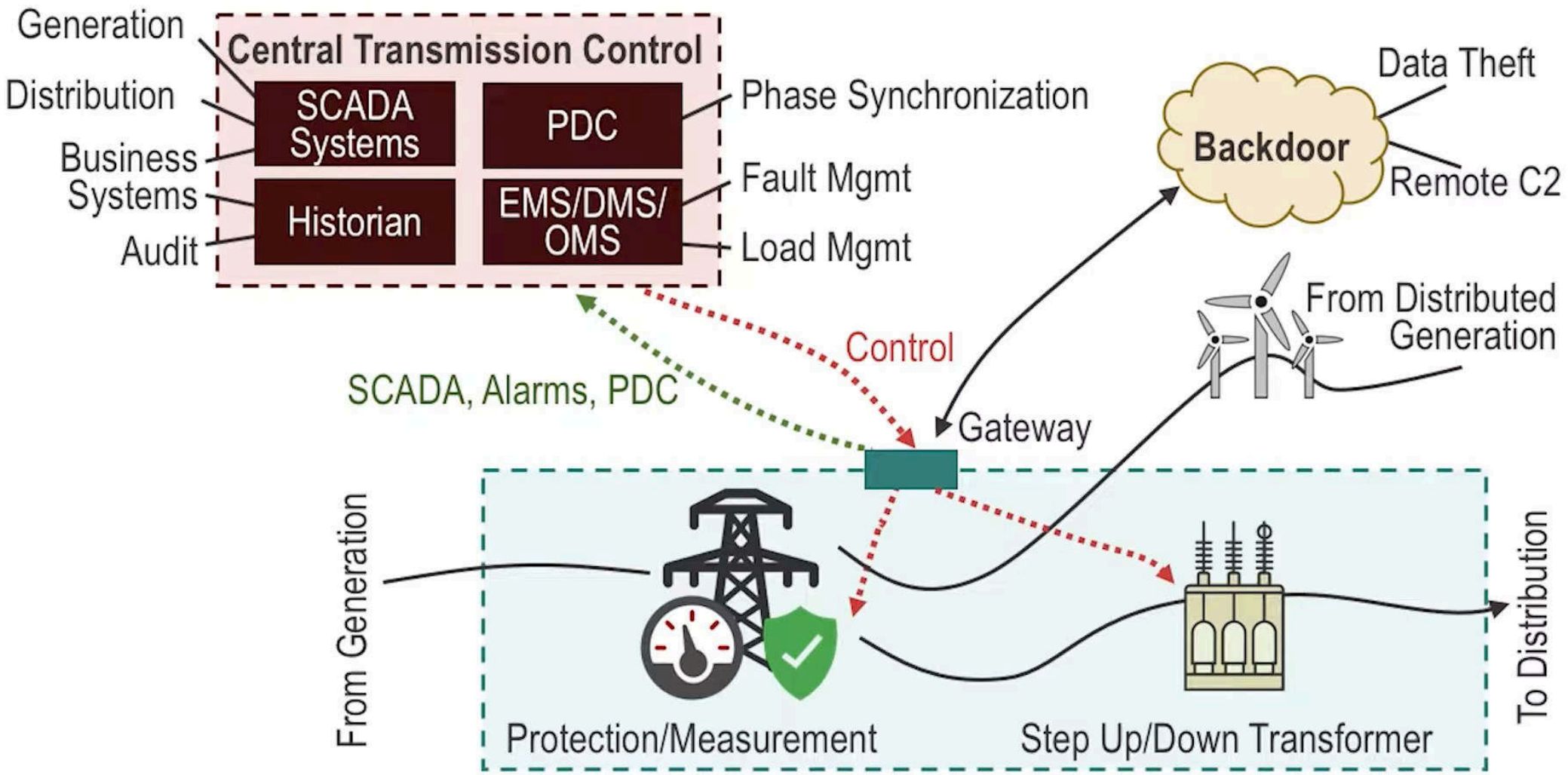
Smart Grid

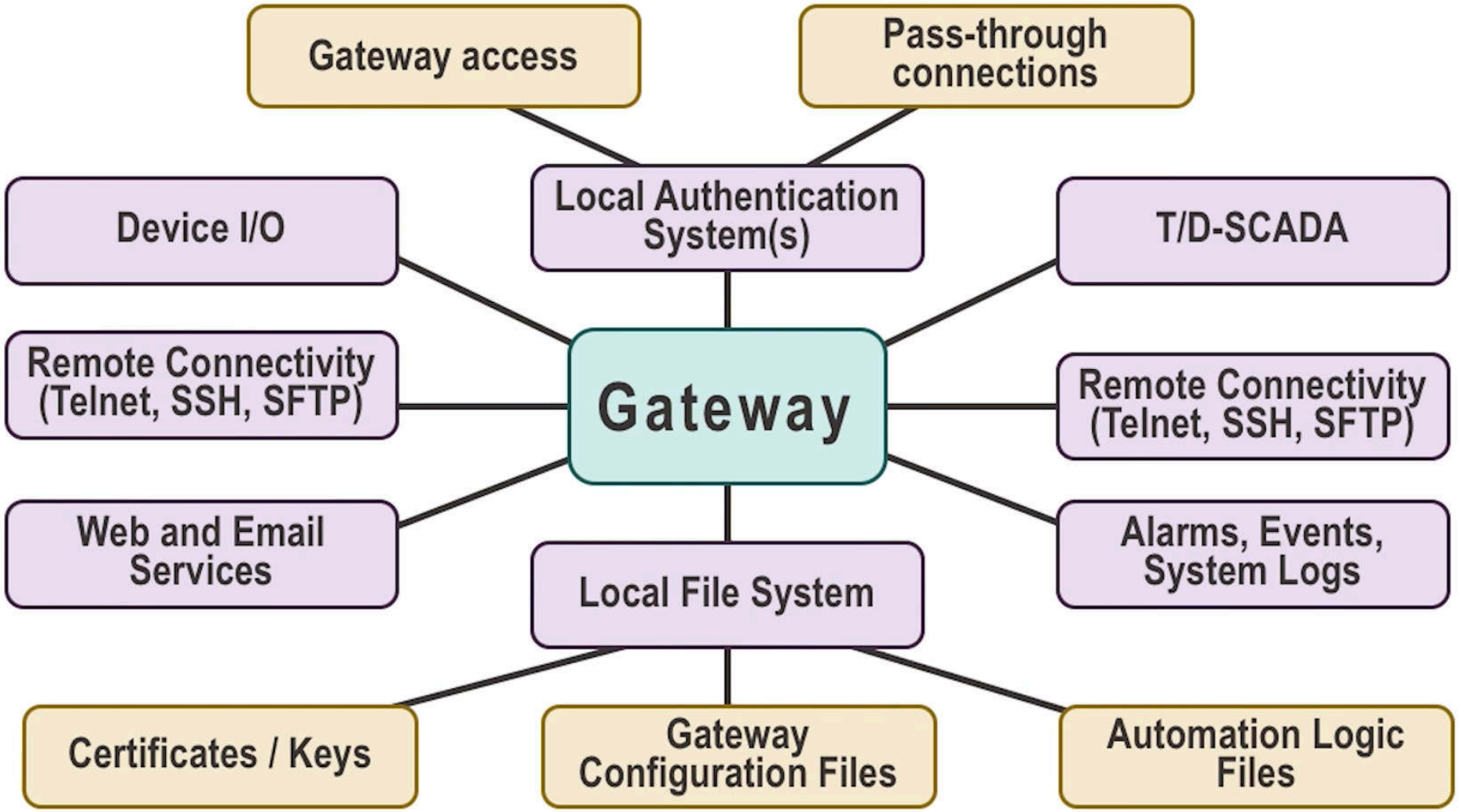

1. Volume
2. Motor
3. Valve
4. Motor
5. Valve
6. Temp
7. PSI
8. Burner
9. Pump
10. RPM
11. Valve
12. Pump
°C
I/O
CPU
Eth
PLC 1: Coal Pre-processing
I/O
CPU
Eth
PLC 2: Steam Generation
HMI 1
HMI 2
SCADA Server

Smart Grid


Generation
Distribution
Business Systems
Audit
Central Transmission Control
SCADA Systems
PDC
Historian
EMS/DMS/ OMS
Phase Synchronization
Fault Mgmt
Load Mgmt
Control
SCADA, Alarms, PDC
From Distributed Generation
Gateway
From Generation
To Distribution
Protection/Measurement
Step Up/Down Transformer

Smart Grid


Generation
Distribution
Business Systems
Audit
Central Transmission Control
SCADA Systems
PDC
Historian
EMS/DMS/ OMS
Phase Synchronization
Fault Mgmt
Load Mgmt
Backdoor
Data Theft
Remote C2
From Distributed Generation
Control
SCADA, Alarms, PDC
Gateway
From Generation
Protection/Measurement
Step Up/Down Transformer
To Distribution


Gateway access
Pass-through connections
Local Authentication System(s)
Device I/O
T/D-SCADA
Remote Connectivity (Telnet, SSH, SFTP)
Gateway
Remote Connectivity (Telnet, SSH, SFTP)
Web and Email Services
Alarms, Events, System Logs
Local File System
Certificates / Keys
Gateway Configuration Files
Automation Logic Files

COMPROMISE OF THE SUBSTATION GATEWAY

COMPROMISE OF THE SUBSTATION GATEWAY

Direct Manipulation

COMPROMISE OF THE SUBSTATION GATEWAY

Direct Manipulation

Indirect Manipulation

COMPROMISE OF THE SUBSTATION GATEWAY

Direct Manipulation

Indirect Manipulation

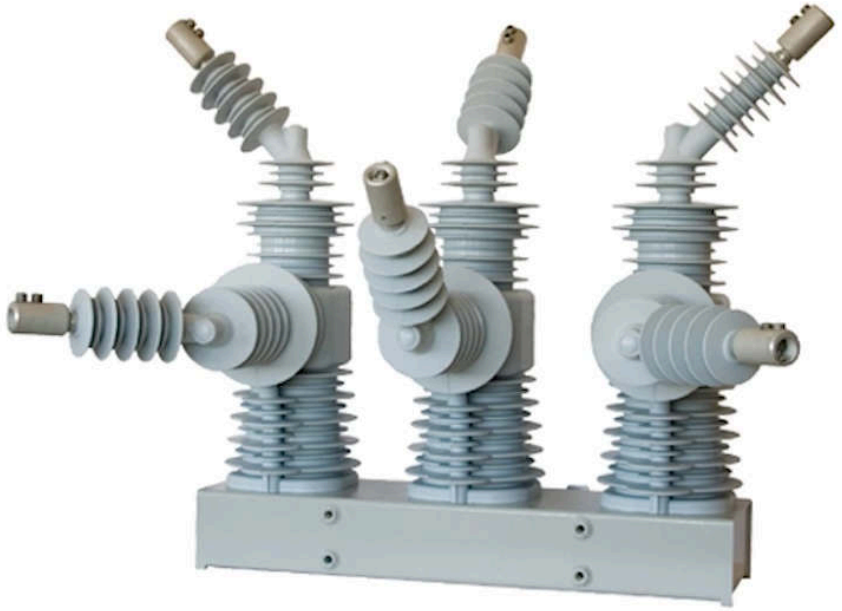
Remote Manipulation

COMPROMISE OF DISTRIBUTION FIELD DEVICES

Ranging from inefficiencies in operations, to inaccuracies in reported data and to outages

COMPROMISE OF DISTRIBUTION FIELD DEVICES

Auto-reclosers are designed to protect against power surges and to recover once conditions are normal



Manipulation of line conditions could cause a recloser to trip unnecessarily

COMPROMISE OF DISTRIBUTION FIELD DEVICES

Complete compromise of an RTU could allow a cyber attacker to insert malicious logic into the controller

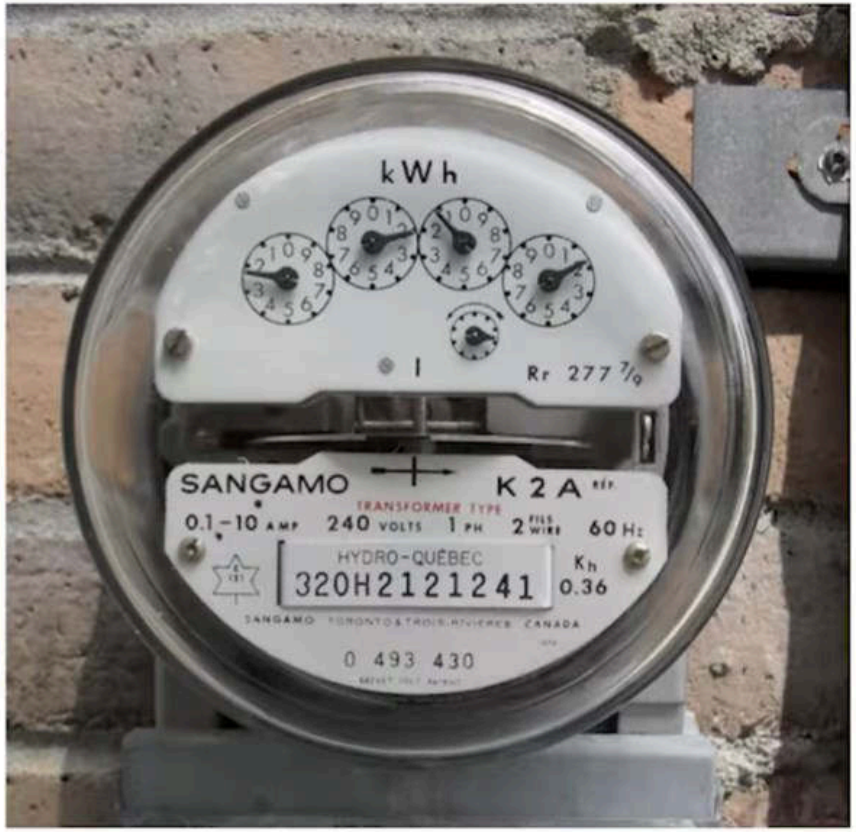
METERING AND AMI

By Dwight Burdette (Own work) [CC BY 3.0 (http://creativecommons.org/licenses/by/3.0)], via Wikimedia Commons

ADVANCED METERING ARCHITECTURE

Hacking analog meters by manipulating the magnetic resistance that controlled the analog meter dials, the result of such an attack was:

- Isolated to the source
- Fairly easy to detect



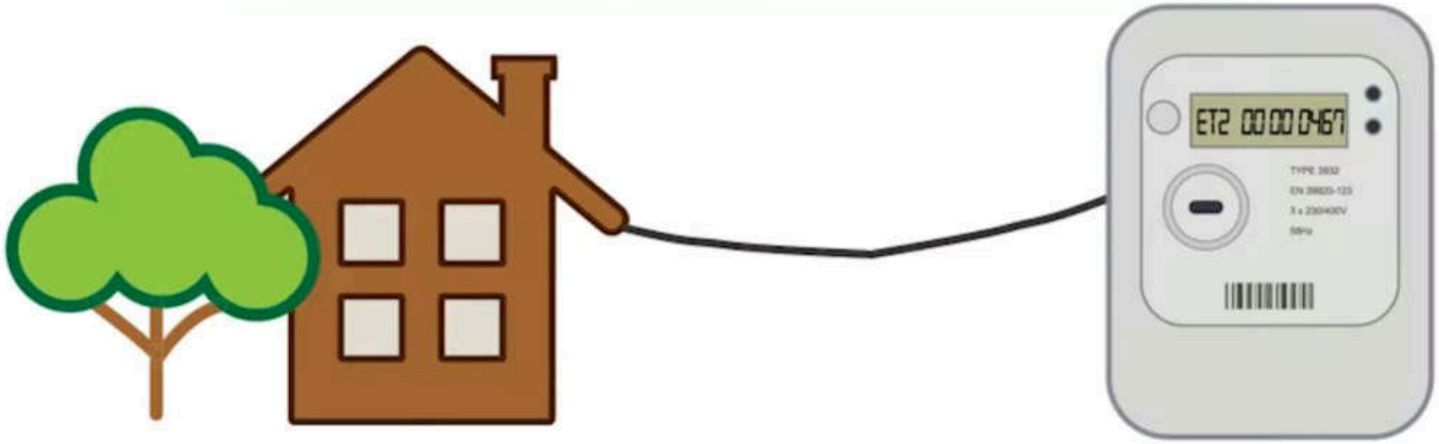
ADVANCED METERING ARCHITECTURE

More modern meters provide contact-free reading.

ADVANCED METERING ARCHITECTURE

Smart Grids add considerable sophistication to metering, "smart meters" can:

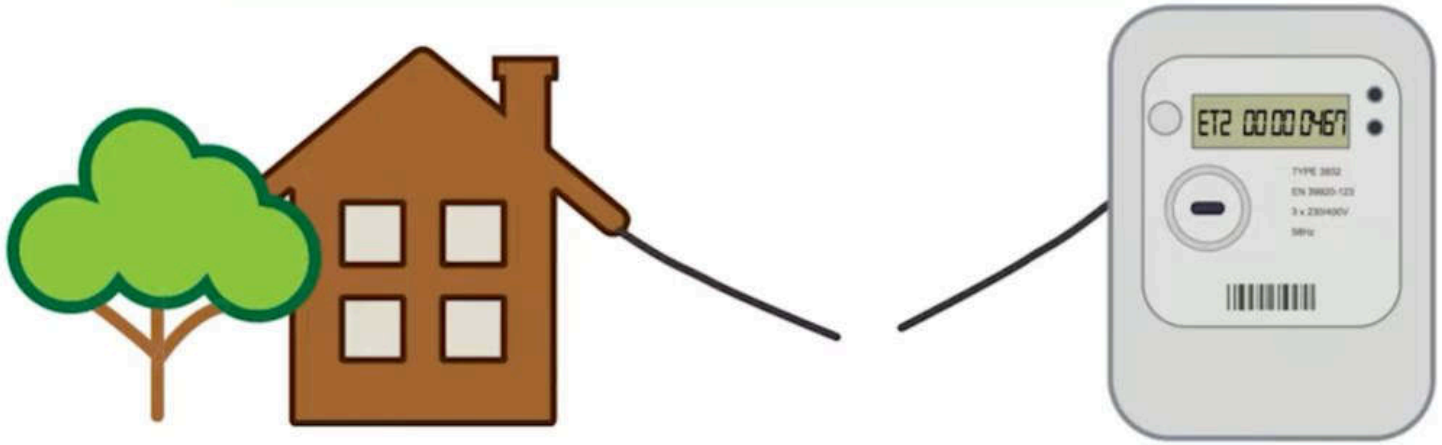
- measure energy utilization
- Be remotely connected/disconnected



ADVANCED METERING ARCHITECTURE

Smart Grids add considerable sophistication to metering, "smart meters" can:

- measure energy utilization
- Be remotely connected/disconnected



ADVANCED METERING ARCHITECTURE

The Advanced Metering Infrastructure (AMI)

Energy

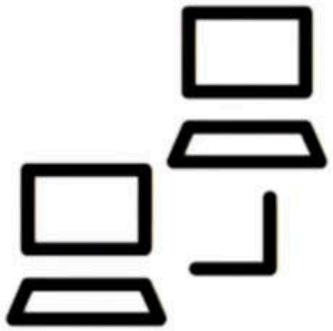
Water

Gas

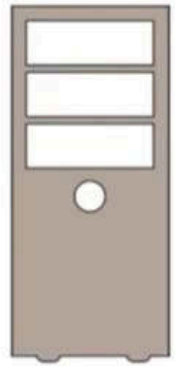
ADVANCED METERING ARCHITECTURE

AMI architecture consists of three primary components:

Smart meters



Communication network



AMI server or headend

ADVANCED METERING ARCHITECTURE

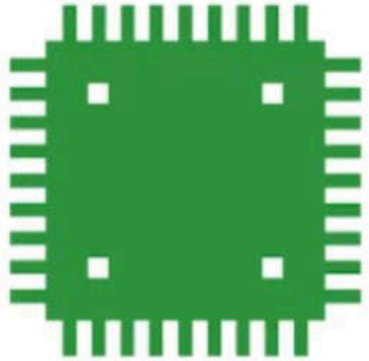
The smart meter is a digital meter consisting of a few key elements:

A solid-state meter for real-time data collection

ADVANCED METERING ARCHITECTURE

The smart meter is a digital meter consisting of a few key elements:

A microprocessor and local memory to store and transmit digital meter measurements.

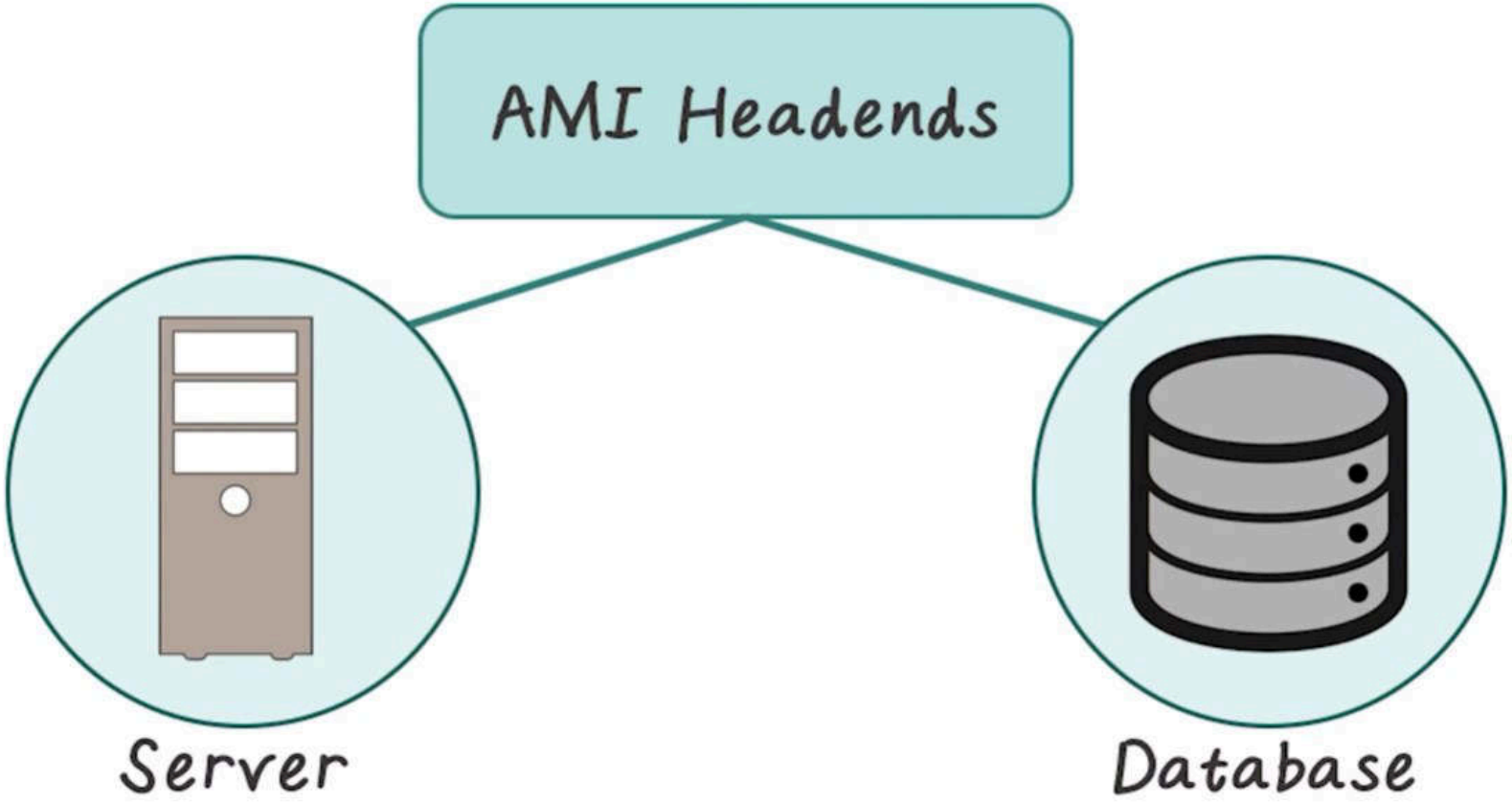


ADVANCED METERING ARCHITECTURE

The smart meter is a digital meter consisting of a few key elements:

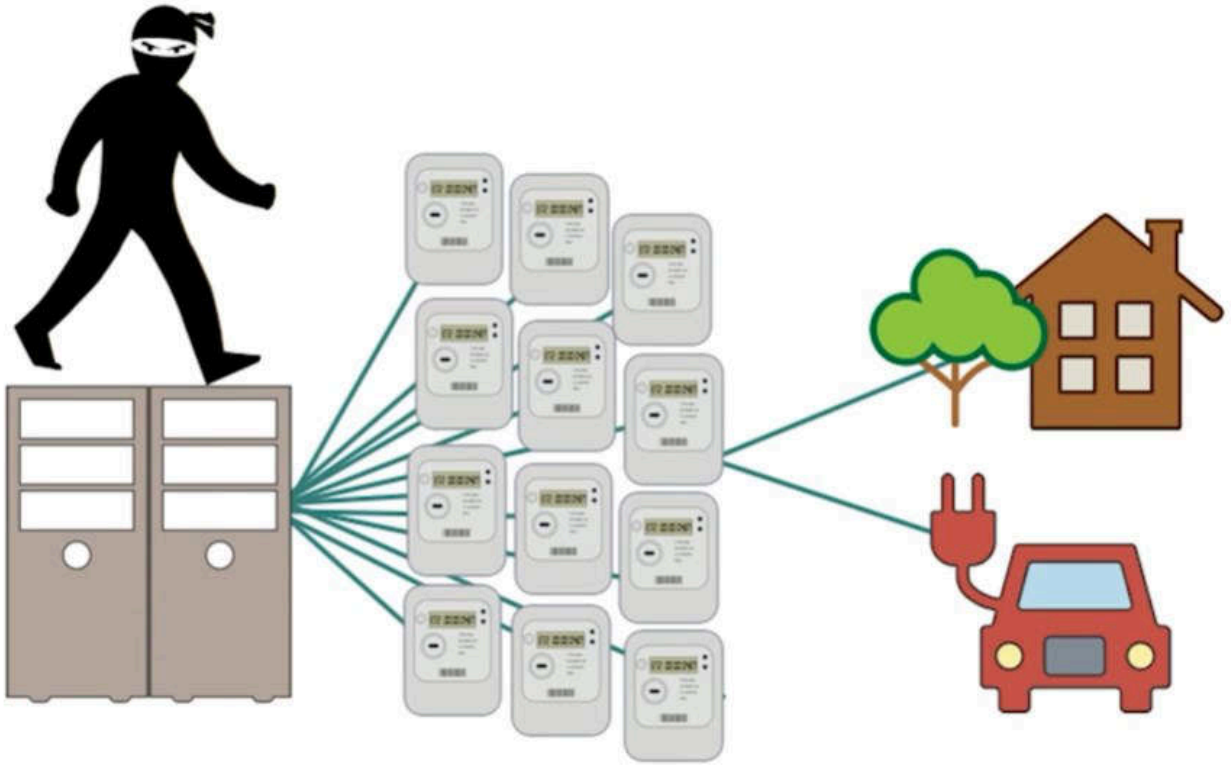
A communication network often including a home network connection for home automation and other advanced in-home services.

ADVANCED METERING ARCHITECTURE



COMPROMISE OF THE SMART METER AND THE AMI

COMPROMISE OF THE SMART METER AND THE AMI



Thanks a lot

If you are taking a Nap, **wake up**.....Lecture Over