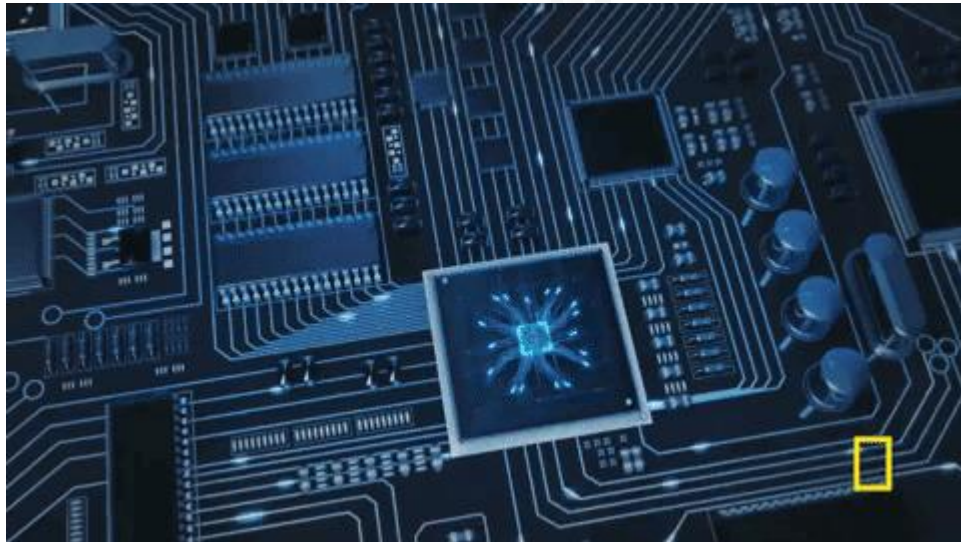


BEE714D

Big Data Analytics in Power Systems

Module-3: Security Methods for Critical Infrastructure Communications

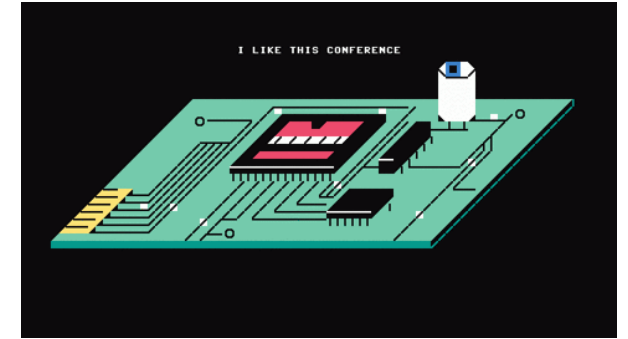
Data - Mining Methods for Electricity Theft Detection



Presented by,
Mr.Shreeshayana R
Assistant Professor
Electrical and Electronics Engineering
ATME College of Engineering, Mysuru

Course Overview

- **Course Code:** BEE714D
- **Course Title:** Big Data Analytics in Power Systems
- **Type:** Professional Elective
- **Prerequisite:** Power System Analysis-I
- **Contact Hours:** 40 Hours



3. Security Methods for Critical Infrastructure Communications:

3.1 Introduction

3.2 Effects of Successful Communication System Threats

3.3 General Communication System Operations,

3.4 Industrial Control Networks and Operations,

3.5 High-Level Communication System Threats,

3.6 Cyber Threats and Security.

Data - Mining Methods for Electricity Theft Detection:

3.7 Introduction

3.8 Transmission and Distribution System Losses

3.9 Electricity Theft Methods, Data Mining and Electricity Theft,

3.10 Issues and Directions in Electricity Theft-Related Data-Mining Research.

3.1 Introduction

- **Definition & Importance of CI** – Critical infrastructure (CI) includes essential systems like power grids, water, hospitals, and transport, whose disruption threatens lives, economies, and governance.
- **Industrial Control Networks (ICNs)** – ICNs monitor and control physical devices in CI (e.g., power utilities), making them vital for reliability and protection against unauthorized access.
- **Cybersecurity Challenges** – The adoption of IoT and commercial networks in CI increases connectivity but also introduces vulnerabilities, requiring a balance of performance, security, reliability, and availability.

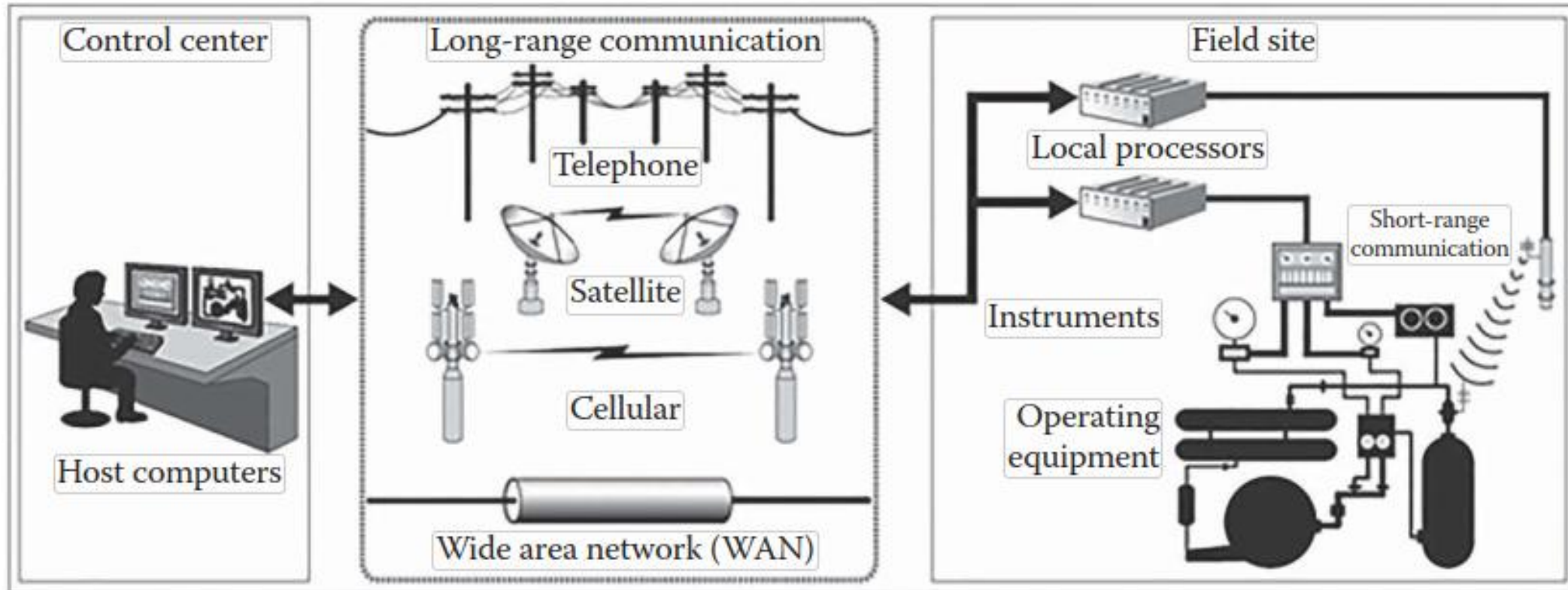


FIGURE Conceptualization of an Industrial Control Network.
(From Government Accountability Office (GAO), 2008.)

3.2 Effects of Successful Communication System Threats

- Risk analysis considers **Likelihood of Successful Attack (LAS)** as a function of **Threat (T)**, **Vulnerabilities (V)**, and **Target Attractiveness (AT)**.
- Consequences (C) of attacks must also be analyzed alongside LAS.

A **threat** is anything that can use a vulnerability to obtain access to, harm, or destroys an asset, whether deliberately or inadvertently.

Risk is the possibility of an asset being lost, damaged, or destroyed as a result of a threat exploiting a vulnerability

Possible consequences of successful attacks include:

- Distortion or modification of files/information.
- Disruption of network access.
- Unauthorized disclosure of information.
- Destruction of files or systems.
- Loss of human life.



3.3 General Communication System Operations

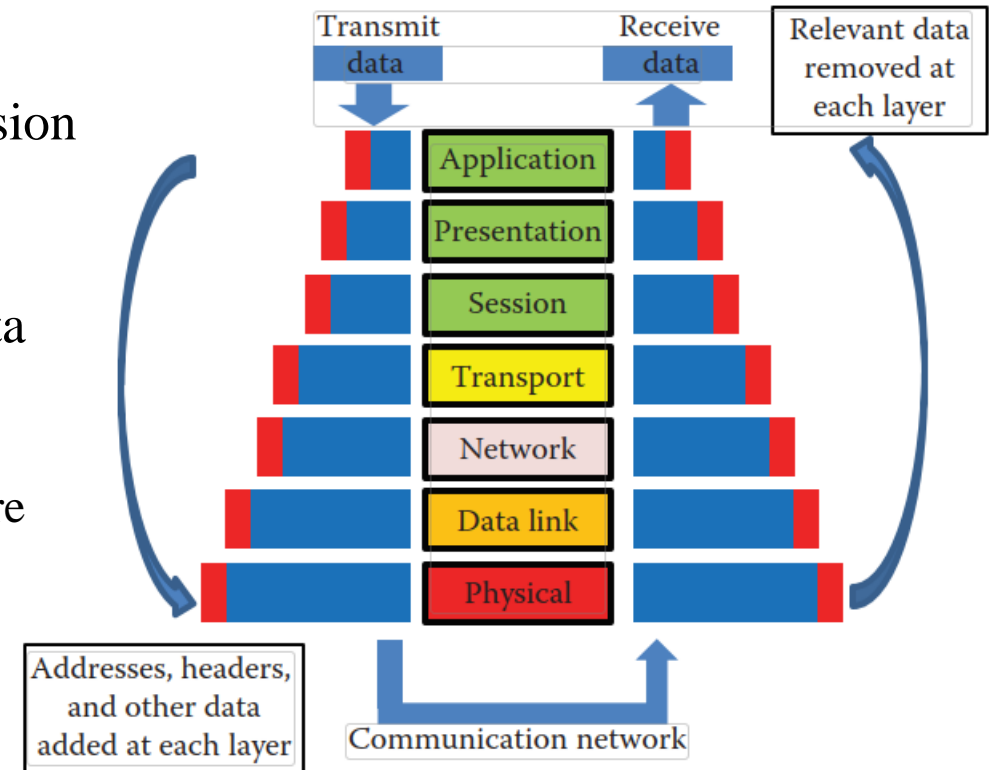
Industrial Control Network Role – Used for communication, monitoring, and control of devices/processes.

Data Initiation – A software application initiates a transmission (e.g., operator clicks to open a valve).

Packet Creation – Data/commands are packaged into a data packet.

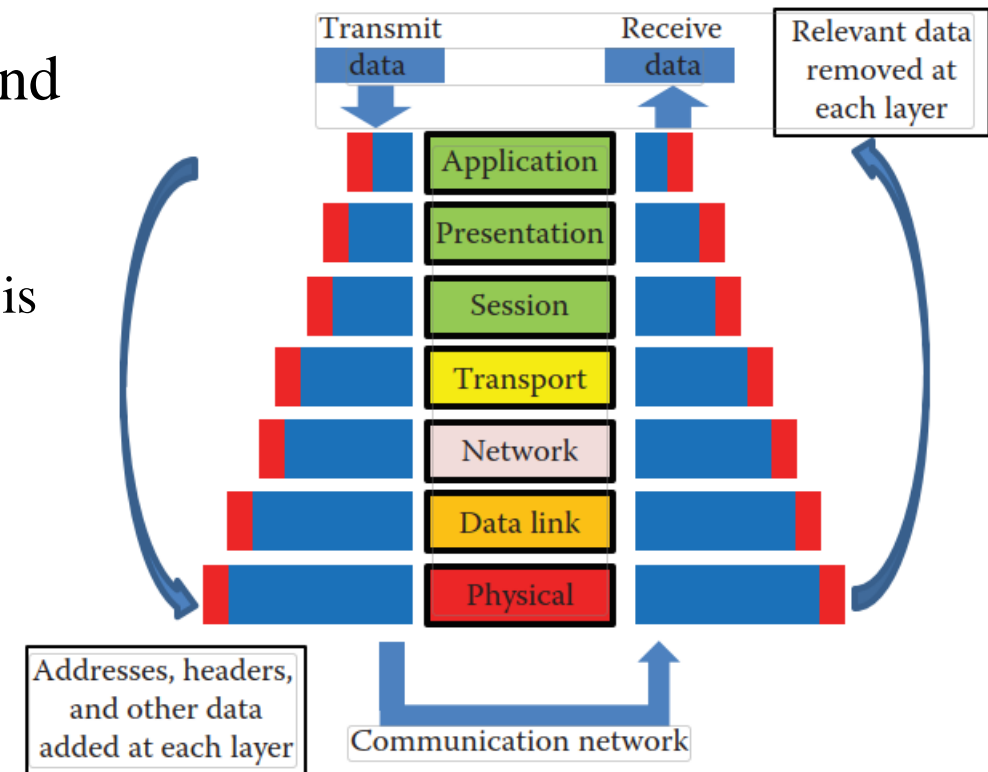
OSI Layer Processing – Packet passes through OSI layers where additional details (headers, addresses, identifiers) are added.

Transmission Medium – Final message sent via wired or wireless medium.



Reception – Receiving device gets the signal and reverses OSI process.

Data Handling – Headers/addresses are removed, and data is interpreted and executed appropriately.



FIGURE

General digital communication operation. (From Bihl, 2015.)

TABLE

Communication Layers per the OSI Stack with Descriptions and Examples

	Data	Layer	Description	Example
Host layers	Data	Application	Software to access network	End user
		Presentation	Applies formatting to data, encrypts data, and facilitates application layer interaction.	Syntax and data manipulation
		Session	Interhost connections and session establishment	Synching
	Segments	Transport	Connection protocols	TCP and host-to-host
Media layers	Packets	Network	Determines physical path for data routing	Packets and routing
	Frames	Data link	Transfer of signal between nodes via physical devices	Frames and MAC addresses
	Bits	Physical	Signals, transmission, communication, and reception over a medium; physical components/devices	Cables, devices, physical mediums, and transmission methods

- **Application Layer** – Operator/software initiates communication (e.g., click to open a valve).
- **Presentation Layer** – Data formatted, translated, or encrypted for transmission.
- **Session Layer** – Communication session is established, maintained, and managed.
- **Transport Layer** – Data broken into segments, error checking and reliable delivery ensured.
- **Network Layer** – Logical addressing and routing information (IP addresses) added.
- **Data Link Layer** – Frames created with physical addressing (MAC addresses) and error detection bits.
- **Physical Layer** – Actual transmission of bits over wired or wireless medium.
- **Reception (reverse process)** – Receiving device strips headers at each OSI layer, reconstructs original message, and delivers it to the application.

Scenario: An operator wants to **open a valve** in a chemical plant using an industrial control network.

- 1.Application Layer** – Operator clicks on valve symbol in SCADA software.
- 2.Presentation Layer** – **Command ("Open Valve")** is encoded into a standard protocol format.
- 3.Session Layer** – Communication session between SCADA system and PLC (Programmable Logic Controller) is established.
- 4.Transport Layer** – Data broken into TCP segments; reliability ensured.
- 5.Network Layer** – IP address of the PLC is attached for correct routing.
- 6.Data Link Layer** – Frame created with PLC's MAC address for delivery within local network.
- 7.Physical Layer** – Bits transmitted via Ethernet cable (wired) or Wi-Fi (wireless).
- 8.Reception (reverse process)** – PLC receives data, strips headers, interprets the command, and triggers actuator to physically **open the valve**.

3.4 Industrial Control Networks and Operations

- **Infrastructure** – Networks link devices and operators via wired/wireless systems.
- **HMI Role** – Provides graphics, animations, and schematics for operator interaction.
- **Control Systems** – SCADA, DCS, PCS, CPS manage data acquisition and control.
- **Reliability** – Industrial networks differ from commercial ones by requiring high reliability, low latency, and small packets.

Operations and Components

Four Layers – Process & field equipment → Devices (RTUs, PLCs) → Station/Substation → Enterprise.

Field Equipment – Sensors, actuators, instrumentation.

Devices – RTUs (collect data) and PLCs (control processes); often integrated RTU/PLC devices.

Enterprise Level – End user/operator oversight.

Communication Layer – Networks, protocols, and host software (e.g., SCADA) bridge field and enterprise.

Clients – Operators use HMIs to monitor/control.

Security – Firewalls and IDS protect against unauthorized access.

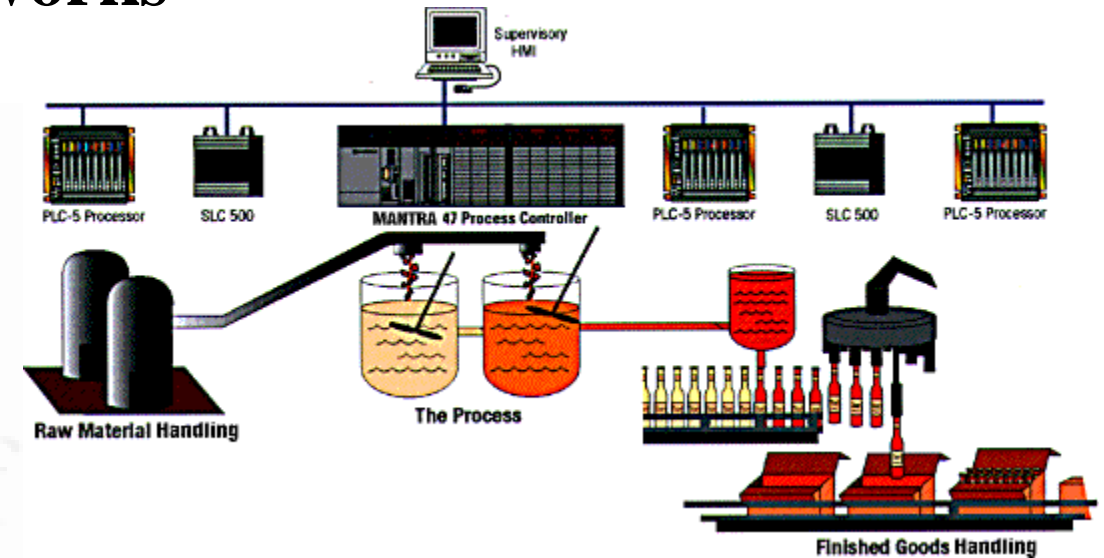
Interoperability – Different RTUs/PLCs and mixed protocols coexist; older devices often remain in use.

TABLE
Integration and Control (I&C) System Levels, per Dolezilek and Schweitzer (2000)

Level	Description	Example
Enterprise	Highest level, includes all end users who are inside or outside the substation.	Workstation at the corporate office.
Station/Substation	Third level, performs data acquisition and local input/output for the entire station.	Human machine interfaces, controller software, and decision support systems running on a local PC.
Device	Second level, contains PLCs and RTUs that collect and react to data.	Protective relays, meters, fault recorders, load tap changers, VAR controllers, RTUs, and PLCs
Process	Lowest level, connected to physical components for monitoring control.	Current transformers, voltage transformers, resistance thermal detectors, and transducers

Commercial Technology Inroads into Industrial Control Networks

- **Commercial Entry** → Industrial control networks (ICNs) now use **Internet pathways** + **COTS** (Commercial Off-the-Shelf) devices.
- **Old ICNs** → Initially isolated, security was secondary.
- **Internet Growth** → Direct & indirect links via Internet portals, mobile apps, etc.
- **IoT & Wireless** → Widely adopted in Critical Infrastructure (CI) systems for monitoring & communication.



• **Examples** → Smart grids, smart cities, e-government, hospitals.

• **Security Issues** → Many commercial standards/devices have vulnerabilities.

• **Big Data Factor** → IoT in CI creates high **volume, variety, velocity** of data.

• **Analytics Needed** → Security monitoring now requires big data analytics to detect threats.

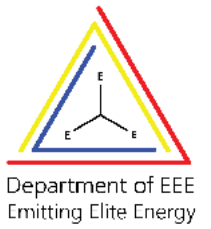


3.5 High-Level Communication System Threats

- **Purpose** → Understanding threats is key to choosing proper security measures.
- **Threat Categories** → Grouped by approach (taxonomy model).
- **Examples** → Source-based (physical vs. cyber), Agent-based (insider vs. outsider).
- **Adapted Taxonomy** → Simplified from Nawir et al. (2016):
 - Removed redundancy (info damage \approx access).
 - Added new fields (e.g., supply chain threats).
- **Defense Strategy** → Requires **technological** + **non-technological** solutions.



A T M E
College of Engineering



Thank You

