

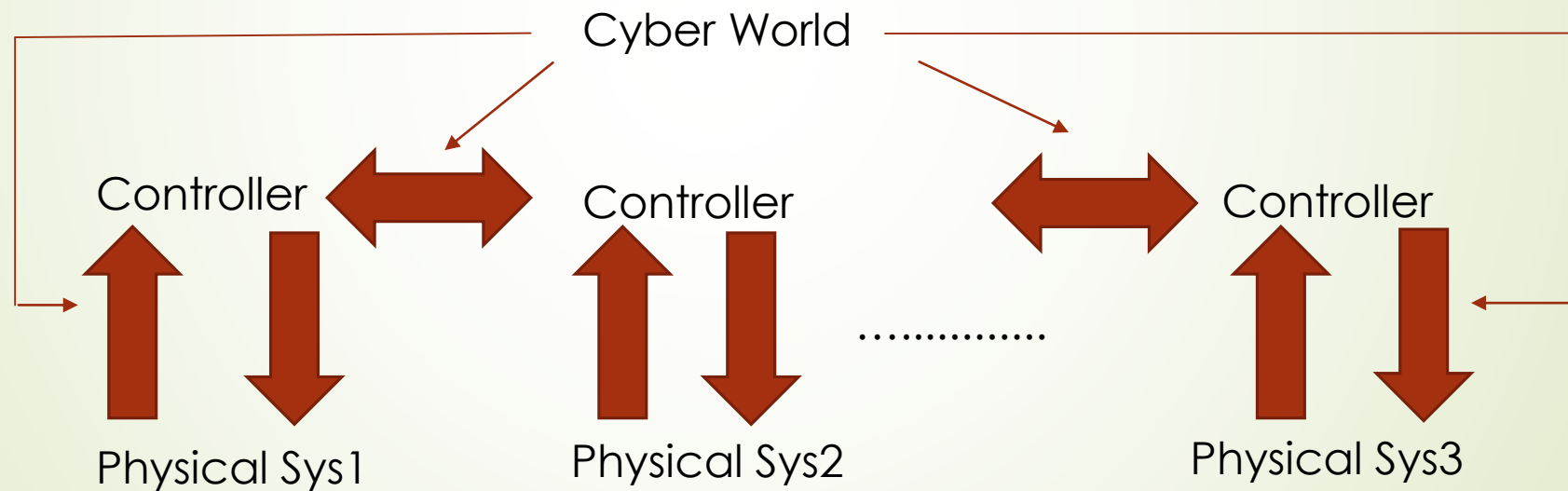


CPS Security : attack modeling and verifiability

Dr. Soumyajit Dey
CSE Dept, IIT Kharagpur

CPS vs Cyber Security

- CPS is not limited to “Hacking into computers over the Internet”
- The Physical part of “Cyber Physical Systems” creates more possibilities





Role of control theory

- CPS systems, owing to the physical part, can be modelled as control systems (plant and controller) with real valued variables and their gradients
- We can borrow analysis techniques from a whole lot of areas
 - Automata theory : discrete event simulation, formal analysis
 - (Convex) Optimization with variables from mixed domains (real and integers)
 - Queuing theory for NCS
 - Probabilistic Analysis for Almost Sure Guarantees



Safety Criticality : requirement of many CPS

- ▶ SmartGrid
 - ▶ Dynamical System state : power flow in electrical buses
- ▶ Nuclear Installations
 - ▶ Dynamical System state : position of cooling rods
- ▶ Connected Vehicles
 - ▶ Vehicle Dynamics, Surrounding behavior,
- ▶ Irrigation Systems (Network of Dams, Sluice Gates)
 - ▶ Dynamical System state : Water flow rates and water level
- ▶ Insulin Infusion Pump
 - ▶ Dynamical System state : Blood Sugar level




COVERAGE

We divide our coverage as follows

- **Attack Models**
- Control Theoretic modeling of attacks
- SCADA Systems and vulnerabilities



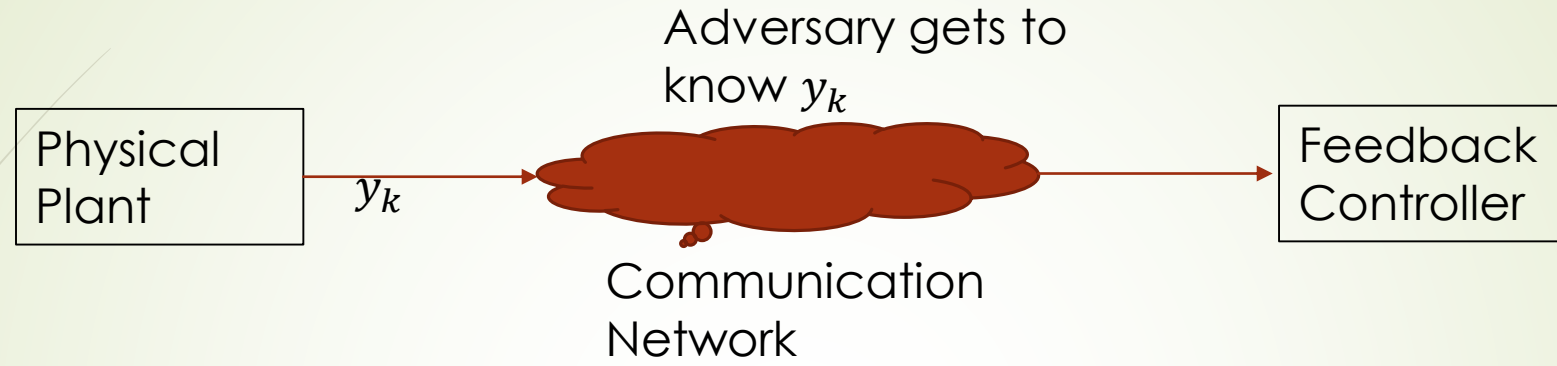
Attack Models



Attacks disturb Confidentiality, Integrity, Availability (CIA)

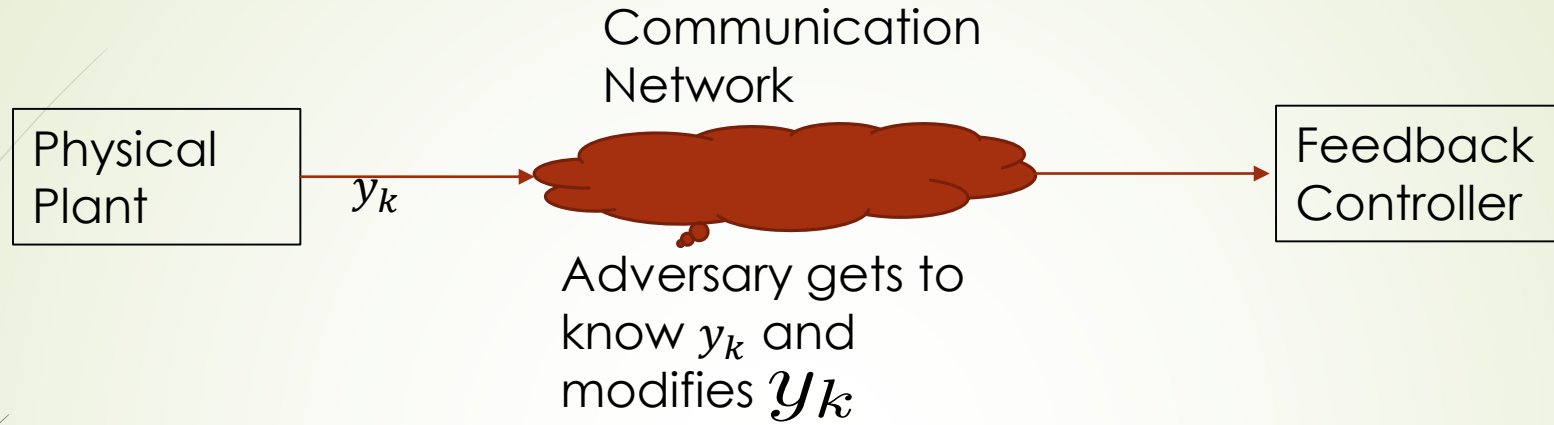
- Disclosure attacks : enable adversary to gather data sequences (intelligence gathering, no direct side effect)
 - Used to design harmful attacks like Replay attacks
 - Deception attacks : modify control action u_k and sensor measurements y_k without being detected
 - Disruption attacks : hold up suitable control actions (denial of service)
 - False Data Injection Attack.
-
- Objective : Drive system to an **UNSAFE** state

CIA



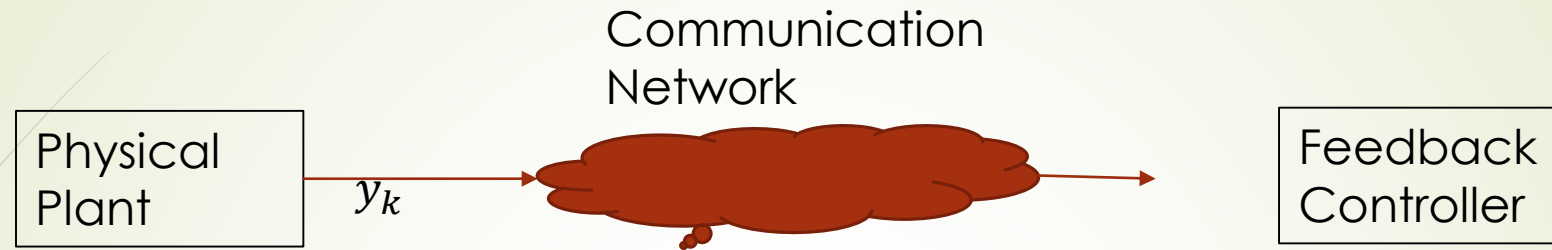
Disclosure Attack : violates confidentiality

CIA



Disclosure Attack followed by False data
Injections : violates data integrity

CIA



DoS : adversary closes down availability



COVERAGE

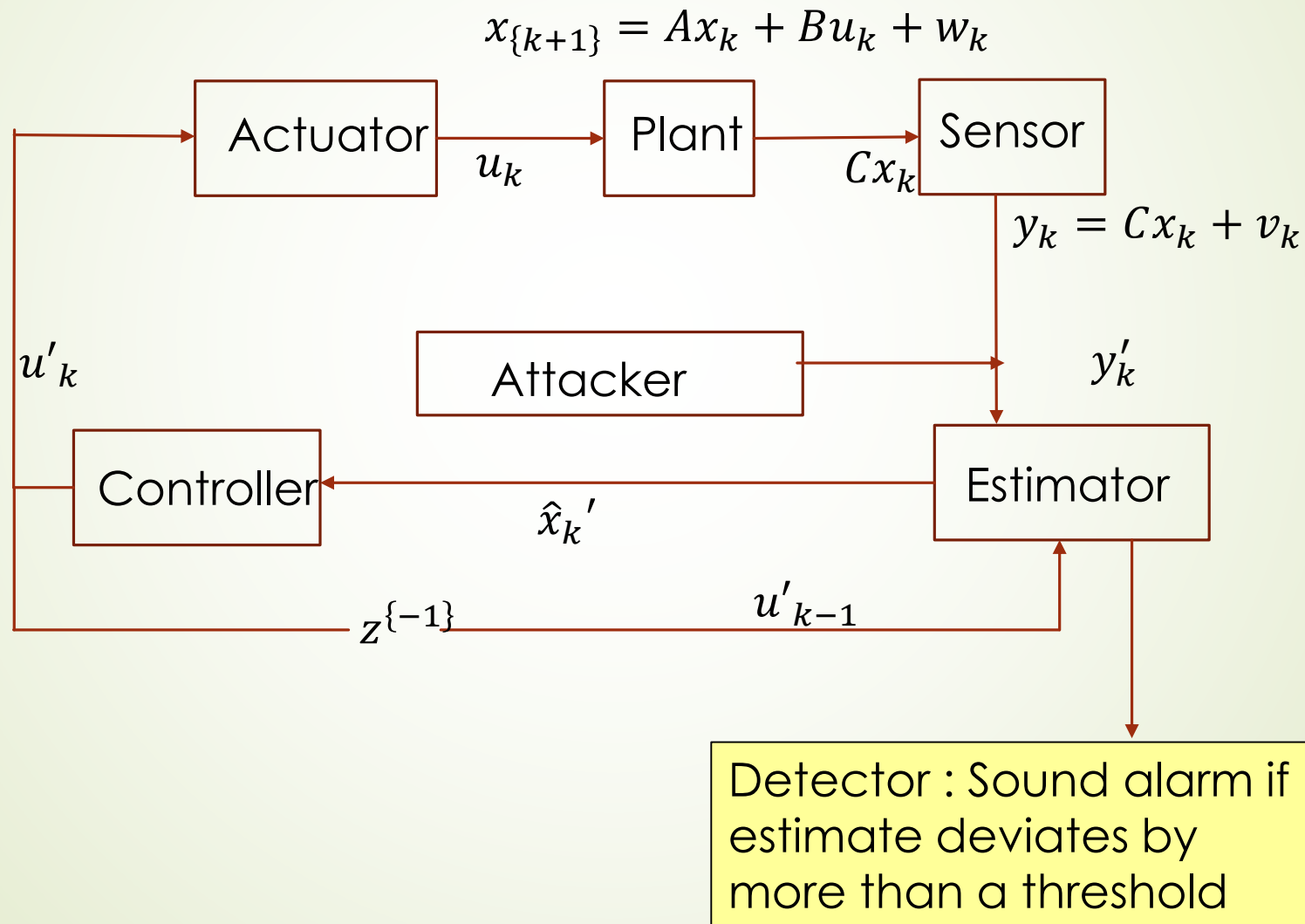
We divide our coverage as follows

- Attack Models
- **Control Theoretic modeling of attacks**
- SCADA Systems and vulnerabilities



Control Theoretic Attack Modeling n Risk Analysis

Control Theoretic Attack Model

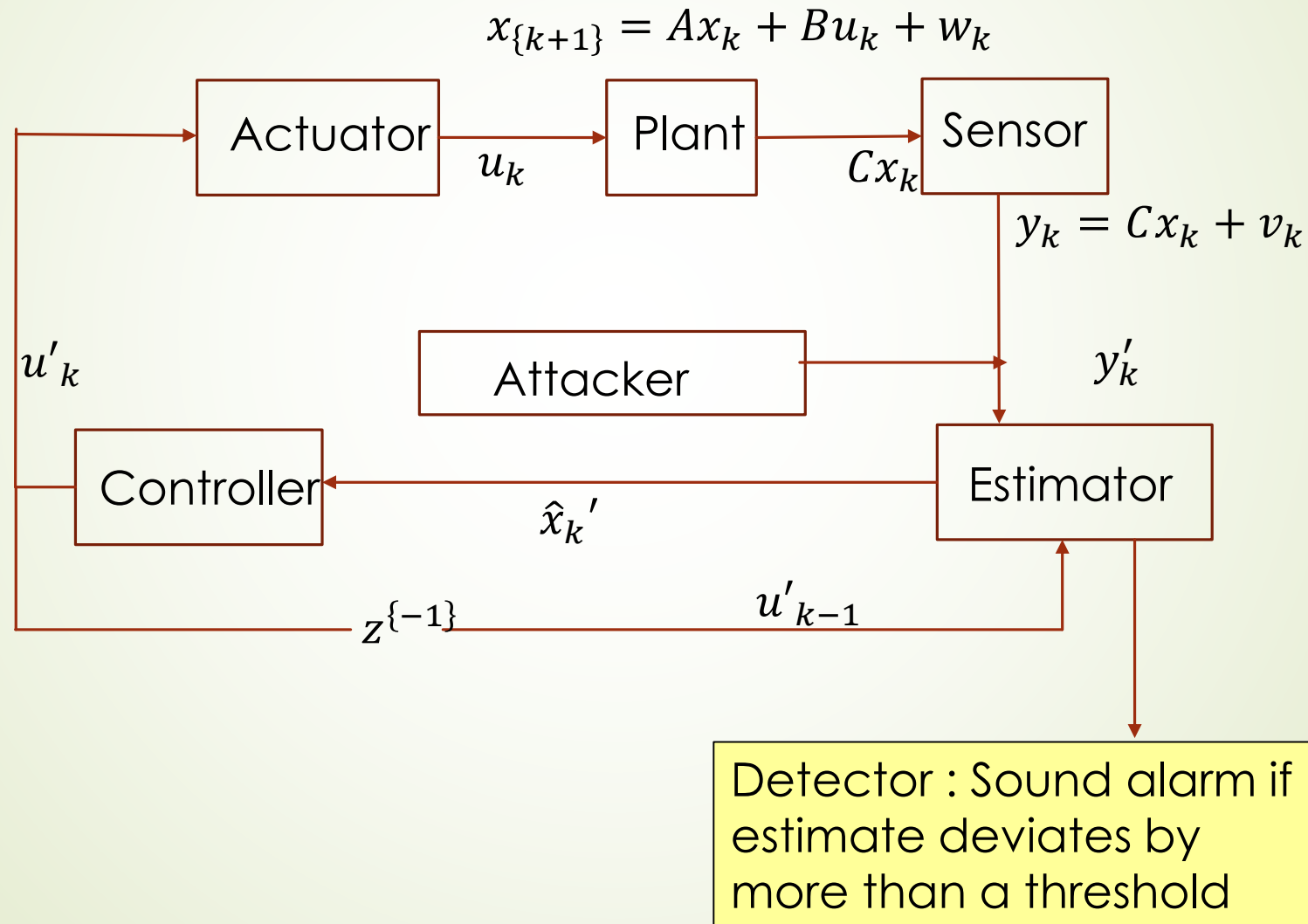




We focus on Replay type attack

- Assume : attacker wishes to disrupt the system in steady state
 - Inject exogenous control inputs (**w/o being detected**)
 - Observe and record readings and repeat them after some time
 - Hollywood movies : **thieves hack into security cameras, record and replay while performing the theft !!!!!!!!!!!!!!!!!!!!!!!!!!!!!**
 - However, control designers are not dumb
 - They will employ a **detector system**

Control Theoretic Attack Model





Success of Replay Attack

- The intruder should be able to insert sufficient number of false data packets
 - Drive system into unsafe state
- The false data packets should not deviate too much from estimated states
 - Then the detector will catch the attacker



COVERAGE

We divide our coverage as follows

- Attack Models
- Control Theoretic modeling of attacks
- **SCADA Systems and vulnerabilities**



SCADA Systems and Vulnerabilities

SCADA

- **Supervisory Control and Data Acquisition** (SCADA) systems are used to manage and automate processes in critical infrastructures
 - electricity grids
 - water distribution facilities
 - Industrial Automation



Figure 2: Upstream of the Avencq station with level sensor, offtake, and sluice gate with local controller.



Ex : Water distribution system

- Numerous parts of the world are now using automation methods for management of their water distribution systems.
 - For example, modern day irrigation systems are monitored and controlled by SCADA systems.
 - SCADA systems enable the management agencies to remotely *monitor* water levels and velocities at desired locations as well as *control* the water flow through automated hydraulic structures.
 - Based on the information gathered by level and velocity sensors, the control actions are generated by the SCADA system. Operators can also respond to *faults* by taking the necessary maintenance actions.
 - The architecture of SCADA systems for irrigation canal networks is similar to that of many physical infrastructure systems such as waste-water treatment plants, oil and gas distribution, and process control systems.



SCADA-based Industrial and Automation Control Systems

- According to the ISA definition, SCADA-based Industrial and Automation Control Systems (IACS) are structured into five distinct levels.
 - **Level 0:** reserved for the sensors and actuators
 - **Level 1:** contains devices such as Programmable Logic Controllers (PLC's) and Remote Terminal Units (RTU's)
 - **Level 2:** composed of supervisory control equipment's such as the Human-Machine Interface (HMI)
 - **Level 3:** for the Manufacturing Execution Systems (MES), such as the systems hosting production planning software
 - **Level 4:** for the remaining business related systems



PLCs

- An industrial digital computer which has been ruggedised and adapted for the control of manufacturing processes,
 - assembly lines,
 - robotic devices,
 - any activity that requires high reliability control
 - ease of programming and process fault diagnosis.



SCADA and Cyber-Attacks

- Probably the most vulnerable points of IACS infrastructures.
 - The interconnection of **level 0** and **level 1** devices (e.g . PLC's and RTU's) a
 - The interconnection of **level 1** devices with **level 2** devices (e.g. HMI's)
- **CYBERSECURITY** is currently one of the main concerns for SCADA and industrial control system (ICS) operators.
- A series of recent successful cyber-attacks against several targets:
 - such as electric power substations and distribution grids, sewage processing units, or even nuclear power plants.
- These have had far reaching impact, affecting a substantial number of persons, potentially causing significant damage and ultimately threatening human lives .



SCADA and Cyber-Attacks

- ICS typically incorporate sensors and actuators that are controlled by PLCs, and which are themselves managed by the HMI.
- Most SCADA network traffic is generated by automated processes and mainly for data acquisition, in the form of periodic polling of field devices.
- ICS network components
 - do not verify the identity and permissions of other components with which they interact (i.e., no authentication and authorization mechanisms)
 - do not verify message content and legitimacy (i.e., no data integrity checks);



Network based attacks against SCADA systems,

- Hijack the communication channels between the HMI and PLCs
- Manipulate the HMI-to-PLC queries going through **Modbus**
- Modbus is a de facto standard for ICS communication
- TCP port 502 is reserved for Modbus communications.



Modbus protocol

- The master device initiates transactions (called queries) and the slaves respond by supplying the requested data to the master or by performing the action requested in the query.
- Only one device can be designated as the master (usually the HMI) while the remaining devices are slaves (usually PLCs). A slave sends a response message for every query that is addressed to it.
- The Modbus protocol does not defend itself in any way against a rogue master that sends commands to slaves.
- Modbus only relies on TCP sequence numbers to provide session semantics and has no message integrity defences, thus TCP session hijacking is quite straightforward.

SCADA in Electrical Distribution

- An electricity supply chain is usually divided into three subsystems: generation, transmission, and distribution

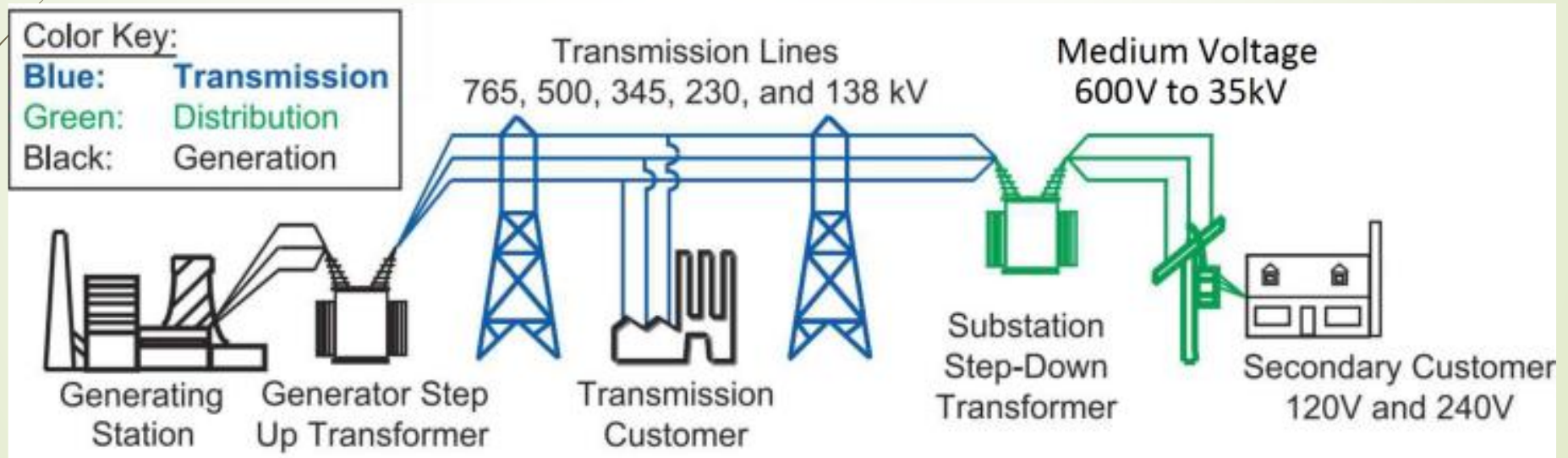



Fig. 1: Basic Structure of the Electric System (following [1])

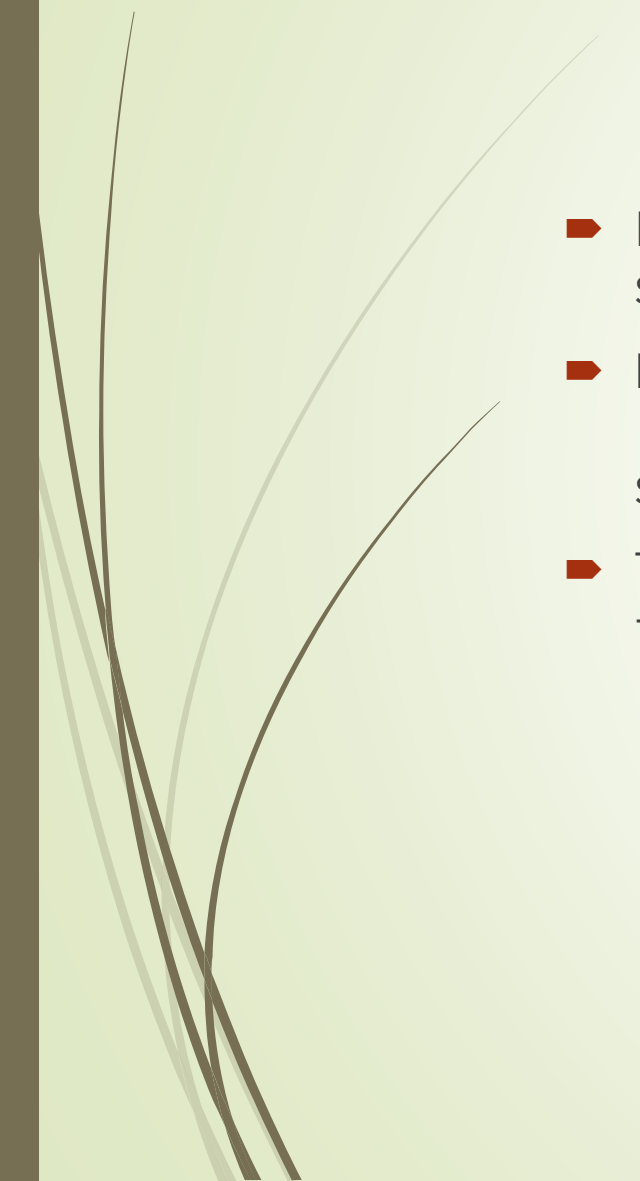


SCADA in Electrical Distribution

- 
- Electricity is transported along high voltage transmission lines (the transmission network) over long distances, from generation sites to major distribution points. The transmission lines are connected to distribution substations.
 - At a distribution substation, a substation transformer takes the incoming transmission-level voltage (138 to 765 kV) and steps it down to several distribution primary circuits (“medium-voltage” circuits, 600V to 35kV), which fan out from the substation.
 - Close to each end user, a distribution transformer takes the medium-voltage and steps it further down to a low-voltage secondary circuit (commonly 120/240V).



SCADA in Electrical Distribution

- For improved reliability, distribution circuits are often provided with “tie switches” to other circuits which are normally open (i.e., disconnected)
 - If a fault occurs on one of the circuits, the tie switches can be closed (connected) to let electricity flow into the faulted circuit, and to allow some portion of the service to be restored.
 - The tie switches can be operated either manually, or automatically from the SCADA system interface.
- 



Possible Adversary models



- The adversary has a Man-In-The-Middle (MITM) position between the HMI and all the PLCs.
- The adversary can inject, delete, and delay arbitrary packets with any source and destination addresses on the communication channels it controls.
- The adversary can also replay previously overheard messages, or manipulate messages in transit.



Possible Adversary models

- Modify message length - SCADA-aware anomaly detection that has even minimal Modbus understanding can flag messages with unusual lengths.
- Injecting messages into a hijacked connection is also detectable.
- Zero Values Deception Attack
 - attacker simultaneously changes the values of the registers that hold the current and the voltage reported by PLCs to zero.
 - This view is consistent with a natural fault – and causes the operator to implement unneeded remediation.



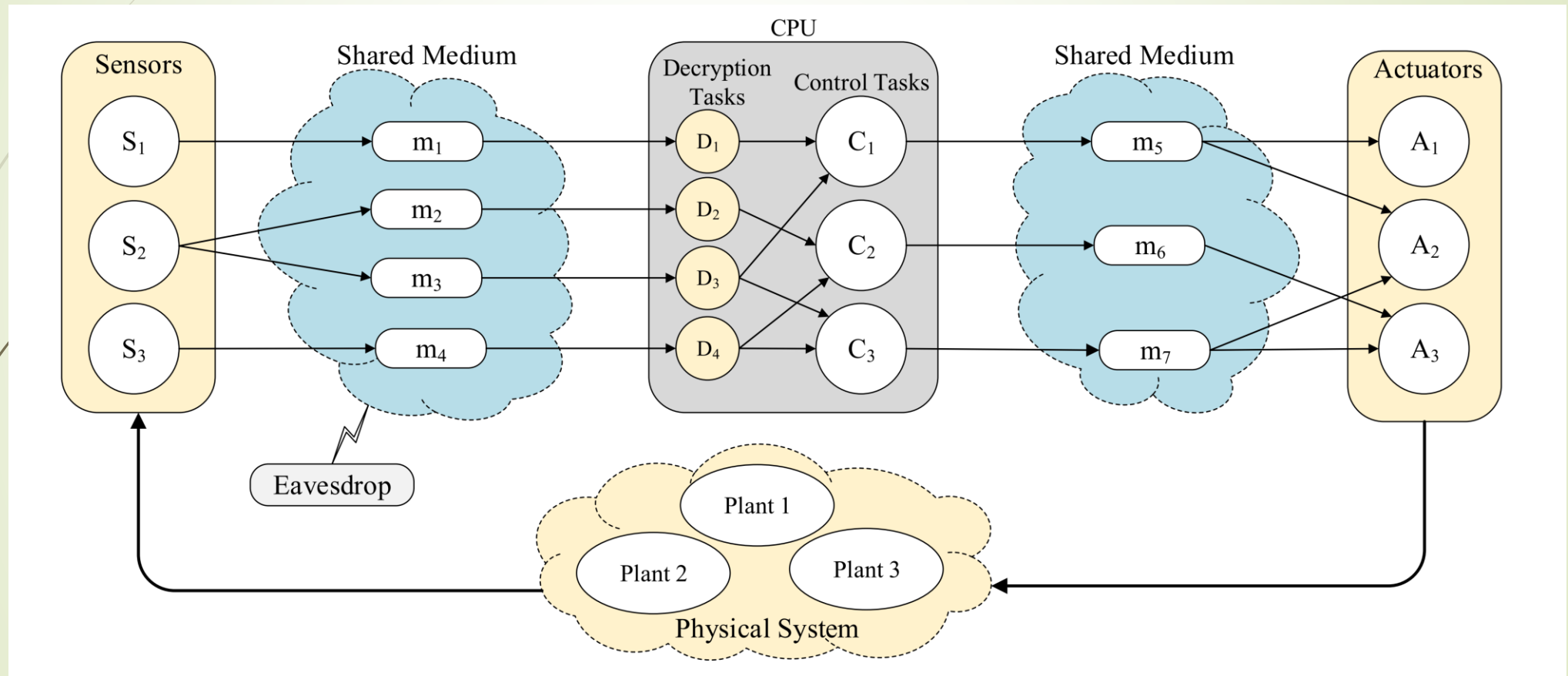
Multi stage Attack

- Zero Values Deception Attack motivates the operator to start disconnecting and reconnecting switchgears according to the operating procedures.
- Whenever the operator issues a switchgear open/close command, the attack tool replaces it with the opposite command.

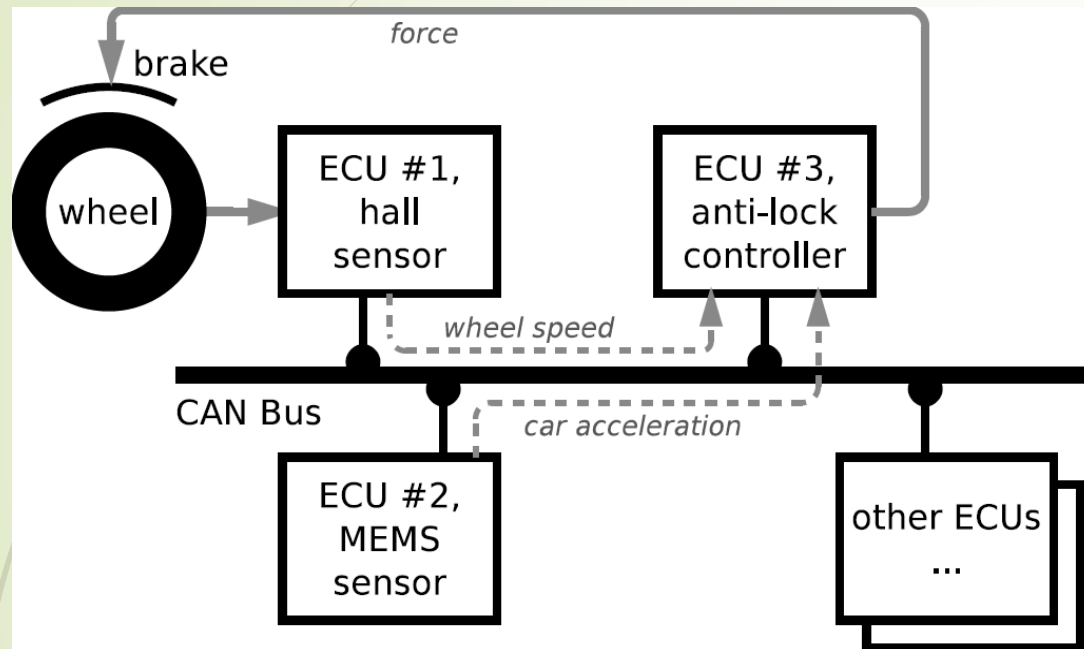


Some related topics

Securing Software based control in CPS



Securing Software based control in CPS

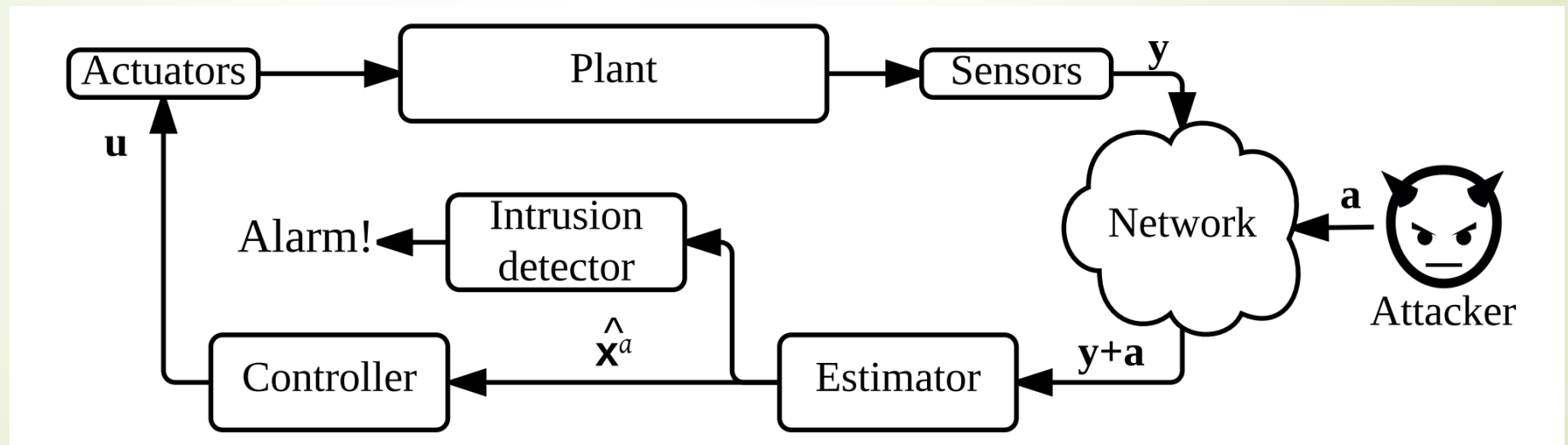


Anti-lock braking system with distributed sensors and controller

- Automotive control loops like ABS operate at a high speed
- Most such control loops are safety critical in nature
 - ABS
 - Suspension control
 - Transmission control
 - Fuel Injection control
 -

ABS hacking

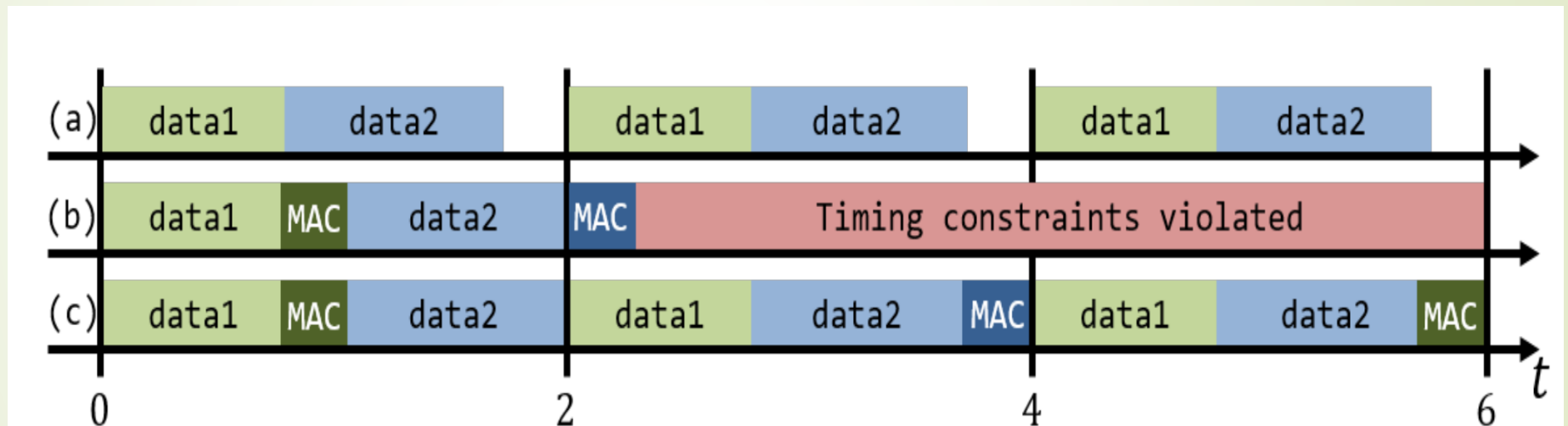
- If the speed sensors of a car suffer remote attacks and provide false speed readings to a vehicle ECU, an emergency functionality like braking gets compromised



“Sporadic Data Integrity for Secure State Estimation ” - Ilija Jovanov, Miroslav Pajic

Securing ABS messages

➤ How about securing such messages ?



"Sporadic Data Integrity for Secure State Estimation" - Ilija Jovanov, Miroslav Pajic



Sporadic data integrity

- ▶ How do we decide what is a good period for message encryption such that
 - ▶ Control loop safety and stability is not violated
 - ▶ Control loop performance is not compromised for long
 - ▶ Sensor data with sporadic encryption remains schedulable

Using PUF based security in ABS control loop

