A tool to detect abnormal events and cyberattacks

Konstantinos Lessis, WINGS ICT SOLUTIONS,
George Agapiou, Scientific Coordinator of Hellenic Branch of FITCE

Overview of Presentation

- General aspects
- Role of tools in protection from Cyberattacks
- Intelligent gateways with IoT sensors (tools used for cyberattacks)
- Cybersecurity
- Processes Involved
- Key takeaways

What is Cybersecurity

What it is

Cybersecurity is an ongoing process that takes action to protect transmitted data, unauthorized access and other malicious attempts from intruders, acts just as an umbrella that protects us from rain

What it does

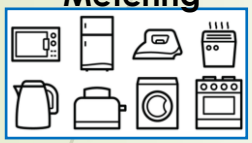
- Protects the digital world (computers, transmitted data) from intruders
- Detects threats
- Identifies vulnerabilities (prediction and prevention)

Role of tools for detection of cyberattacks

Pulses, Wireless/Wired M-Bus, RS232, RS485, serial, analogs, SDI12

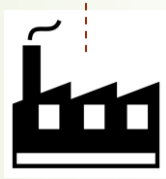
5G (B5G), 4G, NB-IoT, GPRS, Cat-M, LoRa

Sensors / **Metering**



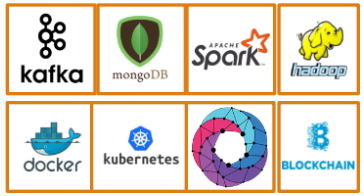
Residential
Business
Buildings (appliances)

ARTEMIS Gateway



Industrial environments

Public Private Hybrid



CAPABILITIES

- ✓ **Faults:** faulty meters, outage.
- ✓ **Security:** false data detection, anomaly detection, power thefts, physical intrusion.

Tools to protect from cyberattacks

- 5G modem
- Sensors
- Graphical tools

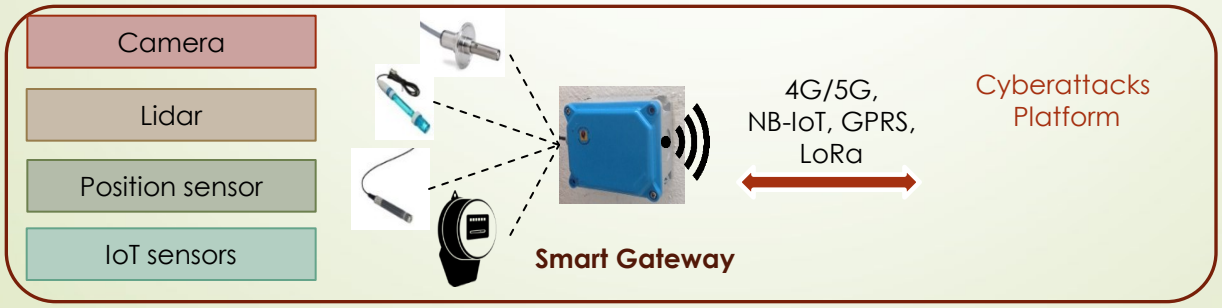
Smart Gateway for intelligent control through IoT Sensors

WINGS Smart Gateway capabilities:

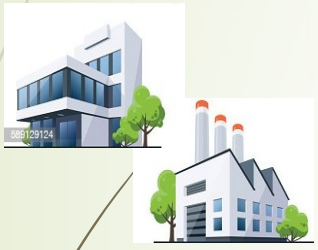
- Interfaces to IoT sensors and transmits data & measurements over any available network (5G, NB-IoT, GPRS, LoRa)
- Over the air parameterization and customization of user defined measurement and transmission profiles
- Versatile interfacing based on variety of protocols (pulse-counting, Wired/Wireless M-Bus, OMS etc.)
- Edge Computing capabilities, identifying alerts at local level and adapting measurement and transmission profiles accordingly (e.g., more frequent measurements /transmissions in case of alerts – push notifications)
- Remote management capabilities (e.g., firmware updates)
- Alerts for meter / gateway tampering and violation

Benefits of using Smart Gateway:

- Lower cost per sensor compared to commercial connected devices (e.g. NB-IoT devices)
- Modular approach: one module for any type of sensor, with lifespan longer than the life expectancy of the meter/sensor
- Simultaneous Connection with multiple sensors
- Connection to existing sensors without replacing/upgrading the entire network (high CAPEX)



Cybersecurity



Data ingestion

CYBERSECURITY

- Ensuring correct data from measurements
- Ensuring correct predictions
- Ensuring proper decisions / recommendations

HOW TO ACHIEVE CYBERSECURITY

- Analysis of patterns
- Anomaly detection
- Mitigation measures

Cybersecurity

SCOPE

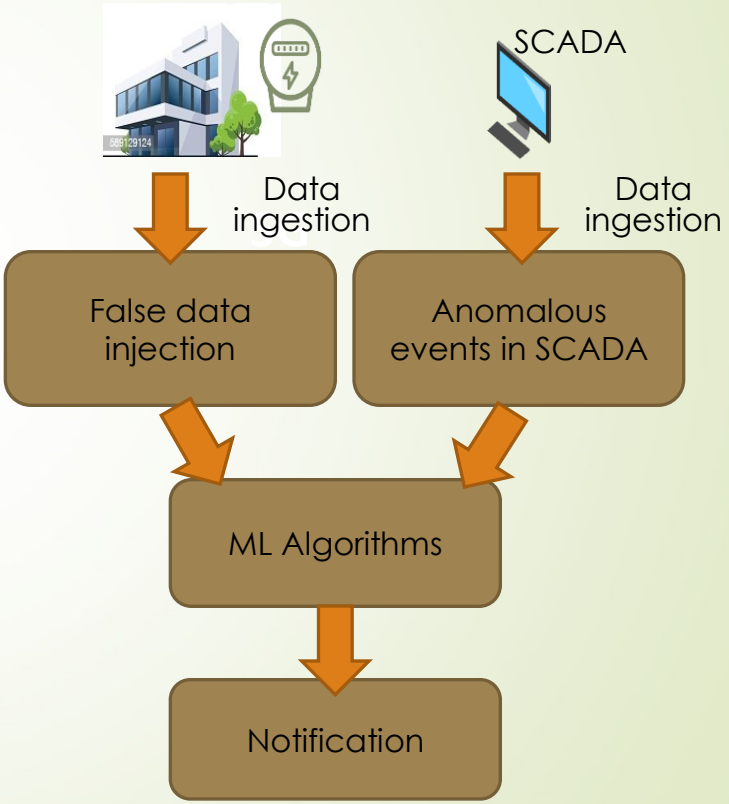
Notify the platform operator (end-user) regarding potentially dangerous situations

Forecast possible threats based on real-time event sequence

Rate possible sequence events as:
- Normal / Informational,
- Alarm
based on input-events' statistical distribution

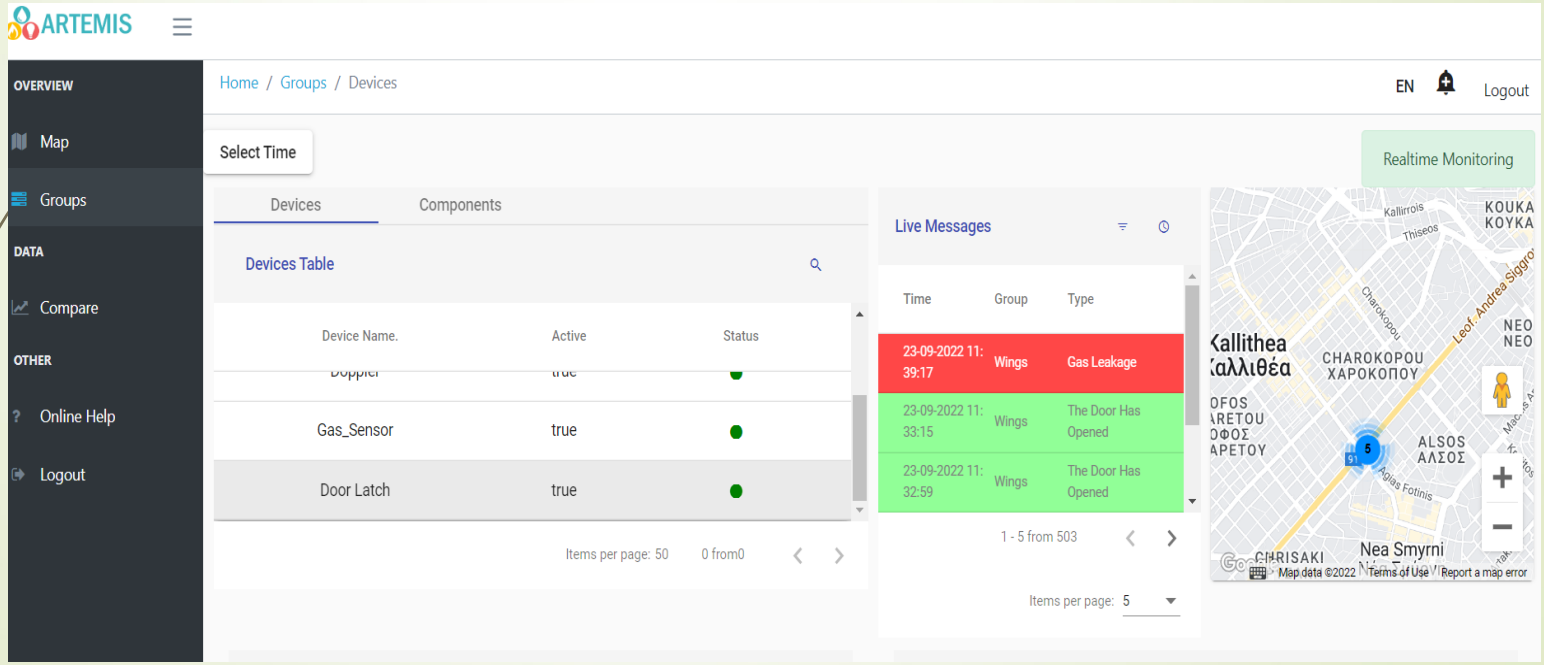
Cybersecurity

- **Suspicious event detection:**
  - Detection of False Data Injection Attacks: detection of abnormal sensor's data that has been intentionally altered to cause damage to equipment or get benefit by cheating (e.g. energy theft)
  - Detection of anomalous events and traffic in the system: analyze traffic flow of the network in order to identify attacks. Analyze data from controllers, valves, motors (e.g. pressure, temperature, speed, flow-rate, energy consumption) to identify anomalous behavior.



Physical Security

- The gateway reads the "FIELD" Sensors and other Event generating modalities (Cameras and Camera Analytics, Wireless Presence Detectors, Flame and Gas Detectors etc.) and after processing (via Machine Learning Algorithms) can issue warnings and alarms.



Processes involved

Sensors and Actuators

1. Water Quantity and Quality Control

- a. *Physical (Flowrate, Pressure, Conductivity, Temperature)*
- b. *Chemical (pH, ORP, Chlorine)*

Communication Technologies

2. Data Collection and Transmission

- a. *Protocols (Modbus, DNP3, IEC 870-5-104, MQTT, CoAP, lwM2M)*
- b. *Technologies (4G-5G, NB-IoT, GPRS, LoRa/LoRaWAN, Zigbee, Sigfox, Bluetooth)*

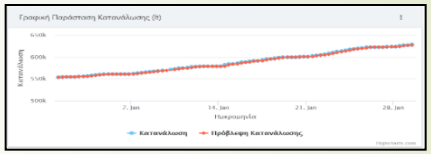
Artificial Intelligence

3. Analytics and Decision Making

- a. *Behavior monitoring*
- b. *Disease diagnosis*
- c. *Intelligent feeding*
- d. *Feed waste management*
- e. *Water quality management*

Dashboard

4. Real time monitoring, Data visualization



Uses Cases

- *Inland, Coastal, Offshore production*
- *Fish, Shellfish, Seaweed*

Benefits

- *Increase production*
- *Minimize costs*
- *Ensure animal welfare*
- *Increase product quality*
- *Minimize environmental impact*

Key Takeaways

- Cybersecurity is a pivotal task in todays network systems
- Data analytics and IoT sensors play a crucial part for identifying threads
- Robust security means, monitoring E2E systems and prediction means through ML modeling are the means to protect systems and data

Thank you

George Agapiou –
Scientific Coordinator FITCE Greece