Cyber Secure Sensor Network

For Fossil Fuel Power Generation Assets Monitoring DE-FE0031666

Project Description and Objectives

- **Project Objective**
  - ❑ Develop technology framework for integrating cyber security solutions with sensors that are deployed in fossil fuel based power generation plants
  - ❑ Respond to DOE FE Area of Interest (AOI) I: Sensor & Control Technology Development for Cyber Fossil Power
  - ❑ A paper study that includes comprehensive analyses of potential approaches to reduce cyber risks for power generation assets
- **Status at the beginning of project**
  - ❑ Cybersecurity technology gap analysis (current solutions versus desired solutions)
  - ❑ Effective cyber monitoring framework development based on advanced data analytics
  - ❑ Overview of technology development processes for sensors with extreme environment capabilities

Project Description and Objectives

- ❑ High temperature capable wireless telemetry design for data transfer inside power plant
- ❑ System Integrations, technology stack selection issues for an on-premise installation
- ❑ Feasibility study of cloud adoption in the future

- **Technology benchmarking & Results Validation**
  - ❑ Test results show developed security monitoring framework is a more effective solution for detecting plant operation anomalies
  - ❑ Comparative analysis shows advantages of cloud-based plant monitoring (uncompromised security, better availability and scalability, lower operation cost)
- **Current Project Status**
  - ❑ Collaboration with Siemens Energy. Technology components are validated in Siemens ICS lab, and are already deployed in existing on-premise installations

Project Update

- **Development Power Plant Security Monitoring Framework**
    - ❑ Data analytics based
    - ❑ Results validated in ICS labs in consultation with Siemens Energy
    - ❑ Technology components already deployed in on-premise installation
    - ❑ Feasibility of Cloud Adoption is evaluated

- **Key Challenges**
    - ❑ Disconnected data repositories from both IT and OT sources
    - ❑ Solution supports every protocol and standards (IT and OT)
    - ❑ Solution supports network including OT devices (field level, SCADA systems)
    - ❑ Real time monitoring objective requires low latency processing solutions
    - ❑ Rarity of OT incidents data (not released) requires suitable detection methods
    - ❑ Balance of system user's confidence and the false alarm rate (FAR)

Project Update

- **Data Sources – most relevant**
  - ❑ ICS event log files (SCADAs, PLCs)
  - ❑ Industrial network data (Syslog, packets for DPI, network traffic statistics)
  - ❑ Process data (readings from sensors, data associated with process tags, actuation commands, status information)

- **Data Processing**
  - ❑ May requires open interface OPC UA for accessing data historians
  - ❑ Data conversions required for deadbands data to ensure fixed data sampling rate
  - ❑ Efficient data storage technology required for real time data processing
  - ❑ Consistent timestamp among different data sources, so data can be combined
  - ❑ Data sources must be available for data analytics processing during training/testing of solutions and during the production

Use Case I

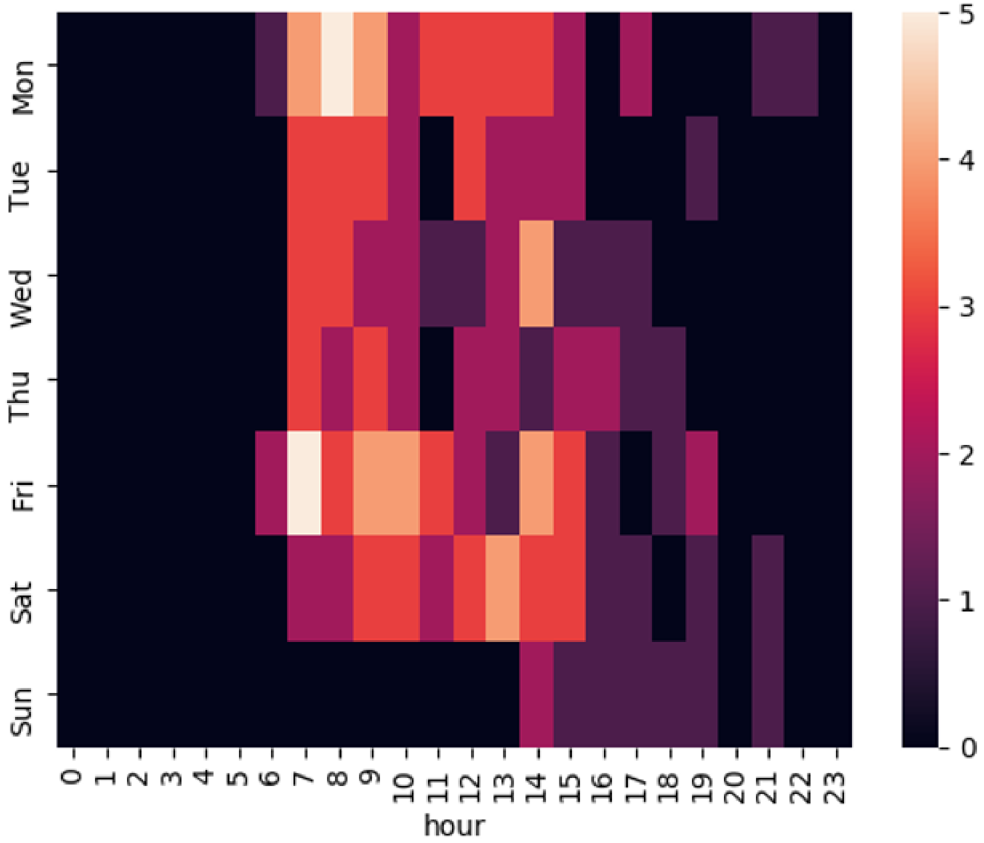

Figure 14. Normalized frequency of operator actions aggregated by weekday and time of day

- Operator access time anomaly detection
- Relies on the Hypothesis: operations requiring high access levels occurred only or mostly during regular office hours
- Data analysis are done on log files containing recording operator actions with corresponding timestamps

Use Case II

- Log Data Anomaly Detection
- Two types of logs are combined: operator actions with alarms
- Use LogCluster algorithm to implement data clustering
- Categorical information transformed into numerical inputs by counting frequency of their occurrences
- Multivariate distance methods used for anomaly detection

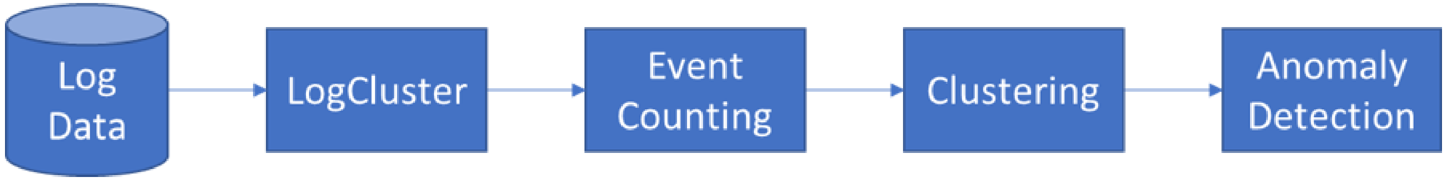

Figure 15. Processing pipeline for log data anomaly detection

Use Case III

- Process Anomaly Detection
- Implementation based on unsupervised learning models, i.e. clustering using the sensor information directly as inputs
- Pre-processing steps use dimension reduction methods, e.g. PCA, or autoencoder neural network
- Regression models can be created to represent input-output relations, anomaly detections can be applied to the residuals
- Lessons Learned: anomaly detection based on process data would be more effective if correlated with additional inputs from IT/OT domains
- Lessons Learned: process variables selection for OT environment anomaly detection should be aware of its contexts (e.g. type of variables affected by known attack vectors)

Future Outlook

Market Benefits/Assessment

- Advanced industrial cyber attacks require advanced cyber defense capabilities
- Advanced OT security monitoring makes an organization more cyber mature than current security technology, e.g. firewall, IDS/IPS, SIEMs
- Developed data analytics based monitoring framework can be easily integrated with existing security operation expertise and installations

Technology Challenges

- More robust sensor wireless telemetry operations in harsh power generation environment
- More intelligent and effective detection methods to reduce FAR
- More cloud adopted monitoring solutions due to its scalability, availability, and security

Concluding Remarks

- Thanks DOE for the funding of the project DE-FE0031666
- Project provides a technology framework for developing mature security monitoring solutions for power generation assets
- Developed technology framework enhances a power plant’s cybersecurity operation capabilities