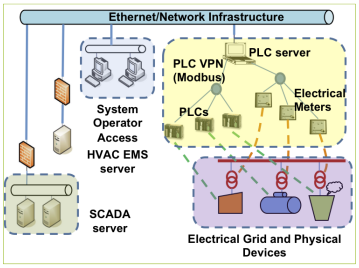
TCIPG

Functional Security Enhancements for Existing SCADA Systems

Intrusion Detection Based on Verification of Hybrid Automata Models

Georgia Koutsandria and Anna Scaglione

GOALS



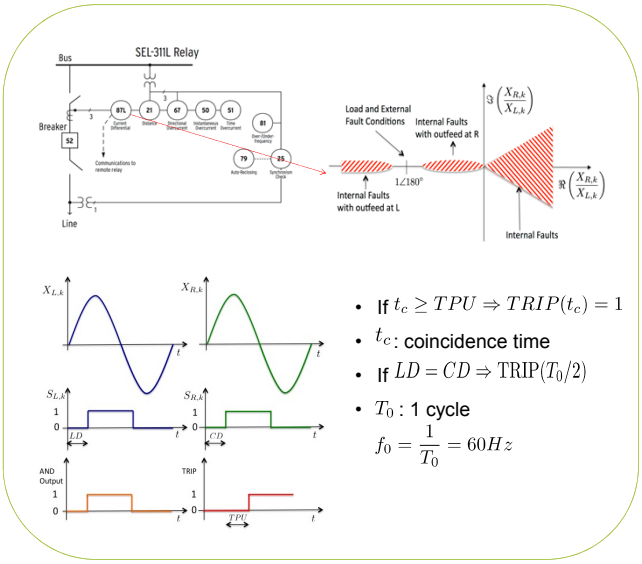
- Supervisory Control and Data Acquisition (SCADA) systems: control and monitor industrial/critical infrastructures such as the power grid.
- Network intrusion detection systems (IDS): identification of malicious actions by monitoring and analyzing the network traffic.
- Our goal: **determine and develop effective security enhancements that could guarantee the stability of the system and moderate the system's vulnerability to malevolent attacks.**
- Our idea: system identification and intrusion detection of any potential jeopardy based on the expected behavior of the system.

FUNDAMENTAL QUESTIONS/CHALLENGES

- Can we predict/prevent a hazard by taking into account the anticipated performance of a system?
- What are the interactions between the different components within a SCADA system?
- What are the physical policies and conditions that should be satisfied in order to ensure the normal secure operational state of the system?

RESEARCH PLAN

- Analyze existing industrial devices/relays (ex. SEL-311L relay) and commonly used protection schemes.



- If $t_c \geq TPU \Rightarrow TRIP(t_c) = 1$
- t_c: coincidence time
- If $LD = CD \Rightarrow \text{TRIP}(T_0/2)$
- T_0 : 1 cycle

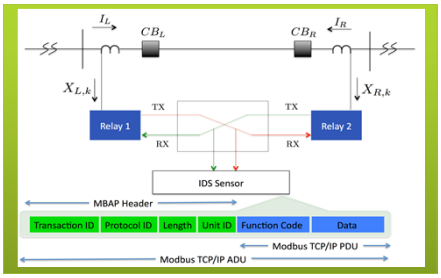
$$f_0 = \frac{1}{T_0} = 60Hz$$

- Define physical models and their corresponding automata, and implement them on a programmable logic controller (PLC).
- Develop rules of permissible device actions.
- Develop intelligent anomaly detection techniques.
- Monitor in real time the network traffic, confuse the system, and detect intrusions or malicious actions.

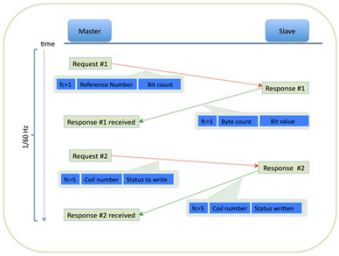
[1] **Modern Solutions for Protection, Control, and Monitoring of Electric Power Systems.** *Edited by Héctor J. Altuve Ferrer and Edmund O. Schweitzer, III.*

RESEARCH RESULTS

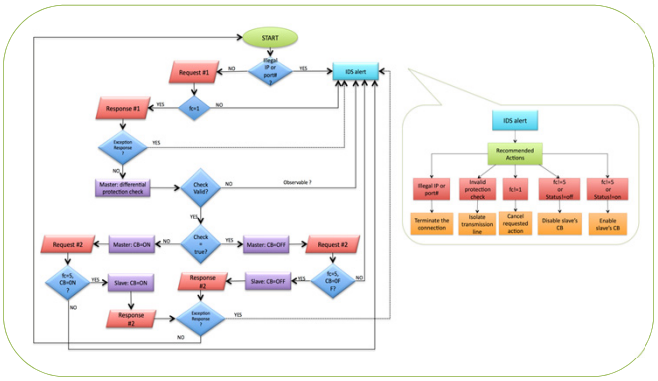
- Single transmission line with two relays.
- Current differential protection:
  - Equal and in phase current magnitudes: $\frac{\tilde{X}_{R,k}}{\tilde{X}_{L,k}} = 1\angle 180^\circ$
  - Local current: $\tilde{X}_{R,k} = X_{R,k}\angle\theta^\circ_{R,k}$, where $X_{L,k} = I_L(t_k)$
  - Remote current: $\tilde{X}_{L,k} = X_{L,k}\angle\theta^\circ_{L,k}$, where $X_{R,k} = I_R(t_k)$



- **Expected packet sequence exchange**
  - Protocol ID: zero for Modbus TCP/IP
  - normal response: MSB=0
  - exception response: MSB=1
  - packet exchange on specific frequency (1 cycle)
  - fc 1: read coils
  - fc 5: write single coil



- **Expected system behavior**



BROADER IMPACT

- The same approach for intrusion detection can be applied to current existing SCADA systems.
- System identification based on the expected behavior can be used for control systems that follow a specific pattern of actions/events.

INTERACTION WITH OTHER PROJECTS

- TCIPG's Specification-based IDS for the DNP3 Protocol.
- CEDS project with Lawrence Berkeley National Lab (LBNL).

FUTURE EFFORTS

- Define more complicated physical models for the Modbus TCP/IP and the corresponding hybrid automata, and implement them on a PLC.
- Determine and implement effective mitigation techniques that could ensure the stability of the system.

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T