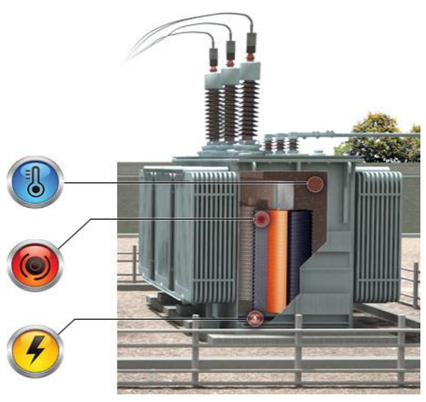
TCIPG

Functional Security Enhancements for Existing SCADA Systems

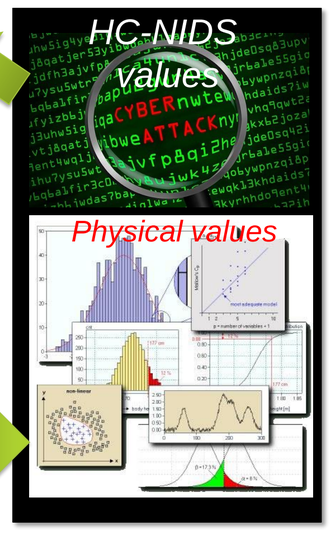
Cyber-Physical Data Analytics Based on "Hybrid Control" Network Intrusion Detection

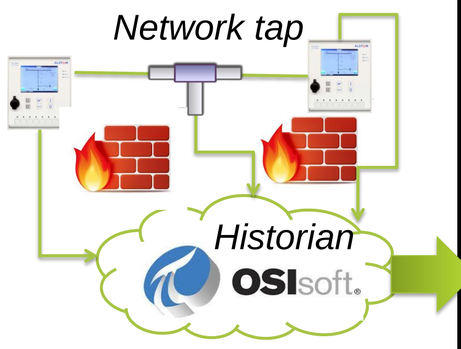
Georgia Koutsandria, Masood Parvania, Reinhard Gentz, Mehdi Jamei, Vishak Muthukumar
Researchers: Masood Parvania, Sean Peisert, Chuck McParland, and Anna Scaglione

GOALS



Cyber-Physical Process Control Data Analytics





- Design is "physics-aware" Network Intrusion Detection System (NIDS) for process control.
- Integrate NIDS cyber-physical state analytics within the process data historian in EMS.

FUNDAMENTAL QUESTIONS/CHALLENGES

- Control environments include physical systems, switches, and control programs.
- CONTROL: receive data from field devices → process → decide → issue switching commands.
- The combination of the safe operations of the protective schemes and the physical assets can be described by a Hybrid Automaton model.
- **Basic question:** Can we use such models as the baseline for "safe" behavior and use any set of message and command that is inconsistent with that as the indication of an attack/anomaly?

RESEARCH PLAN

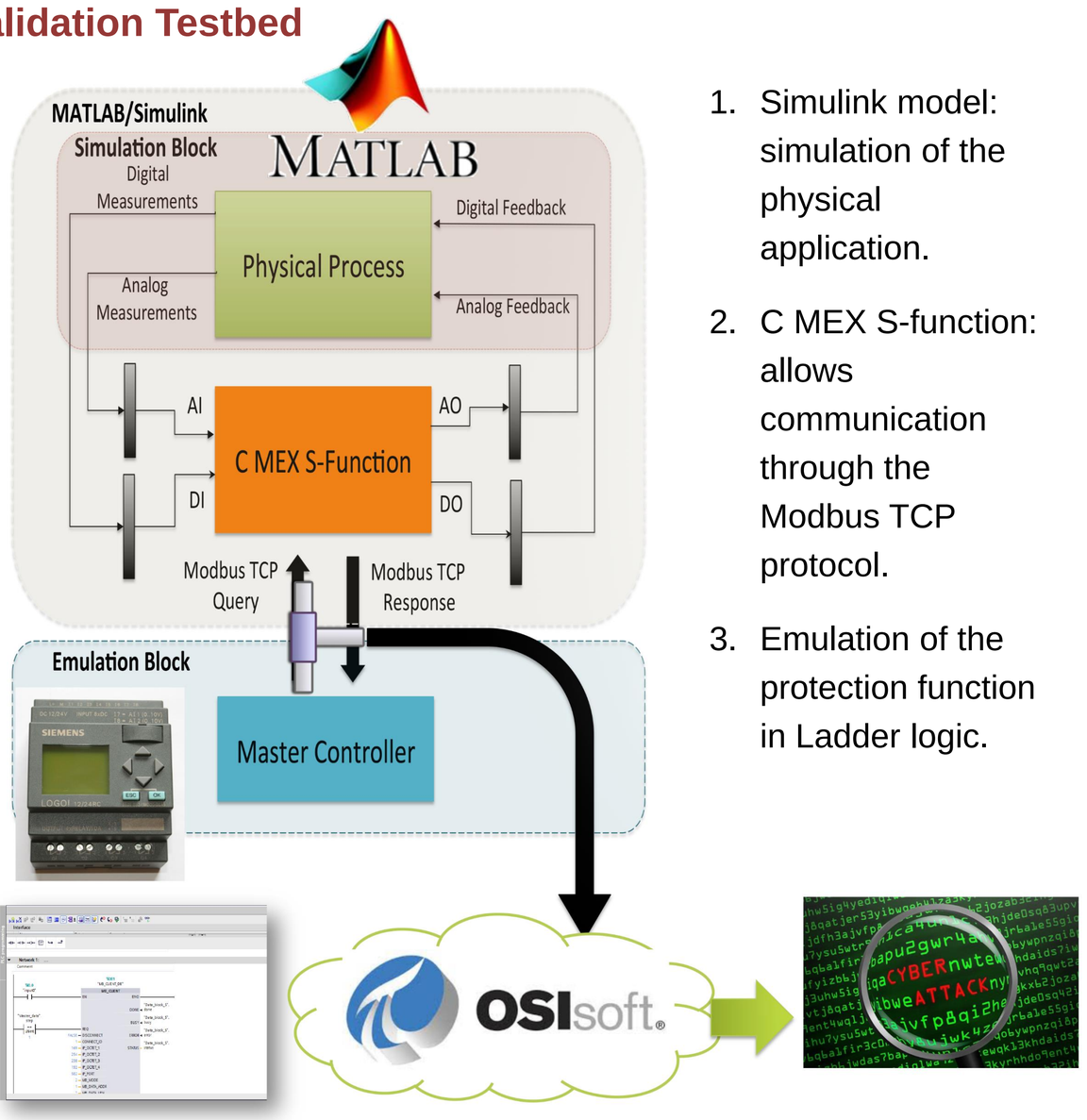
- **Design methodology for Hybrid Control NIDS (HC-NIDS).**
  - Each hybrid state corresponds to specific values for the switches and specific ranges for the current, voltage, temperature, etc.
  - Transitions between hybrid states are triggered by physical changes and commands.
  - Network packets, flowing between field devices and central controllers, should only produce "allowed" transitions and "allowed" hybrid states.
  - HC-NIDS continuously monitors and analyzes the network traffic exchanged by field devices that are used to activate the protection schemes.
  - **HC-NIDS Rule generation** → commands and information exchanged must be consistent with the protection hybrid automaton model.

RESEARCH RESULTS

- **Validation of Hybrid Control NIDS (HC-NIDS).**
  - We developed an experimental framework to test HC-NIDS that combines simulated physical and control environments interacting with actual logic controllers (Siemens PLC using Modbus TCP).
- **Integration with Data Management Services (OSIsoft case study).**
  - We are collaborating with OSIsoft, one of the industry leaders in ICS data management systems, to implement inclusion of sensor tags for appropriately located **network taps**.
  - HC-NIDS rules are then implemented as analytics/queries of the OSIsoft database.

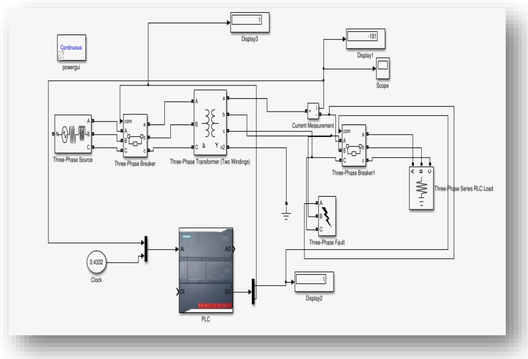
RESEARCH RESULTS (CON'T)

Validation Testbed

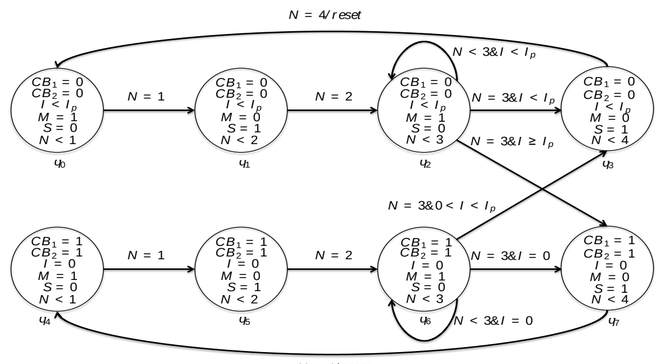


1. Simulink model: simulation of the physical application.
2. C MEX S-function: allows communication through the Modbus TCP protocol.
3. Emulation of the protection function in Ladder logic.

Example: Overcurrent Protection



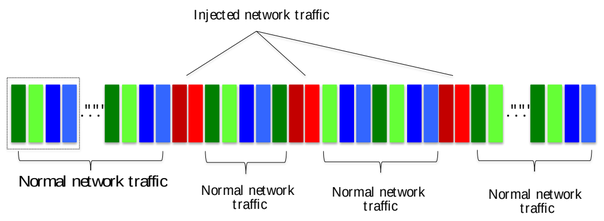
Simulink model



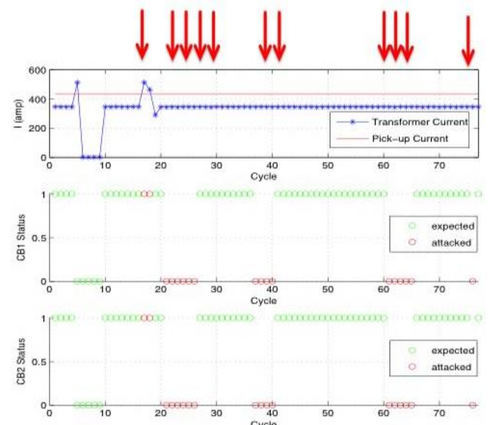
Hybrid Automaton

Cyber-Physical Analytics

- The different data items of the different controllers have different colors.
  - Source ID/Destination ID, function code, register, and value range (set) are different.
- The normal sequence is green-light green-blue-turquoise.
- Red packets are not part of it, so they are anomalies.



Arrows indicate phenomena that can be identified as attacks, since the switches' state (CB) and current are not in the right combination.



BROADER IMPACT

- Operators are made aware of Cyber-Physical State.

INTERACTION WITH OTHER PROJECTS

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

FUTURE EFFORTS

- **Blind HC-NIDS:** Learn the rules by analyzing traffic.
- Integrate OSIsoft with Wireshark so that it can leverage the extensive literature.

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