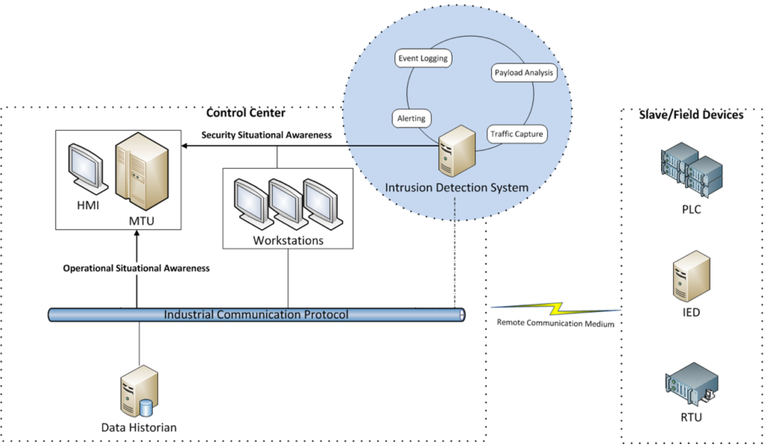
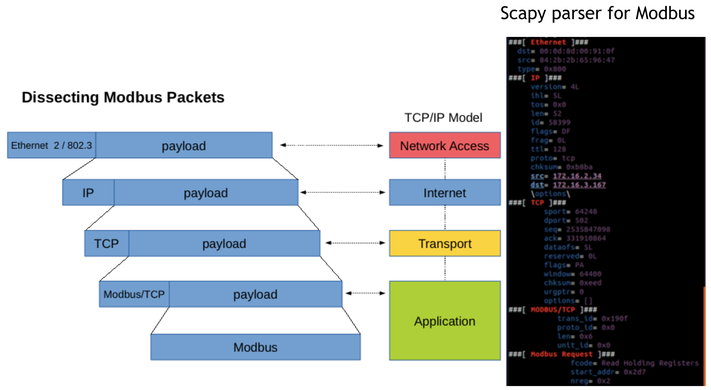
Intrusion Detection for ICS



Deep-Packet Inspection for Industrial Control Protocols

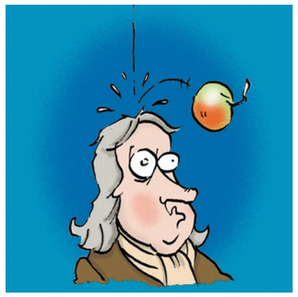


Key Questions

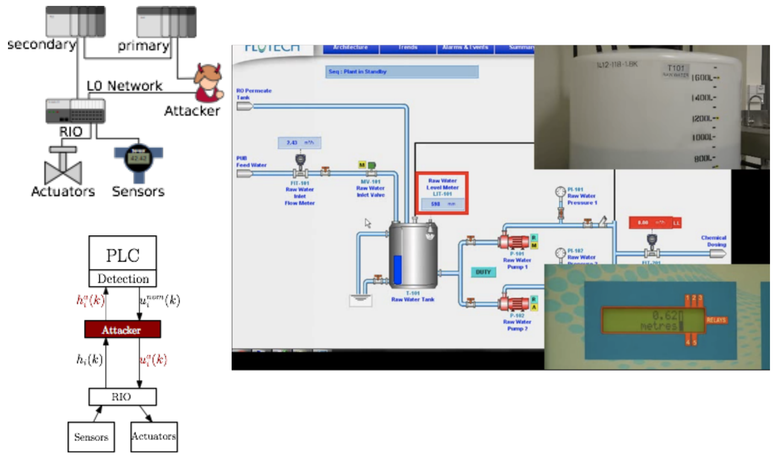
- Where to deploy network monitors (sensors)?
- How “deep” to look?
  - DFA network protocol, communication patterns, command codes, enough?
- Protocol specification correct but false info
  - Exact value of sensor and control commands (can’t model with DFA)

We Need to Monitor the Physics of The System

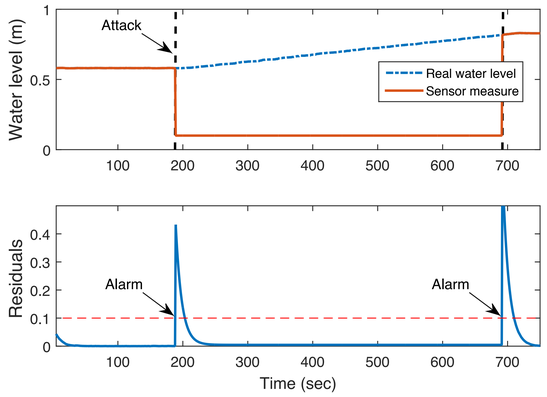
- Protocol specification/patterns correct but false info
- Physical systems follow immutable laws of nature
  - Fluid dynamics (water systems) or Electrodynamics (power grid) used to create time-series models
- These models can be used to check
  - If control commands were executed correctly
  - Sensor values are consistent with expected behavior



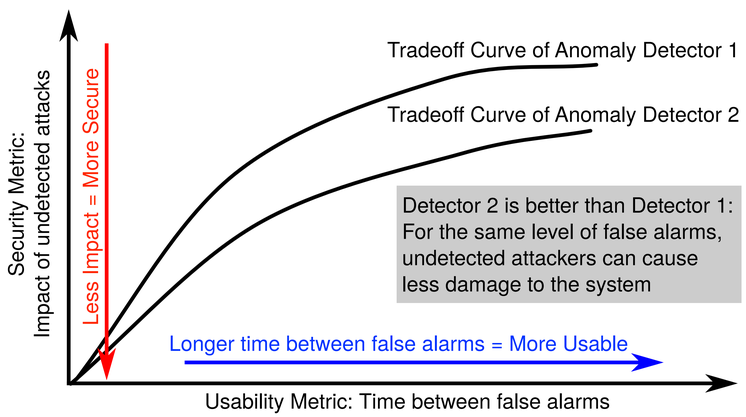
Implementing an Attack



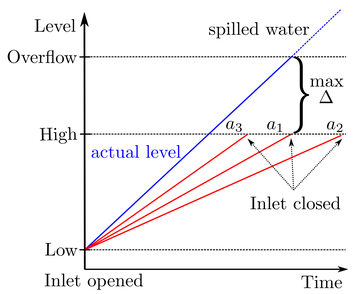
Problem: We Can Always Create Attacks That Are Detected

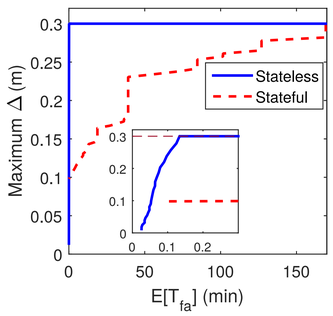


Our Proposed Metric



Goal: Set Up Anomaly Thresholds to Avoid Undetected Safety Violations While Minimizing False Alarms





Publication

Limiting the Impact of Stealthy Attacks on Industrial Control Systems **ACM CCS 2016**
David I Urbina, Jairo Giraldo, Alvaro A Cardenas, Nils Ole Tippenhauer, Junia Valente, Mustafa Faisal, Justin Ruths, Richard Candell, Henrik Sandberg

Award Info

CAREER: Practical Control Engineering Principles to Improve the Security and Privacy of Cyber-Physical Systems
NSF CNS 1553683