NSTB

National SCADA Test Bed

enhancing control systems security in the energy sector

Visualization and Controls Program Peer Review 2006 AGA-12 Performance Testing

Jeff Dagle

Pacific Northwest National Laboratory

(509) 375-3629

jeff.dagle@pnl.gov

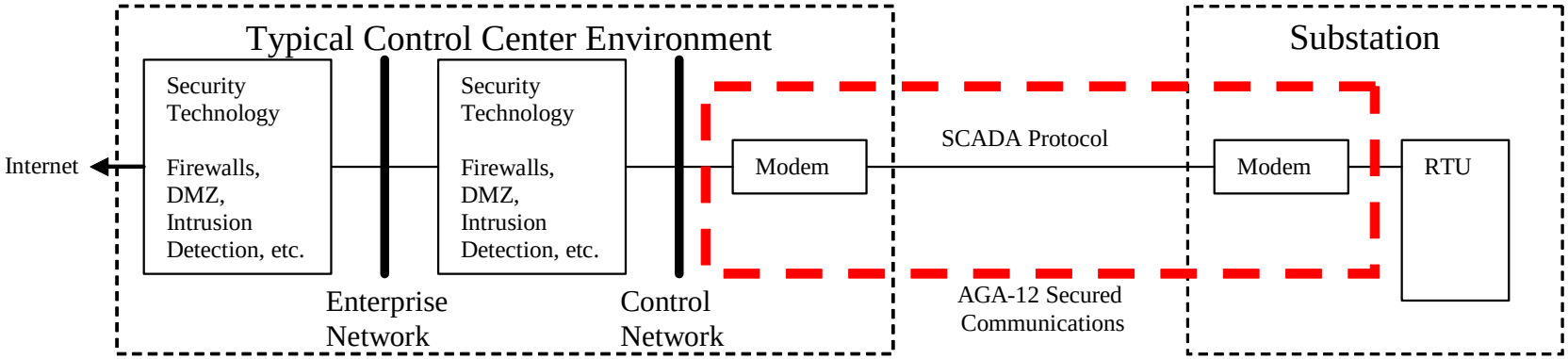
The Pacific Northwest National Laboratory is a multiprogram laboratory operated by Battelle for the United States Department of Energy under contract DE-AC05-76RL01830.

U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability

Work Package Description

- Develop a detailed test plan and conduct performance testing on commercial devices built to the AGA-12 standard in environments representing electric power distribution
- Companion task to cryptographic security review conducted by Sandia National Laboratories
- **Primary Roadmap Goal:** Develop and integrate protective measures
- **Budget:** $200K

Scope of the AGA-12 Encryption Technology



Industry Needs

- The American Gas Association developed a draft standard for securing serial communications through encryption (the AGA-12 Standard)
  - Developed primarily for protecting SCADA systems used by the natural gas industry
- Proponents for the AGA-12 Standard were advocating its use in other industry SCADA applications
  - e.g., electric power
- The NERC Control System Security Working Group through it's liaison relationship with the NSTB requested a thorough performance and security evaluation of the AGA-12 encryption standard in an environment representative of the electric power industry

Technical Approach

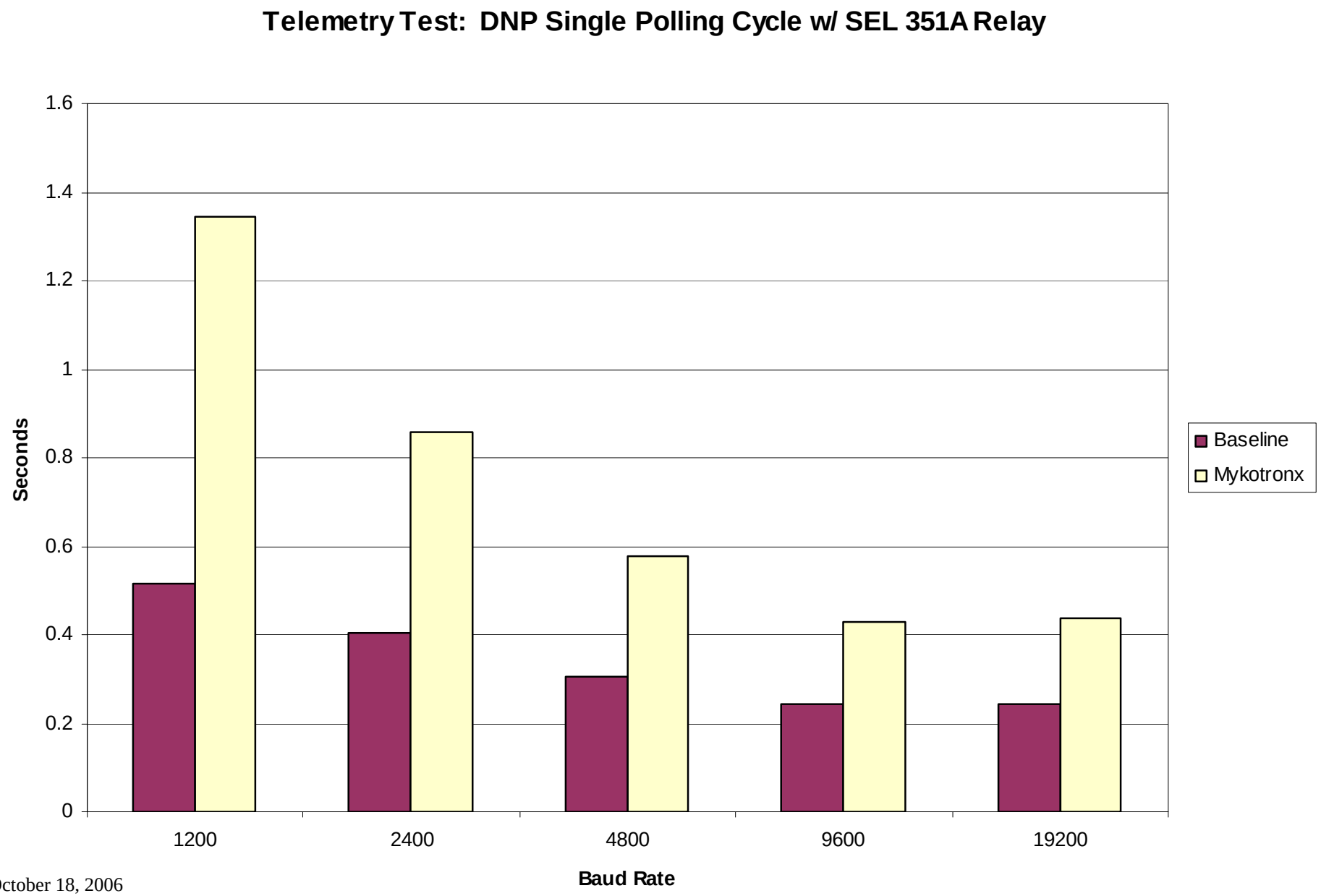
- Evaluate commercial versions of appliances built to the AGA-12 Part 1 and Part 2 standard in a laboratory setting that simulates an electric utility's environment
- Detailed test plan prepared and reviewed by industry
- Tests conducted using a representative assortment of equipment from the electrical industry using Modbus and DNP serial communication protocols
- Performance and reliability impact upon serial communications were measured

Technical Progress - Accomplishments

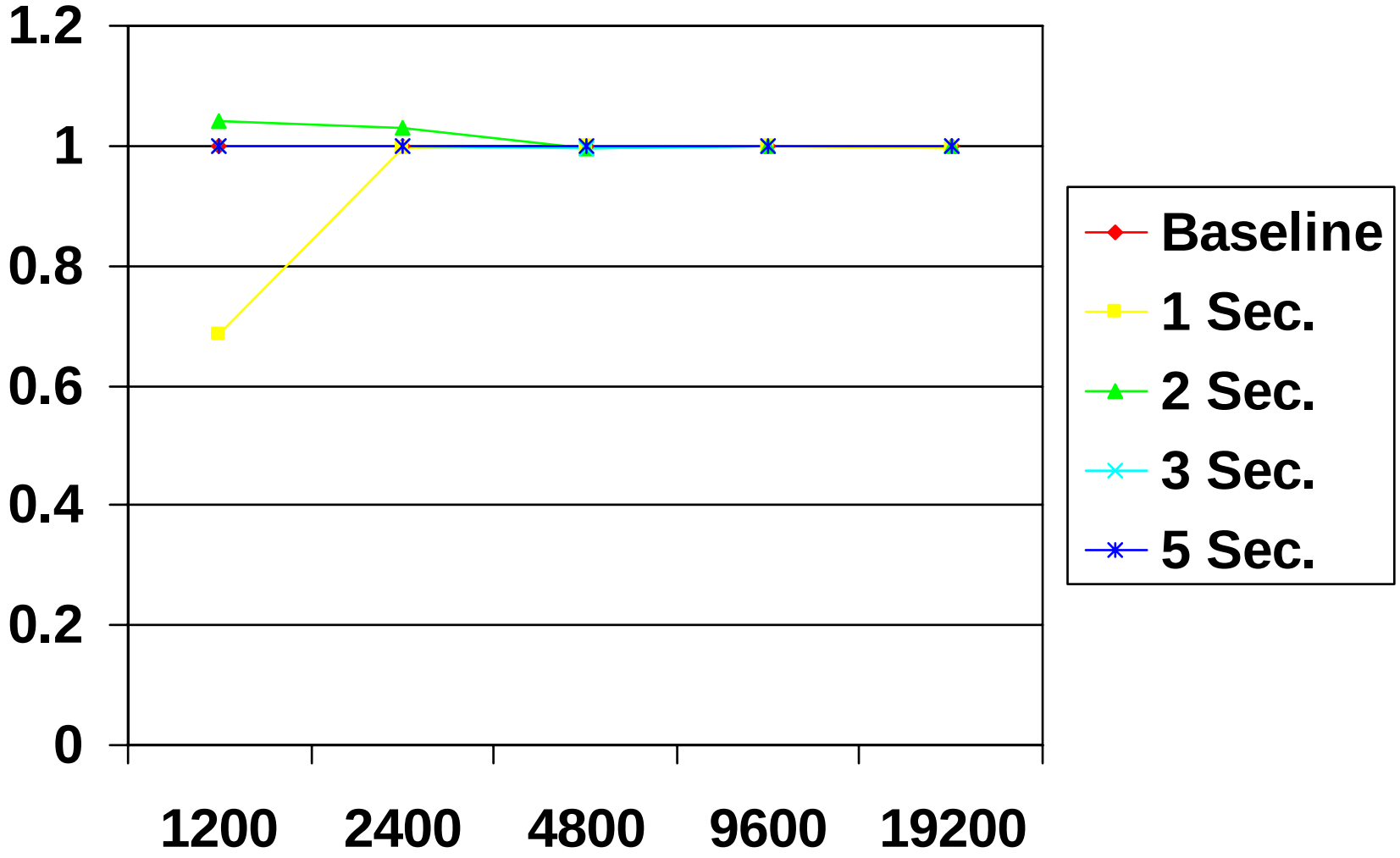
- Deviations from original work scope and schedule
  - SEL did not develop AGA-12 compliant encryption hardware, so testing limited to Mykotronx and Thales
  - Thales did not deliver DNP-compliant modules until late August, delaying testing
- Progress report (98% funds expended as of 9/30/06)
  - Test report complete and reviewed by industry
  - Baseline testing with null modem, leased line analog modem, and SCADA Radio complete
  - Performance testing with Mykotronx devices complete
  - Performance testing with Thales devices 90% complete
  - Presentations given at AGA and API meetings regarding preliminary test results

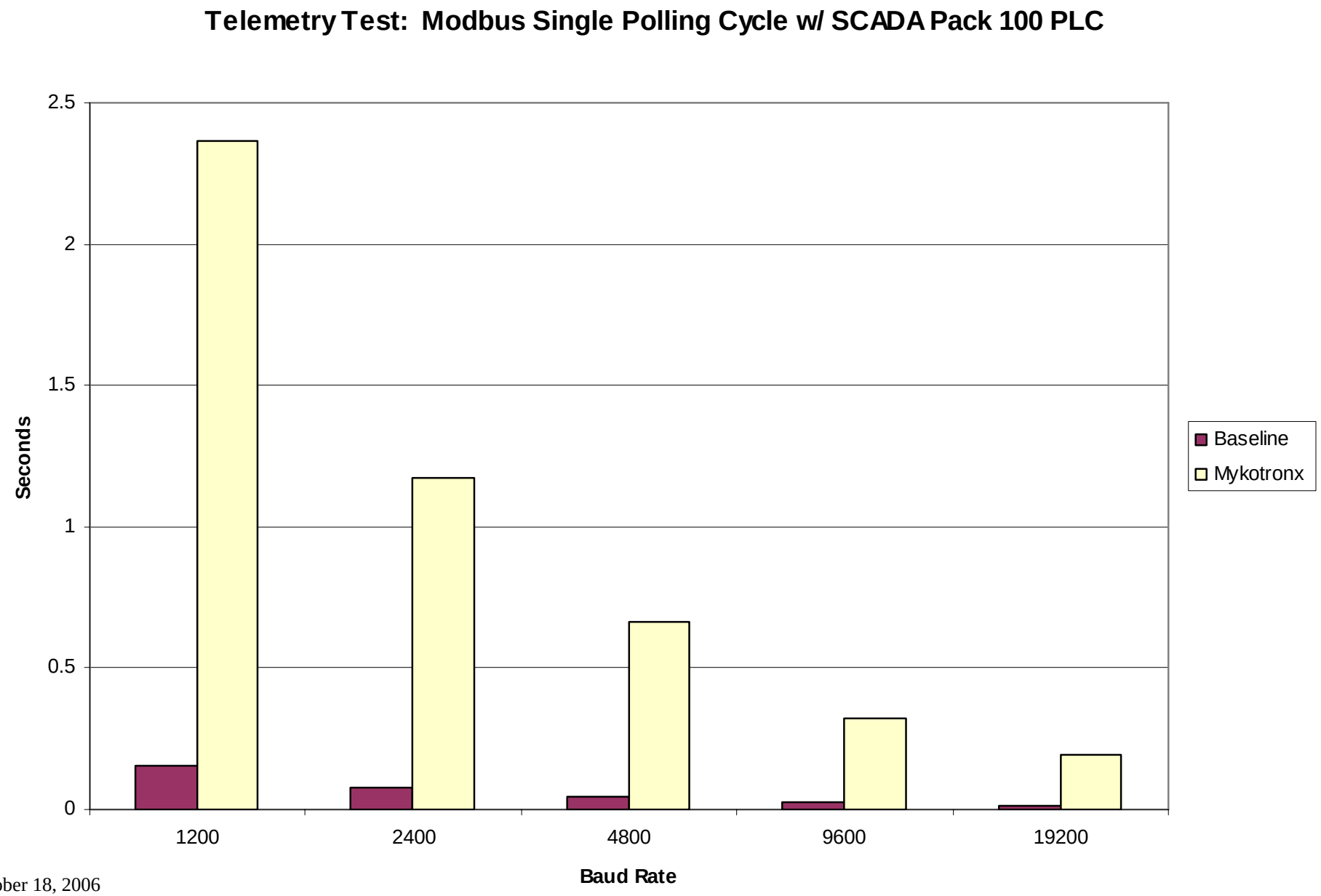
Test Results

- Telemetry tests
  - DNP
    - Minimal impact beyond 2400 baud
  - Modbus
    - Fast polling rates not possible for slower baud rates
- Control tests
  - Significant time delay added

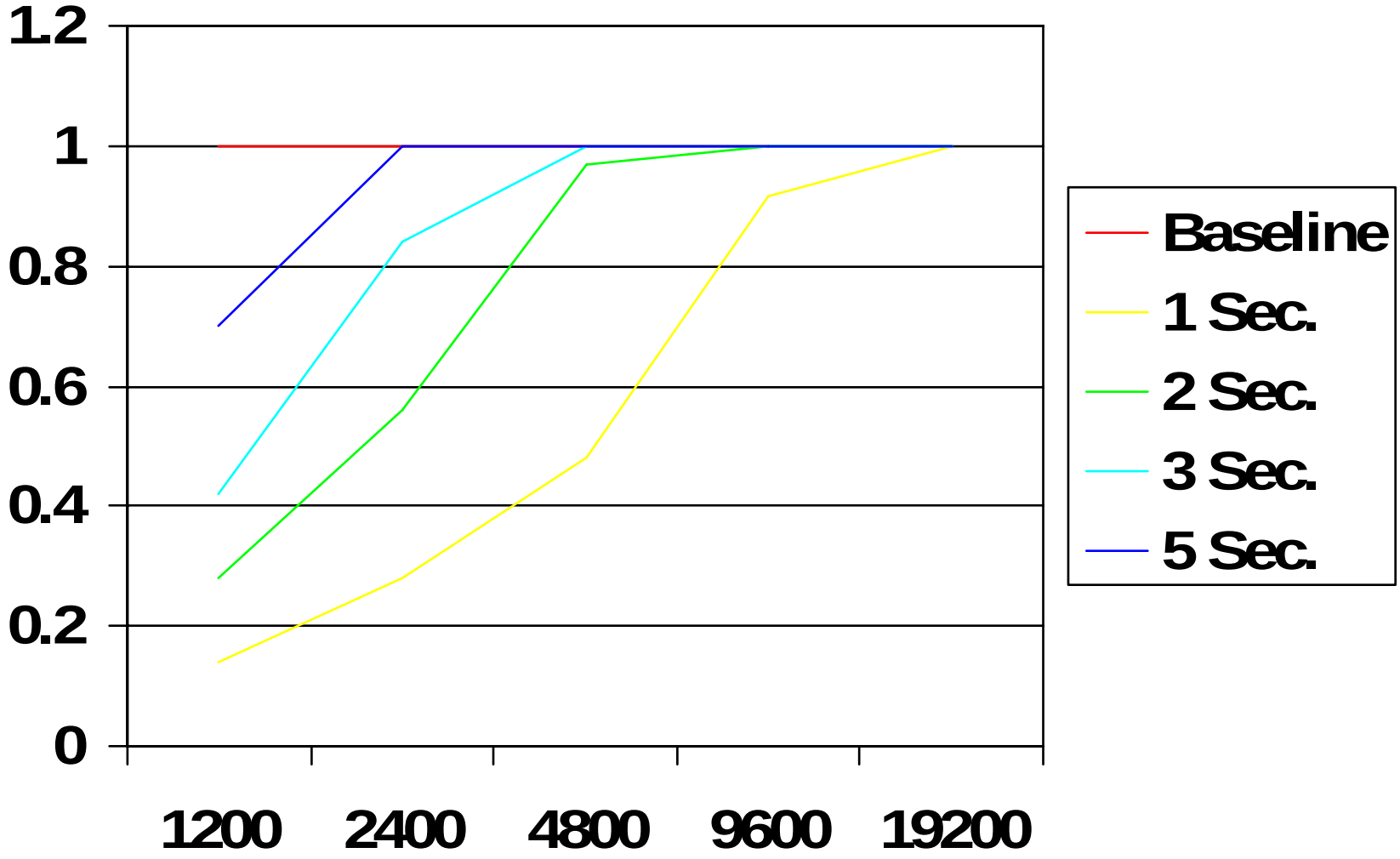

Telemetry Test: DNP Single Polling Cycle w/ SEL 351A Relay
1.6
1.4
1.2
1
0.8
0.6
0.4
0.2
0
Seconds
1200
2400
4800
9600
19200
Baud Rate
Baseline
Mykotronx

Point-to-Point Polling Cycles per Hour (Fraction of Baseline)

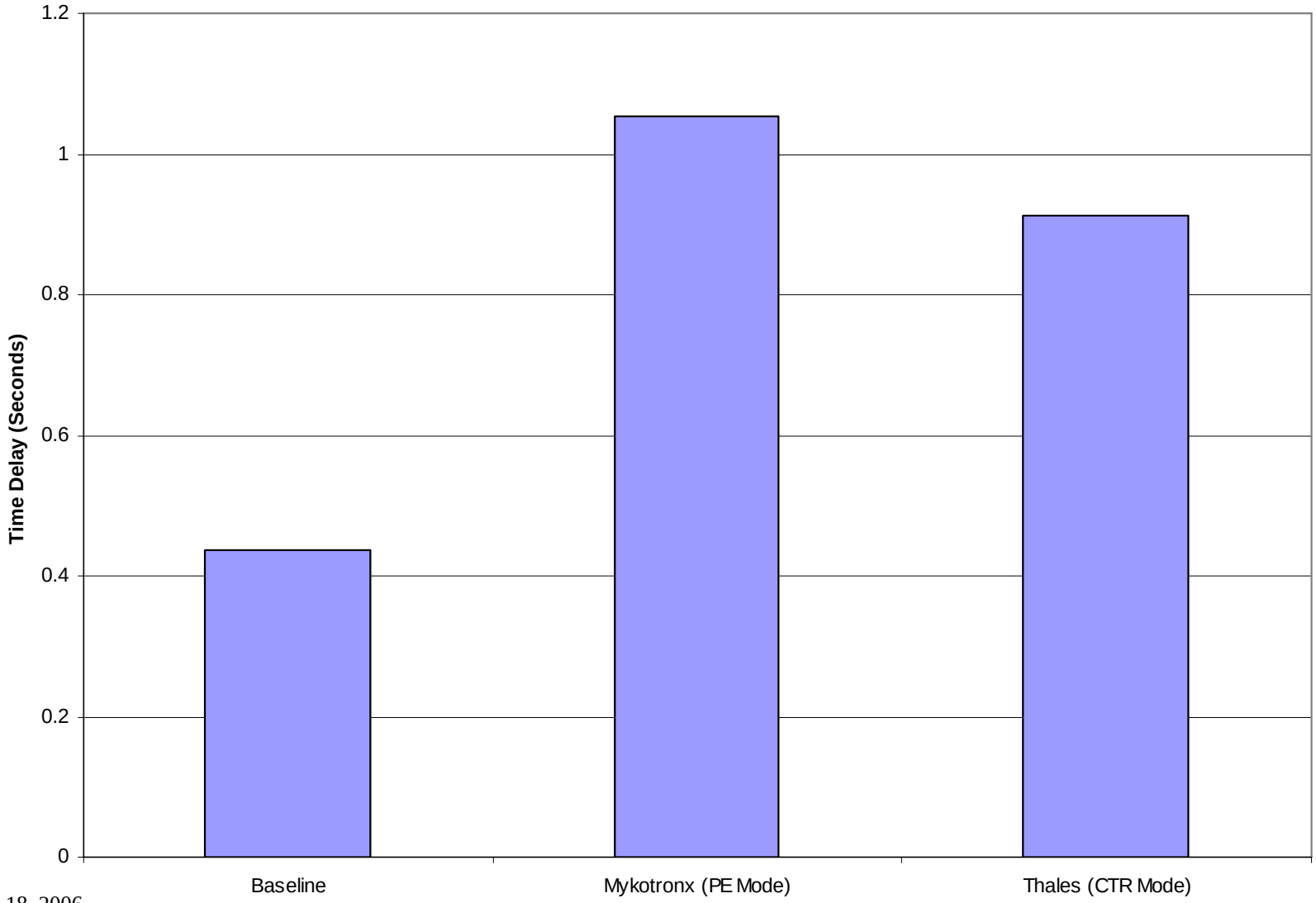



Telemetry Test: Modbus Single Polling Cycle w/ SCADA Pack 100 PLC
2.5
2
1.5
1
0.5
0
Seconds
1200
2400
4800
9600
19200
Baud Rate
Baseline
Mykotronx

Point-to-Point Polling Cycles per Hour (Fraction of Baseline)



DNP Control Test (9600 Baud)



Collaborations and Partnerships

- SafeNet Mykotronx
- Thales e-Security
- Schweitzer Engineering Labs
- Gas Technology Institute
- American Gas Association
- Andrew Wright – Cisco
- NERC Control Systems Security Working Group
- Sandia National Laboratory

Industry Benefits

- Provide knowledge to industry regarding the expected performance impacts associated with introducing AGA-12 cryptographic modules into serial communication environments
- Detailed test plan for use by multiple industries
- Impartial review of performance data