
U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cyber Security for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

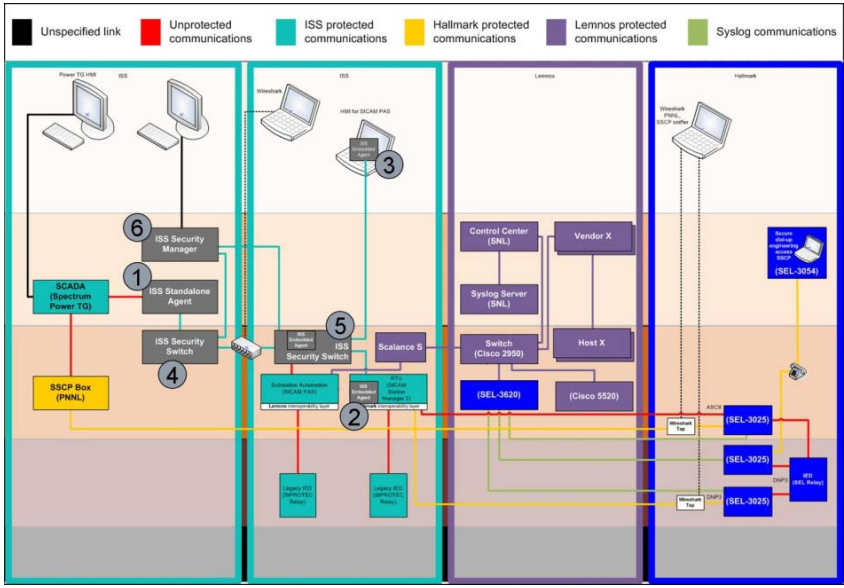
Dr. Dong Wei

Siemens Corporation, Corporate Research

# Protecting Intelligent Distributed Power Grids against Cyber Attacks

# Protecting Intelligent Distributed Power Grids against Cyber Attacks

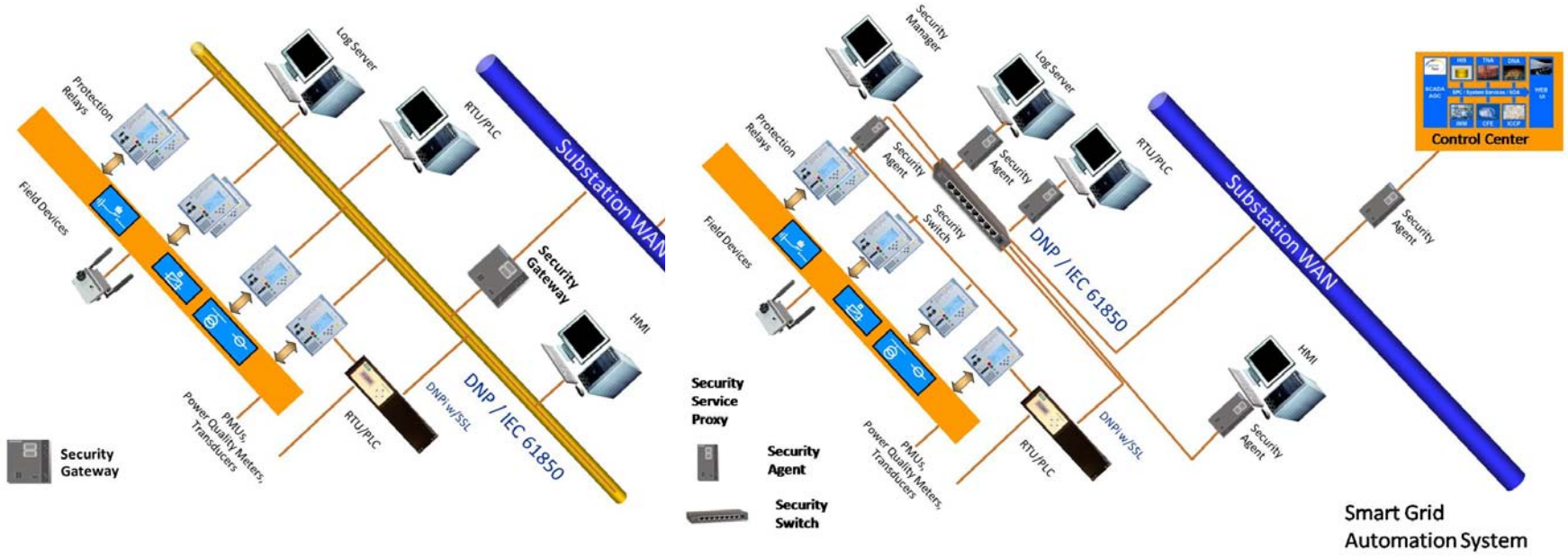
- **Outcomes:** Prototype of the Integrated Security System (**ISS**) with three major components: Security Agent, Managed Security Switch and Security Manger
- **Roadmap Challenges:** 1) Growing risks from increasingly interconnected systems 2) Poorly designed connections to SCADA and business networks; 3) Security upgrades hard to retrofit to legacy systems
- **Major Successes:** The ISS prototype has been validated and verified by INL and demonstrated at DistribuTECH 2010



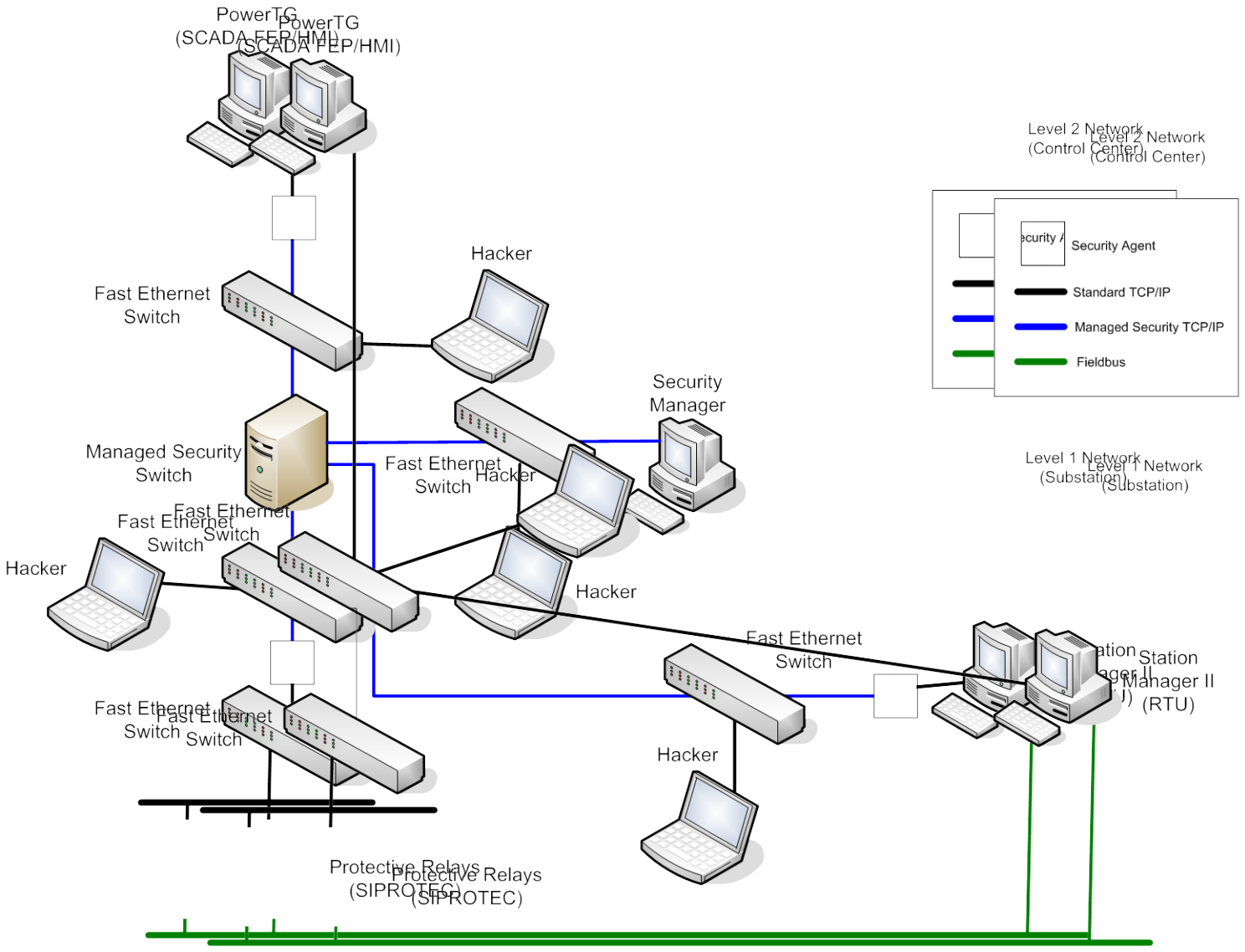

- **Schedule:** vulnerability test in Dec. 2009; demonstration in Mar. 2010; prepare final report September 2010
- **Level of Effort: $** 1,994 K
- **Funds Remaining: $** 100 K
- **Performers:** Siemens Corporate Research, Siemens Energy
- **Partners:** INL, LANL, Rutgers University

# Technical Approach and Feasibility

- **Approach**
  - "gateway" to "security service proxy"
  - "bump-in-the-wire"
  - Central management and distributed control



# Technical Approach and Feasibility

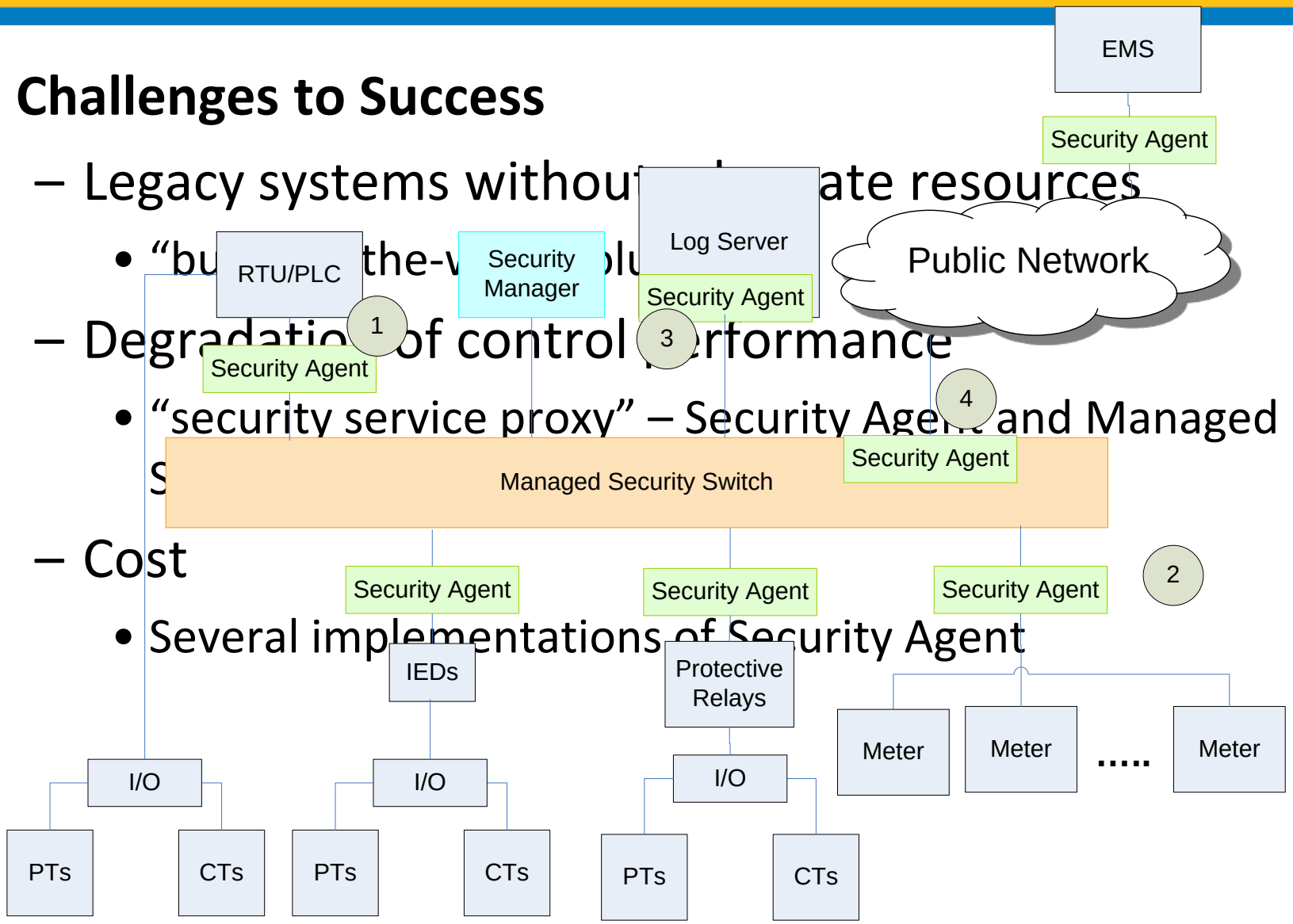


# Technical Approach and Feasibility

- **Metrics for Success**
  - INL on-site test: 104 vulnerabilities were identified; 67 were mitigated or partially mitigated by the ISS prototype. Most attacks were detected and reported.
  - The ISS does not introduce significant delay
    - Maximum round trip delay: 105 ms vs. 110 ms
    - Maximum connection creation: 130 ms vs. 135 ms
  - The ISS does not add significant communication overhead < 10%

# Technical Approach and Feasibility

- **Challenges to Success**
  - Legacy systems without [illegible]ate resources
    - "bu[illegible] the-v[illegible]lu[illegible]
  - Degradatio[illegible] of control [illegible]erformance
    - "security service proxy" – Security Agent and Managed S[illegible]
  - Cost
    - Several implementations of Security Agent



# Technical Approach and Feasibility

- **Technical Achievements to Date**
  - Protects legacy control systems
  - Meets Quality of Service requirements for automation and control communication
  - Protects against Denial of Service attacks
  - Independent of the underlying operating system
  - Conforms to NERC CIP 005 and 007

# Technical Approach and Feasibility

- **Technical Achievements to Date**
  - Vulnerability test by the INL in 07/09 and 12/09
  - Demonstration, connecting together with Lemnos and Hallmark, at DistribuTECH 2010 in 03/10, Tampa
  - Publications:
    - IEEE PES ISGT, 01/10, NIST;
    - 2010 IEEE PES T&D Conference, 04/10, New Orleans;
    - IEEE Transactions on Smart Grid – Special Issue on Cyber, Physical and System Security

# Collaboration/Technology Transfer

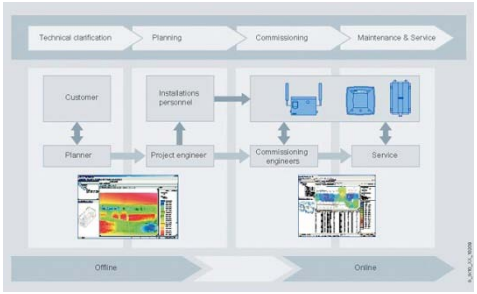
- **Plans to transfer technology/knowledge to end user**
  - Work together with Los Alamos National Laboratory to make it more portable
  - Work with Siemens Industry Inc. to commercialize the developed technologies

Siemens Scalance S

Security Agent

Siemens Scalance X

Security Switch




Siemens Power ™

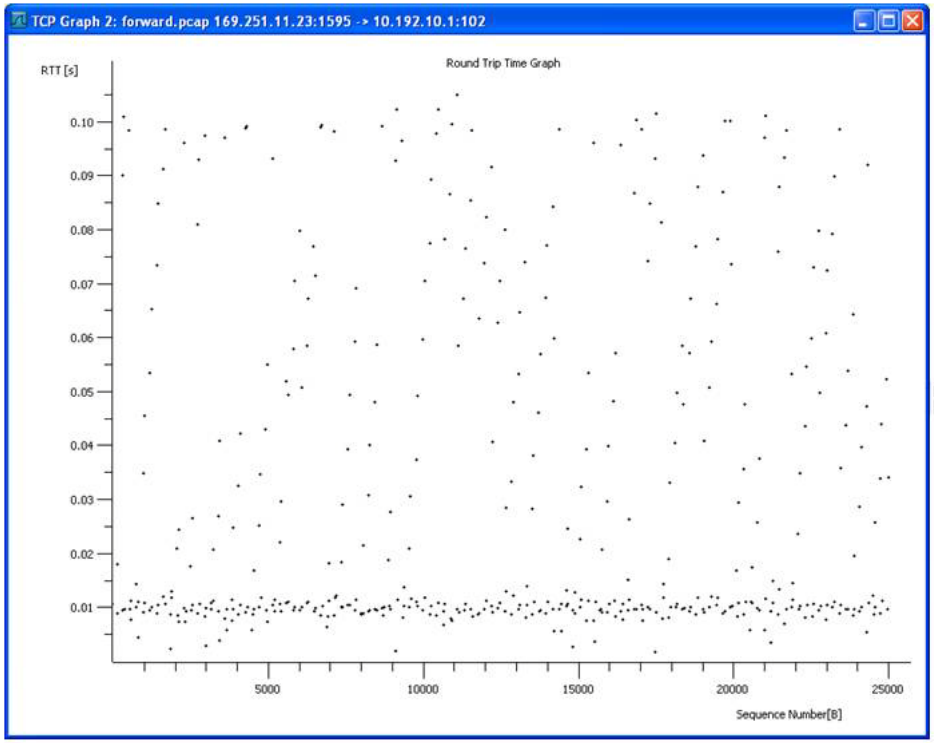
Security Manager

# Next Steps

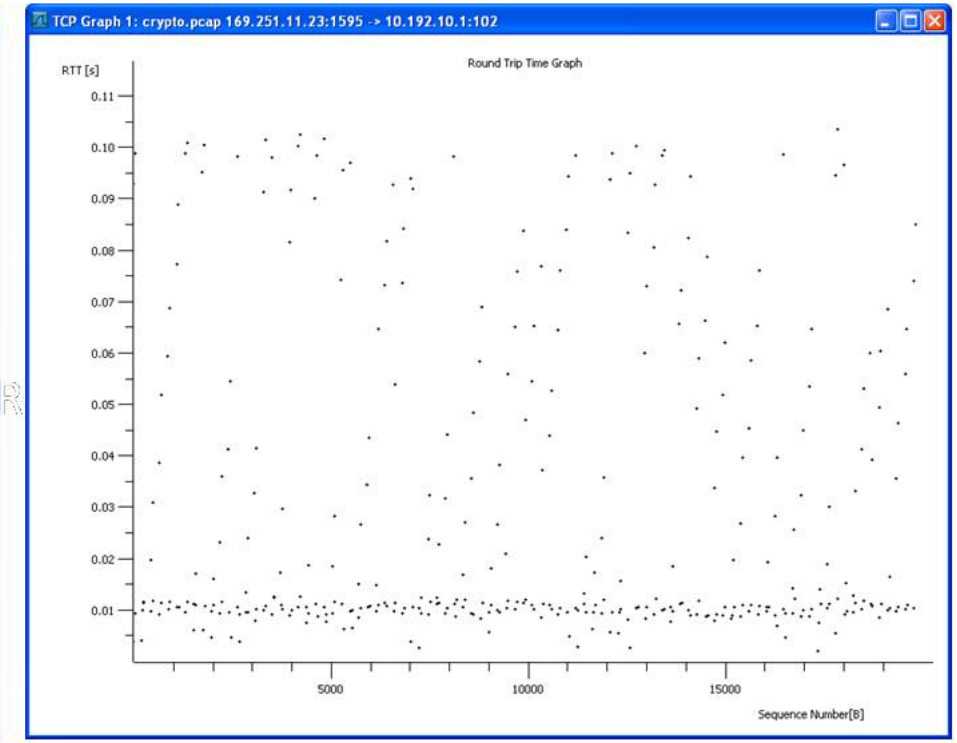
- **Follow-on work**
  - Application layer security (proposed)
  - Timeline
    - Phase I: Investigation, system requirements and specification;
    - Phase II: Technology development, verification and validation
    - Phase III: Prototypes based on Siemens Products

# Backup Slides

# Comparison of Round Trip Delay

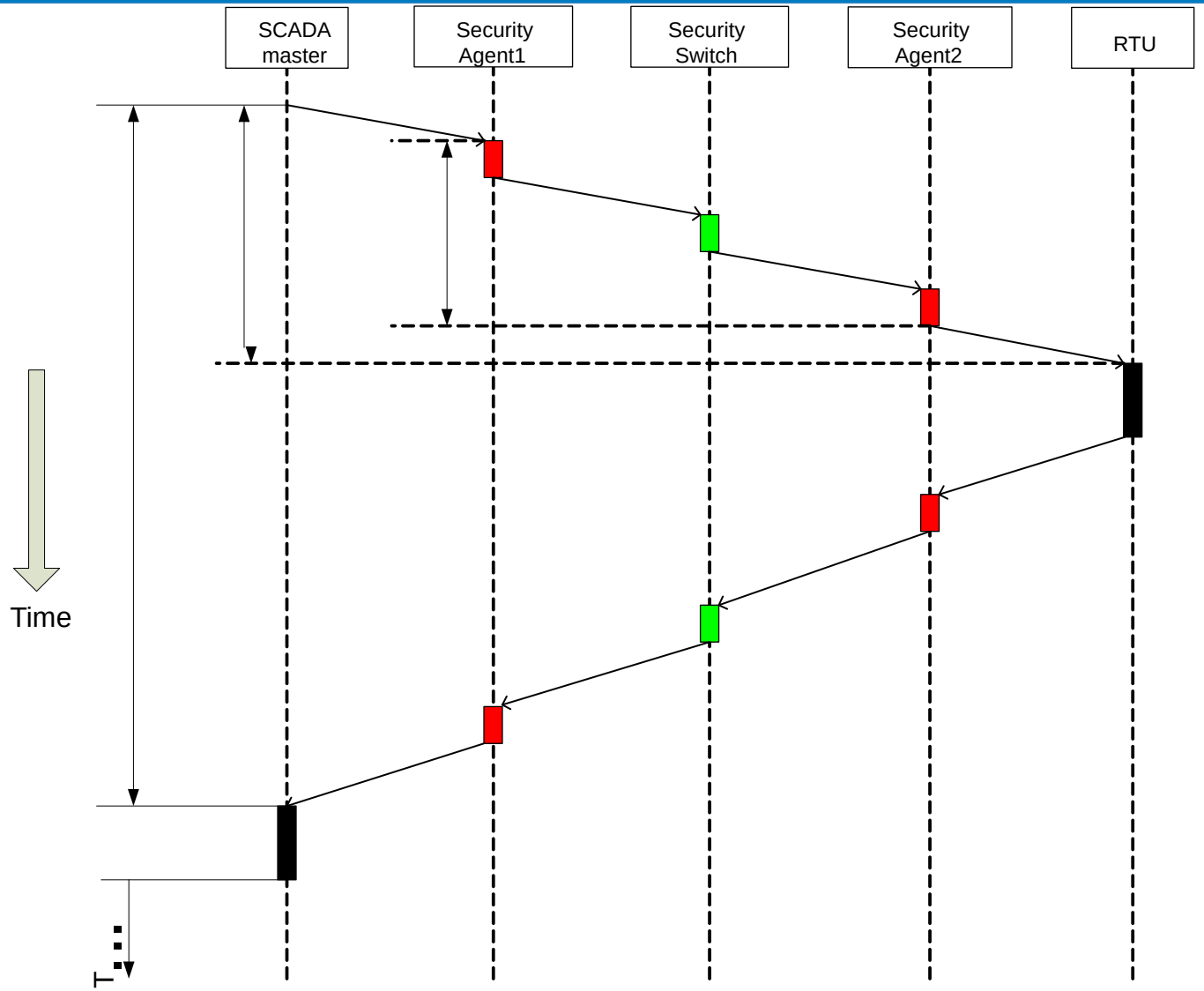



(a)

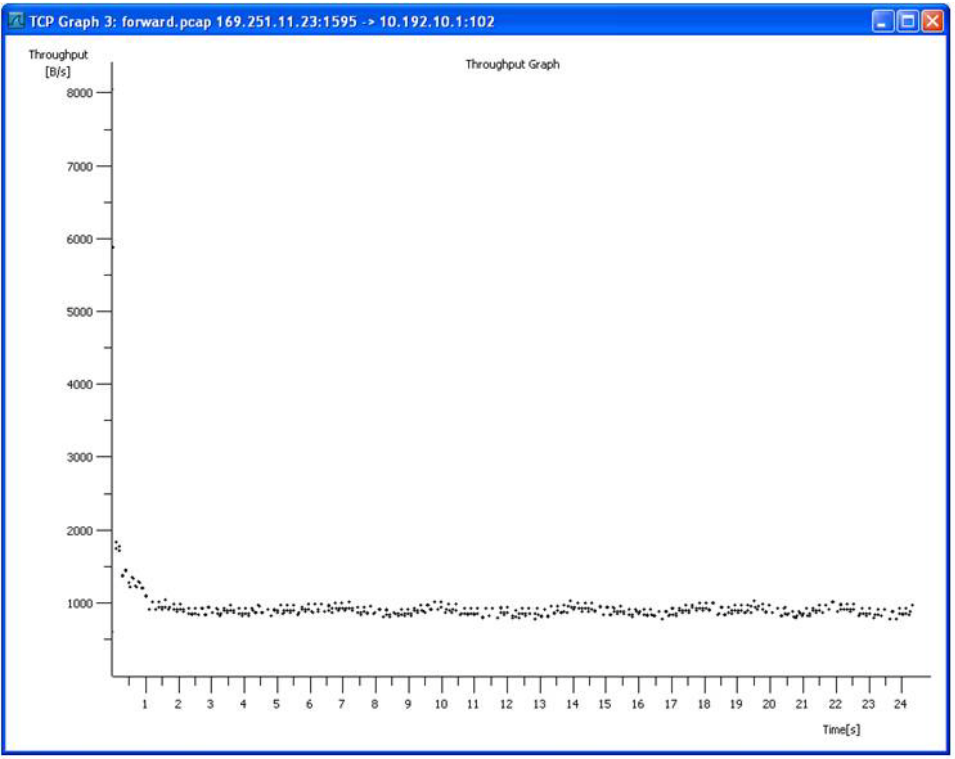



(b)

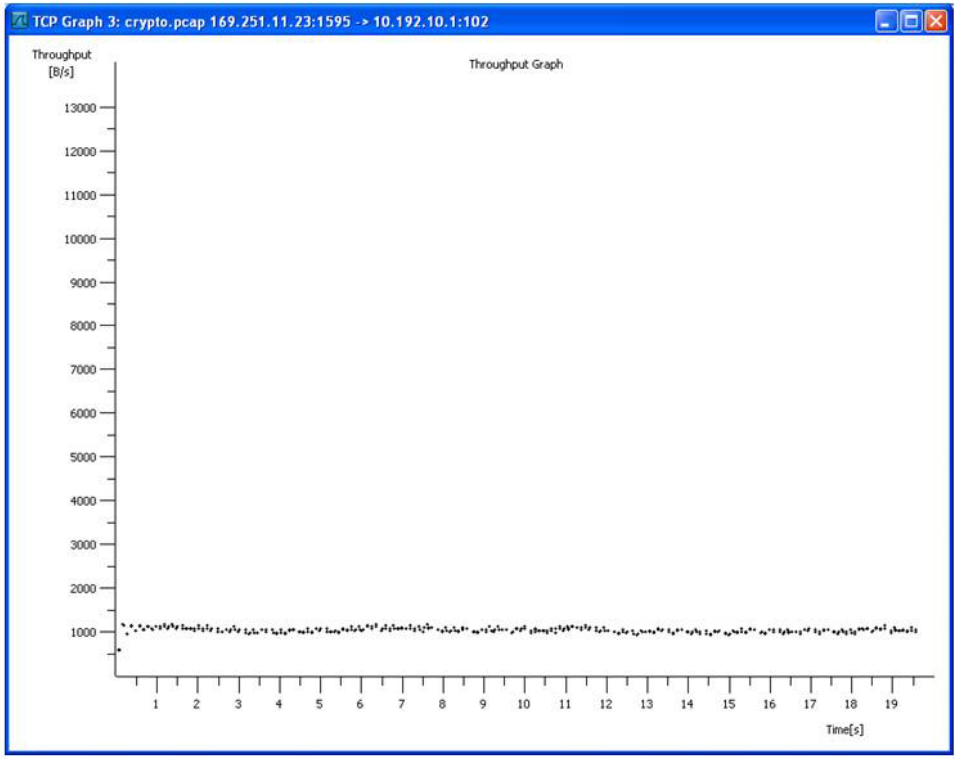
# Delay Time (Round Trip Delay)



# Comparison of Bandwidth Usage




(a)




(b)