

IEEE PES Innovative Smart Grid Technologies Conference

January 20, 2010

Dong Wei, Yan Lu, Mohsen Jafari, Paul Skare, Ken Rohde

*An Integrated Security System of Protecting Smart Grid
against Cyber Attacks*

[funded by DOE OE]

ISS - Overview

Main Challenge:

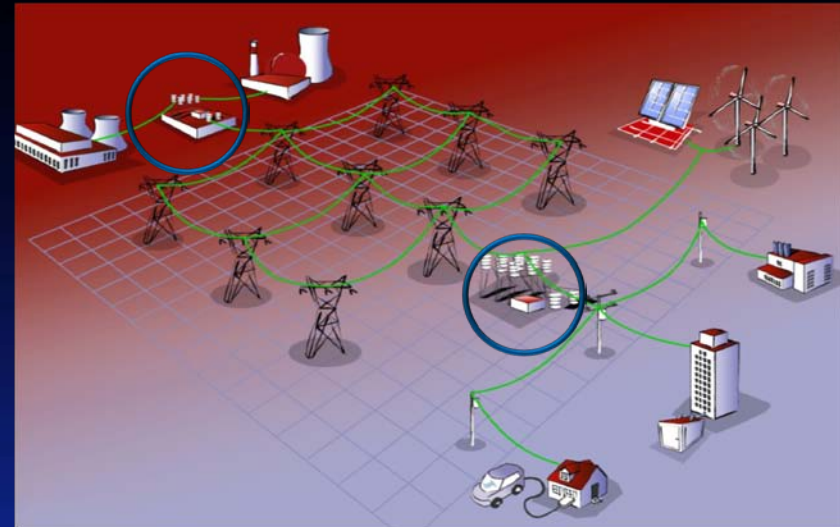
Provide security for new and legacy control systems currently used in the power grid without impacting operation.

Solution:

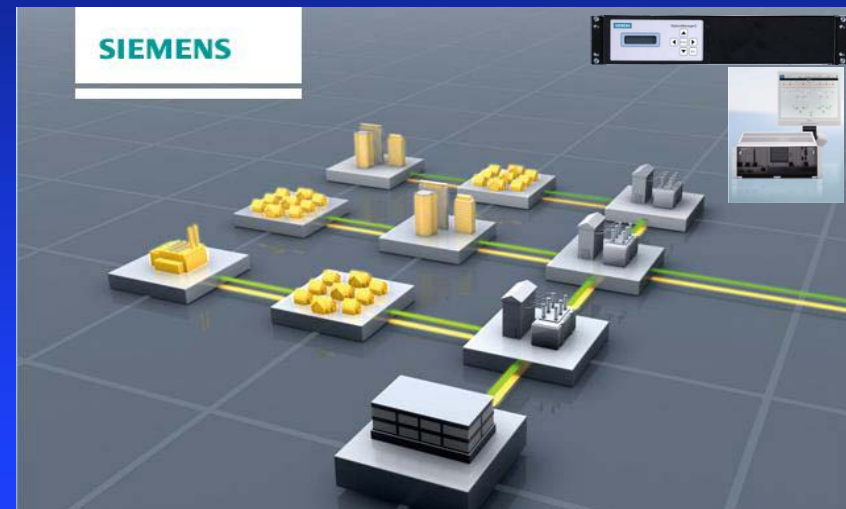
An integrated and distributed security system which overlays the power grid network and consists of three components: Manager, Switch, & Agent. Assessed, verified and validated by Idaho National Laboratory/NSTB.

Benefits:

- Allows asset owners to design a secure control system architecture.
- Enables the securing of legacy control system devices
- Provides centralized management, reporting, and in-band updates for a distributed solution.



Source: US Department of Energy Office of Reliability



Challenges in Smart Grid Communications

SIEMENS

1. Typical Business Objectives
2. Connectivity
3. Protocols
4. Media
5. Quality of Service
6. Possible Cyber Attacks and Adverse Impacts
7. Security Requirements

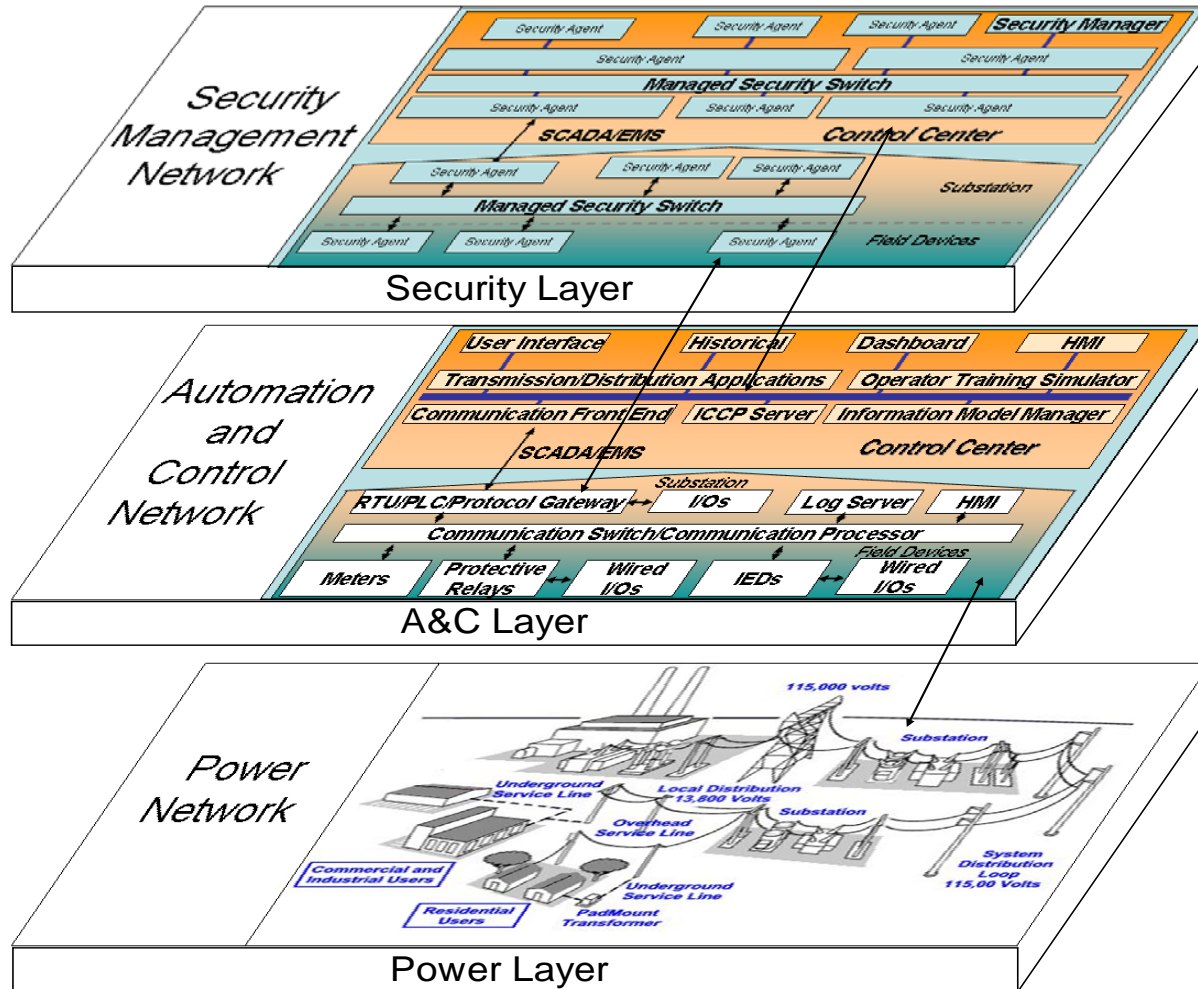
Major challenges with new security solutions

SIEMENS

1. Control System Security vs. IT Security
2. Many communication technologies
3. Legacy systems vs. new systems
4. Emerging requirements for smart grid

Design Principles of the ISS

SIEMENS





1. Non-Intrusive

2. Scalable

3. Extendable

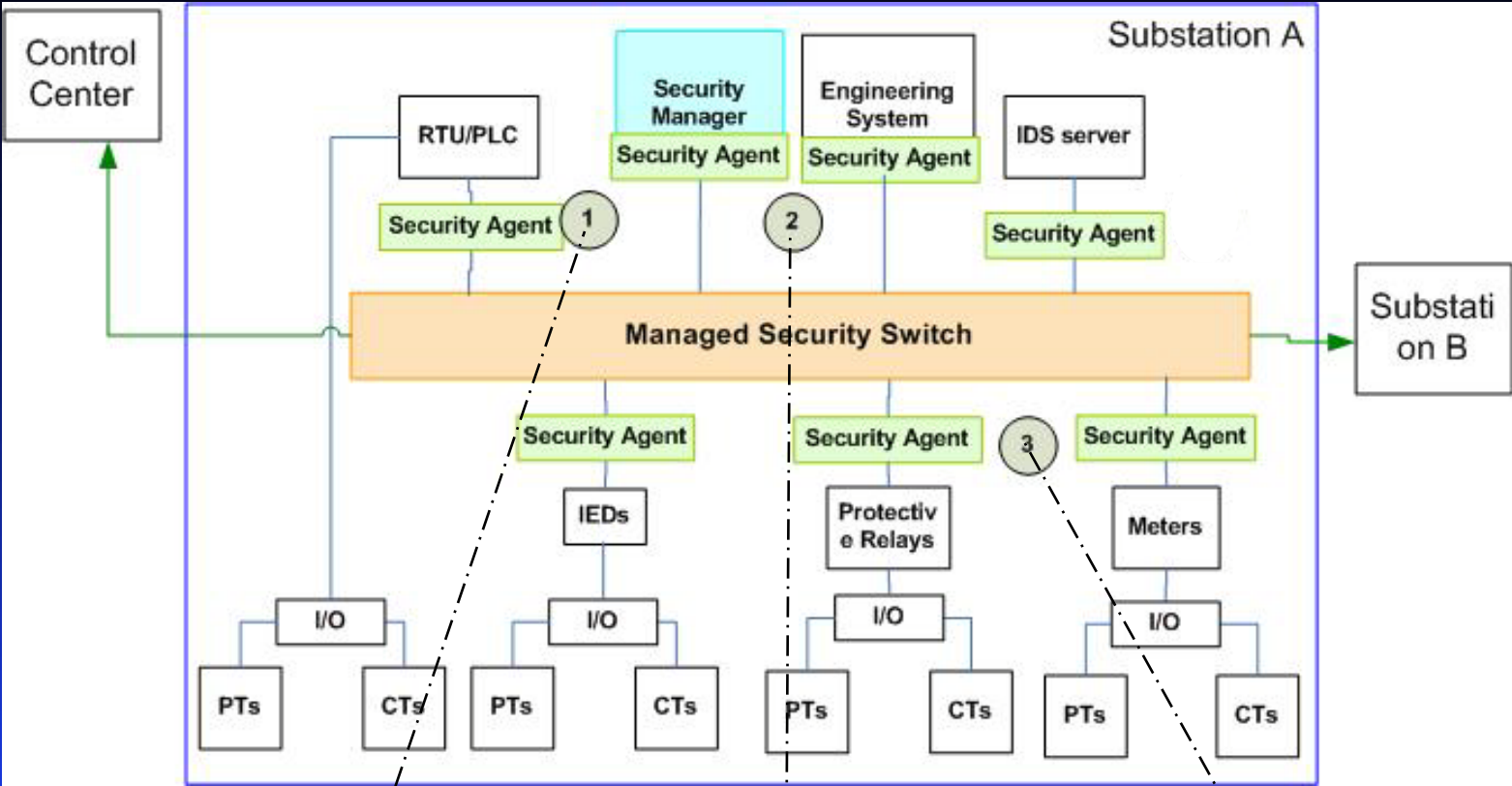
4. Inter-operable

Introduction - ISS

Feature	Agent	Switch	Manager
Cryptography using OpenSSL*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Access Control (AC) / Statefull Firewall	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Intrusion Detection (ID) based on control data pattern	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Quality of Service (QoS)			
- Traffic Shaping		<input checked="" type="checkbox"/>	
- Traffic Differentiation 		<input checked="" type="checkbox"/>	
- Packet Scheduling 		<input checked="" type="checkbox"/>	
Logging	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Key Management			<input checked="" type="checkbox"/>
Alarm Monitoring			<input checked="" type="checkbox"/>
Configuring of the ISS network			<input checked="" type="checkbox"/>
Security Policy Updates			<input checked="" type="checkbox"/>
AAA Server			<input checked="" type="checkbox"/>



Deployment View

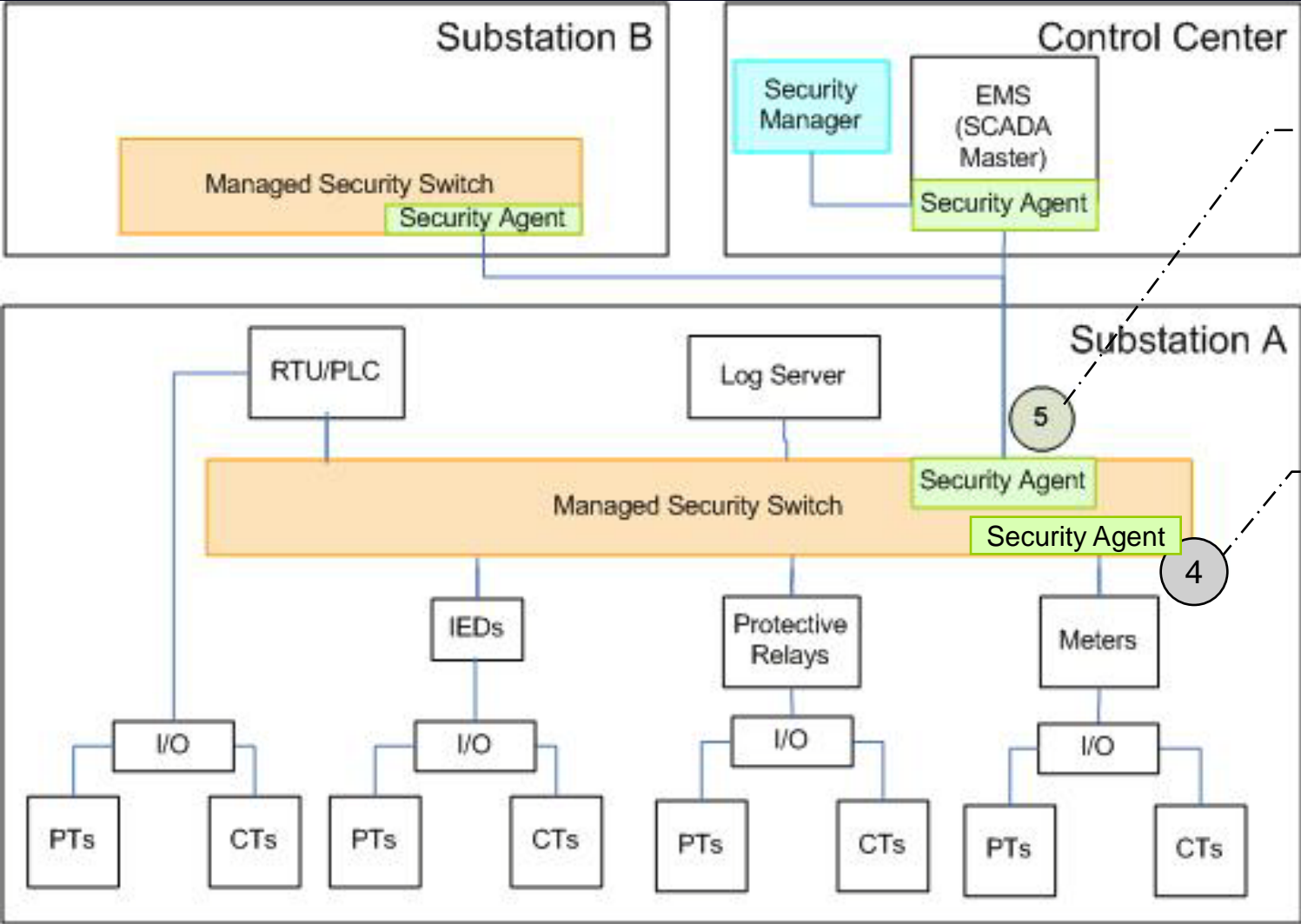


1) Security Agent as a stand alone device

2) Security Agent embedded into a device or application

3) Security Agent as stand alone protecting a group of devices

Deployment View



5) Security Agent embedded into the Security Switch. We assume that all connected devices are secure.

4) Security Agent embedded into the Security Switch. Allows securing of legacy devices

Benefits of the ISS

SIEMENS

- *Protects legacy control systems*
- *Meets Quality of Service requirements for control communication*
- *Protects against Denial of Service attack*
- *Independent of the underlying operating system*
- *Conforms to NERC CIP 005 and 007*
- *Designed to also protect SCADA systems outside of the Smart Grid (Oil & Gas Pipeline, etc)*

Vulnerability Assessment @ INL

SIEMENS

1st on-site test was performed in July 2009

- *104 vulnerabilities were identified*
- *19 were mitigated by the ISS*
- *48 were partially mitigated by the ISS*

2nd test was performed in December 2009