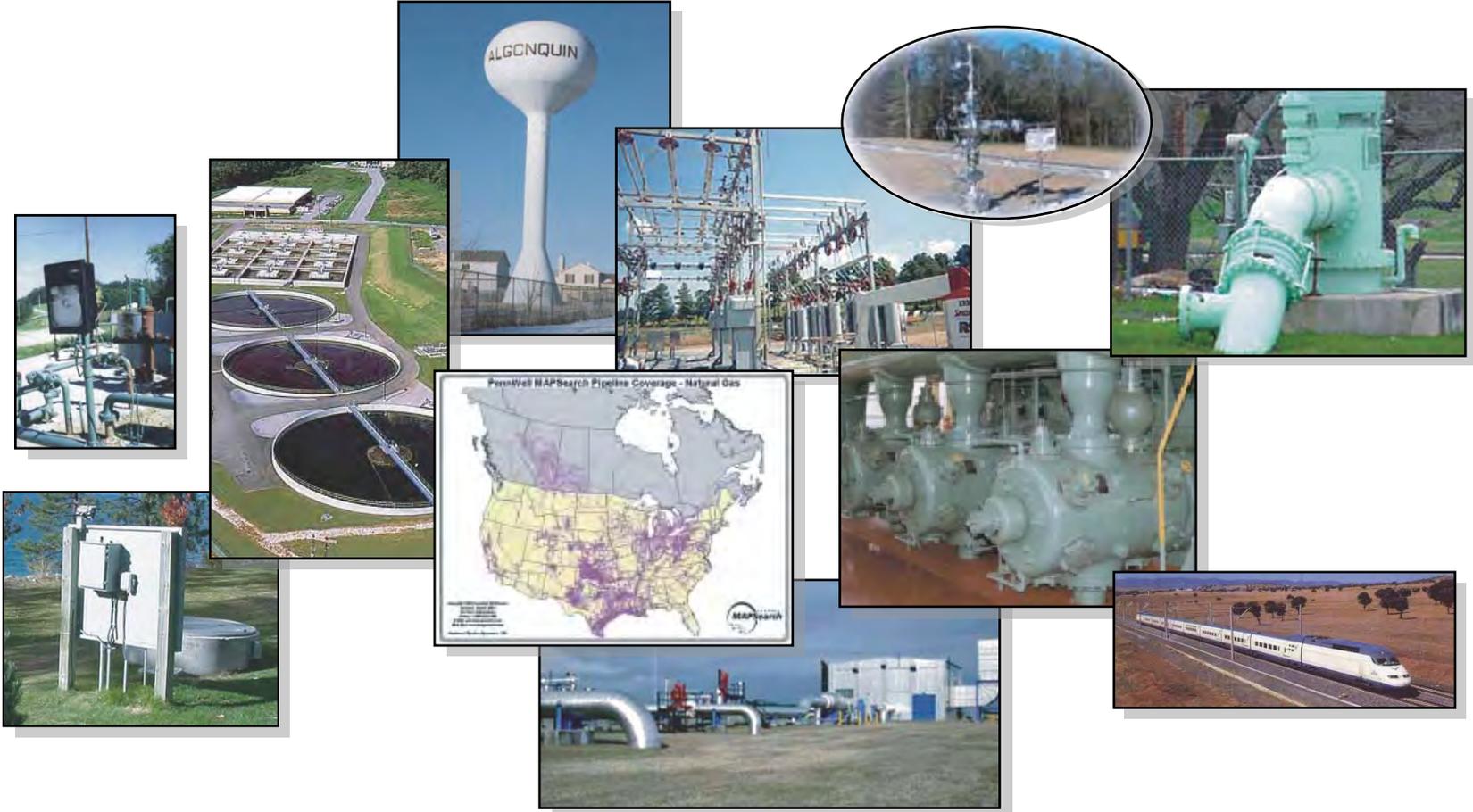


Control Systems Security Metrics Interest Group

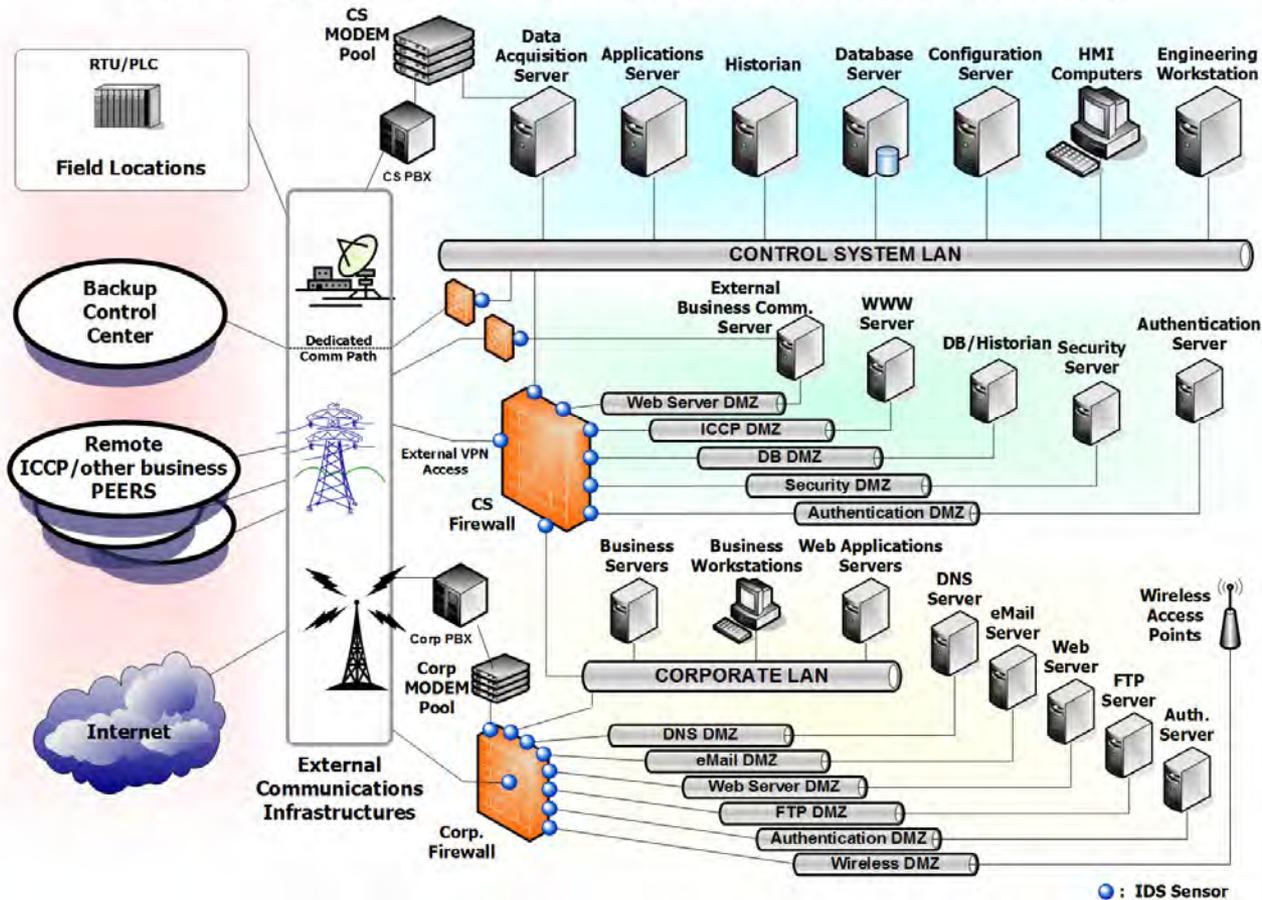
**Control Systems Security Metrics Interest Group
Miles McQueen
Idaho National Laboratory
PCSF March 6, 2007**

Critical Infrastructure (CI)



Critical Infrastructure Control Systems

CONTROL SYSTEM/ENTERPRISE ARCHITECTURE



Securing CI from Control System Compromise

Risk = F (threats_{CS}, vulnerabilities_{CS}, consequences_{CI})

◆ Threats

- Natural
- Intelligent adversary
 - Random
 - Targeted

◆ Vulnerabilities

- Applications
- Components
- Systems

◆ Consequences

- Firm
- Infrastructure
- Across infrastructures

Security Metrics Interest Group Objectives

- ◆ **Propose, develop, field, and refine (technical) security metrics to support**
 - Frameworks and taxonomies for system security thinking
 - Improved system security awareness
 - Identification of measurement tool needs (drive development)
 - Development of security standards and good practices
 - Improved identification of system security R&D needs
 - Risk reduction efforts

What Makes a Great Metric

◆ Correlation

- Measure correlates to security goals

◆ Objectivity

- Not influenced by the measurer

◆ Repeatability

- Should return the same result if repeated in the same context

◆ Easy

- Measurement is simple to perform

◆ Clarity

- Easy to interpret
- Units are explicit

◆ Succinctness

- Incorporates only the important aspects

◆ Completeness

- Captures all relevant information

Levels of Measurement

- ◆ **Nominal scale**
- ◆ **Ordinal scale**
- ◆ **Interval scale**
- ◆ **Ratio scale**

Breakout Session Objectives

- ◆ **Share current work and accomplishments in security metrics**
- ◆ **Establish relationships and initiate new collaborations in further development, use, and refinement of (technical) security metrics**
- ◆ **Discuss needs, issues, and opportunities related to security metrics**

Agenda

- Miles McQueen, INL/CSSP Introduction (10 m)
- Cliff Glantz, PNNL/I3P I3P accomplishments (25 m)
- Ron Halbgewachs, SNL/NSTB Security metrics taxonomy (25 m)
- Eric Byres, Byres Security MTTC metric: R&D (25 m)
- Wayne Boyer, INL/CSSP Security ideals and baseline set of technical metrics (25 m)
- Miles McQueen, INL/CSSP Open discussion and closeout (10 m)