U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

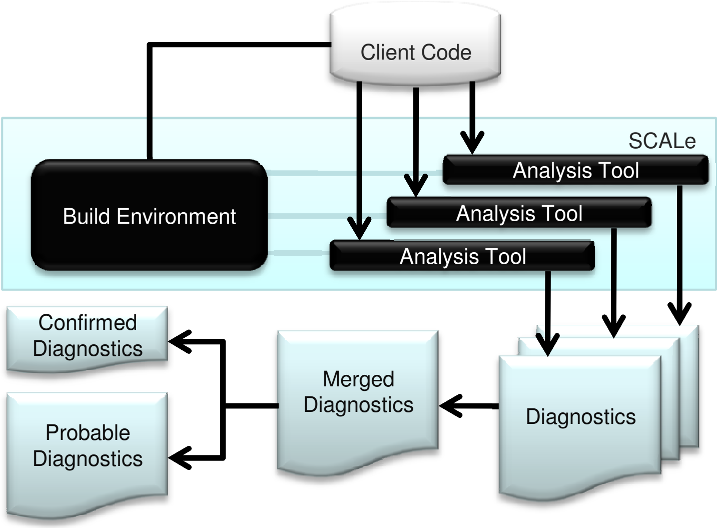
Robert C. Seacord

CERT / Software Engineering Institute

Source Code Analysis Laboratory (SCALe)

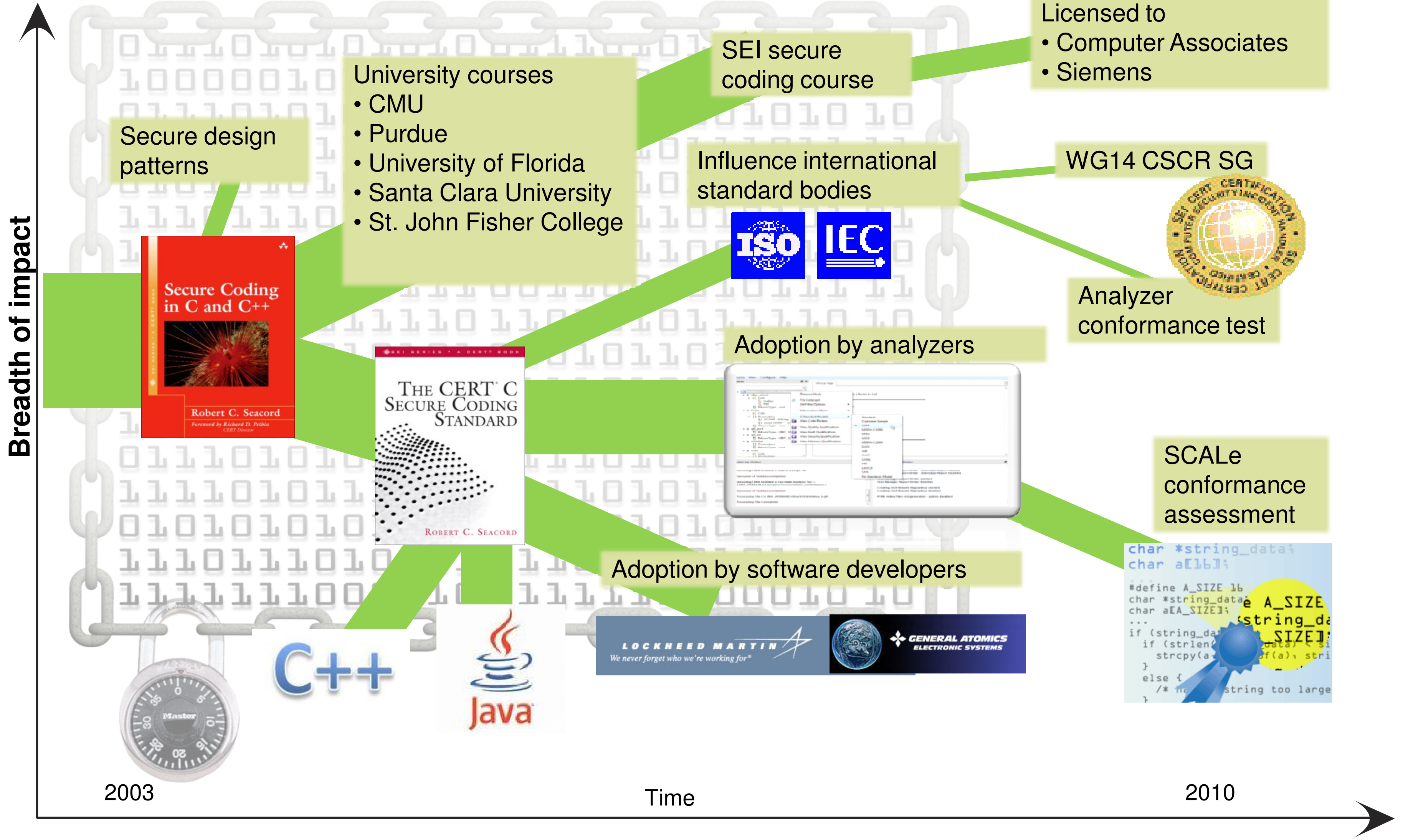
Summary Slide: SCALe

- **Outcomes:** Create an operational capability for application conformance testing and certification against CERT secure coding standards.
- **Roadmap Challenge:** Limited ability to measure and assess cyber security posture/no consistent cyber security metrics/increasingly sophisticated hacker tools
- **Major Successes:** Preliminary analysis of SCADA system completed



- **Schedule:** Draft TR 7/10; assessment and certification of commercial SCADA application 11/10
- **Level of Effort:** $250K
- **Funds Remaining:** $214K
- **Performers:** SEI CERT
- **Partners:** NETL and NSTB-participating laboratories, software and system vendors

SCALe in Context



Secure design patterns

University courses
- CMU
- Purdue
- University of Florida
- Santa Clara University
- St. John Fisher College

SEI secure coding course

Licensed to
- Computer Associates
- Siemens

Influence international standard bodies

WG14 CSCR SG

Analyzer conformance test

Adoption by analyzers

SCALe conformance assessment

Adoption by software developers

Breadth of impact
Time
2003
2010
Secure Coding in C and C++
Robert C. Seacord
The CERT C Secure Coding Standard
Robert C. Seacord
ISO
IEC
C++
Java
Lockheed Martin
We never forget who we're working for
General Atomics Electronic Systems

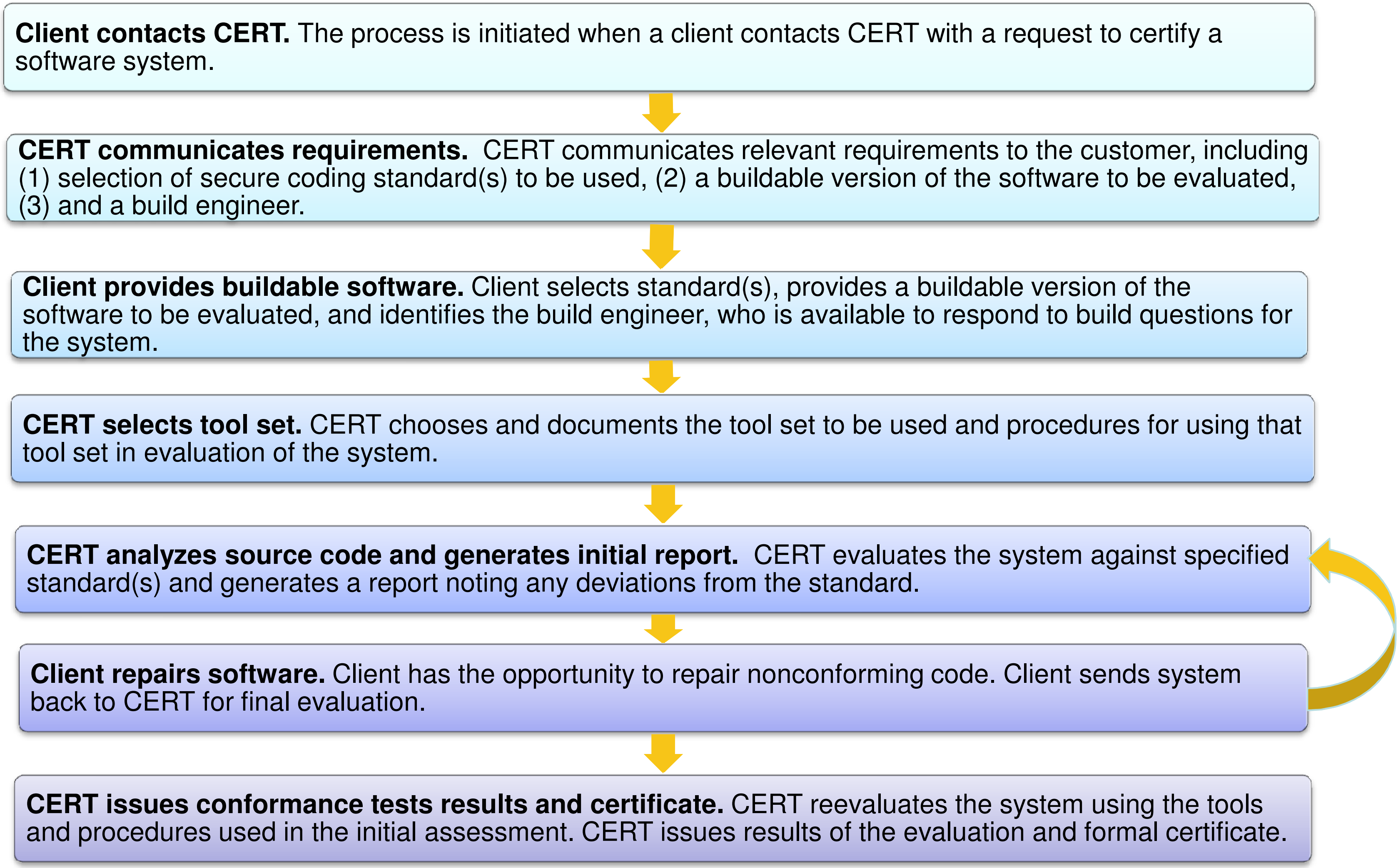
CERT SCALe (Source Code Analysis Lab)

- Satisfy demand for source code assessments for both government and industry organizations.
- Assess source code against secure coding standards.
- Provide a detailed report of findings.
- Assist customers in developing conforming systems.

Technical Approach and Feasibility

- Approach
  - Establish an operational SCALe capability, including
    - automatic processing of the results of static analysis tools
    - incorporation of instrumented fuzz testing
    - evolving the secure coding standards and analysis checkers for Compass/ROSE and other analysis tools
  - Assess and certify a SCADA application to
    - validate the approach and demonstrate the capabilities of the SCADA SCALe
    - tune the CERT Secure Coding Standards and analyzers to effectively diagnose vulnerabilities present in SCADA systems
- Metrics for Success
  - Successful certification of a SCADA system
  - Conforming systems are free from software vulnerabilities

SCALe Process Overview



Client contacts CERT. The process is initiated when a client contacts CERT with a request to certify a software system.

CERT communicates requirements. CERT communicates relevant requirements to the customer, including (1) selection of secure coding standard(s) to be used, (2) a buildable version of the software to be evaluated, (3) and a build engineer.

Client provides buildable software. Client selects standard(s), provides a buildable version of the software to be evaluated, and identifies the build engineer, who is available to respond to build questions for the system.

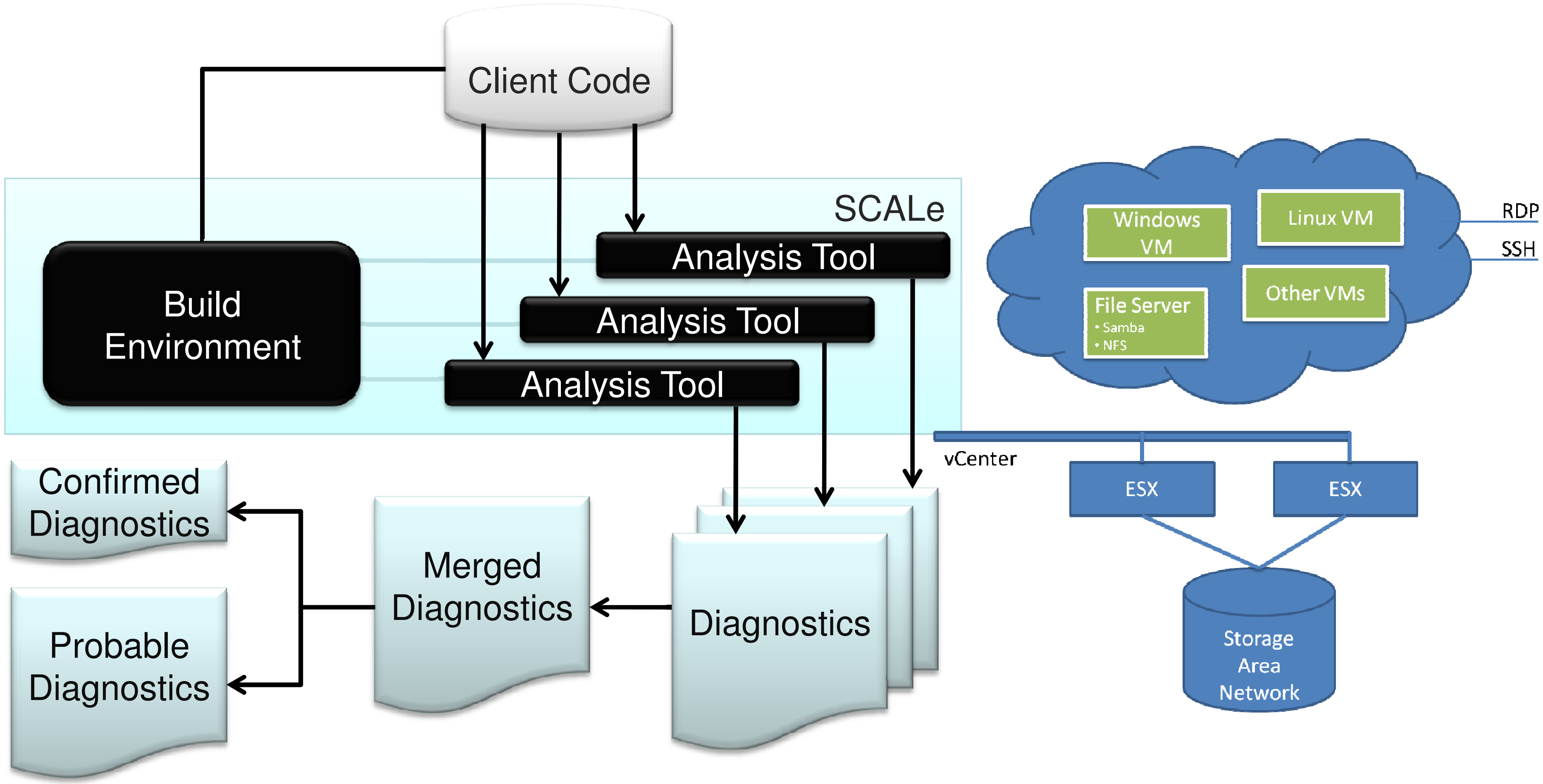
CERT selects tool set. CERT chooses and documents the tool set to be used and procedures for using that tool set in evaluation of the system.

CERT analyzes source code and generates initial report. CERT evaluates the system against specified standard(s) and generates a report noting any deviations from the standard.

Client repairs software. Client has the opportunity to repair nonconforming code. Client sends system back to CERT for final evaluation.

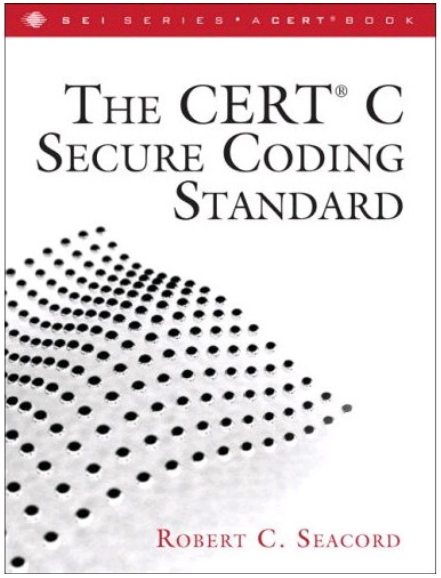
CERT issues conformance tests results and certificate. CERT reevaluates the system using the tools and procedures used in the initial assessment. CERT issues results of the evaluation and formal certificate.

Source Code Assessment Laboratory



Conformance Testing

- The use of secure coding standards defines a proscriptive set of rules and recommendations against which the source code can be evaluated for compliance.



INT30-C.	Provably nonconforming
INT31-C.	Documented deviation
INT32-C.	Conforming
INT33-C.	Provably Conforming

Technical Approach and Feasibility

- **Challenges to Success**
  - Legal, business challenges of software certification
    - Working with CMU counsel
  - Not all software is created equal
    - Adapting SCALe to control systems in the electricity sector
- **Technical Achievements to Date**
  - Development of CERT C Secure Coding Standard
  - Successful analysis of a dozen systems across a range of domains
  - Draft technical report describing the SCALe methodology and how users access and benefit from the facility
  - Initial assessment of candidate system for certification

True Positives vs. Flagged Nonconformities

- Do not apply the `sizeof` operator to an expression of pointer type (ARR01-C) Applying the **`sizeof`** operator to an expression of pointer type can result in under allocation, partial initialization, partial copying, or other logical incompleteness or inconsistency if, as is usually the case, the programmer means to determine the size of an actual object. If the mistake occurs in an allocation, subsequent operations on the under-allocated object may lead to buffer overflows.
- Ratio of true positives (bugs) to flagged nonconformities:

Software System	TP/FNC	Ratio
Mozilla Firefox version 2.0	6/12	50%
Linux kernel version 2.6.15	10/126	8%
Wine version 0.9.55	37/126	29%
xc, version unknown	4/7	57%

Each checker can be adapted to control systems in the electricity sector

Collaboration/Technology Transfer

- **Plans to gain industry input**
  - We have completed an initial assessment of a software component from a major vendor and are working with others to identify candidate systems.
  - A software version that passes conformance testing is certified as conforming to standards.
    - Certification is published in a registry of certified systems maintained on the CERT website.
    - Vendor is licensed to use the "CERT SCALe" seal to market their investment in security.
  - Challenges are providing this service in a defined, repeatable fashion at a predictable and reasonable cost.
- **Plans to transfer technology/knowledge to end user**
  - Developing a transition plan for operationalization and ongoing management of the SCADA SCALe in the context of the NSTB.
  - CERT will accredit laboratories to perform conformance assessment and certification.
  - Source code assessment extends (without interference) existing capabilities to protect the reliability of power systems.

Plans to Gain Industry Adoption

- Conformance with CERT Secure Coding Standards can represent a significant investment by a software developer, particularly when it is necessary to refactor or otherwise modernize existing software systems.
- It is not always possible for a software developer to benefit from this investment because it is not always easy to market code quality.
- SCALe provides a mechanism by which vendors can benefit from investing in software security by marketing and promoting their investment with a "CERT SCALe" seal indicating that
  - The software system has undergone third-party evaluation by CERT.
  - The software system has been determined to conform with a CERT Secure Coding Standard.

Next Steps

- **Approach for the next year:**
  - Analyze and certify additional systems.
  - Use results to iteratively improve
    - secure coding rules
    - analysis checkers
    - automation of analysis process
- **Source code analysis of security vulnerabilities must be an integral part of an effort to secure control systems in the energy sector.**
- **Complete analyzable C Secure Coding Rules ISO/IEC technical report, implement corresponding checkers, and integrate into SCALe**
  - Submission to ISO/IEC WG14 in September 2012