Taking the Guesswork out of the NIST CSF

IADC Cybersecurity Workshop

Perry Pederson
The Langner Group
Washington DC | Hamburg | Munich

Agenda

- Asset Identification
- Vulnerability Assessment
- Governance Process

The RIPE Program

Robust Industrial Control Systems Planning and Evaluation

Langner

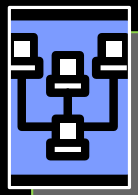
RIPE in Critical Infrastructure

- The Loviisa nuclear power plant (Finland) trusts RIPE for efficient and measurable cyber security
- Fact-based performance in the real world
  - Not unfounded claims and hyperbole

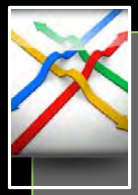
Langner

RIPE Domains

System Inventory



Network Diagrams



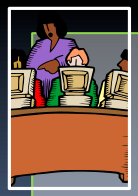
Dataflow Diagrams

Plant Planning Guideline

Procurement Guideline

Workforce Information Database

Policy & SOP Repository



Training Program

Langner

Standards/Frameworks Crosswalk

Crosswalk Summary Matrix

		RIPE	ISA 99	NERC CIP	RG 5.71	NEI 08-09	ISO 27000	WIB	DOE C2M2	NIST CSF
RIPE Functions & Attributes	Governance									
	Metrics									
	Structural & Behavioral System Model									
	Cyber Security Capability Development									
	Ready-to-use Templates									
	Information Sharing on Problems & Progress									
	Cross-industry Approach									
RIPE Domains	System Population Characteristics									
	Network Architecture									
	Component Interaction									
	Workforce Roles and Responsibilities									
	Workforce Skills & Competence Development									
	Procedural Guidance (Policies & SOPs)									
	Deliberate Design Change									
	System Acquisition									
	Alternative to Risk-Based/Risk-Informed									

Significant differences
Some elements in common
Significant similarities

Asset Identification

NIST CSF Guidance

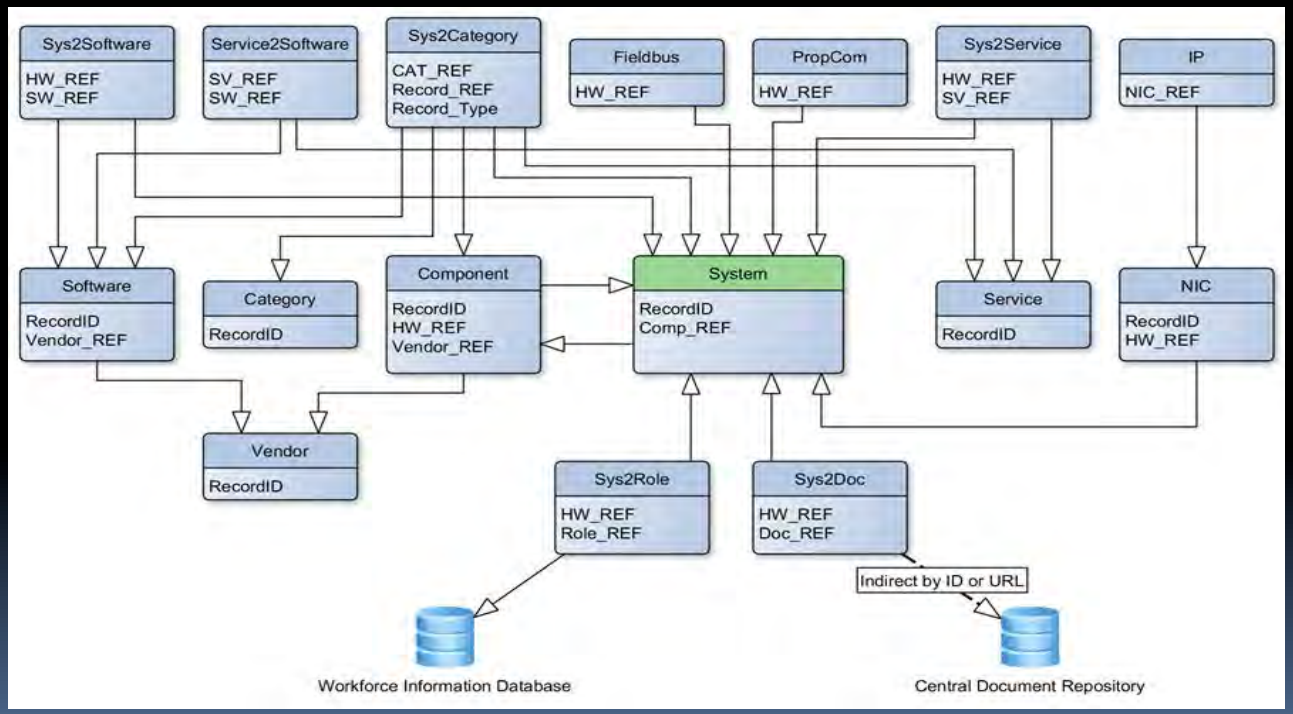
- Points to NIST SP 800-53 Rev. 4 (but also lists five other standards)
  - Baseline configurations include information about information system components, network topology, and the logical placement of those components within the system architecture.

RIPE Guidance

- RIPE System Inventory Database Architecture Guideline
- RIPE Implementation Guideline
- RIPE Plant Planning Guideline

System Inventory

Reference DBMS Architecture



Langner

Vulnerability Assessment

NIST CSF Guidance

- It is important that organizations seek to incorporate emerging risks and threat and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events
- Threat and vulnerability information is received from information sharing forums and sources
- A vulnerability management plan is developed and implemented
- Vulnerability scans are performed

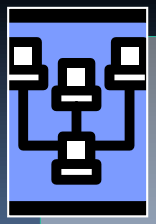
RIPE Guidance

- RIPE System Inventory Database Architecture Guideline
- RIPE Network Diagram Style Guide
- RIPE Data Flow Diagram Style Guide specifies what data flow diagrams should look like.

Advanced Vulnerability Analysis

System Inventory

Dataflow Diagrams



Network Diagrams

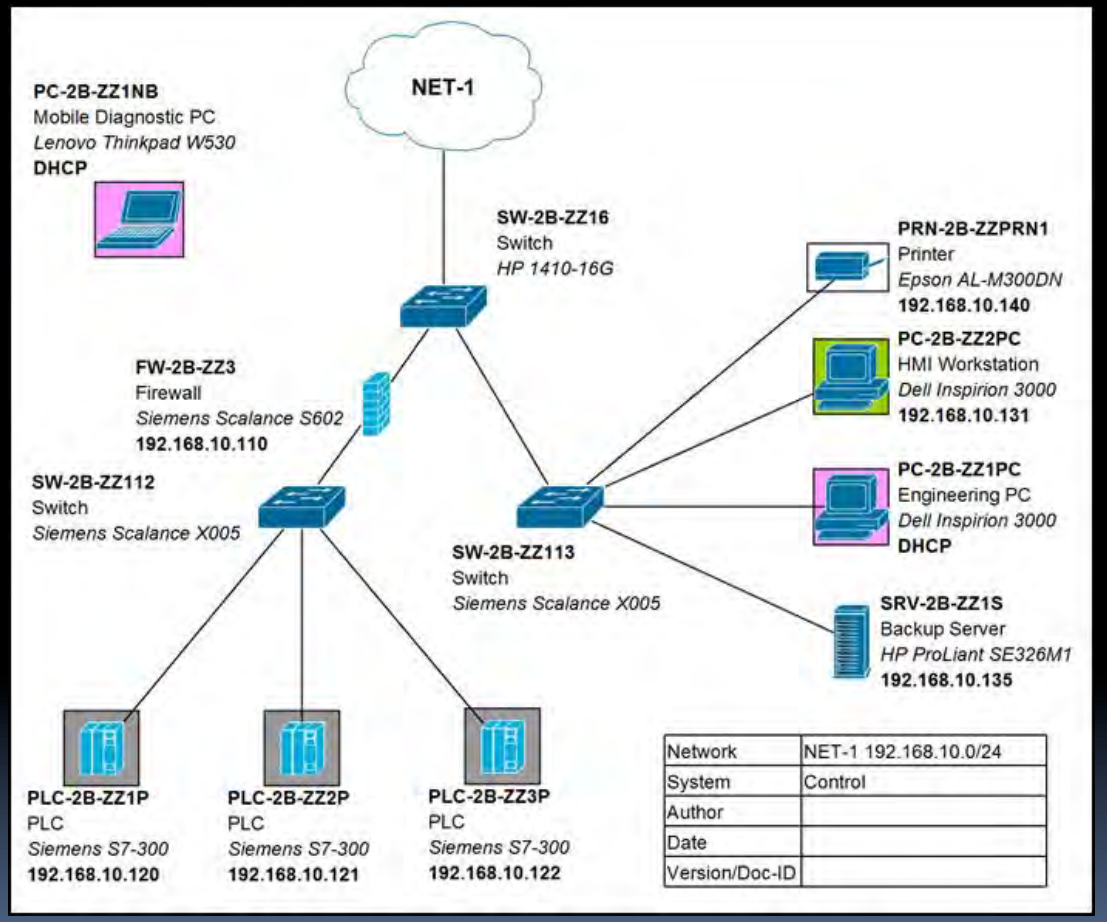
Enumeration of Cyber-Physical Vulnerabilities in Real-World Context (not Artificial Testbed)

RIPE Analysis to Discover Plant-Level Vulnerabilities

Langner

Network Diagrams

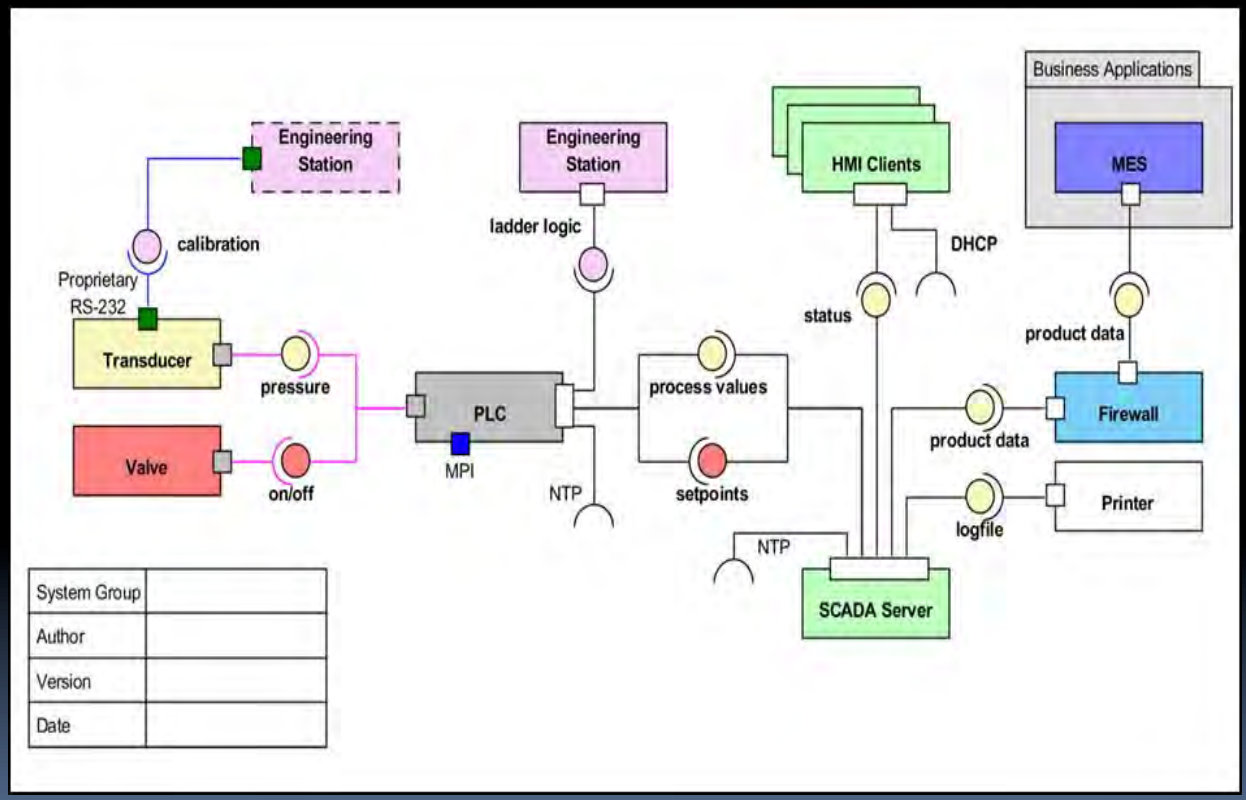
- Shows potential access routes
- Derived from Cisco Systems library
- Color codes highlight functionality
- Step-by-step guidance



Langner

Dataflow Diagrams

- Actual interaction pathways and dependencies as implemented in software (including operating systems)
- Produced as UML (Unified Modeling Language) component diagrams



Langner

Governance Process

NIST CSF Guidance

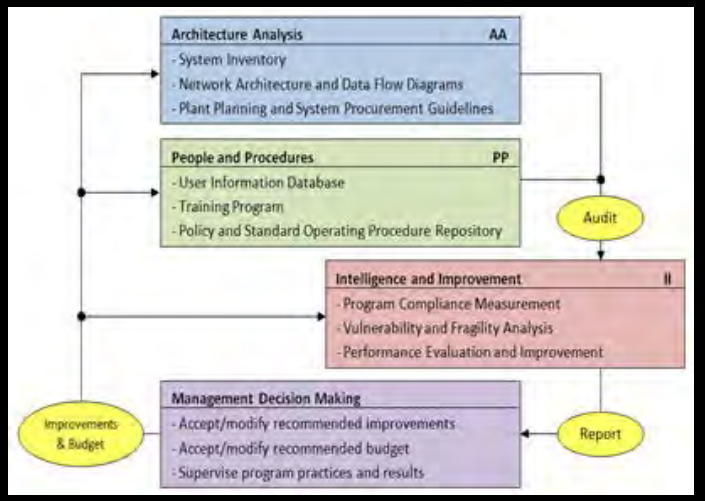
- An organization's assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program
- Individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained
- Process is in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements
- Process is in place to assess implementation of the foregoing organizational measures and controls

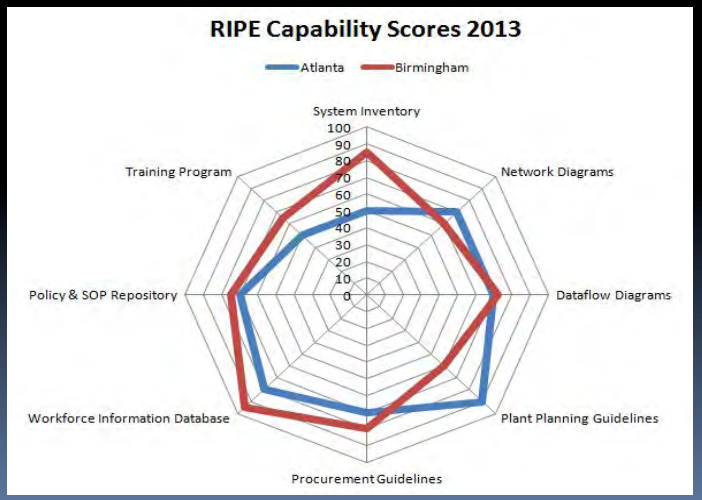
RIPE Guidance

- RIPE Cyber Security and Robustness Program
- RIPE Implementation Guideline
- RIPE Policies and Procedures
- RIPE Training Curriculum
- RIPE Metrics

RIPE Governance Process

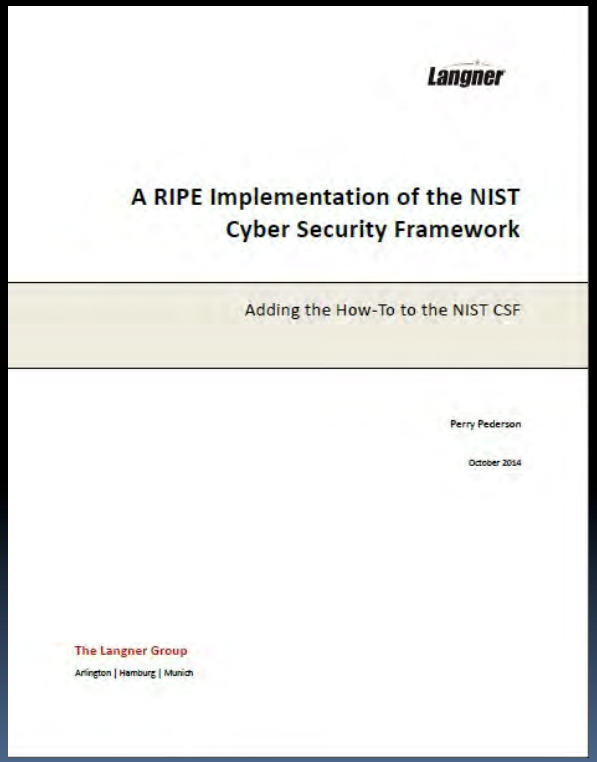
- Evaluate and continuously improve cyber security and robustness of ICS regardless of current state
- RIPE governance consists of:
  - Architecture Analysis
  - People and Procedures
  - Intelligence and Improvement
  - Management Decision Making
- Effective governance is hardly possible without metrics





Langner

Full Whitepaper


Langner

A RIPE Implementation of the NIST Cyber Security Framework

Adding the How-To to the NIST CSF

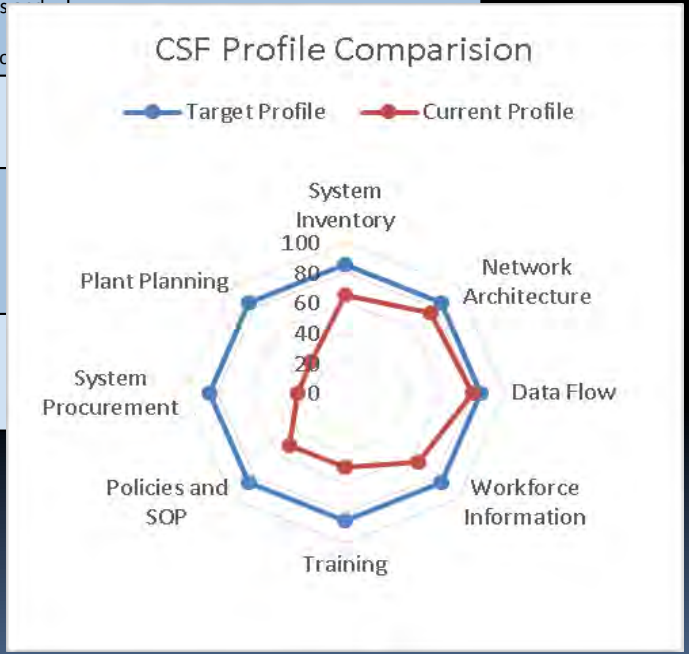
Perry Pederson

October 2014

The Langner Group

Arlington | Hamburg | Munich

NIST CSF Function	NIST CSF Category	Reference RIPE Program Element
Identify	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Architecture Analysis • People and Procedures • Intelligence and Improvement • Reporting and Management Sign-Off • Roles and Responsibilities
Protect	• Access Control • Awareness and Training • Data Security • Information Protection Processes Procedures • Maintenance Protective Technolc	• Architecture Analysis • People and Procedures • Roles and Responsibilities
Detect	• Anomalies and Events • Security Continuous Monitoring • Detection Processes	
Respond	• Response Planning • Communications • Analysis • Mitigation • Improvements	
Recover	• Recovery Planning • Improvements • Communications	



Langner

Additional Reading

- A RIPE Implementation of the NIST Cyber Security Framework
  - http://www.langner.com/en/wp-content/uploads/2014/10/A-RIPE-Implementation-of-the-NIST-CSF.pdf
- The RIPE Brochure
  - http://www.langner.com/en/wp-content/uploads/2014/09/RIPE-Brochure.pdf
- The RIPE Program Whitepaper
  - http://www.langner.com/en/wp-content/uploads/2013/09/The-RIPE-Framework.pdf
- Robust control system networks: How to achieve reliable control after Stuxnet
  - http://www.amazon.com/Robust-Control-System-Networks-Langner/dp/1606503006
- To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve
  - http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf
- Bound to Fail: Why Cyber Security Risk Cannot Be "Managed" Away
  - http://www.brookings.edu/research/papers/2013/02/cyber-security-langner-pederson
- A Cost-Efficient Approach to High Cyber Security Assurance in Nuclear Power Plants
  - http://www.langner.com/en/wp-content/uploads/2014/04/High-Cyber-Security-Assurance-in-NPPs.pdf

Langner

GET RIPE!

The Langner Group
Washington DC | Hamburg | Munich
www.langner.com/en
Twitter: @langnergroup
Email: pp@langner.com
Phone: 571-551-2998

RIPE Take control of your digital plant ecosystem