Cyber Security Requirements for Supply Chain

June 17, 2015

DUKE ENERGY®

Topics

- Cyber Threat
- Legislation and Regulation
- Nuts and Bolts of NEI 08-09
- Nuclear Procurement
- EPRI Methodology for Procurement
- Something to think about
- Wrap it up!

?????

- Is my company’s cyber security posture creating a vulnerability for my customer?

https://www.youtube.com/watch?v=mP4LwIPzcvU

Cyber Threat to the critical infrastructure?

- Premature system failures during usage.
- Access to otherwise secure systems.
- By-passes of encryption systems.
- Intimate access to target systems to inflict damage with malicious intent.

Cyber Threat – what's reality?

…manufacturing most targeted sector in 2012, accounting for 24% of all targeted attacks.[1](Symantec)

"Attackers tend to go after systems that can be successfully compromised, and ICS [industrial control systems] have shown themselves to be a target-rich environment." [2](McAfee)

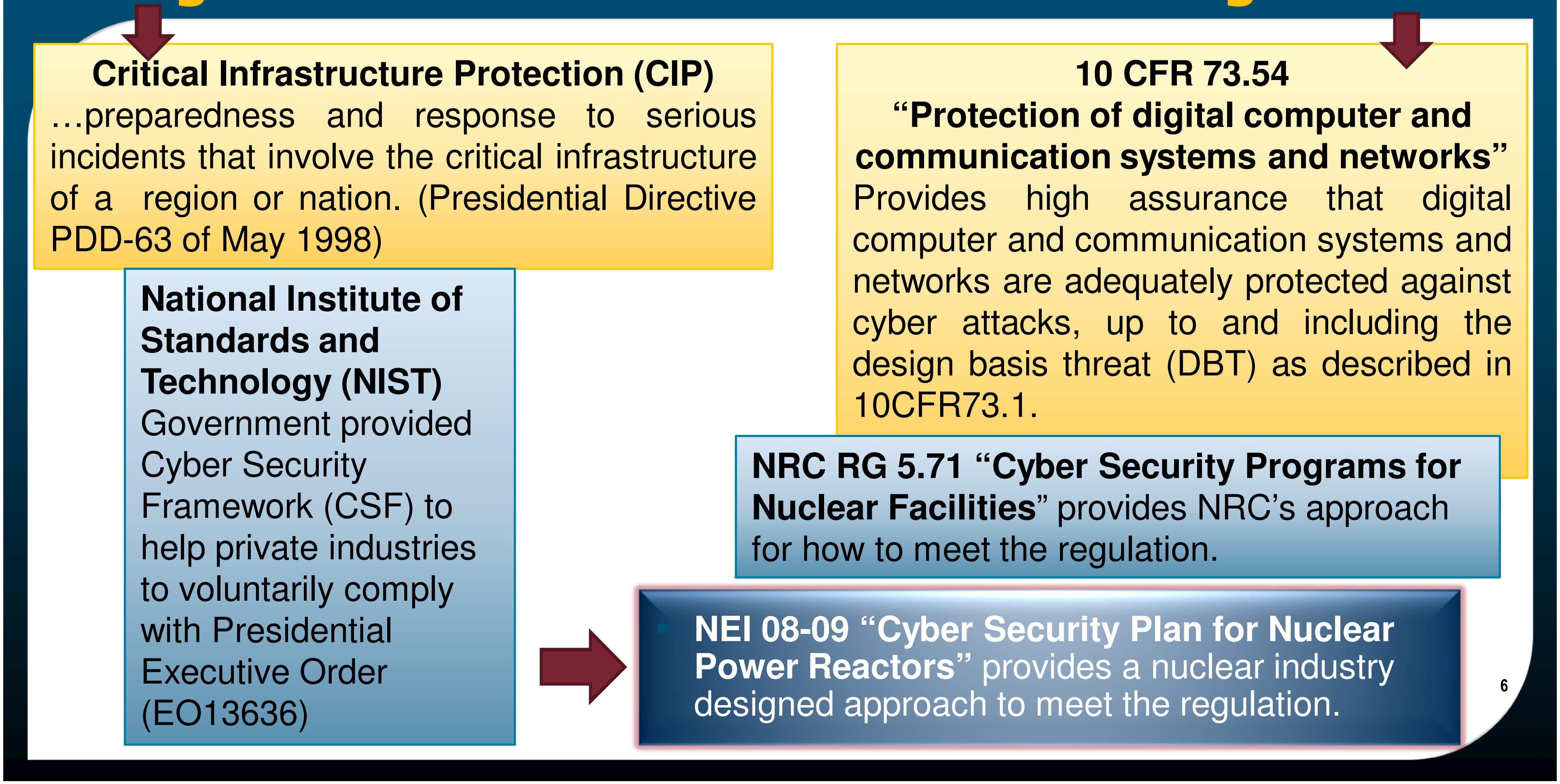
The Energy Sector was the target of 40% of cyber attacks in 2013, according to the Department of Homeland Security.

…largely from sophisticated, well-heeled nation-states looking to inflict damage.[4]

State-sponsored data breaches became the second most common variety of data breaches in 2012, following only organized crime…[3](Verizon)

https://www.youtube.com/watch?v=7g0pi4J8auQ

Legislation and Nuclear Regulation



Critical Infrastructure Protection (CIP)
…preparedness and response to serious incidents that involve the critical infrastructure of a region or nation. (Presidential Directive PDD-63 of May 1998)

National Institute of Standards and Technology (NIST)
Government provided Cyber Security Framework (CSF) to help private industries to voluntarily comply with Presidential Executive Order (EO13636)

10 CFR 73.54
"Protection of digital computer and communication systems and networks"
Provides high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat (DBT) as described in 10CFR73.1.

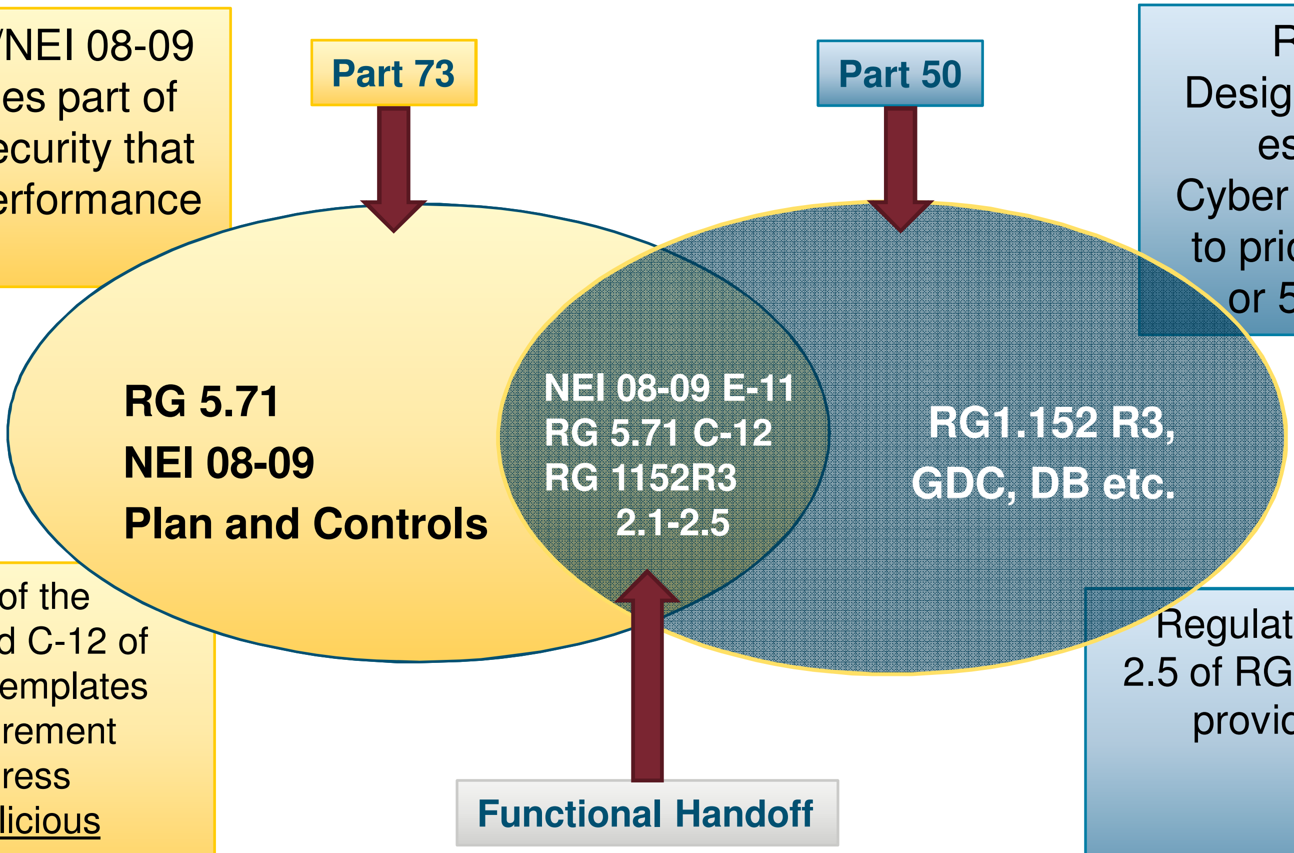
NRC RG 5.71 "Cyber Security Programs for Nuclear Facilities" provides NRC's approach for how to meet the regulation.

- **NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors"** provides a nuclear industry designed approach to meet the regulation.

Integrating Cyber Security into Nuclear

RG 5.71/NEI 08-09 establishes part of Cyber Security that will be performance based.

RG 1.152 R3 and Design Basis Defense establishes part of Cyber Security subject to prior NRC approval or 50.59 evaluation.



Part 73

Part 50

RG 5.71

NEI 08-09

Plan and Controls

NEI 08-09 E-11
RG 5.71 C-12
RG 1152R3
2.1-2.5

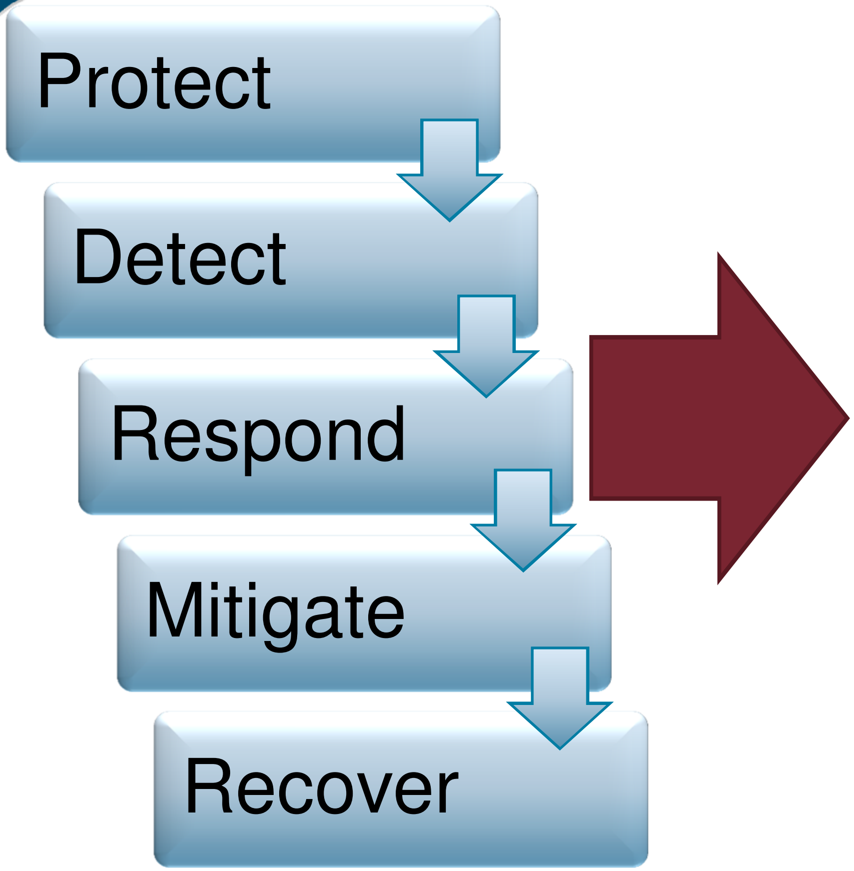
RG1.152 R3,
GDC, DB etc.

Functional Handoff

Section E-11 of the NEI 08-09 and C-12 of the RG 5.71 templates provide procurement criteria to address Intelligent malicious adversaries.

Regulatory Positions 2.1-2.5 of RG 1.152 Revision 3 provide protection from unintentional and undesirable non-malicious events

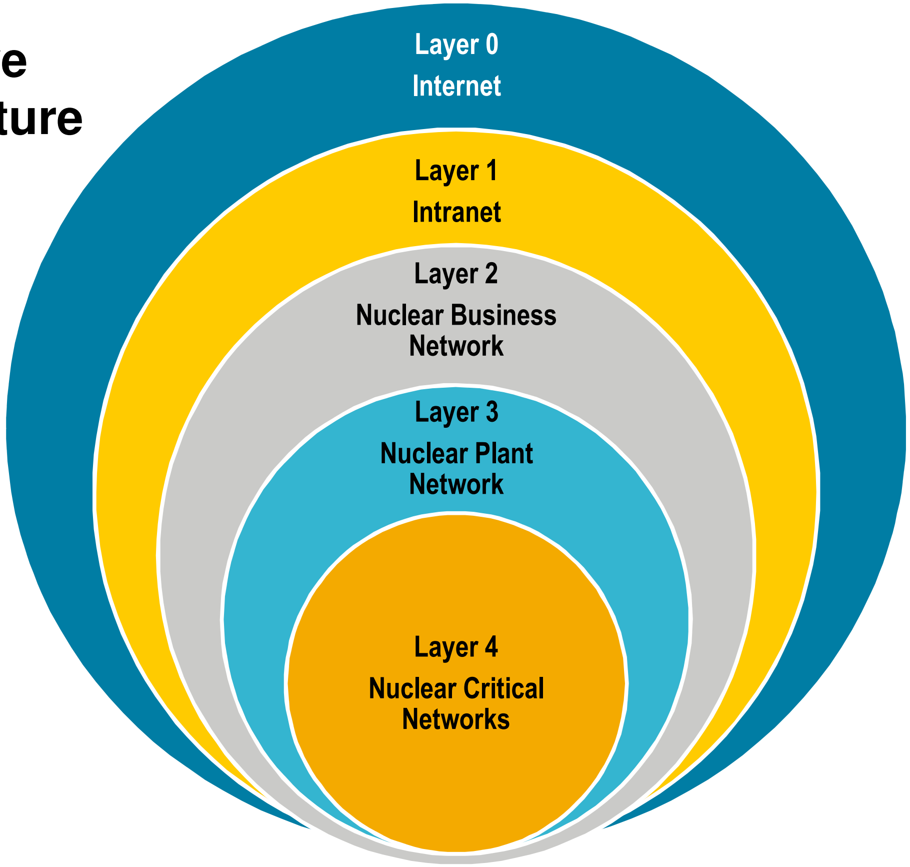
Nuts and Bolts of NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors"



- SSEP
  - Safety
  - Important to Safety
  - Security
  - Emergency preparedness, including off-site communications
- Support systems and equipment that if compromised would adversely impact the SSEP functions.

Nuts and Bolts of NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors"

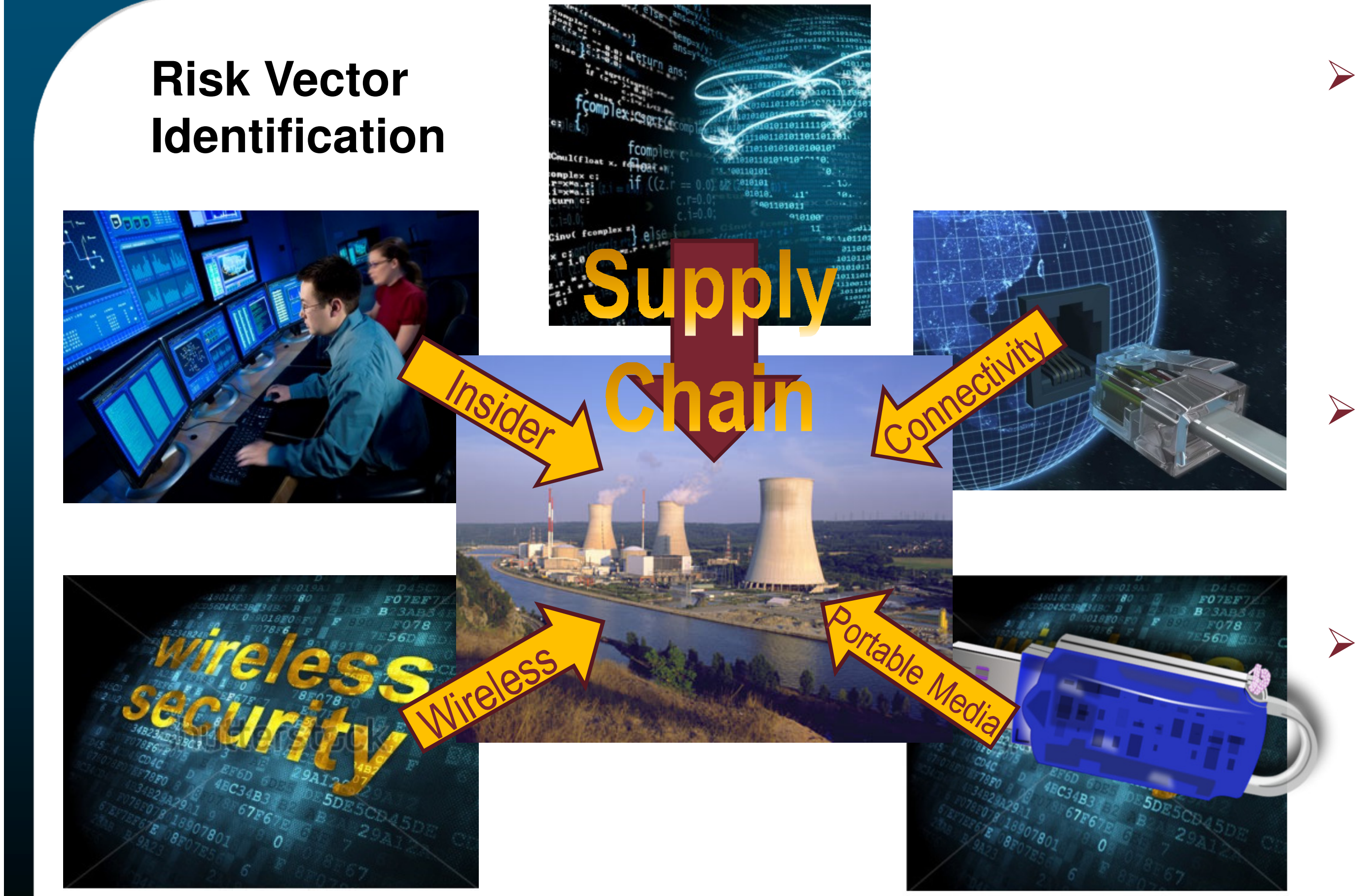
Defensive Architecture Model



- Layers segregated by combinations of firewalls and one-directional diodes.
- Provides layers of network defense.
- Layer's 3 and 4 acquire physical security by placing these networks into the Protected Area.
- **Design criteria must ensure by-pass configurations are not introduced to the architecture.**

Nuts and Bolts of NEI 08-09 "Cyber Security Plan for Nuclear Power Reactors"

Risk Vector Identification



- NEI 08-09 recognized "risk vectors" presenting a vulnerability to the plant critical systems and critical digital assets (CDAs).
- All except Supply Chain can be managed and controlled independently by the utility.
- Supply Chain requires a "trustworthy" relationship based on shared responsibility for cyber security.

Nuclear Procurement

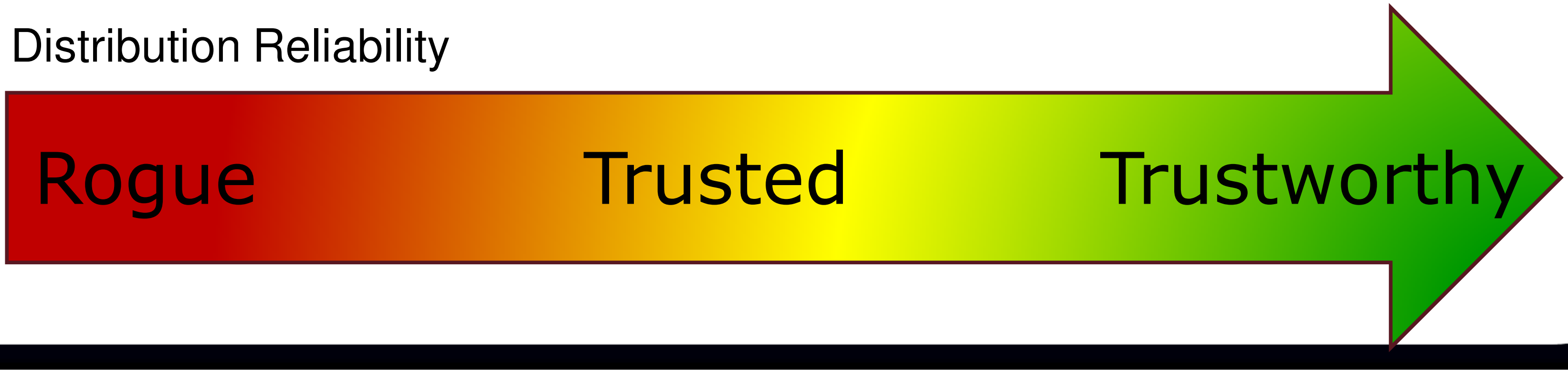
Component Procurement

- COTS transactions
- Shrink-wrapped products
- Limited/no after sales support
- Limited/no direct knowledge of the design criteria.
- Relationship is with a distributor of varying credibility rather than the manufacturer.

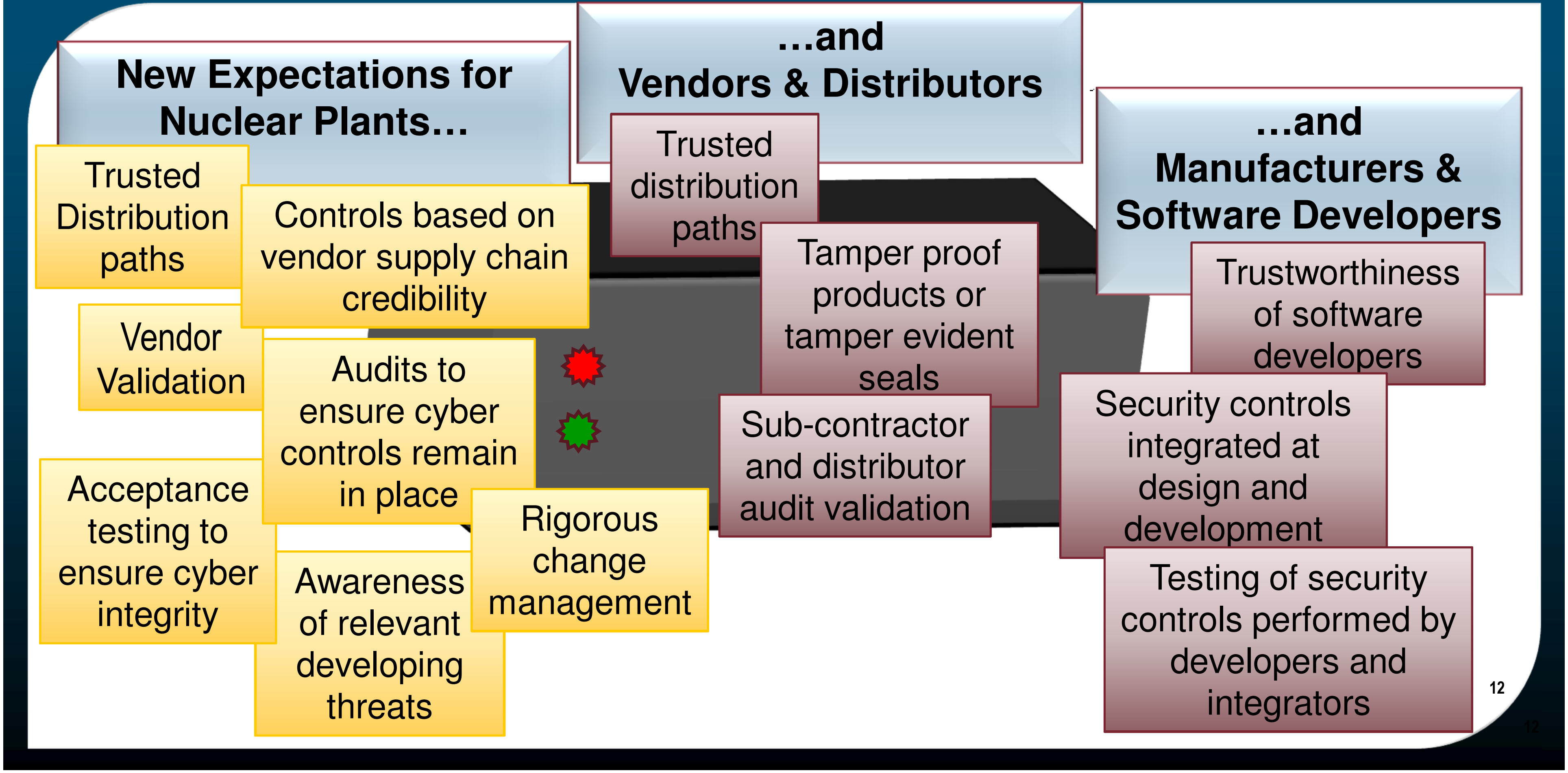
Procurement Contract

- Specifications
- Acceptance Criteria
- Access to service and suppo
- Relationship is with the manufacturer or authorized distributor

Distribution Reliability



Nuclear Procurement
NEI 08-09 “Cyber Security Plan for Nuclear Power Reactors”



New Expectations for Nuclear Plants…

- Trusted Distribution paths
- Controls based on vendor supply chain credibility
- Vendor Validation
- Audits to ensure cyber controls remain in place
- Acceptance testing to ensure cyber integrity
- Awareness of relevant developing threats
- Rigorous change management

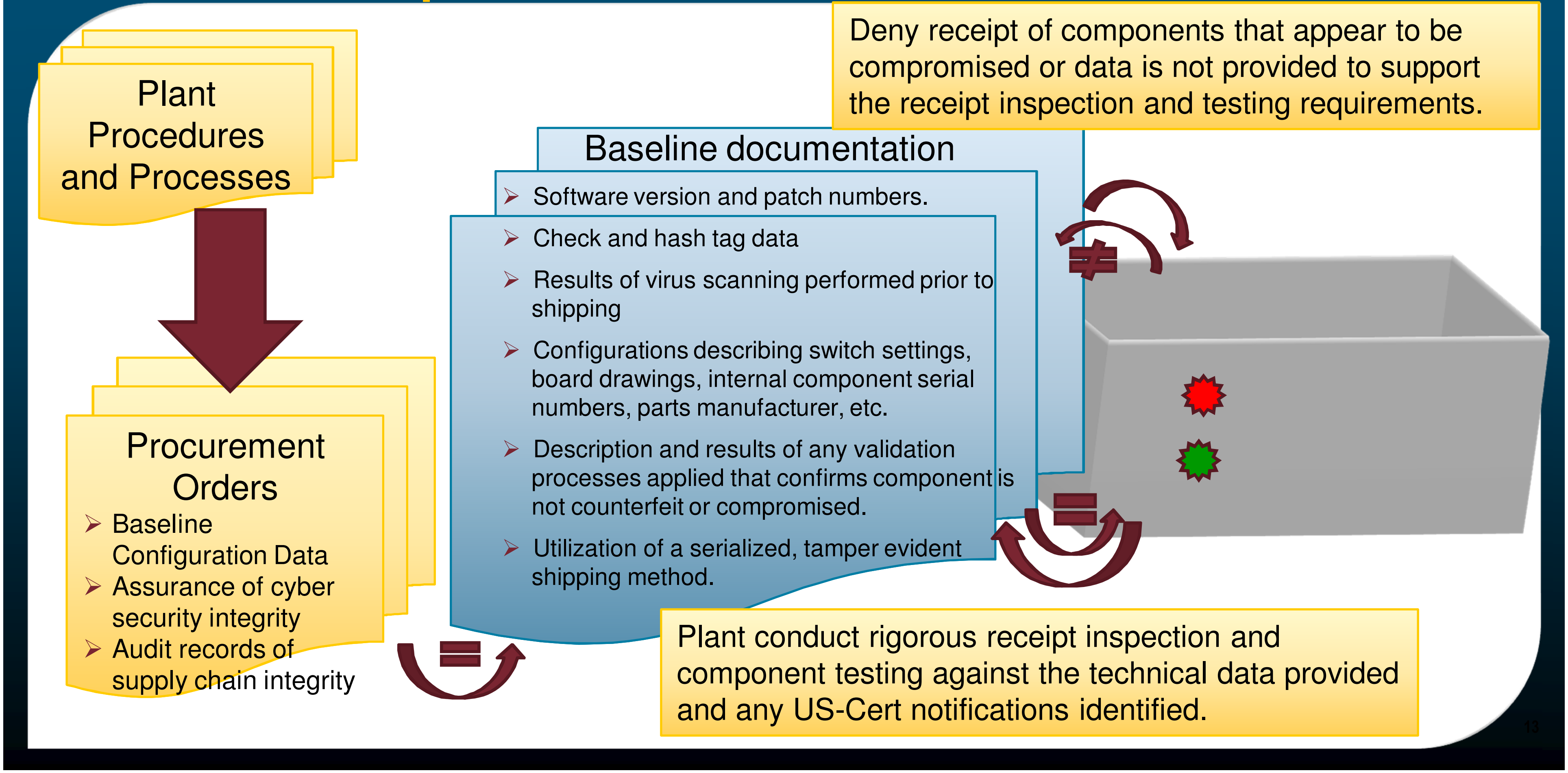
…and Vendors & Distributors

- Trusted distribution paths
- Tamper proof products or tamper evident seals
- Sub-contractor and distributor audit validation

…and Manufacturers & Software Developers

- Trustworthiness of software developers
- Security controls integrated at design and development
- Testing of security controls performed by developers and integrators

Nuclear Procurement
A Path for Component Procurements



Plant Procedures and Processes

Procurement Orders

- Baseline Configuration Data
- Assurance of cyber security integrity
- Audit records of supply chain integrity

Baseline documentation

- Software version and patch numbers.
- Check and hash tag data
- Results of virus scanning performed prior to shipping
- Configurations describing switch settings, board drawings, internal component serial numbers, parts manufacturer, etc.
- Description and results of any validation processes applied that confirms component is not counterfeit or compromised.
- Utilization of a serialized, tamper evident shipping method.

Deny receipt of components that appear to be compromised or data is not provided to support the receipt inspection and testing requirements.

Plant conduct rigorous receipt inspection and component testing against the technical data provided and any US-Cert notifications identified.

Nuclear Procurement
A Path for Future Contracts

Plant Procedures and Processes

Procurement Contracts

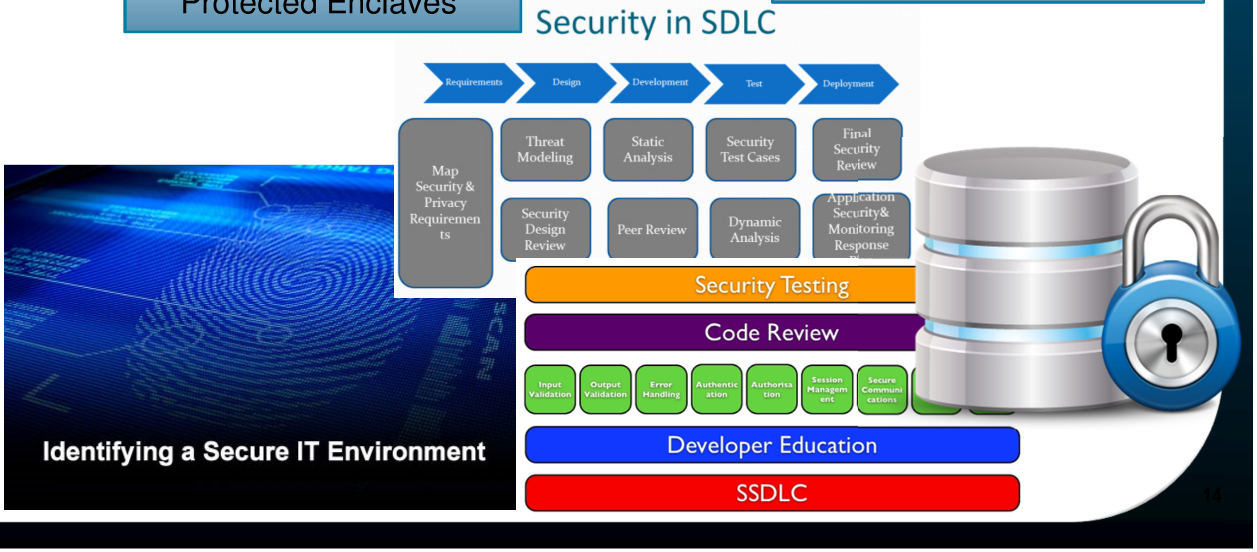
- Implement Safety and Security Procurement Requirements within contracts
- Conduct cyber aware regulatory reviews and evaluations
- Follow ISG-06 processes where applicable

Contractor Procedures and Processes

- Vendor established Development Environment including Protected Enclaves

- meet contract requirements for a Secure Development and Operational Environment (SDOE)

- Vendor assessments of their Development Environment including audit results available for review



UP NEXT…

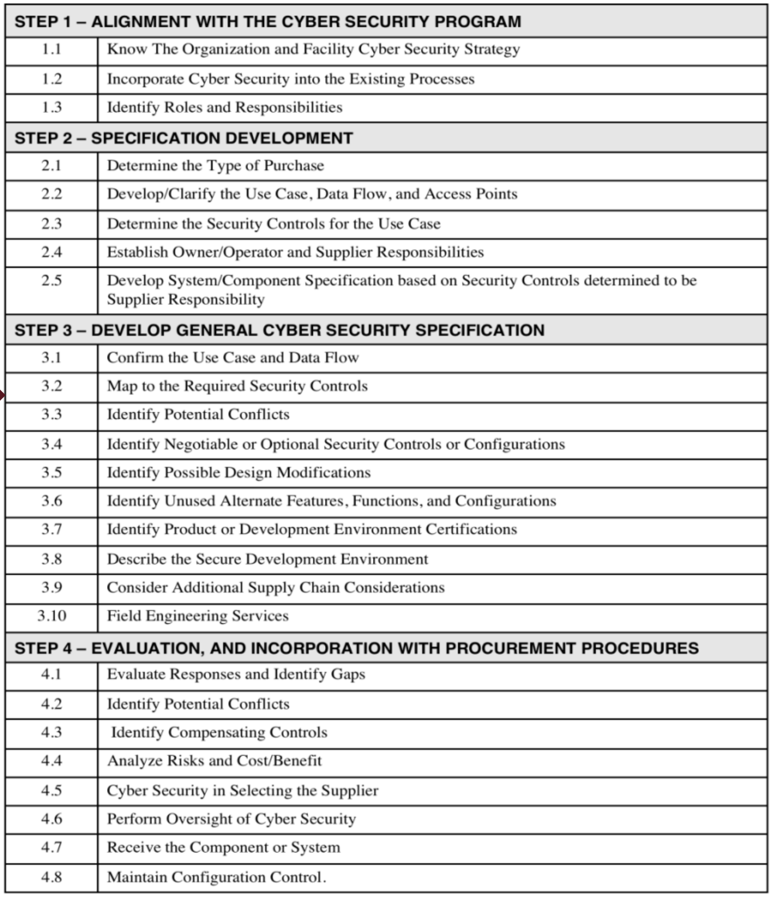
EPRI Procurement Methodology

Cyber Security Procurement Portfolio

- Cyber Security Procurement Methodology, Rev. 1- 3002001824
- Cyber Security Procurement, First Example: Digital Valve Controller **-**3002003257
- Cyber Security Procurement, Second Example: Feedpump TCS **-** 3002001823
- Cyber Security Procurement, Third Example: Digital Feedwater Control **-**3002002069
- ***Cyber Security Procurement CBT Rev 14.00-***3002002499

EPRI Procurement Methodology

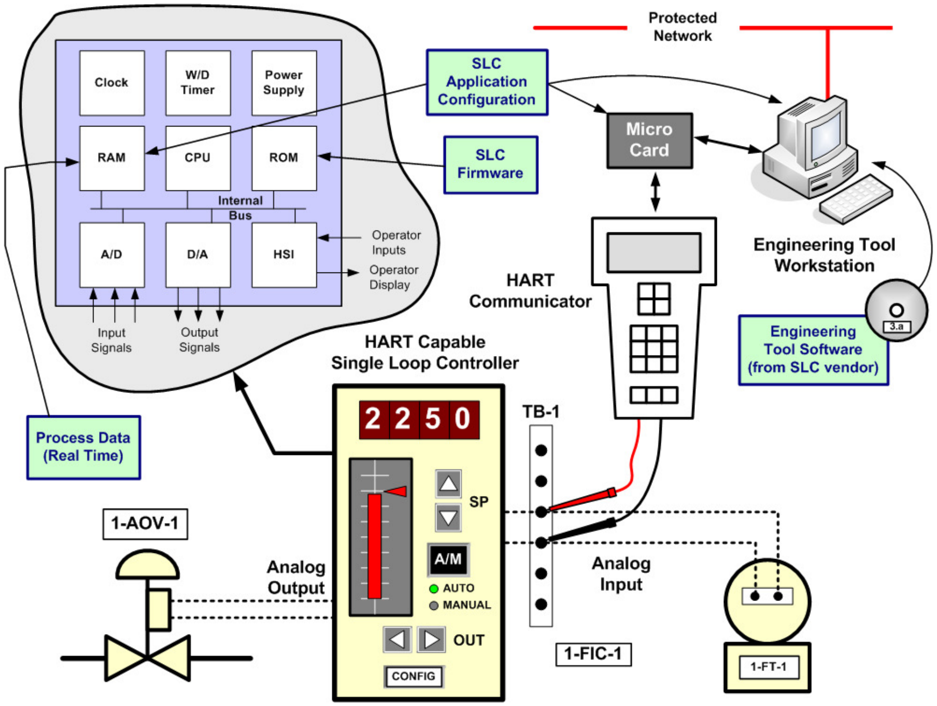
- Four Step Method guides the development of Cyber Procurement Specification.
- Specification results intersect with Utility design and procurement processes
- Allocates requirements between Utilities and vendors
- Inventory of controls applied to procurement reduced.



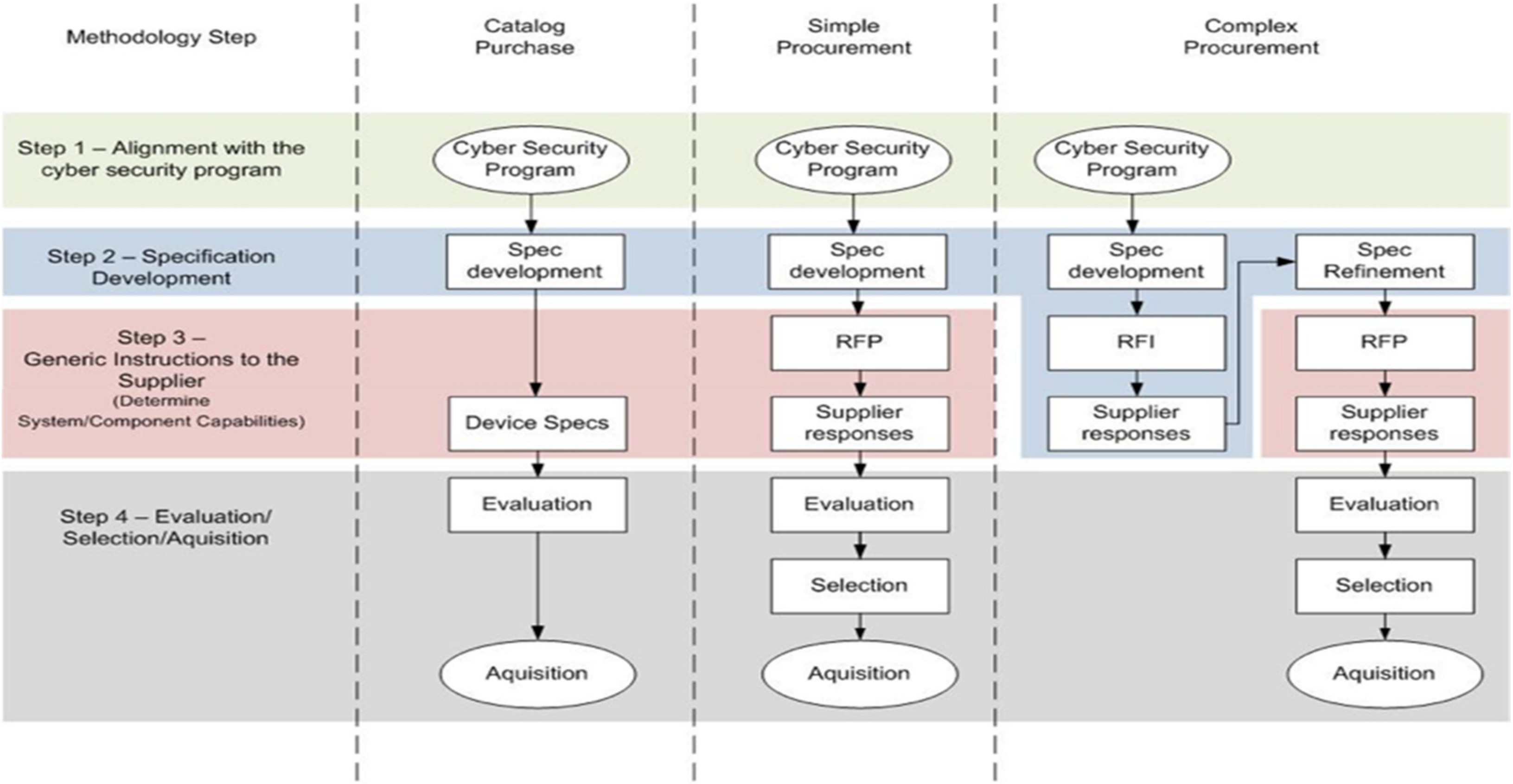
STEP 1 – ALIGNMENT WITH THE CYBER SECURITY PROGRAM	
1.1	Know The Organization and Facility Cyber Security Strategy
1.2	Incorporate Cyber Security into the Existing Processes
1.3	Identify Roles and Responsibilities
STEP 2 – SPECIFICATION DEVELOPMENT	
2.1	Determine the Type of Purchase
2.2	Develop/Clarify the Use Case, Data Flow, and Access Points
2.3	Determine the Security Controls for the Use Case
2.4	Establish Owner/Operator and Supplier Responsibilities
2.5	Develop System/Component Specification based on Security Controls determined to be Supplier Responsibility
STEP 3 – DEVELOP GENERAL CYBER SECURITY SPECIFICATION	
3.1	Confirm the Use Case and Data Flow
3.2	Map to the Required Security Controls
3.3	Identify Potential Conflicts
3.4	Identify Negotiable or Optional Security Controls or Configurations
3.5	Identify Possible Design Modifications
3.6	Identify Unused Alternate Features, Functions, and Configurations
3.7	Identify Product or Development Environment Certifications
3.8	Describe the Secure Development Environment
3.9	Consider Additional Supply Chain Considerations
3.10	Field Engineering Services
STEP 4 – EVALUATION, AND INCORPORATION WITH PROCUREMENT PROCEDURES	
4.1	Evaluate Responses and Identify Gaps
4.2	Identify Potential Conflicts
4.3	Identify Compensating Controls
4.4	Analyze Risks and Cost/Benefit
4.5	Cyber Security in Selecting the Supplier
4.6	Perform Oversight of Cyber Security
4.7	Receive the Component or System
4.8	Maintain Configuration Control.

EPRI Procurement Methodology – Use Case

STEP 2 – SPECIFICATION DEVELOPMENT	
2.1	Determine the Type of Purchase
2.2	Develop/Clarify the Use Case, Data Flow, and Access Points
2.3	Determine the Security Controls for the Use Case
2.4	Establish Owner/Operator and Supplier Responsibilities
2.5	Develop System/Component Specification



EPRI Procurement Methodology – Purchase Type

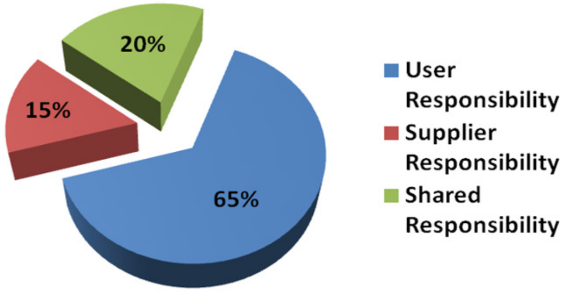


Methodology Step	Catalog Purchase	Simple Procurement	Complex Procurement	
Step 1 – Alignment with the cyber security program	Cyber Security Program	Cyber Security Program	Cyber Security Program	
Step 2 – Specification Development	Spec development	Spec development	Spec development	Spec Refinement
Step 3 – Generic Instructions to the Supplier (Determine System/Component Capabilities)	Device Specs	RFP Supplier responses	RFI Supplier responses	RFP Supplier responses
Step 4 – Evaluation/ Selection/Aquisition	Evaluation Aquisition	Evaluation Selection Aquisition		Evaluation Selection Aquisition

EPRI Procurement Methodology – Controls Allocation

STEP 2 – SPECIFICATION DEVELOPMENT	
2.1	Determine the Type of Purchase
2.2	Develop/Clarify the Use Case, Data Flow, and Access Points
2.3	Determine the Security Controls for the Use Case
2.4	Establish Owner/Operator and Supplier Responsibilities
2.5	Develop System/Component Specification

- **Eliminate**:
  - ✓ Common Security Controls.
  - ✓ Not Applicable (NA) to Use Case and Data Flow
  - ✓ Implemented by the Owner
- **Determine:**
  - ✓ "Shared" security controls
  - ✓ Supplier responsibility



EPRI Procurement Methodology – Create Specification

STEP 2 – SPECIFICATION DEVELOPMENT	
2.1	Determine the Type of Purchase
2.2	Develop/Clarify the Use Case, Data Flow, and Access Points
2.3	Determine the Security Controls for the Use Case
2.4	Establish Owner/Operator and Supplier Responsibilities
2.5	Develop System/Component Specification

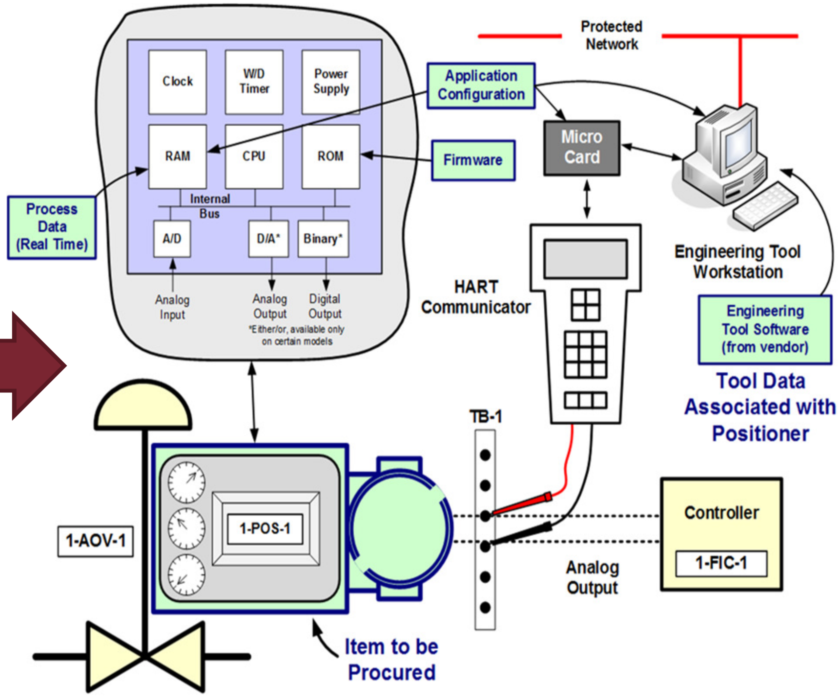
EPRI Procurement Methodology – Requirement Reduction

Example	Total # of Security Controls	Component	Subset of Security Controls that Apply
Example 1 Digital Valve Controller	145	Controller	35
		Configuration Software	65
Example 2 Feedpump Turbine Speed Control Upgrade	135	Governor Positioner	46
		Governor Software Positioner Software	46
Example 3 Digital Feedwater Upgrade	145	Hardware Components	72
		Engineering & Maintenance Workstation with Software	85
		HSI Configuration Data	40

EPRI Procurement Methodology

Example 1: Digital Valve Controller

- Guidance for a low complexity component
- Introduces the interplay between internal architecture functions of the component
- Introduces external dependencies such as the programming devices and portable media.
- Justifies the smallest subset of controls (~70 – 100)

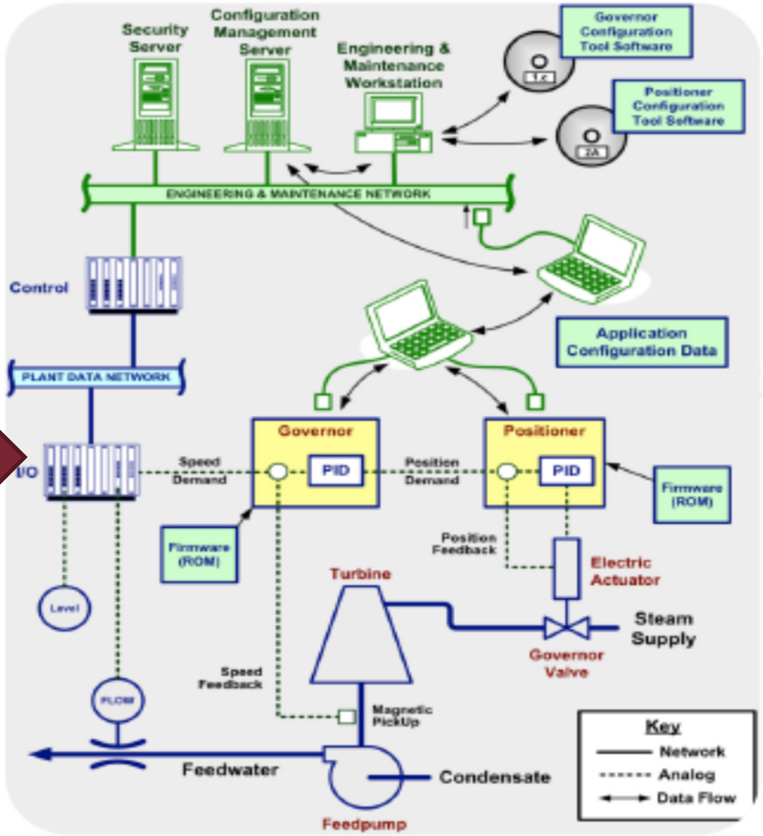


3002003257

EPRI Procurement Methodology

Example 2: Feedpump Turbine Speed Control

- Guidance for a medium complexity subsystem
- Introduces networks and multi-device interfaces.
- Reinforces the need to address external dependencies such as the engineering workstations and portable media.
- Justifies the smallest subset of controls (~140)

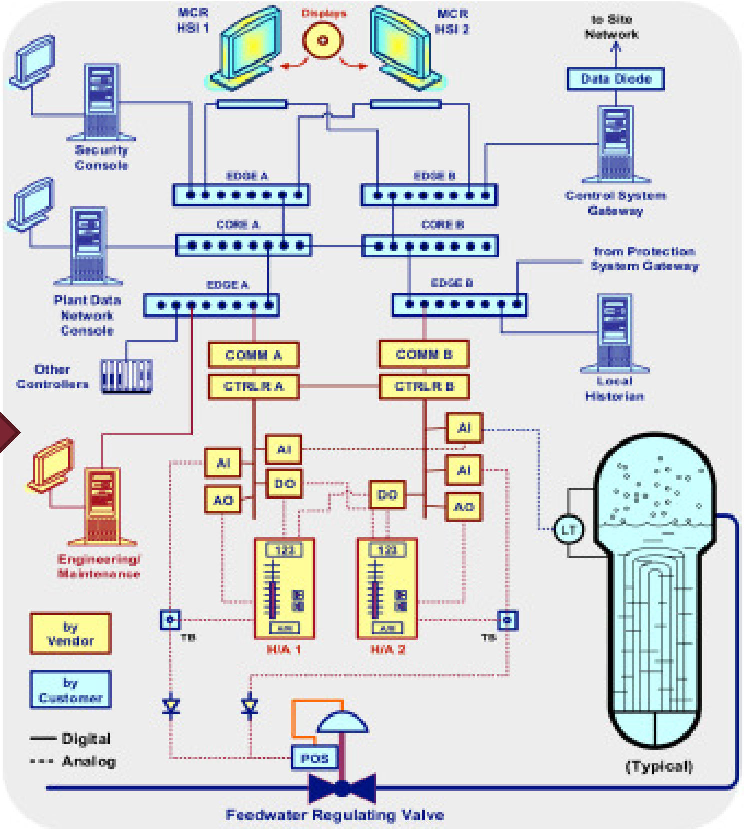


3002001823

EPRI Procurement Methodology

Example 3: Digital Feedwater Control

- Guidance for high complexity system
- Expands on network and interface management
- Introduces server and operator workstation requirements.
- Covers communications to the Business network and higher Enterprise functions such as historians.
- Illustrates the most comprehensive inventory of controls (>200)

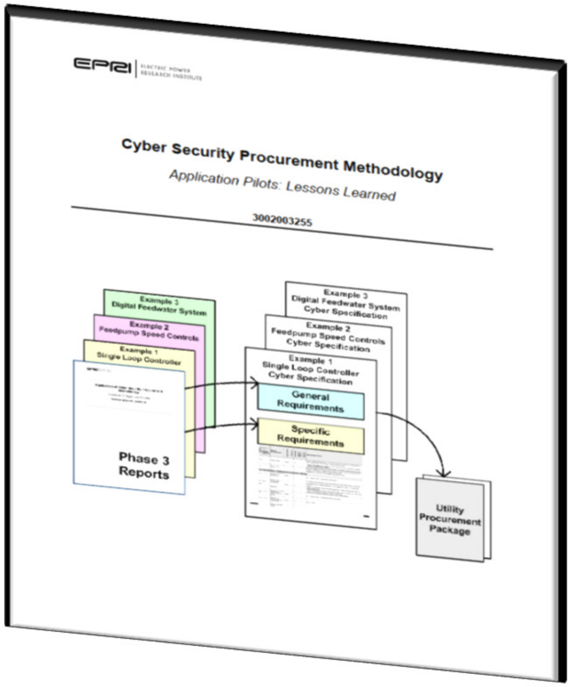


3002002069

Cyber Security Procurement Pilots- 2014

The project results include five (5) low to high complexity pilots.

- ❑ A total of 31 lessons learned are documented in the report
- ❑ Insights will be used to revise “Cyber Security Procurement Methodology , Revision 1
- ❑ ***CBT training was leveraged for the Pilots***
- ❑ Information on Secure Development and Operations Environments(SDOE) was identified for addition.



EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Cyber Security Procurement Methodology

Application Pilots: Lessons Learned

3002003255

3002003255

Something to think about…

- Cyber is not just nuclear
  - All critical infrastructure has the same requirements
  - Only the method for meet the requirements may look different.

- Are you confident that the products carrying your company's name are of the quality advertised?
  - How is your company vetting the products you provide?

- How can you prove it to me every time we perform a business interaction?

Wrap it up…

Questions…Comments

?????