Technical Assessment Methodology (TAM) for Cyber Security

Overview & Considerations for Assessing a Transmission Level Transformer

Matt Wakefield, mwakefield@epri.com
Director - Information, Communication & Cyber Security

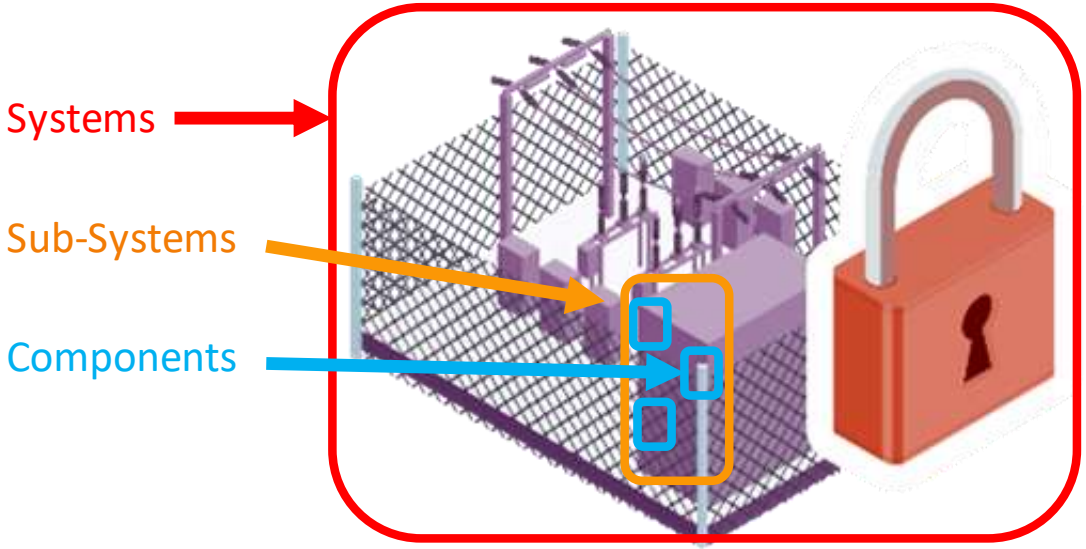
Jason Hollern, jhollern@epri.com
Principal Project Manager, Generation Security

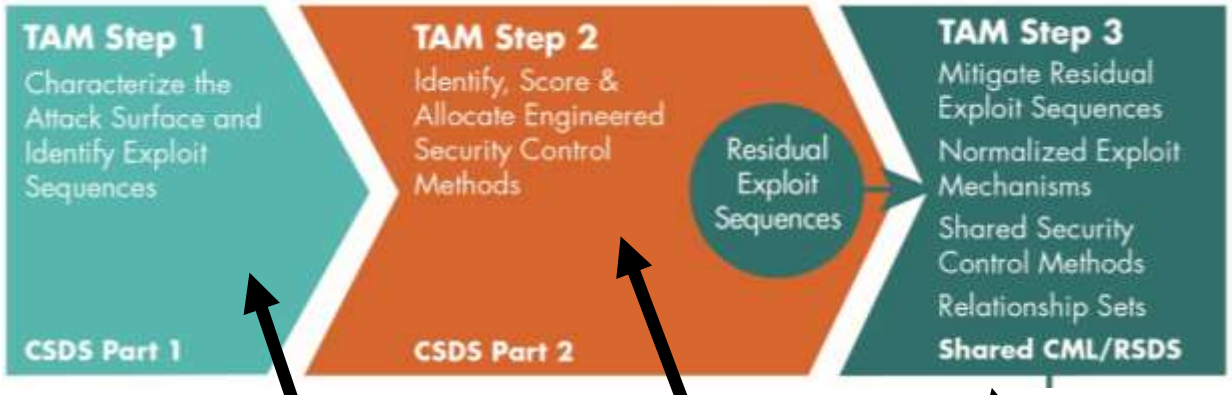
Lee Watkins, lewatkins@epri.com
Senior Technical Leader, Cyber Security

October 2020

The EPRI Technical Assessment Methodology (TAM)

- Security Risk Assessment of Systems, Sub-Systems or Components





Identifies Vulnerabilities

Determines Mitigations

Risks Scored based on how it's used or configured

(RISK INFORMED)

- Supply Chain Applicability:
  - Procurement
  - Design, Commissioning
  - Installed Configuration
- Can be performed by Vendors, Utilities, Systems Integrators, Consultants, EPRI…

Outcome of the TAM – Cyber Security Data Sheet (CSDS)

Analogous to a Material Safety Data Sheet (MSDS)

- Documents
  - Identified attack surfaces
  - Scoring of existing control measures (effectiveness and burden)
  - Unmitigated vulnerabilities
  - "What if" analysis of additional control measures
  - Identifies parties responsible for Mitigations
  - Standardized and scalable

Cyber Security Data Sheet (CSDS)

EPRI Collaboration Fosters Development & Sharing of CSDSs
A Library of technical control methods

EPRI Approach for Industry Supply Chain Collaboration

EPRI Cyber Security Technical Assessment Methodology (TAM)

- Systems Engineering Approach - relevant to design phase & configured evaluation
- Outcome - Cyber Security Data Sheets (CSDSs)

TAM Step 1 (Vulnerabilities)
Product or Generic System

TAM Step 2 (Mitigations)
Product or Generic System

TAM Step 3
(Mitigations for Installed Configuration)
For the site-specific configuration and use

Accelerator
for self evaluation

Developed by Supplier or Other
Opportunity for Sharing

Site specific for installed Configuration
Not Expected to be Shared

Supporting Multiple Aspects of Supply Chain Lifecycle
Procurement | Commission | Operation

When to Apply in the Supply Chain Lifecycle – Example 1

Procurement

Acquire or Develop Reference CSDS at or before Procurement

- TAM Step 1 – Vulnerabilities
- TAM Step 2 - Mitigations

Reference CSDS Provided by Vendor (preferred, working w/Vendor Community)
or
Credentialed organization (EPRI, Utility, Integrator, Consultant)

Example – Product Reference CSDS

SEL 487E Protective Relay CSDS

Developed by EPRI

Transformer protective relay sensing differential current across transformer. Connected to an RTAC for SCADA and remote engineering access.

https://www.epri.com/research/products/000000003002017149

When to Apply in the Supply Chain Lifecycle – Example 2

Commissioning

Develop Tailored CSDS during Design/Commissioning/Implementation

- TAM Step 1 – Vulnerabilities
- TAM Step 2 – Mitigations
- TAM Step 3 – Mitigations Based on Installed Configuration

Tailored CSDS Developed by Utility or Integrator

Example – Commissioning Southern Nuclear Vogtle 3 & 4

16,000 Digital Plant Components Assessed

"This methodology employs a disciplined and repeatable engineering approach that takes into account different levels of risk to meet our business objectives and to satisfy cybersecurity regulations"

Eugene Pisarskiy, digital instrumentation and controls manager.

https://www.southerncompany.com/our-companies/southern-nuclear/southern-nuclear-news-stories/epriaward-200316.html

When to Apply in the Supply Chain Lifecycle – Example 3

Legacy – Installed Equipment

Develop Tailored CSDS during Design/Commissioning/Implementation

- TAM Step 1 – Vulnerabilities
- TAM Step 2 – Mitigations
- TAM Step 3 – Mitigations Based on Installed Configuration

Tailored CSDS

Tailored CSDS Developed by Utility, EPRI or Integrator

Example – Transmission Level Transformer Assessment with AEP and Dominion

(Relates to Executive Order – Securing BPS)

- TAM Step 1 – Vulnerabilities of Digital Equipment on Transformer
- TAM Step 2 – Mitigations of Digital Equipment on Transformer

Reference CSDSs being Developed by EPRI

EPRI Interest Group - Sharing of Reference CSDSs

- TAM Step 3 – Mitigations based on Unique Configuration of AEP & Dominion

Tailored CSDSs being Developed by EPRI

Based on Unique Transformer Equipment and Configuration

Will be Proprietary to AEP and Dominion (not shared)

Technical Assessment Methodology

Cyber Security in the Supply Chain

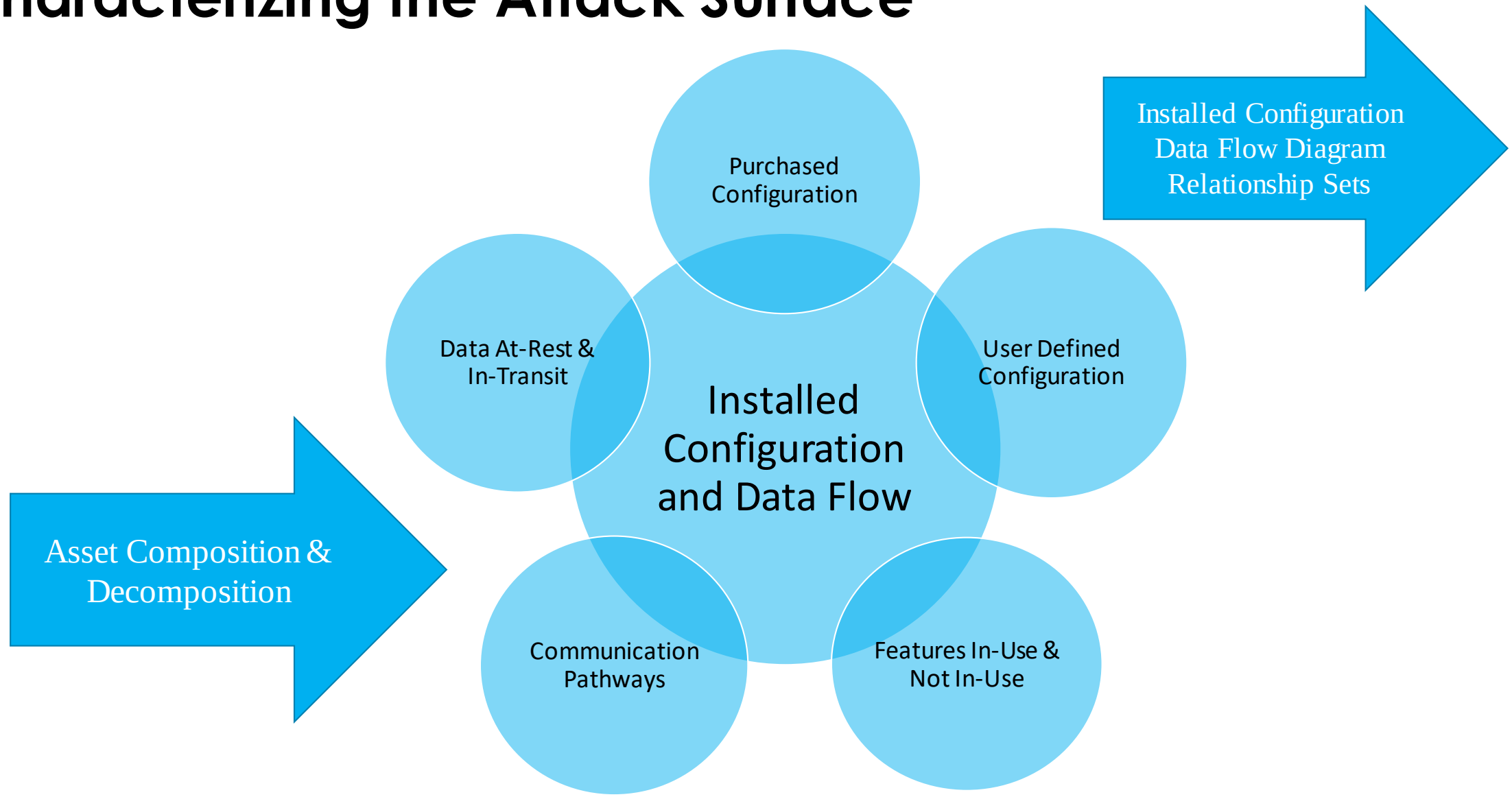
EPRI Technical Assessment Methodology (TAM) Overview and Transformer Examples

Jason Hollern, jhollern@epri.com
Principal Project Manager, Generation Security

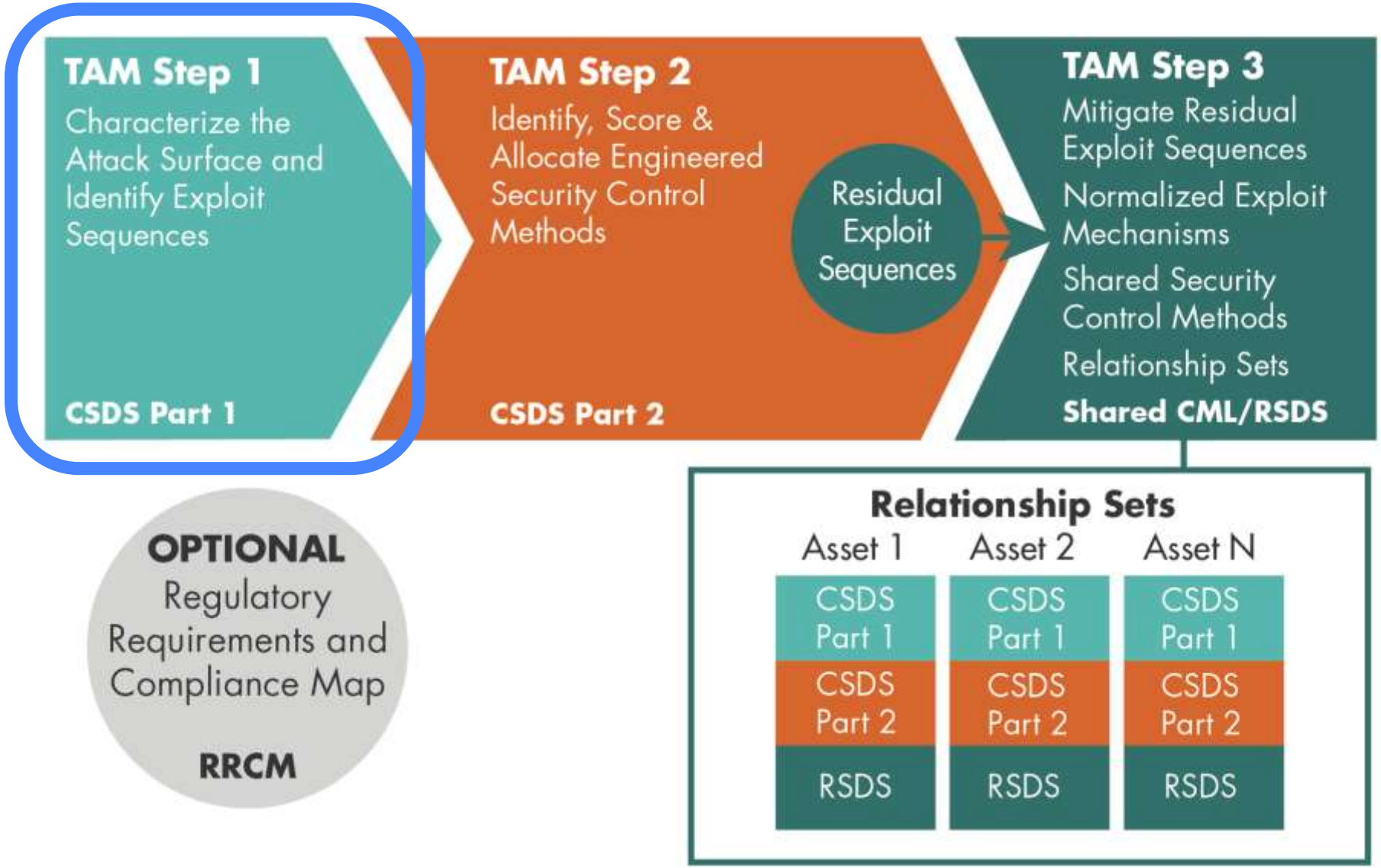
Lee Watkins, lewatkins@epri.com
Senior Technical Leader, Cyber Security

October 2020

Characterizing the Attack Surface



Technical Assessment Methodology Step 1



TAM Step 1: Exploit Sequences (Vulnerabilities)

- The goal of an attacker is to steal or alter critical data or take direct action against an asset in order to achieve an Exploit Objective.

- When Attack Pathways are identified, the Exploit Mechanisms used to exploit those pathways (i.e., achieve an exploit objective) are identified.

- Taken together, each unique combination of Attack Pathway, Exploit Mechanism, and Exploit Objective form a distinct Exploit Sequence:

Exploit Sequence = Exploit Objective + Attack Pathway + Exploit Mechanism

Exploit Sequence = Exploit Objective + Attack Pathway + Exploit Mechanism

Direct Action:

Asset enable/disablement – Immediate. Means exist to immediately initiate or halt asset operation.

Asset disablement – Delayed. Means exist to degrade support systems or the environment for component operations, eventually resulting in component disablement.

Denial of Service (DOS). Means exist to interfere with the normal operation of the asset by presenting false demands for asset interaction at a digital port on the asset.

Malware. Means exist to inject or install unauthorized and undetected program content on the asset that does not constitute an alteration of existing authorized program content.

"Data Flow"	At Rest	In Transit
Theft	Means exist to access and record data while stored on the asset.	Means exist to access and record data while being transmitted to or from the asset.
Alteration	Means exist to alter data while stored on the asset.	Means exist to alter data while being transmitted to or from the asset.

The TAM identifies 28 Exploit Objectives

Exploit Sequence = Exploit Objective + Attack Pathway + Exploit Mechanism

Attack Pathways (more than just the Attack Vector)

- 5 possible Attack Vectors
  - Direct Physical Access
  - Direct Network Connectivity
  - Wireless Network Capability
  - Supply Chain
  - Portable Media and Equipment
- Physical Interface
- Communications Protocol
- Logical Ports
- Interfacing Connections

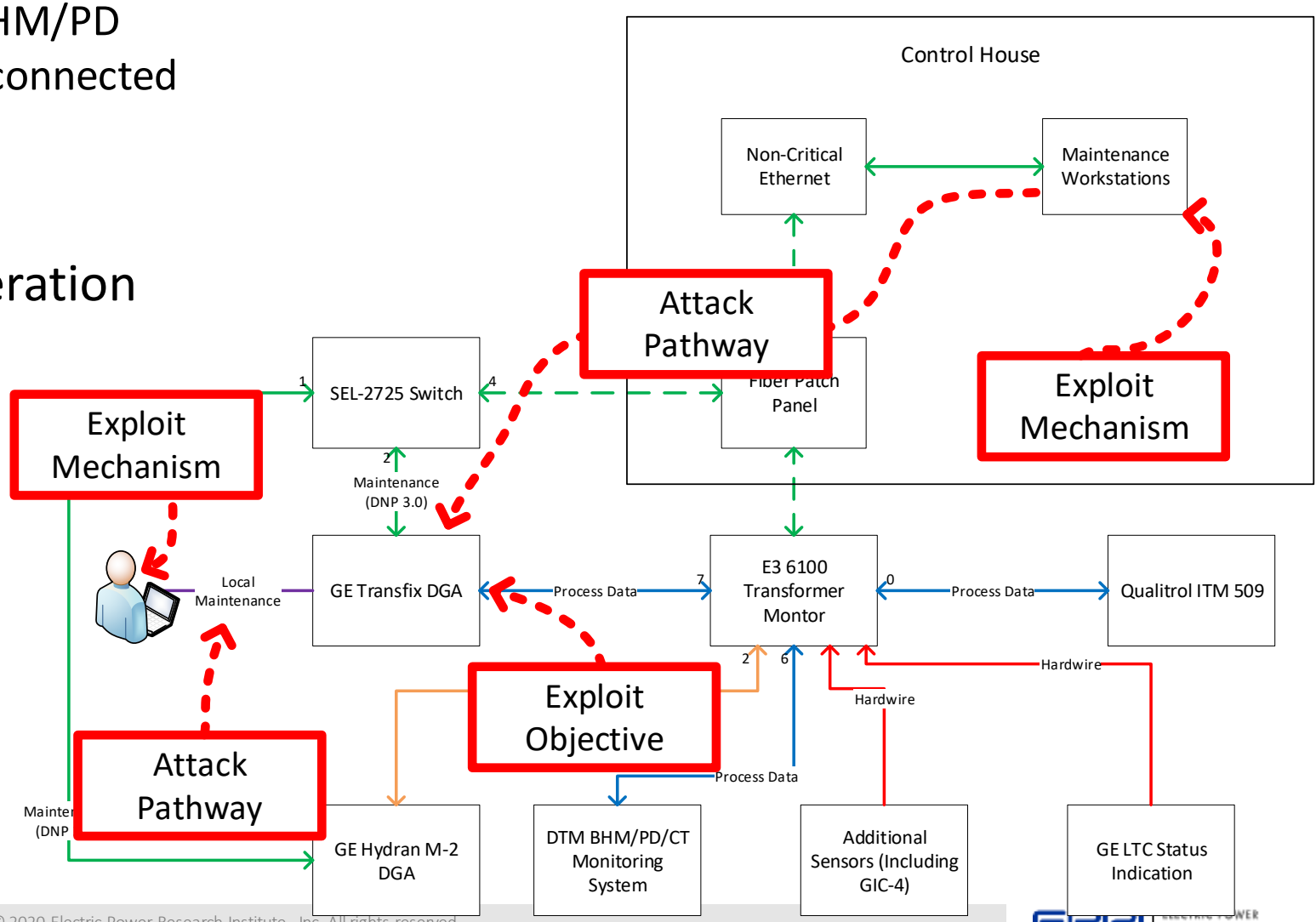
- Attack Pathways are used by adversaries to:
  - Take Direct Action against an Asset or
  - Steal or Alter Critical Data such as operational and configuration data

Exploit Sequence = Exploit Objective + Attack Pathway + Exploit Mechanism

- The specific action that must occur for an attacker to achieve an exploit objective through an attack pathway.
  - Faceplate Configuration Button and Up/Down Buttons to change the controller configuration
  - Maintenance laptop with controller software connected to the asset to change the controller configuration by loading a project file from the controller software into the controller
  - Compromise supplier development environment to inject malware into the controller

Transformer Attack Surface & Exploit Objective

- Typical Transformer Monitoring Package
  - Two DGA, Temperature Monitors, BHM/PD monitoring, analog sensors digitally connected
  - Does not drive protection breakers
- Exploit Objective: User-Defined Program/Configuration Data, Alteration at rest (E18 from the TAM)
  - Two Exploit Mechanisms
  - Two Attack Pathways
- Two Exploit Sequences for same Exploit Objective

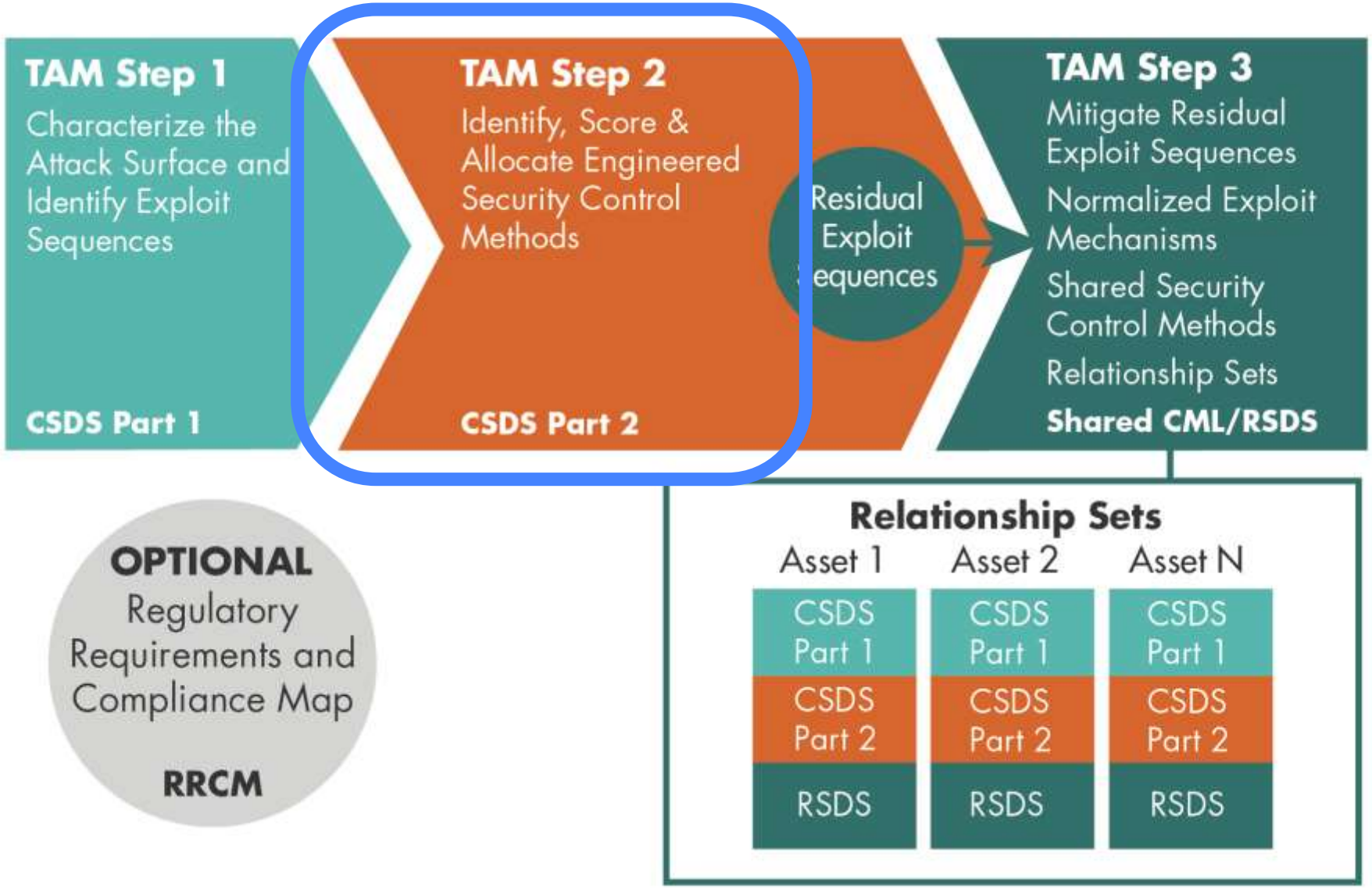


Sample Exploit Sequences for Transformer

- Sequence #1:
  - Attack Pathway: Maintenance workstation communicating with Transfix DGA via Ethernet
  - Exploit Mechanism: Use Workstation to modify DGA calibration and setpoints to provide E3 Transformer Monitor with incorrect process data
- Sequence #2:
  - Attack Pathway: Direct local maintenance connection to DGA with Transient asset (laptop)
  - Exploit Mechanism: Use laptop to modify DGA calibration and setpoints to provide Transformer Monitor with incorrect process data

Electrical & Field Drawings may not show local maintenance connections – Exploit Sequence #2 may have been overlooked!

Technical Assessment Methodology Step 2



Incorporating Risk

Exploit Difficulty
Inverse of "Likelihood"

How difficult is it for an adversary to overcome the control method?

TAM Step 2 - Security Control Methods (Mitigations)

- Exploit sequences must be mitigated via security control methods for all 3 security functions (Protect, Detect, Respond & Recover)
  - Implementation effectiveness (how effective is the method for a function)
  - Exploit Difficulty (how hard is it for an adversary overcome the method)

Control Method Efficacy Score (Three Times, Once for Each Security Function)				
Security Effectiveness Score	**Implementation Burden**			
	High (>2.3 to 3.0)	Medium (>1.3 to 2.3)	Low (0.0 to 1.3)	Conflict
None	None			Do not Implement
Low (0.1 to 1.0)	1	2	3	
Medium (>1.0 to 2.0)	2	3	4	
High (>2.0 to 3.0)	3	4	5	

Security Effectiveness = f(Implementation Effectiveness, Exploit Difficulty)

Dimensions of Security – TAM Control Method Security Functions

- **Protect** – cyber assets are protected from a cyber attack
- **Detect** – if a cyber asset is attacked, the attack is detected
- **Respond & Recover** – the ability to effectively respond and recover from a cyber attack

Synthesizes NIST Cyber Security Framework and IEC 62443

Engineered and Shared Control Methods

Identify Device Engineered Security Control Methods

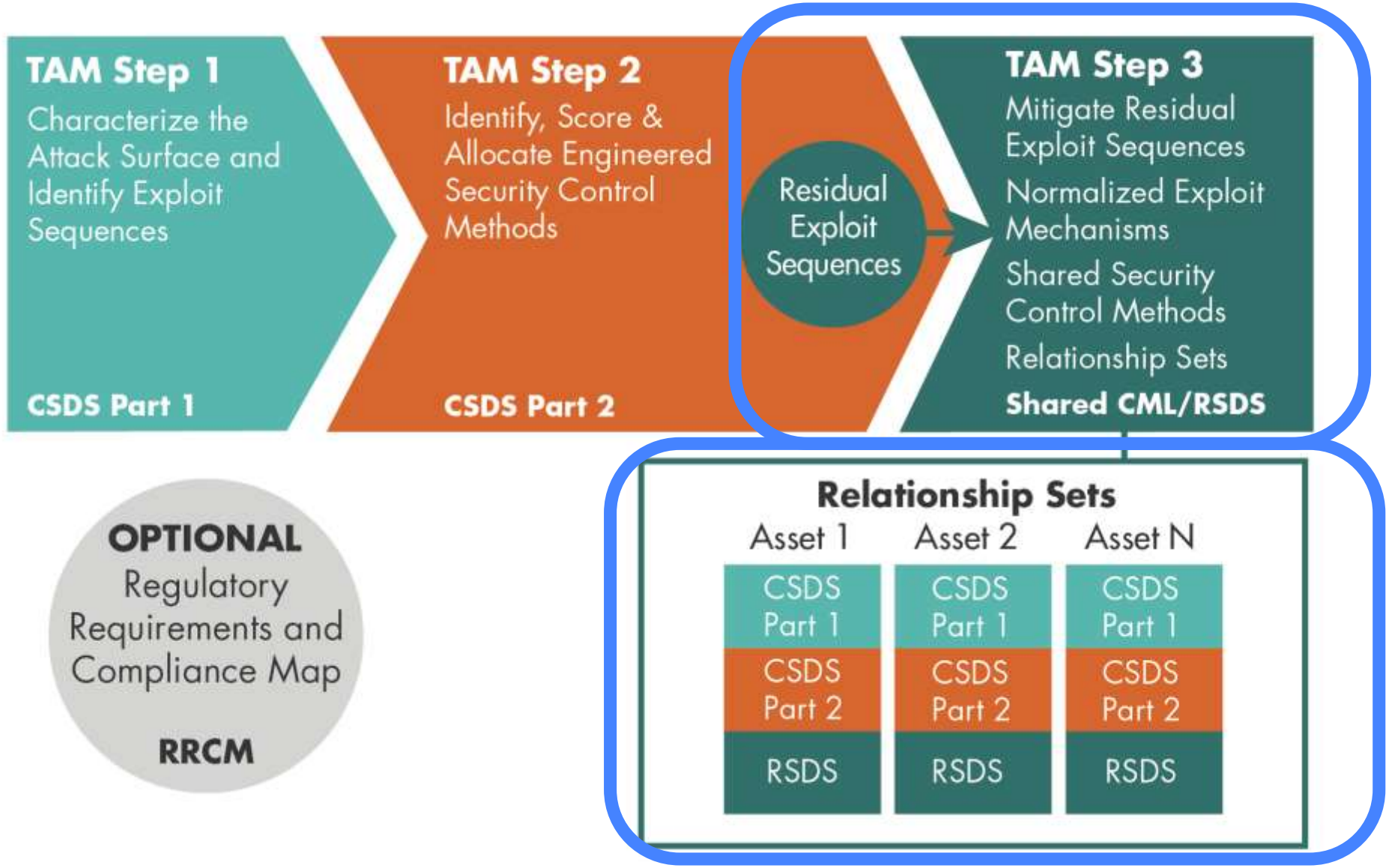
- Evaluate engineered security control methods against exploit sequences
- How to identify a control method on an asset?
  - Feature, function, capability of the asset
  - Other devices or procedures may be used to implement the control method
- Backup example using external device
  - Backup of configuration requires maintenance laptop with device software
  - The asset has a configuration that can be captured and restored
  - "How" the control method is implemented includes the maintenance laptop and procedure
- Likely an iterative and parallel process while developing a complete CSDS

Transformer Engineered Security Control Methods

- Disable unused features, services, ports:
  - Technical control with reasonable Protect, but no Detect or R&R score
  - Difficult to exploit, low ongoing implementation burden

- SCADA Alarms and logs:
  - Technical control with higher Detect and R&R, no Protect score
  - Medium exploit difficulty, moderate burden

Technical Assessment Methodology Step 3



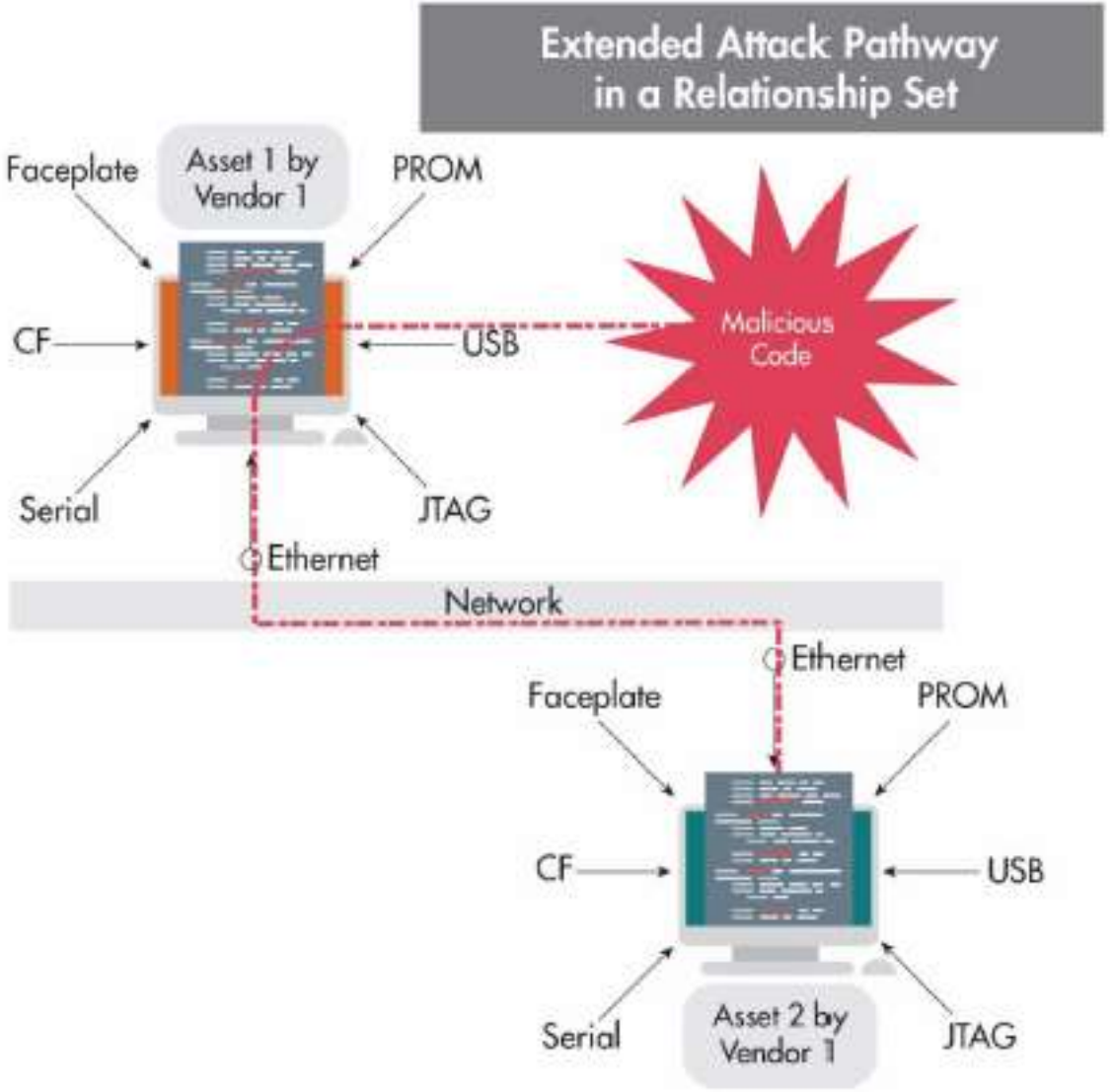
Residual Exploit Sequences

- Residual Exploit Sequences result when the Combined Security Effectiveness Score is below the target level.
  - No Engineered Security Control Method available
  - Efficacy too low (owner decision)
  - Conflict
  - Owner determination not to apply for some other reason

- Residual Exploit Sequences are mitigated by:
  - Shared Control Methods from a higher level CSDS in a Connectivity Relationship Set
  - Site Control Methods from the Site Control Method Library in a Relationship Set

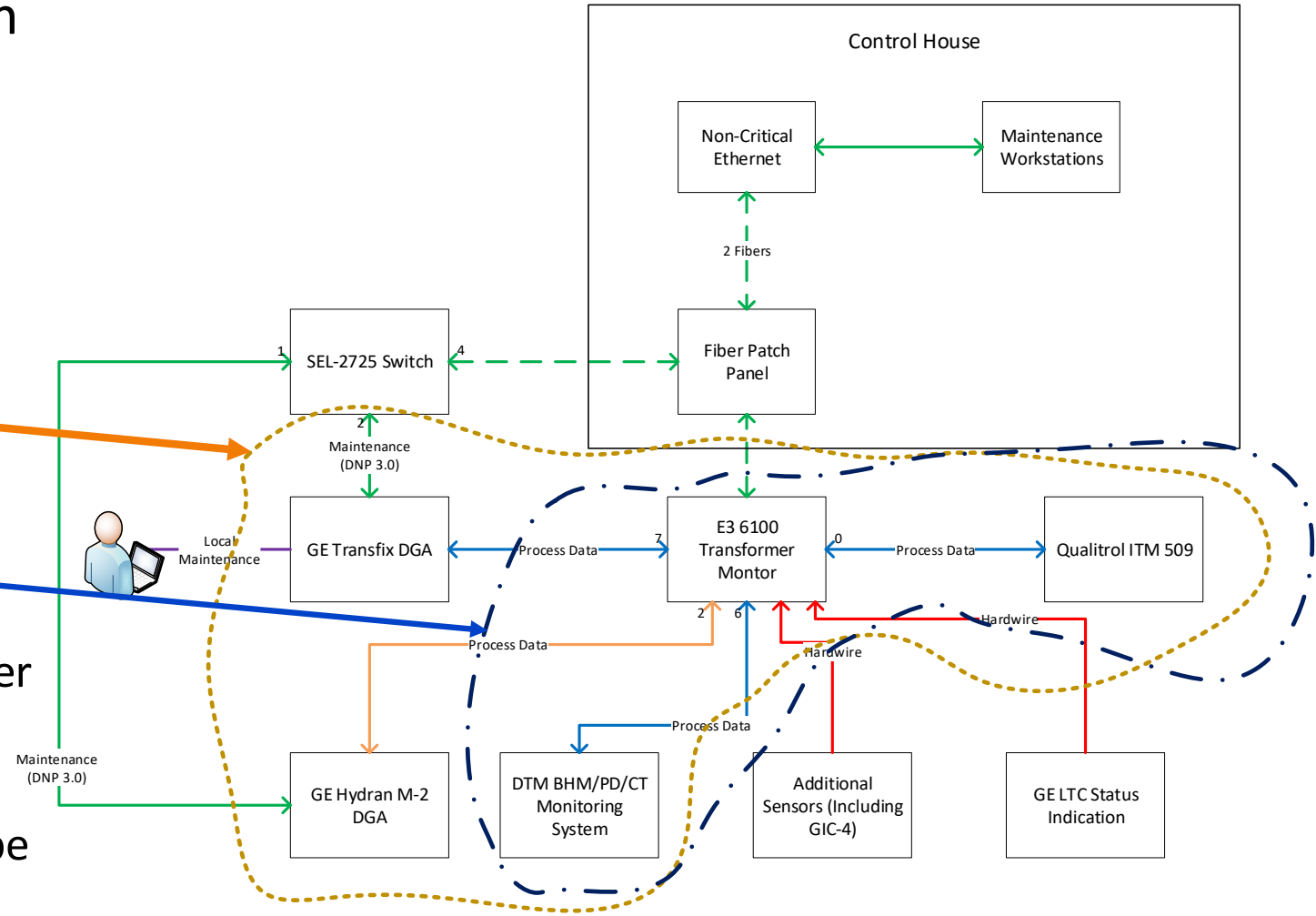
TAM Step 3 – Mitigate Residual Exploit Sequences

- Document Relationship Sets and their inheritance attributes with a Relationship Set Data Sheet (RSDS)
- Associate CSDSs and applicable residual exploit sequences to the relationship set
- Residual exploit sequences are mitigated through the inheritance of shared control methods in a relationship set
- Requires detailed knowledge of the site cyber security program including knowledge of <u>how and where</u> these shared security control methods are implemented.



TAM Step 3 – Transformer Example

- Mitigate Residual Exploit Sequences with Shared Control Method Library and Relationship Sets
- Relationship Sets on Transformer Monitoring:
  - Connectivity: All devices with serial connection to E3 6100 – Gold circle
  - Spatial: All devices located in same cabinet – Dark Blue circle
- Example Residual Exploit Sequence
  - Unauthorized logical access to E3 6100 to alter configuration data
  - Disabling/blocking ports on E3 6100 provides protection on device, but can other devices be used? How can you detect this?



TAM Step 2

Build Exploit Sequences | CSDS Part 2b Allocation of

Refer to the separate instruction shee

Manufacturer	Device Name	CSDS ID
ACME	SLC-01	C12

		Combined Security Effectiveness Score			
Exploit Sequence	Attack Pathway	Protect	Detect	R/R	Residual Present?
E01.A01.N1	A01	0.00	0.00	0.00	Yes
E01.A02.N2	A02	0.99	0.00	0.00	Yes
E01.A03.N1	A03	1.00	0.00	0.00	Yes
E05.A02.N2	A02	0.00	0.00	0.00	Yes
E06.A02.N2	A02	0.99	0.00	0.00	Yes
E06.A03.N3	A03	1.00	0.00	0.00	Yes
E12.A02.N2	A02	0.99	1.20	1.20	Yes
E12.A04.N3	A04	0.83	1.20	1.20	Yes
E12.A05.N1	A05	0.00	0.00	0.00	
E13.A02.N2	A02	0.00	0.00		
E14.A02.N2	A02	0.00	0.00		
E16.A02.N2	A02	0.99	1.64		
E16.A03.N1	A03	1.00	1.64		Yes

TAM Step 3

Build Exploit Sequences | CSDS Part 2b Allocation of Security Control Metho

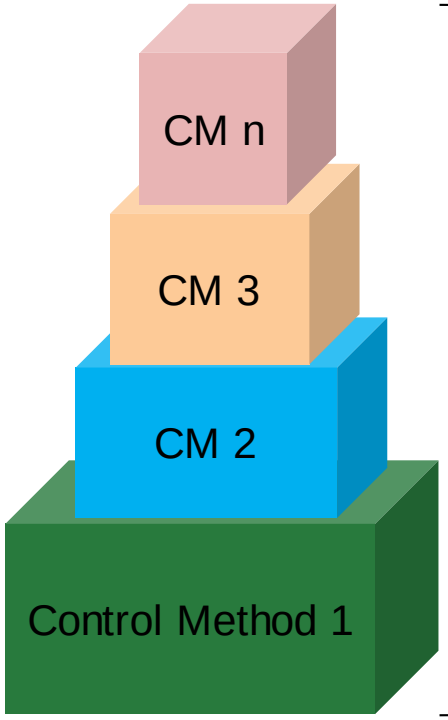
Refer to the separate instruction sheets for how to complete the workbo

Manufacturer	Device Name	CSDS ID
ACME	SLC-01	C12

		Combined Security Effectiveness Score				Target Levels		
Exploit Sequence	Attack Pathway	Protect	Detect	R/R	Residual Present?	Protect	Detect	R/R
E01.A01.N1	A01	4.01	4.02	4.02	No	C	C	C
E01.A02.N2	A02	4.13	2.69	3.59	No	C	C	C
E01.A03.N1	A03	4.45	4.02	4.02	No	C	C	C
E05.A02.N2	A02	3.52	3.27		No	D	D	D
E06.A02.N2	A02				No	D	D	D
E06.A03.N3					No	D	D	D
					No	C	C	C
				2.05	No	C	C	C
			4.02	4.02	No	C	C	C
		3.52	3.27	3.27	No	D	D	D
	A02	4.25	3.27	3.27	No	D	D	D
E16.A02.N2	A02	4.54	4.11	3.98	No	C	C	C
E16.A03.N1	A03	4.45	4.75	4.63	No	C	C	C

Utilizing Shared Controls and RSDS, Residual Exploit Sequences can be fully mitigated

Combined Security Effectiveness Target Level Incorporates Risk



Combined Security Effectiveness Score

Weighted

Security Control Method			Implementation Burden (resources and time)			
			High	Medium	Low	Conflict
Security Effectiveness	Protect	None	None			Do not Implement
		Low	1	2	3	
		Medium	2	3	4	
		High	3	4	5	
	Detect	None	None			
		Low	1	2	3	
		Medium	2	3	4	
		High	3	4	5	
	Respond and Recover	None	None			
		Low	1	2	3	
		Medium	2	3	4	
		High	3	4	5	

A Systems Engineering Approach

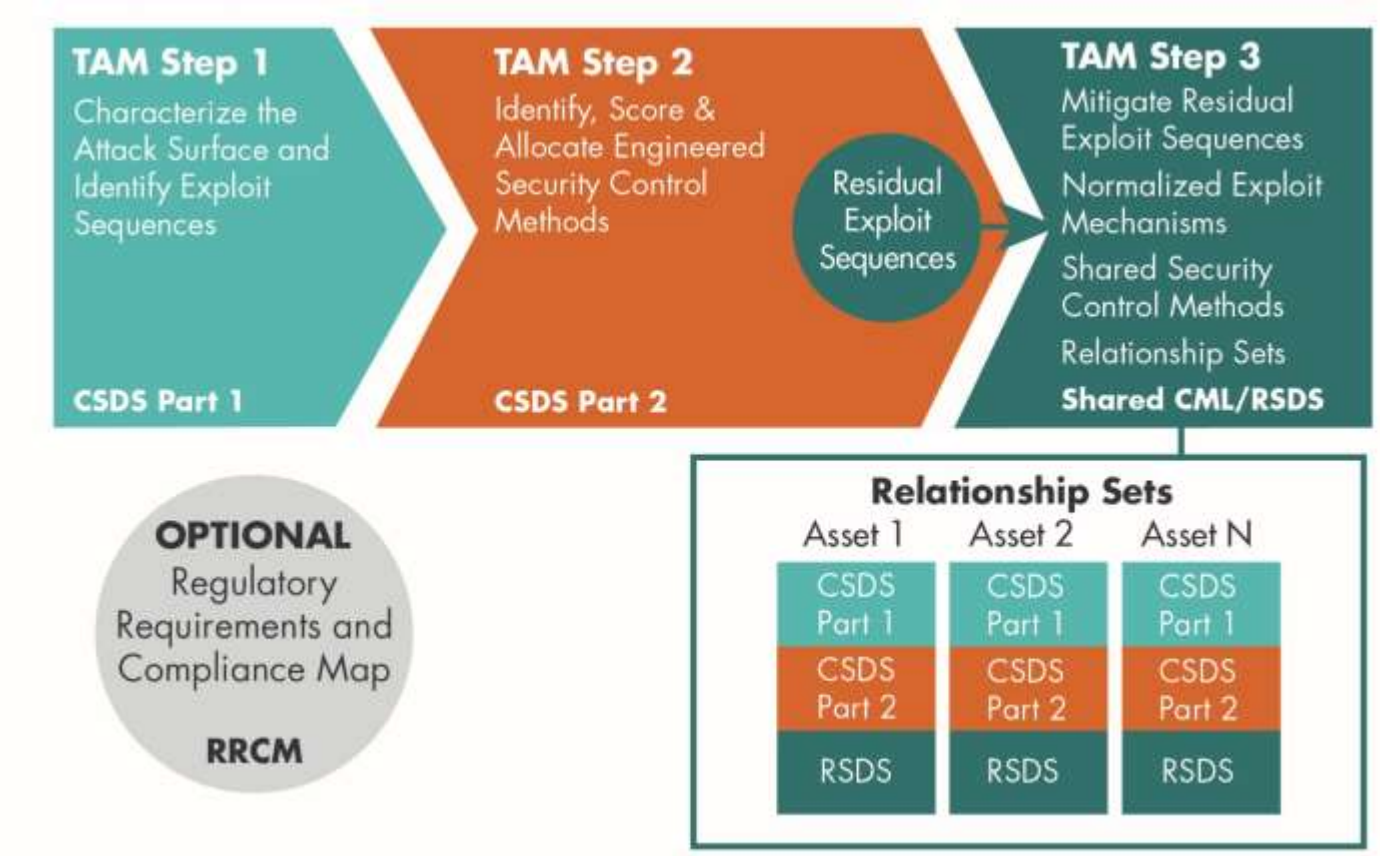
Engineering Process

Modular

Efficient

Scalable

Standardized



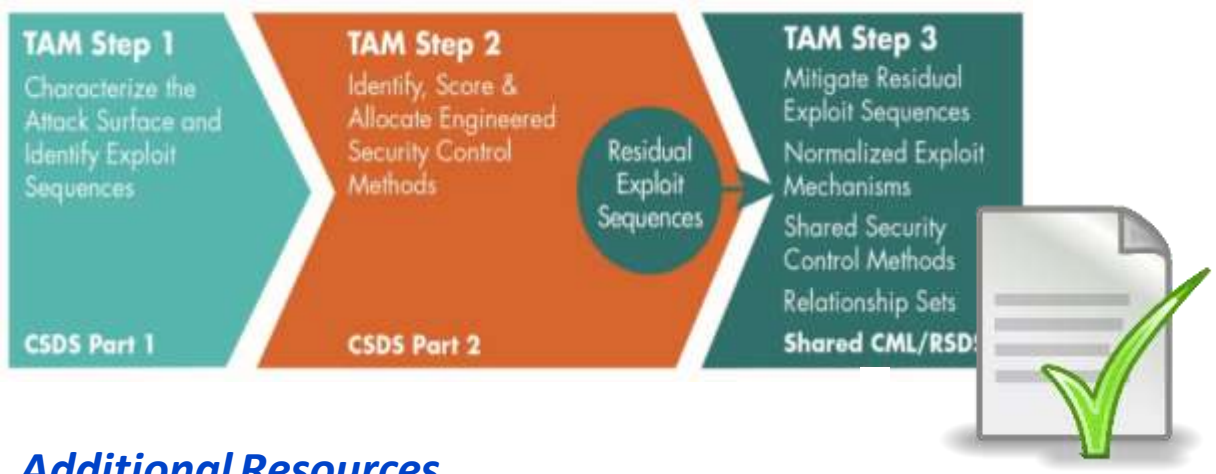
EPRI Cyber Security TAM Interest Group – Industry Collaboration

Objectives and Scope

- Tech transfer and cross-sector implementation of the EPRI Cyber Security TAM.
- Use-case identification and demonstration – Applicability to the Executive Order
- Utility peer collaboration → workshops, training, webcasts, and interaction.
- Feedback for enhancements and revisions.
- Building Reference Library of CSDSs

Project Manager: Jason Hollern

- jhollern@epri.com , (704) 595-2570
- Project Overview: https://www.epri.com/research/products/000000003002018342



Additional Resources

- Video Cyber Security TAM Overview - https://www.youtube.com/watch?v=MCNfjGrn-uY
- The Technical Assessment Methodology, Rev 1
  - https://www.epri.com/research/products/000000003002012752
- Cyber Security in the Supply Chain: Cyber Security Procurement Methodology, Rev 2
  - https://www.epri.com/research/products/000000003002012753

Exploring Information Sharing Approaches with Utilities, Vendors, NATF, DOE, Stakeholders

Questions or Discussion

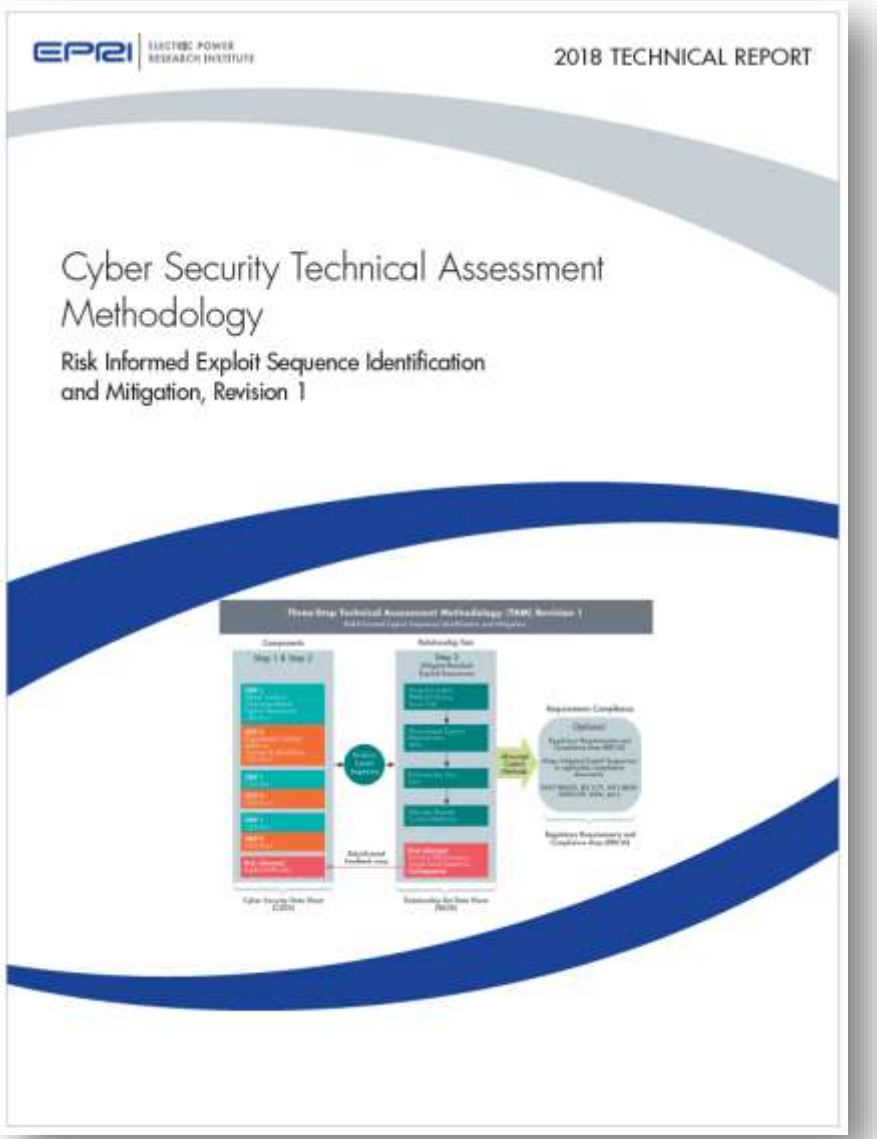
Together…Shaping the Future of Electricity

TAM Introduction Video

https://www.youtube.com/watch?v=MCNfjGrn-uY

The EPRI Cyber Security Technical Assessment Methodology

https://www.epri.com/research/products/000000003002012752



Provides an actionable, risk-informed, systems engineered based approach that guides users to:

- Understand their systems and components,
- Analyze the actual vulnerabilities and how the system can be attacked,
- Mitigate those vulnerabilities to an acceptable risk level,
- By applying effective control measures.