Hazmat Signs for Industrial Software

...if they existed, what would they look like?

Bryan Owen PE, OSIsoft LLC

Most Industrial Software is ‘Toxic’

Toxicity

The degree to which a chemical substance can damage an organism

- Whole organism
- Organs,
- Tissue,
- Or even cellular damage.

Toxin Categories

Biological Hazard

Corrosive Hazard

Physical Hazard

Non-Ionizing Radiation Hazard

“Cyber” – Bio Hazard

Biological Hazard

Abuse of legitimate ICS functionality

- Stuxnet
- Crashoverride / Industroyer

- Eg Protocols: IEC101, IEC104, and IEC61850

“Cyber” – Corrosive Hazard

Corrosive Hazard

Non-ICS specific Ransomware & Wipers

- Brickerbot
- Not Petya / WannaCry
- Shamoon

- Eg Protocols: SMB, Telnet

“Cyber” – Physical Hazard

Physical Hazard

Enlistment in bots

- Carna
- Mirai
- Reaper
- And many other similar threats

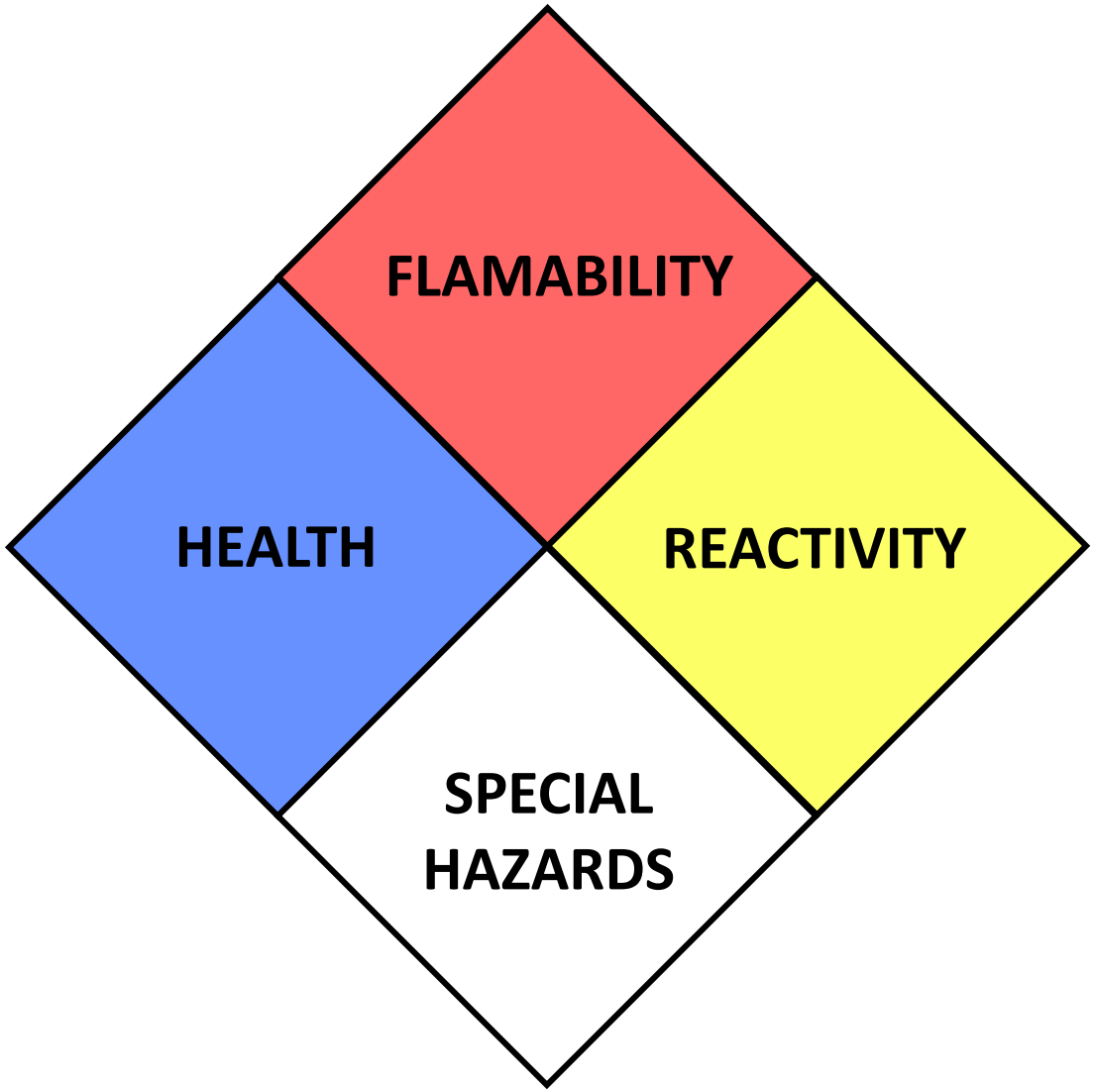
“Cyber” – Radio Hazards

Non-Ionizing Radiation Hazard

Recent malware targeting radios

- BadBIOS
- BlueBorne
- WPA2 Krack

Chemical Hazard Labels – NFPA Diamond



0 → **4**

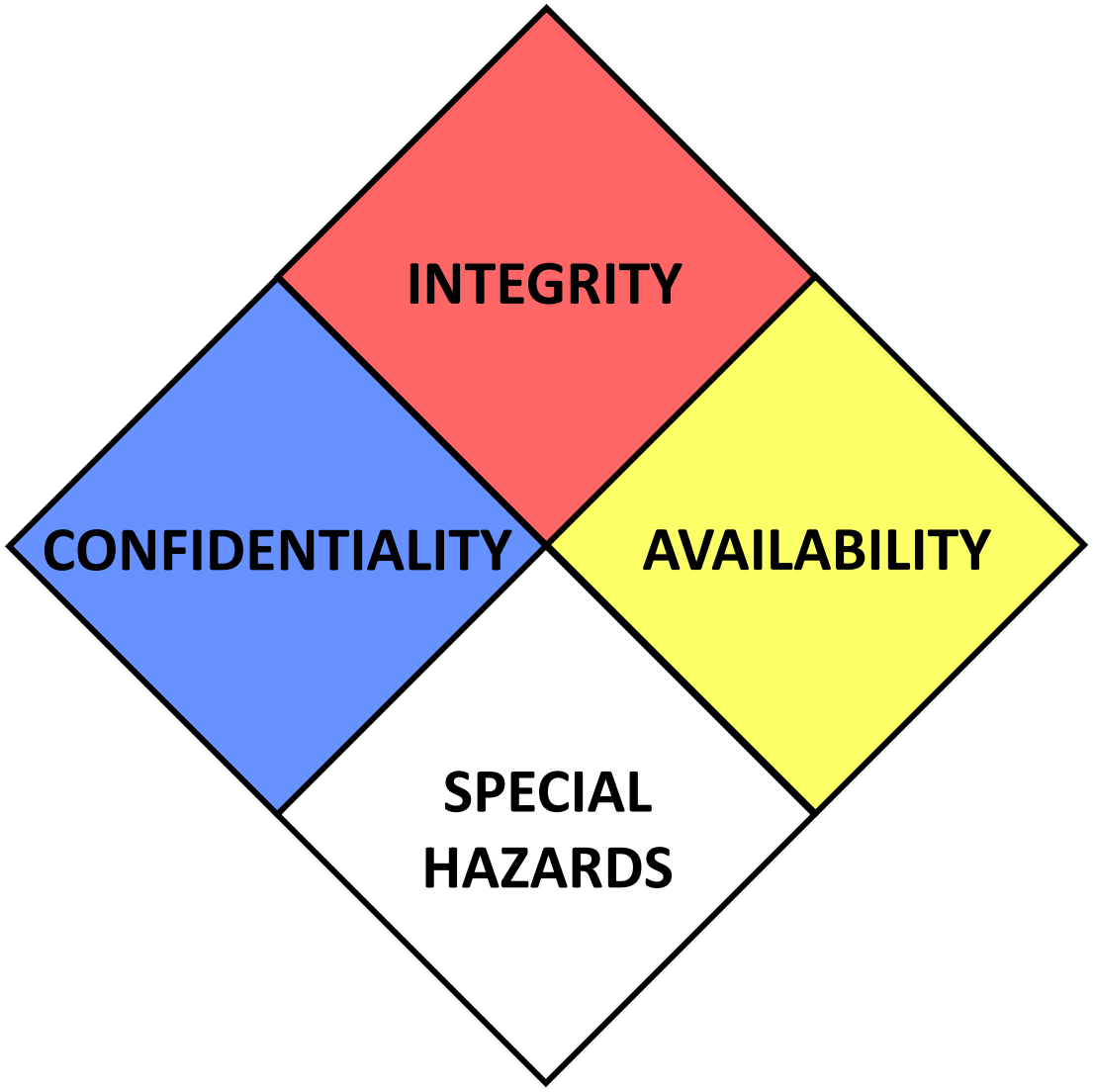
Least Serious — **Most Serious**

0 — **Will Not Burn**

3 — **Shock and Heat May Detonate**

CREDC

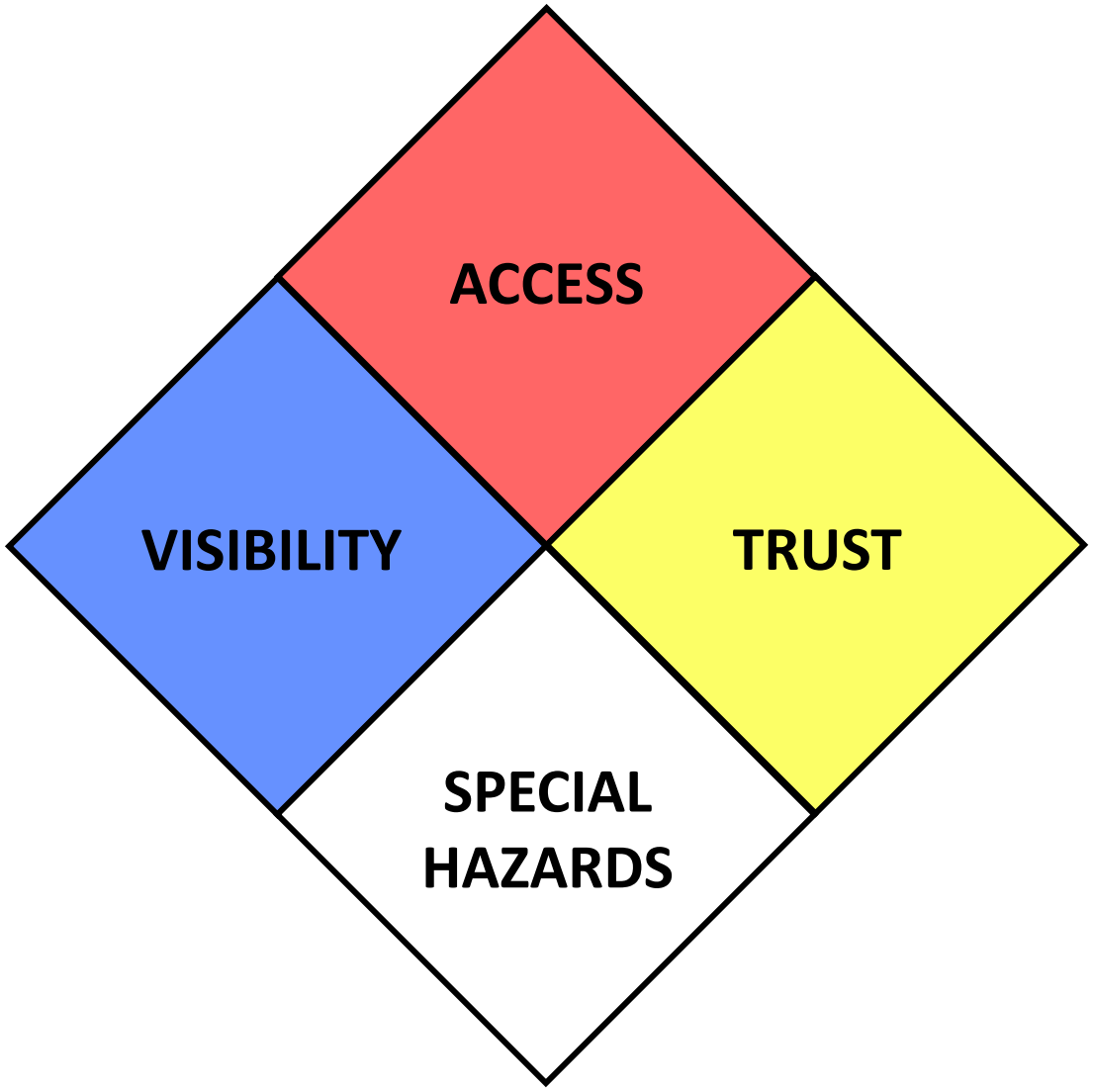
Cyber Hazard Labels: “C-I-A Triad Model”



4	Remote, Anonymous, Default Configuration, Root Access
3	Remote, Anonymous, Default Configuration, User Access
2	Remote, Authenticated, Default Configuration, Root Access
1	Remote, Authenticated, Custom Configuration, Write Access
0	Remote, Authenticated, Read Access

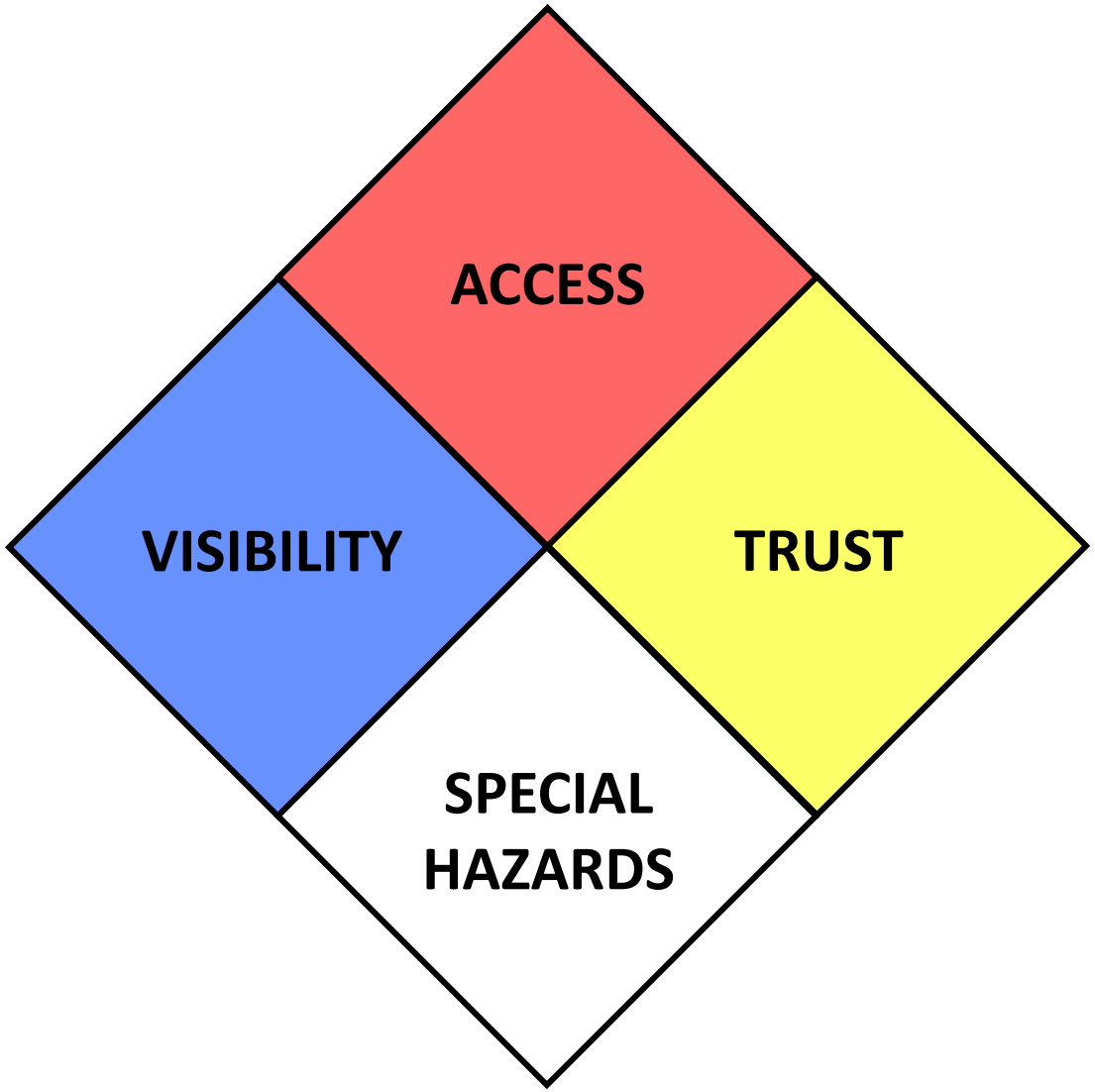
CREDC

Cyber Hazard Labels: “V-A-T Model (OSSTMM)” 1/2



VISIBILITY	
4	Remote management endpoints
3	Remote write access endpoints
2	Remote read access endpoints
1	Device broadcasts
0	No targets visible remotely

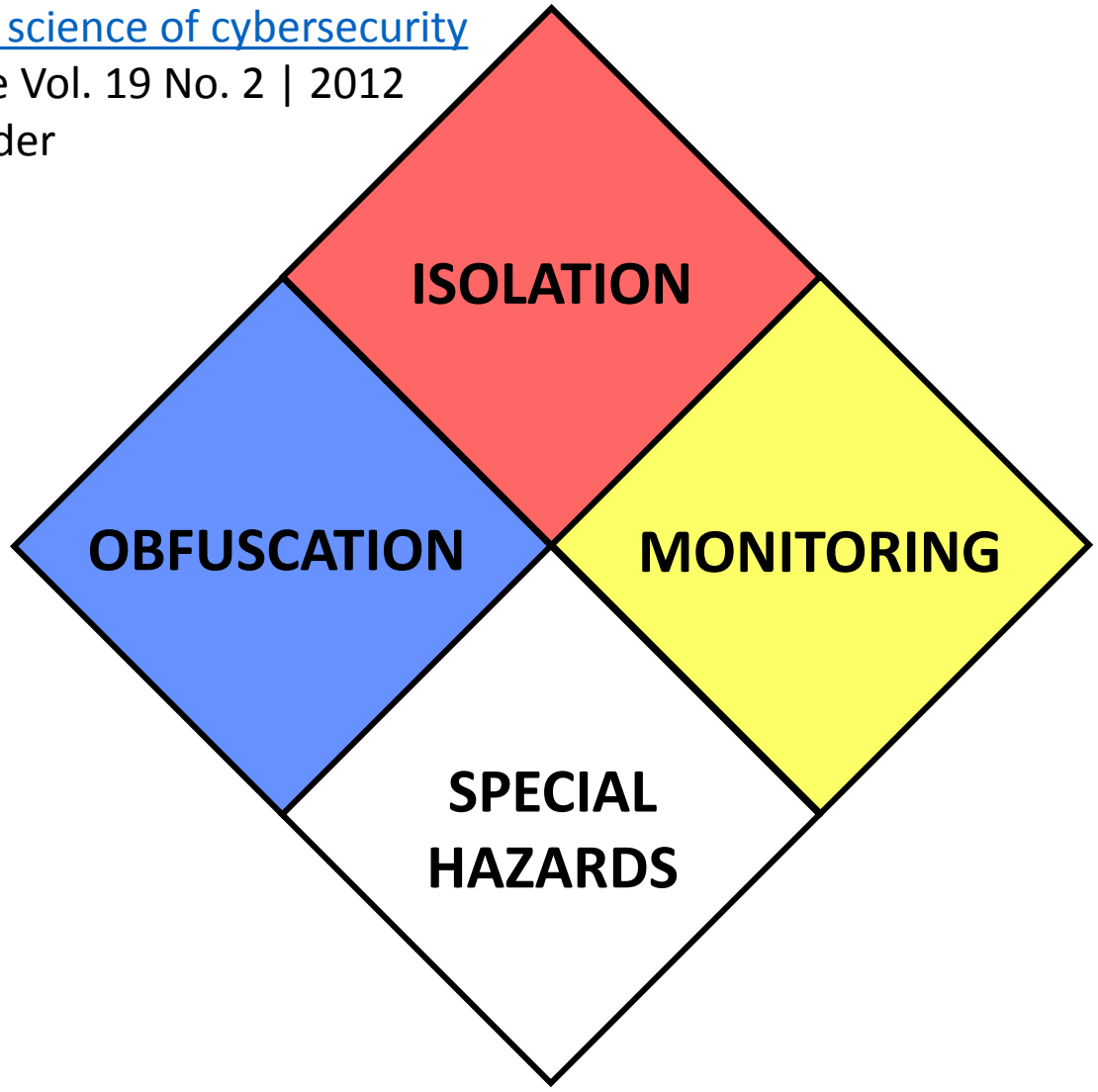
Cyber Hazard Labels: “V-A-T Model (OSSTMM)” 2/2



TRUST	
4	Unmanaged 3P components, 3P managed trust infrastructure
3	Unmanaged 3P components
2	3P managed trust infrastructure
1	Self-managed 3P components, trust infrastructure
0	Trusted foundry with transparency

Cyber Hazard Labels: Cornell “SoS” Blueprint

[Blueprint for a science of cybersecurity](#)
The Next Wave Vol. 19 No. 2 | 2012
Fred B. Schneider



Safety

- No ‘bad thing’ happens

Liveness

- Some ‘good thing’ happens

Special Cyber Hazards: “Observables”

- Digital signature or unique hash
- Documentation of third party components
- Important dates (creation, last modified)
- Memory safe frameworks and languages
- User mode vs kernel or root
- Execution flags (ASLR, CFG, DEP, NX, etc…)
- Network protocol safety
- Software update mechanism

badness-ometer

A badness-omemter can’t tell you that you’re secure. It can only tell you that you’re not.

Badness-ometers are good. Do you own one? by Gary McGraw
https://www.synopsys.com/blogs/software-security/badness-ometers-are-good-do-you-own-one

Idea: Safety Data Sheets

MATERIAL SAFETY DATA SHEET

Trade Name: **ACETONE**

Chemical Family: Acetone

Formula: C3 H6 O

FIRE AND EXPLOSION DATA

Flashpoint & Method:0% F (TCC)
Flammable Limits: LFL 2.0 , UFL 13.0
Extinguishing Media: water spray, dry chemical, CO_2, alcohol foam
Special equip. & procedures: Self contained breathing apparatus & complete protective clothing. Acetone is extremely flammable, any source of ignition will ignite it. Vapor is extremely explosive.

REACTIVITY DATA

Conditions Contributing to Instability: Heat, Sparks & Open Flame
Incompatible Substances: Acids, Oxidizing materials, Alkalis, Amines, Potassium T-Butoxide, Alkanolamines, Ammonia, Aldehydes, Chlorinated compounds.
Hazardous Decomposition Products: Carbon Monoxide, Carbon Dioxide
Hazardous Polymerization: will not occur.

PREVENTATIVE MEASURES

Skin: Wear impervious gloves (butyl rubber), coveralls and safety footwear.
Eyes: Chemical proof goggles or full face respirator if vapors cause eye discomfort.
Ingestion: Wash thoroughly before consuming food stuffs.
Inhalation: Use only in well ventilated areas or use NIOSH approved respiratory protection with organic vapor cartridges.

CONTROL MEASURES AND PRECAUTIONS

Keep container tightly closed. **DO NOT** consume food, drink or tobacco in work or material storage areas. **Flame or any source of ignition is to be kept away from this product.** Use caution and personal cleanliness to avoid skin and eye contact. Avoid breathing vapors.

Cyber Security Data Sheets

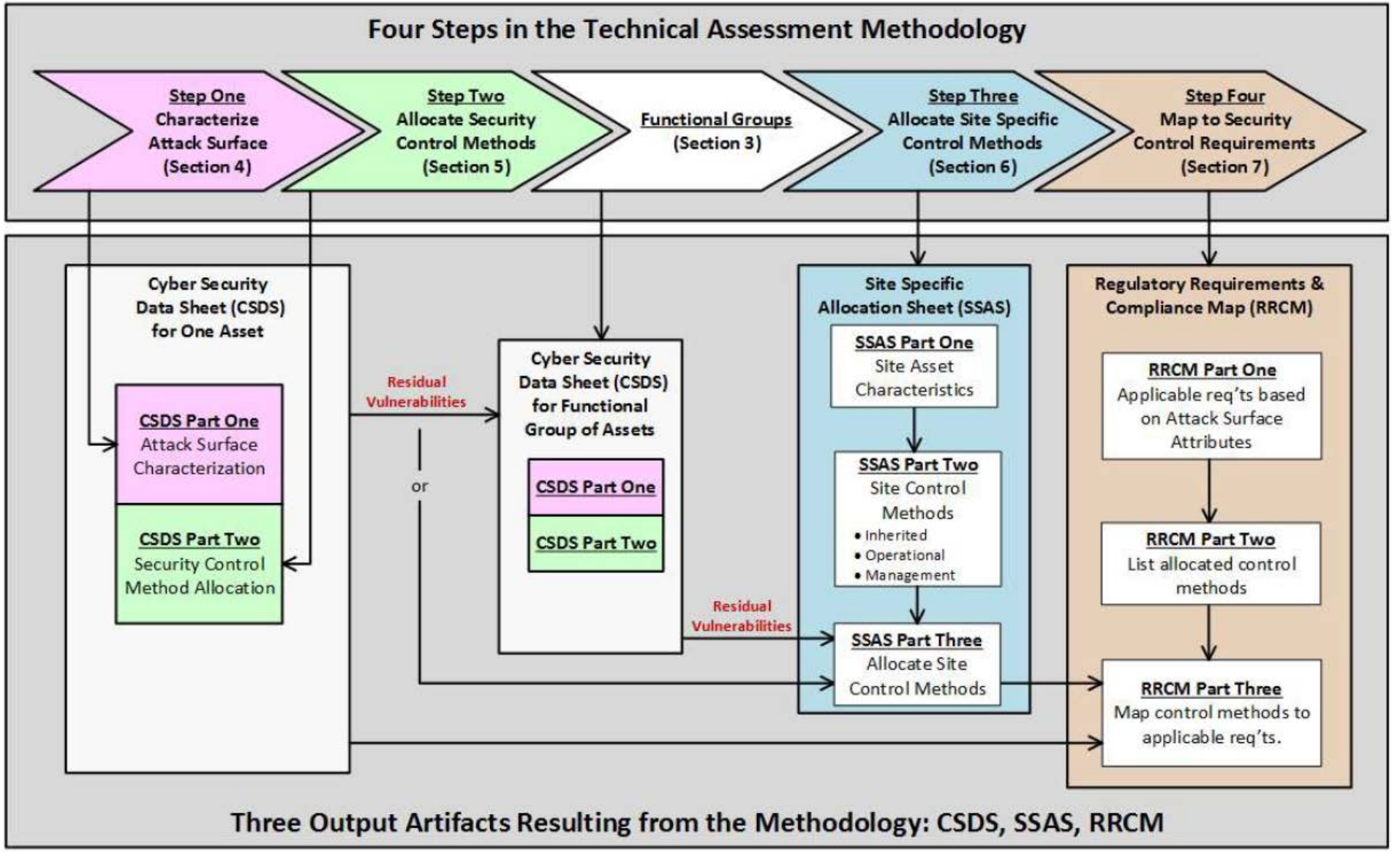
Cyber Security Technical Assessment Methodology: Vulnerability Identification and Mitigation

3002008023

Final Report, October 2016

Michael Thow – EPRI	Steve Hagan – Fisher Valves	Dan Griffin – JW Secure
John Connelly – Exelon	Inman – Lanier – Fisher Valves	Justin Kosar – Assoc. Electric Cooperative
Manu Sharma – Exelon	Mike Hagen – Fisher Valves	Andrew Dettmer – Assoc. Electric Cooperative
Kenneth Levandoski – Exelon	Andrew Clark – Sandia National Laboratory	Steve Ricker – East Kentucky Power Cooperative
Brad Yeates – Southern Company	Matthew Coulter – Duke Energy	Phillip Turner – Sandia National Laboratory
Scott Junkin – Southern Company	Susan Ritter – Duke Energy	Tim Wheeler – Sandia National Laboratory
Richard Atkinson – Arizona Public Service	Mark Denton – Duke Energy	Alice Muna – Sandia National Laboratory
Sandra Bittner – Arizona Public Service	Norman Geddes – Southern Eng. Services	Christine Lai – Sandia National Laboratory

EPRI TAM Overview



EPRI TAM – Attack Surface Characterization

Objective Criteria that Bounds and Groups Exploit Objectives

- 28 Classes of Exploit Objectives
- Based On:
  - Direct Action
  - Critical Data
- Bounding
- Complete

- 5 Attack Vectors
  - Wired Network
  - Wireless Network
  - Portable Interfaces
  - Physical Access
  - Supply Chain
- Determine Specific Attack Pathways
- Determine Specific Exploit Mechanisms

Reference Cyber Security Data Sheets

A key part of the Supply Chain

- Step 1 & 2 by EPRI, Vendors, and other Stakeholders
- Starting point for tailored CSDS

CSDS Organization	
Step 1: Attack Surface Characterization	**Work Product**
Part 1a: Asset Characteristics	MS-Word document
Part 1b: Target Installation Configuration and Data Flow	
Part 1c: Attack Pathways	MS-Excel spreadsheet
Part 1d: Exploit Mechanisms for Applicable Classes of Exploit Objectives	MS-Excel spreadsheet
Step 2: Engineered Security Control Method Identification, Efficacy, and Allocation	
Part 2a: Engineered Security Control Method Identification and Efficacy	MS-Excel spreadsheet
Part 2b: Engineered Security Control Method Allocation	MS-Excel spreadsheet

Big Idea:
You can create a CSDS too!

Cyber Security Technical Assessment Methodology: Vulnerability Identification and Mitigation
3002008023

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security