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

Abuse of legitimate ICS functionality
- Stuxnet
- Crashoverride / Industroyer
- Eg Protocols: IEC101, IEC104, and IEC61850
“Cyber” – Corrosive Hazard

Non-ICS specific Ransomware & Wipers
• Brickerbot
• Not Petya / WannaCry
• Shamoon

• Eg Protocols: SMB, Telnet
“Cyber” – Physical Hazard

Enlistment in bots
• Carna
• Mirai
• Reaper
• And many other similar threats
**“Cyber” – Radio Hazards**

Recent malware targeting radios

- BadBIOS
- BlueBorne
- WPA2 Krack

**Non-Ionizing Radiation Hazard**
Chemical Hazard Labels – NFPA Diamond

- **FLAMABILITY**: Will Not Burn
- **HEALTH**: Least Serious
- **REACTIVITY**: Shock and Heat
- **SPECIAL HAZARDS**: May Detonate

0 - Least Serious
4 - Most Serious
Cyber Hazard Labels: “C-I-A Triad Model”

- **Confidentiality**: Remote, Anonymous, Default Configuration, Root Access
- **Integrity**: Remote, Anonymous, Default Configuration, User Access
- **Availability**: Remote, Authenticated, Default Configuration, Root Access
- **Special Hazards**: Remote, Authenticated, Custom Configuration, Write Access
- **Remote, Authenticated, Read Access**
Cyber Hazard Labels: “V-A-T Model (OSSTMM)” 1/2

![Diagram showing the V-A-T Model (OSSTMM) with categories of Visibility, Access, Trust, and Special Hazards.](image)

<table>
<thead>
<tr>
<th>VISIBILITY</th>
<th>Count</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td></td>
<td>Remote management endpoints</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Remote write access endpoints</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Remote read access endpoints</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>Device broadcasts</td>
</tr>
<tr>
<td>0</td>
<td></td>
<td>No targets visible remotely</td>
</tr>
</tbody>
</table>
Cyber Hazard Labels: “V-A-T Model (OSSTMM)” 2/2

![Diagram of the V-A-T Model (OSSTMM)]

**Special Hazards**

- 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

A badness-ometer 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
Idea: Safety Data Sheets

MATERIAL SAFETY DATA SHEET

Trade Name: ACETONE
Chemical Family: Acetone
Formula: C₃H₆O

FIRE AND EXPLOSION DATA
Flashpoint & Method: 60°F (TCC)
Flammable Limits: LFL 2.0, UFL 13.0
Extinguishing Media: water spray, dry chemical, CO₂, 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
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 Technical Assessment Methodology: Vulnerability Identification and Mitigation

**Final Report, October 2016**

<table>
<thead>
<tr>
<th>Name</th>
<th>Company/Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michael Thow – EPRI</td>
<td>Steve Hagan – Fisher Valves</td>
</tr>
<tr>
<td>John Connelly – Exelon</td>
<td>Inman – Lanier – Fisher Valves</td>
</tr>
<tr>
<td>Manu Sharma – Exelon</td>
<td>Mike Hagen – Fisher Valves</td>
</tr>
<tr>
<td>Kenneth Levandoski – Exelon</td>
<td>Andrew Clark – Sandia National Laboratory</td>
</tr>
<tr>
<td>Brad Yeates – Southern Company</td>
<td>Matthew Coulter – Duke Energy</td>
</tr>
<tr>
<td>Richard Atkinson – Arizona Public Service</td>
<td>Mark Denton – Duke Energy</td>
</tr>
<tr>
<td>Sandra Bittner – Arizona Public Service</td>
<td>Norman Geddes – Southern Eng. Services</td>
</tr>
</tbody>
</table>
### EPRI TAM – Attack Surface Characterization

**Objective Criteria that Bounds and Groups Exploit Objectives**

<table>
<thead>
<tr>
<th>28 Classes of Exploit Objectives</th>
<th>5 Attack Vectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Based On:</td>
<td>Wired Network</td>
</tr>
<tr>
<td>– Direct Action</td>
<td>– Wireless Network</td>
</tr>
<tr>
<td>– Critical Data</td>
<td>– Portable Interfaces</td>
</tr>
<tr>
<td>Bounding</td>
<td>– Physical Access</td>
</tr>
<tr>
<td>Complete</td>
<td>– Supply Chain</td>
</tr>
</tbody>
</table>

- 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

Big Idea: You can create a CSDS too!

Cyber Security Technical Assessment Methodology: Vulnerability Identification and Mitigation

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