Crown Jewels Analysis for Industrial Control Systems

Cedric Carter Jr.

Peter Kertzner

Last Updated January 25, 2023

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

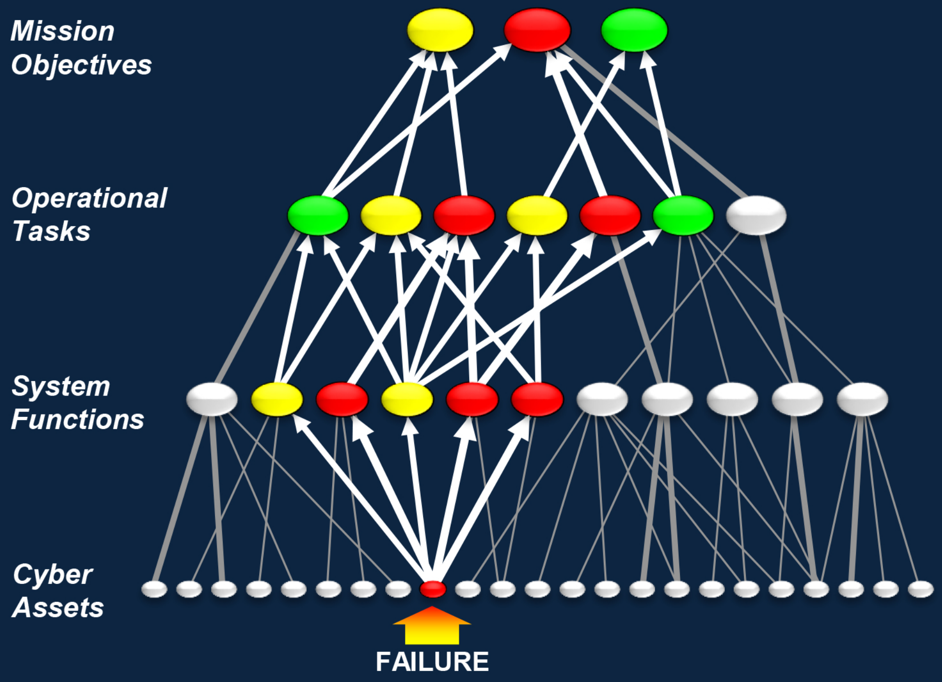
Motivation of Applying CJA for ICS

- Every mission, every business in every country relies on critical infrastructure (e.g., energy, water & wastewater, transportation, etc.) – they are National level assets
- There are functions associated with both operations and safety of critical infrastructure systems that must be resilient for sustainment
- These functions are dependent on underlying Industrial Control Systems (ICS)
- Critical components associated with these functions need to be identified in order to safeguard them from non-kinetic threats, including cyber-attacks, and to develop and apply resiliency measures

It is imperative that large, complex control systems be analyzed to discover their critical components

Agenda

- Background
- Complexity in Critical Infrastructure
- Mission Assurance Engineering Process
- Crown Jewels Analysis Overview and Process
- Sample Research Questions for Customers
- Mission Focused Architectures
- Managing Subjectivity During Criticality Scoring
- References



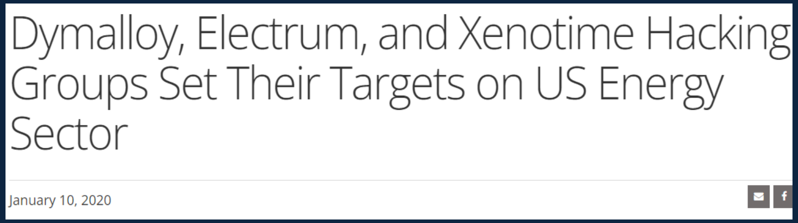
Background

- Industrial Control Systems (ICS) were not originally designed to be resilient, nor survivable against cyber malicious actors
- Cyber malicious actors are targeting common cyber security gaps in critical infrastructure
- There is a need to *integrate* and *operate* cyber defenses (e.g., mitigations) for ICS supporting critical infrastructure
- Mitigations exist; however not all mitigations are viable for existing designs and architectures that have longer life cycles

Hacker group discloses ability to encrypt an RTU device using ransomware, industry reacts

JANUARY 13, 2023

Source: IndustrialCyber.co



Dymalloy, Electrum, and Xenotime Hacking Groups Set Their Targets on US Energy Sector

January 10, 2020

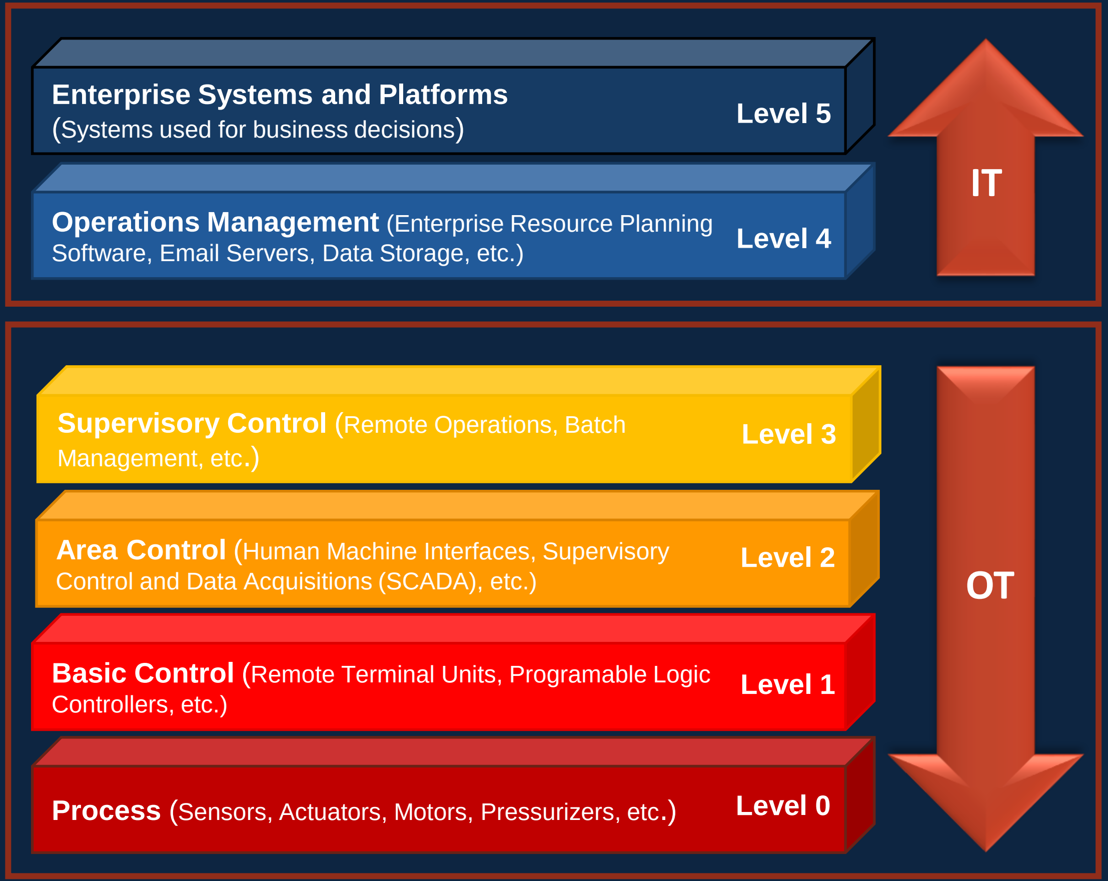
Source: Trendmicro

Images of Complex Systems

Source: (1) ERCOT Control Room Video; https://www.youtube.com/watch?v=-KatQ9Q_IQk;
(2) Astute Engineering; (3) Preshizek Geospacial Consultancy

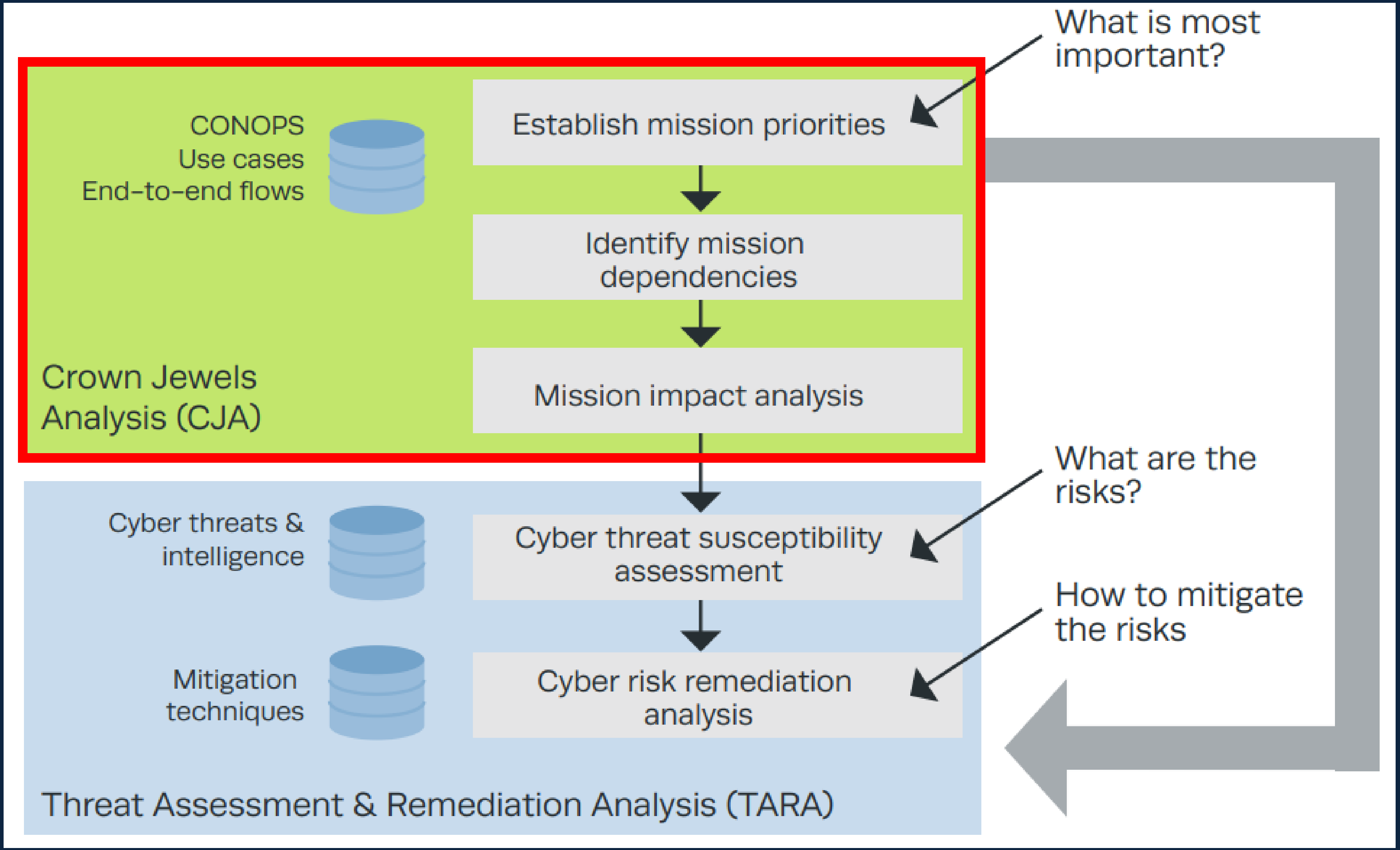
The Purdue Model

- Developed in the 1990s, the Purdue model is a reference architecture and general data flow diagram to help mission owners, assessment teams, operators, etc. understand the following:
    - Interconnections and interdependencies of assets' technological components
    - Segmentation of various technological domains (e.g., operational technology (OT), information technology (IT), mobile technology)
    - Where to apply security measures effectively



Enterprise Systems and Platforms (Systems used for business decisions) Level 5
Operations Management (Enterprise Resource Planning Software, Email Servers, Data Storage, etc.) Level 4
IT
Supervisory Control (Remote Operations, Batch Management, etc.) Level 3
Area Control (Human Machine Interfaces, Supervisory Control and Data Acquisitions (SCADA), etc.) Level 2
Basic Control (Remote Terminal Units, Programable Logic Controllers, etc.) Level 1
Process (Sensors, Actuators, Motors, Pressurizers, etc.) Level 0
OT

Mission Assurance Engineering Process


What is most important?
CONOPS
Use cases
End-to-end flows
Establish mission priorities
Identify mission dependencies
Mission impact analysis
Crown Jewels Analysis (CJA)
What are the risks?
Cyber threats & intelligence
Cyber threat susceptibility assessment
How to mitigate the risks
Mitigation techniques
Cyber risk remediation analysis
Threat Assessment & Remediation Analysis (TARA)

Source: The MITRE Corporations System's Engineering Guidebook

MITRE

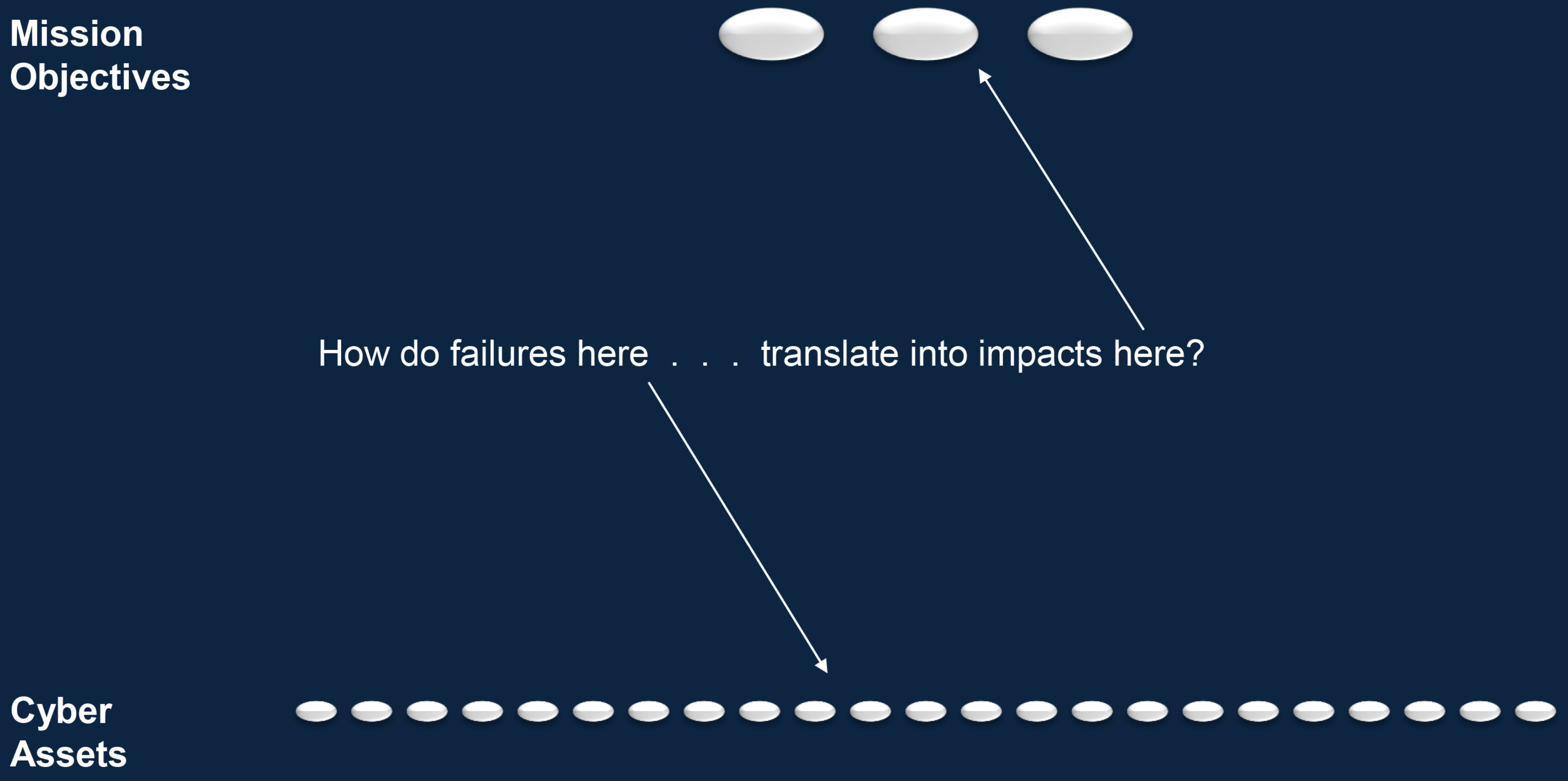
Crown Jewels Analysis Overview

- A crown jewel is logic-bearing or non-logic bearing device, whose failure – *or failure to perform as intended* – can cause one or more mission objectives to fail
- Methodology developed by MITRE and practiced since late 2000s
- A process for identifying assets most critical to mission sustainment/accomplishment
- Determined through Mission Impact Analysis (MIA) after functionally decomposing an organization's mission into *objectives* → *tasks* → *functions* → *assets*
- Approach combines expert input with established techniques:
  - Analytic Hierarchy Process (AHP)
  - Quality Function Deployment (QFD)
  - Failure Modes and Effects Analysis (FMEA)

Crown Jewels Analysis Definitions

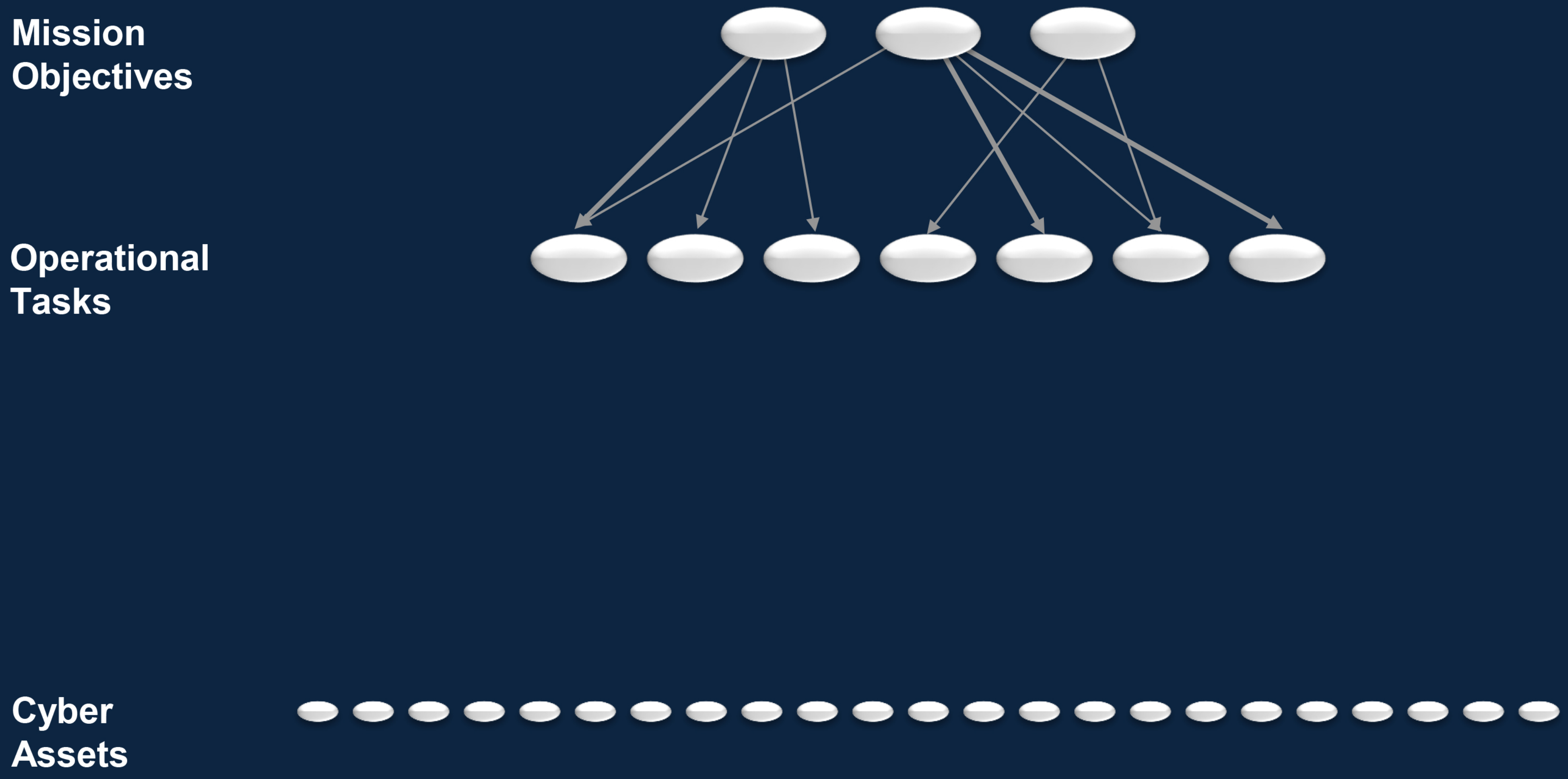
- **Mission Objective (Level 4)**
  - One of a set of typically three to six objectives that comprise an overall mission goal (e.g., maintain hand-off from local electric utility; maintain uninterrupted distribution of electricity to customers)
- **Operational Task or Human Task (Level 3)**
  - Activities carried out by personnel where task performance supports achievement of mission objectives (e.g., monitor electricity distribution status; control end devices)
- **System Function (Level 2)**
  - Enable performance of operational tasks
    - Monitor (e.g., poll and process OT data; store historical data)
    - Control (e.g., open/close breakers remotely/locally; provide precision timing to controllers and end devices)
- **Asset (Level 1)**
  - A logic-bearing or non-logic bearing device essential to task performance and achievement of mission objectives (e.g., SCADA server, RTU, PLC, operator workstation, IT switch, IT/OT gateway, protection system/breaker, power transmission cable, etc.)

CJA Helps Us Answer a Key Question



How do failures here . . . translate into impacts here?

We Start by Identifying the Tasks that Support Each Mission Objective

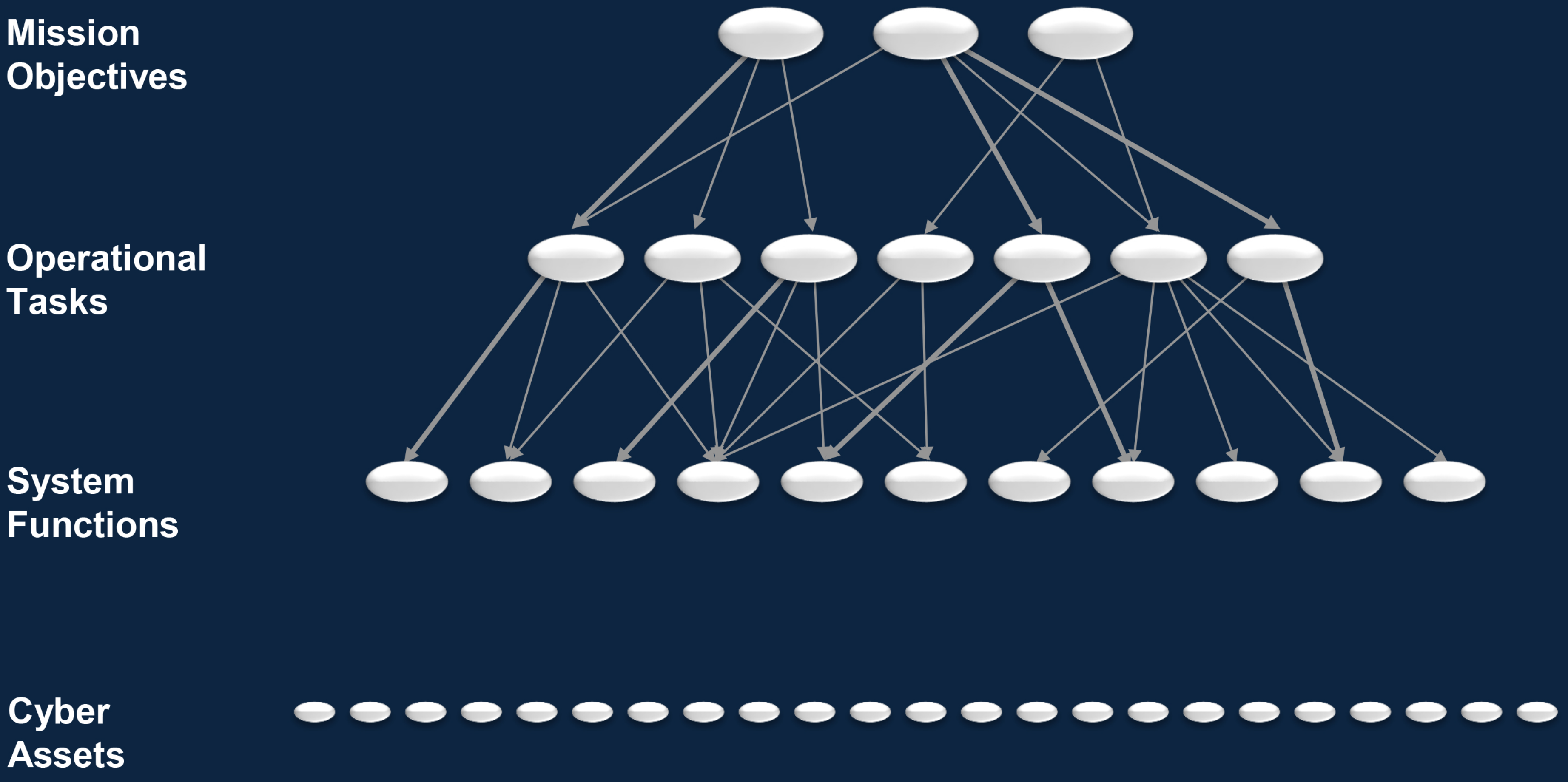


Mission Objectives

Operational Tasks

Cyber Assets

Next, We Identify the System Functions that Support Each Task



Mission Objectives

Operational Tasks

System Functions

Cyber Assets

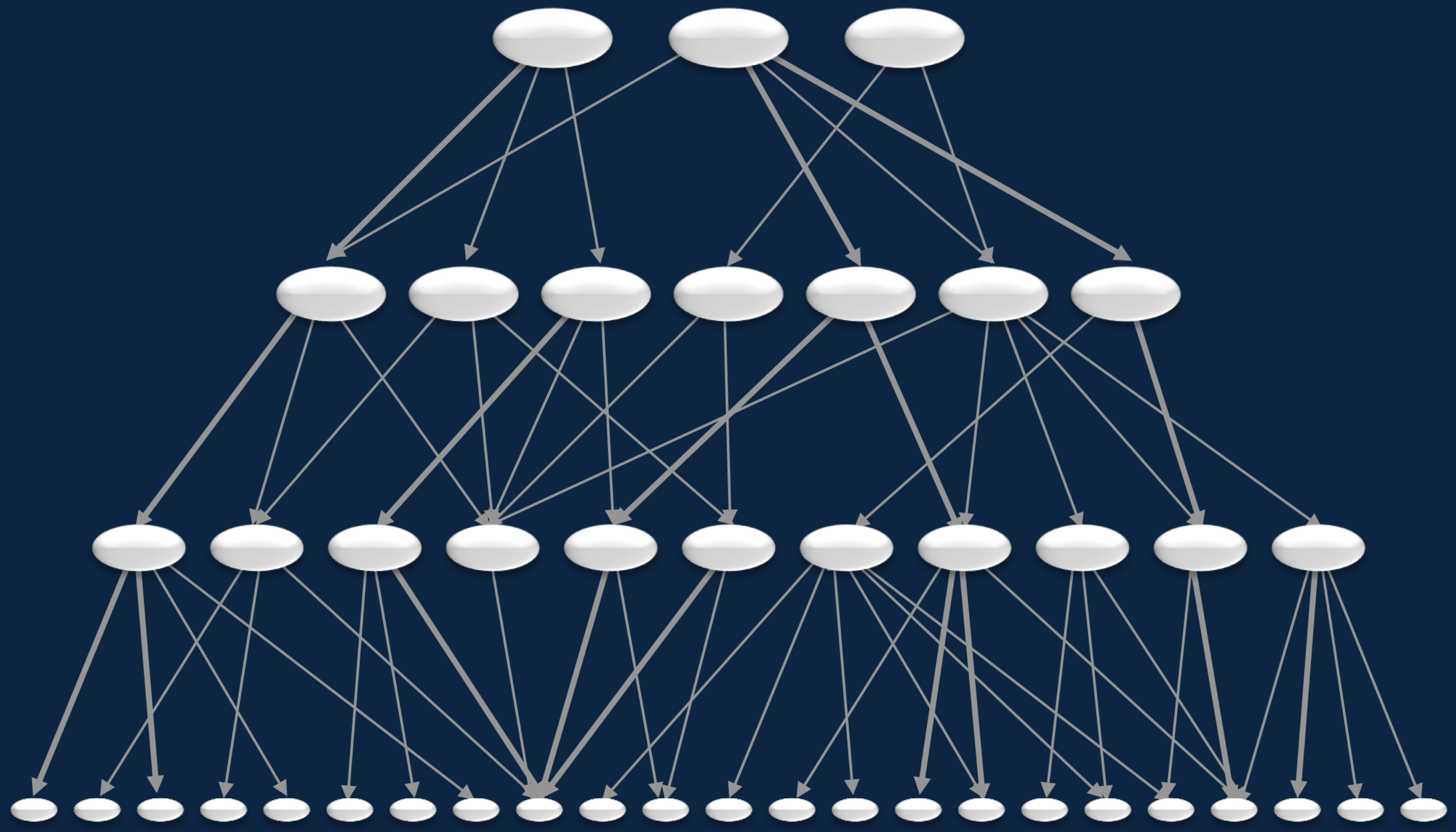
Finally, We Identify the Cyber Assets That Support Each System Function

Mission Objectives

Operational Tasks

System Functions

Cyber Assets



MITRE

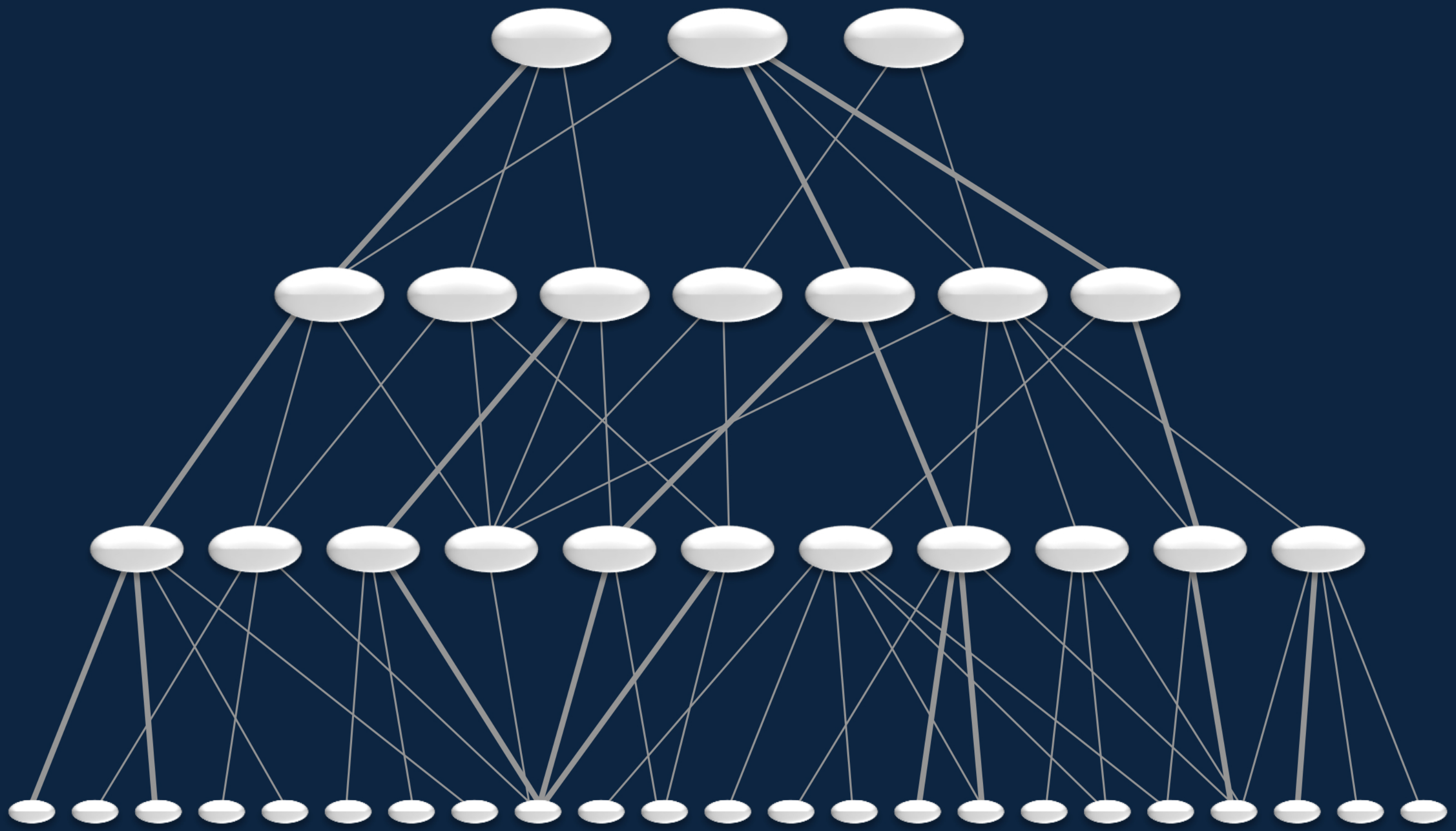
We Now Have a Complete Map of Mission Dependencies

Mission
Objectives

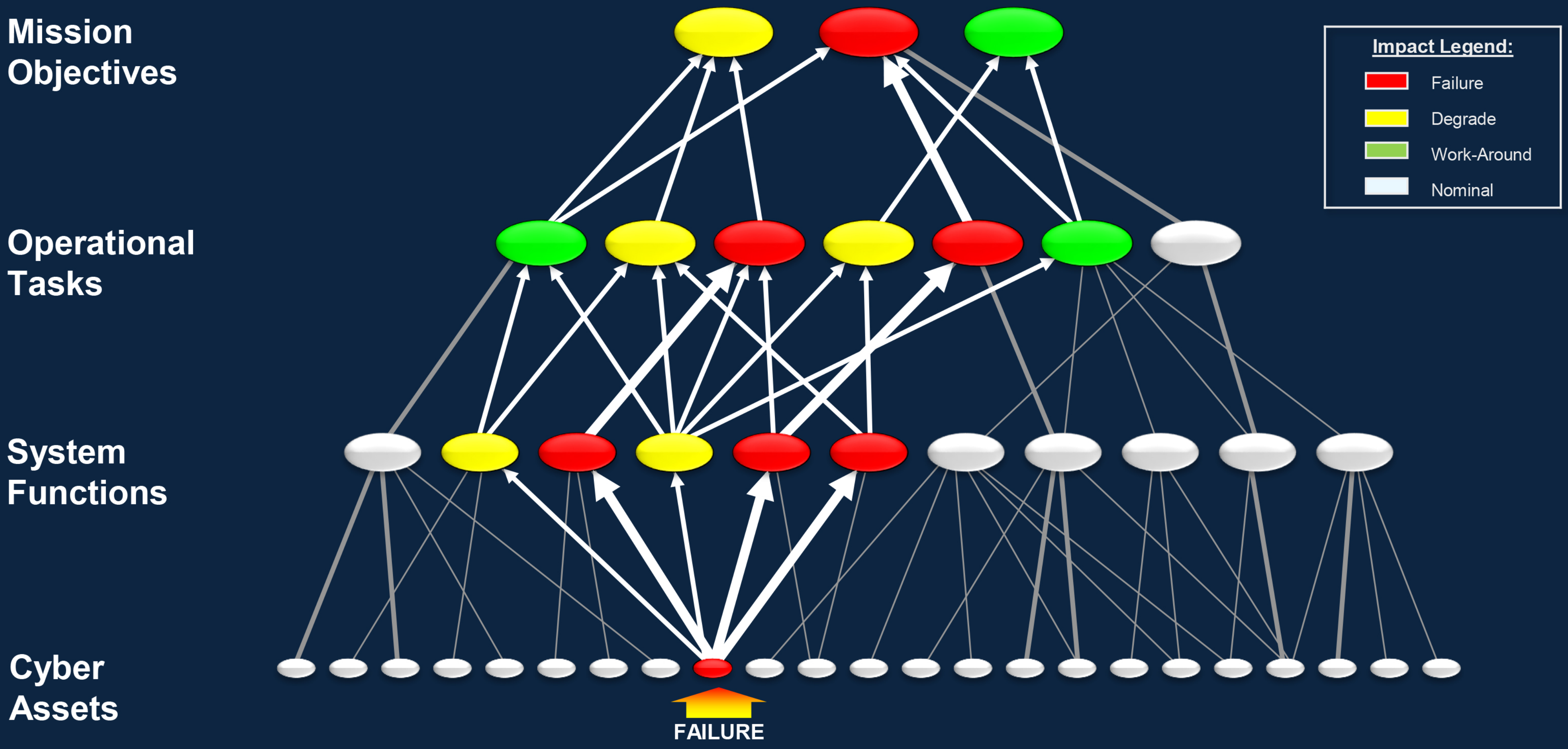
Operational
Tasks

System
Functions

Cyber
Assets



We Use Dependency Maps to Predict the Impact of Cyber Asset Failures



Mission Objectives

Operational Tasks

System Functions

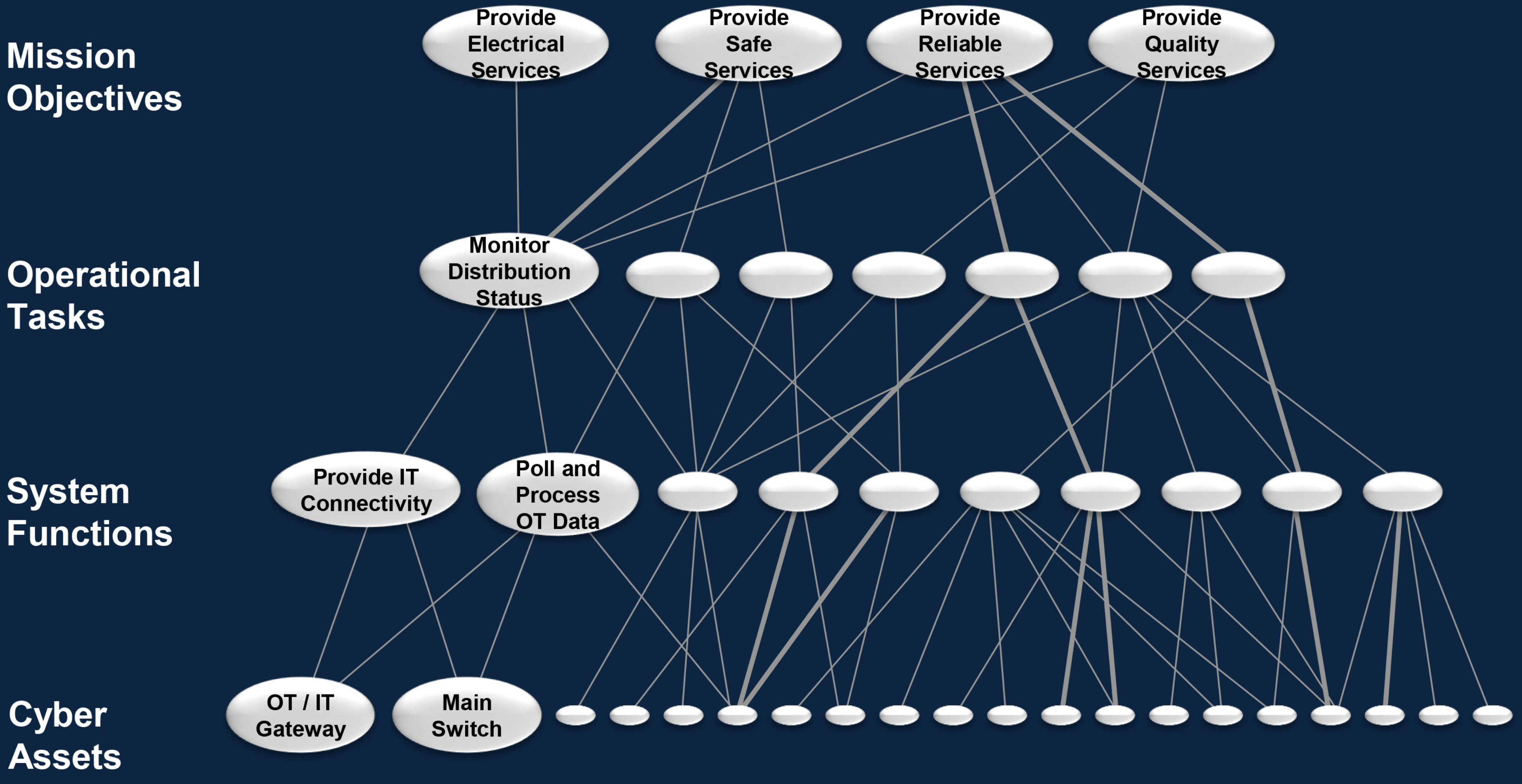
Cyber Assets

FAILURE

Impact Legend:

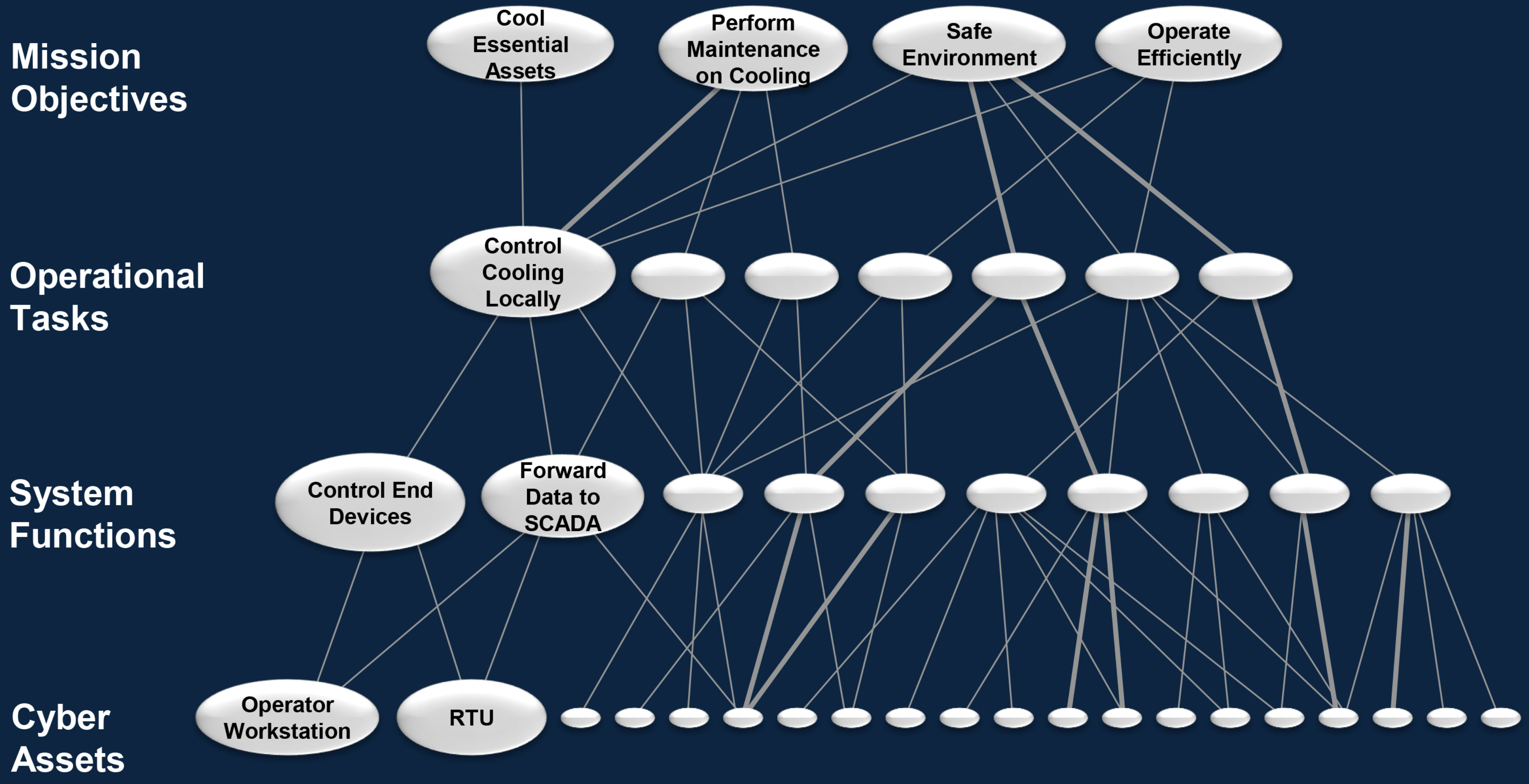
- 🟥 Failure
- 🟨 Degrade
- 🟩 Work-Around
- ⬜ Nominal

Dependency Mapping Example:
Power Distribution

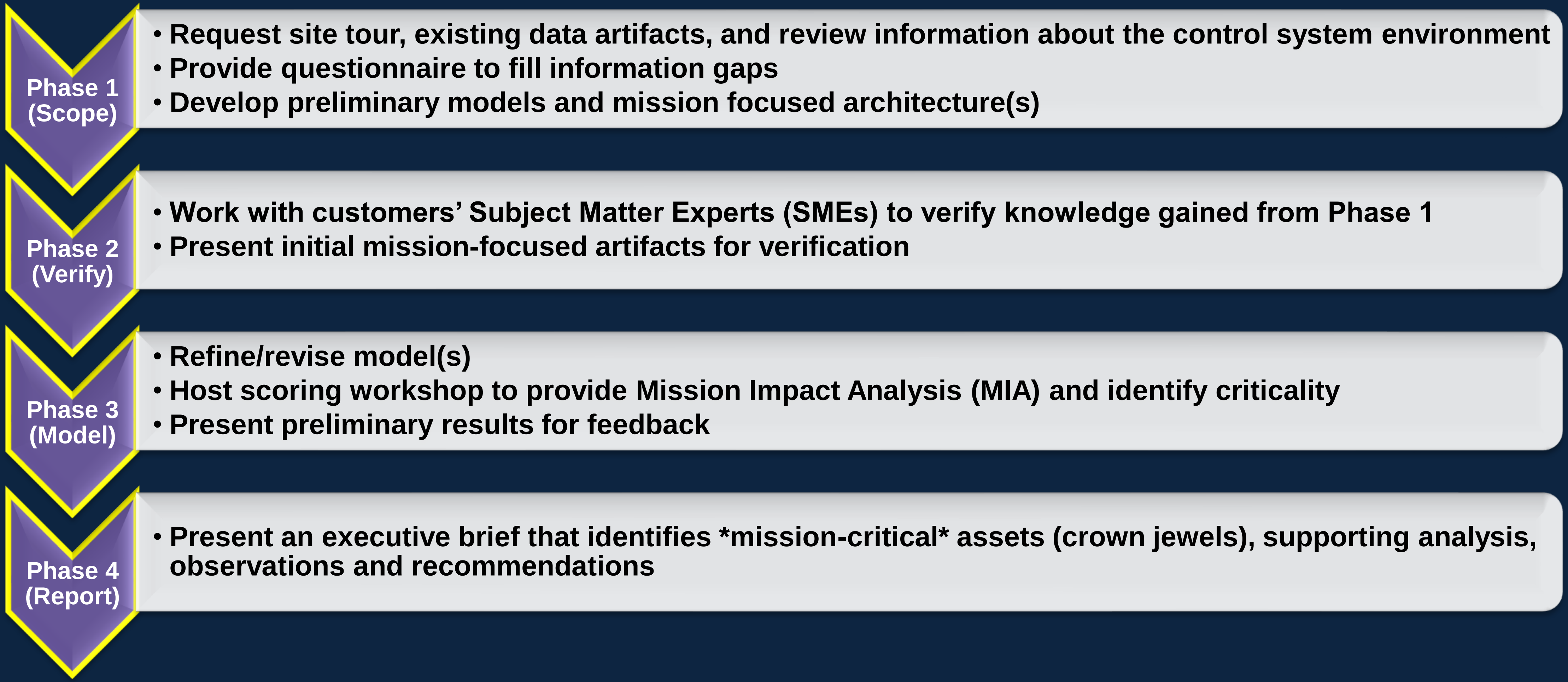


MITRE

Dependency Mapping Example:
Building Automation System



Crown Jewels Analysis for ICS Process



Phase 1 (Scope)

- Request site tour, existing data artifacts, and review information about the control system environment
- Provide questionnaire to fill information gaps
- Develop preliminary models and mission focused architecture(s)

Phase 2 (Verify)

- Work with customers' Subject Matter Experts (SMEs) to verify knowledge gained from Phase 1
- Present initial mission-focused artifacts for verification

Phase 3 (Model)

- Refine/revise model(s)
- Host scoring workshop to provide Mission Impact Analysis (MIA) and identify criticality
- Present preliminary results for feedback

Phase 4 (Report)

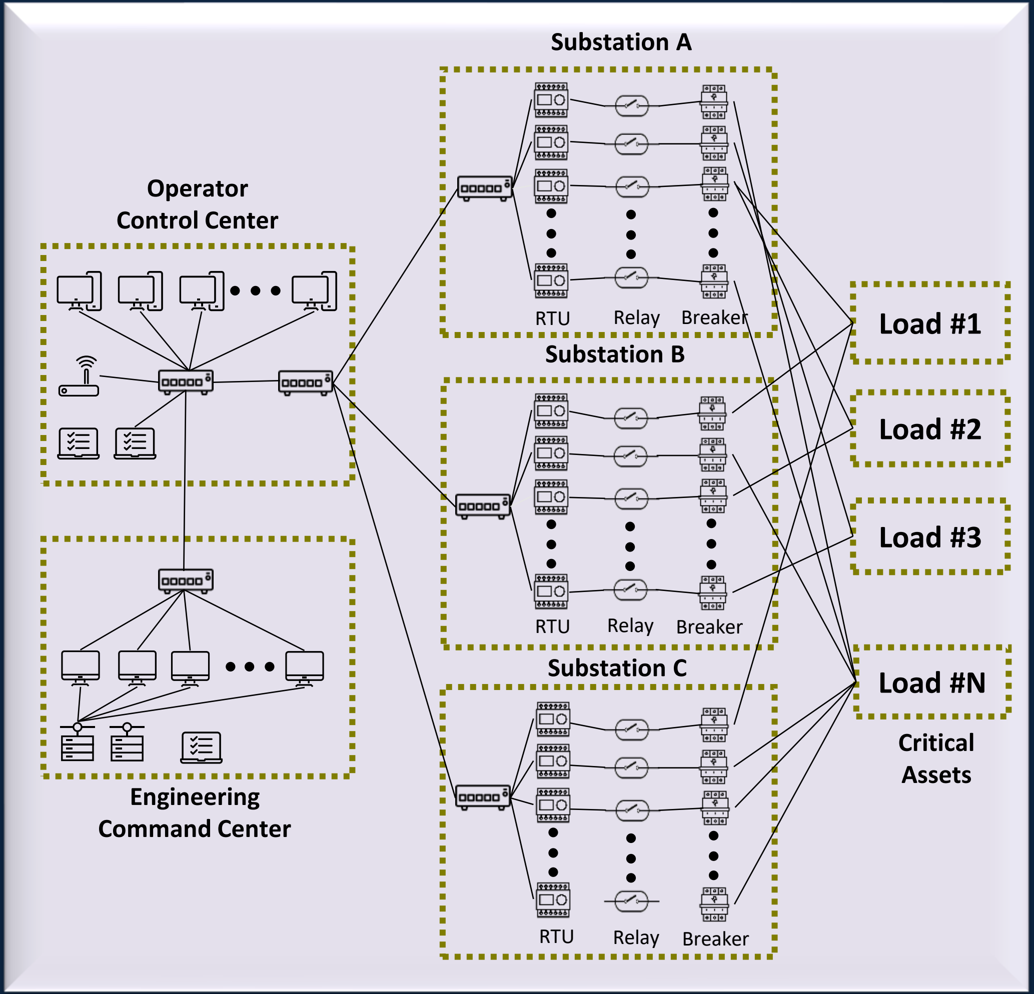
- Present an executive brief that identifies *mission-critical* assets (crown jewels), supporting analysis, observations and recommendations

Sample Assessment Questions

Focus of Assessment Question	Example Questions Used for Information Gathering
Developing and populating the Crown Jewels Analysis model	• Is there an operational technology (OT) functional specification describing systems functions involved for supporting operations? • What information technology (IT) solutions are used for configuration management and security patching? • Please describe how the system equipment is used and maintained for operators, contractors, vendors, etc.?
Failure scenario development using the ATT&CK™ knowledge base and mitigation planning	• How are software (SW) and firmware (FW) patches managed? Are SW/FW patches evaluated and tested prior to being installed on operational equipment? • In the event of a cyber malicious activity, what policies, protocols, procedures are in place for operations? What is the current state for incident response? • How are equipment vulnerabilities and risk being tracked?

Mission Focused Architectures

- In many cases organizations may not have sufficient data or focused datasets for CJA. These artifacts can include, but not limited to:
  - Asset Inventories
  - Networking Diagrams
  - Cyber Assessments (Discovery)
- There may be opportunities to leverage CJA findings to produce data-driven architectures that are mission focused



Managing Subjectivity

- Mission owners and operators participate along with CJA analysts in the criticality scoring of mission dependencies
- Mission owners and operators may have extensive experience executing their mission and operating their systems
  - However, prolonged mission/system involvement can lead to entrenched notions of which systems may or may not be critical to mission, notions that may not be correct
  - These "biases" have the potential of being reflected in criticality scoring
- Dependency criticality evaluations are made pairwise between model elements (e.g., if system function X is unavailable, how does that affect my ability to perform operational task Y?)
  - This reduces the risk of biases *unintentionally* or even *intentionally* influencing the outcome of the analysis

Criticality scores are agreed upon through group consensus – any differences of opinion should be discussed and settled

References

- The MITRE Corporation’s Crown Jewels Analysis
  - https://www.mitre.org/our-impact/intellectual-property/crown-jewels-analysis
- The MITRE Corporation’s Crown Jewels Analysis for Industrial Control Systems
  - https://www.mitre.org/news-insights/publication/crown-jewels-analysis-industrial-control-systems
- Dragos Webinar – Crown Jewels Analysis for Government-Owned Industrial Control Systems
  - https://hub.dragos.com/on-demand/crown-jewels-analysis-for-industrial-control-systems
- The MITRE Corporation’s Systems Engineering Guidebook
  - https://www.mitre.org/sites/default/files/2022-09/MITRE-SEG.pdf
- The MITRE Corporation’s ATT&CK® Knowledge Base
  - **Enterprise**: https://attack.mitre.org/matrices/enterprise/
  - **Mobile**: https://attack.mitre.org/matrices/mobile/
  - **Industrial Control Systems:** https://attack.mitre.org/matrices/ics/