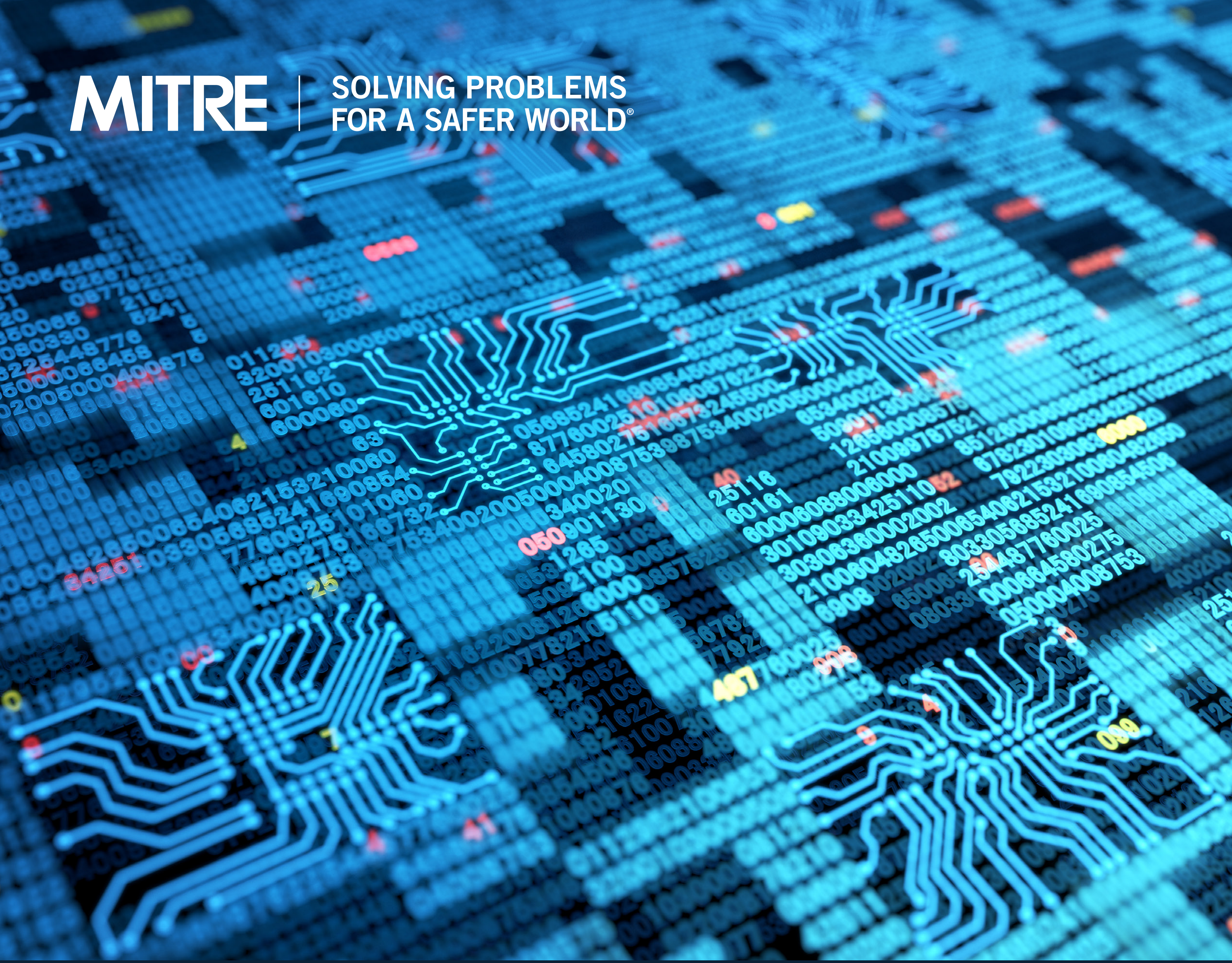
MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®



CROWN JEWELS ANALYSIS (CJA) FOR INDUSTRIAL CONTROL SYSTEMS (ICS)

AUTHORS: PETER KERTZNER, CEDRIC CARTER, ADAM HAHN

Summary

To help assess risks to mission from cyber and non-kinetic threats, organizations need repeatable processes to analyze how failure or compromise of an asset could degrade or cause failure of a critical mission. In Department of Defense Directive 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, an asset is described as being "A distinguishable entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and employed, owned, or operated by domestic, foreign, public, or private sector organizations." Understanding mission impacts from cyber, non-kinetic, or kinetic attack(s), and how to achieve mission resilience, requires an understanding of mission tasks, their dependence on various infrastructure elements, and how failure of an asset can translate into a mission-level impact. The Crown Jewels Analysis (CJA) process provides a repeatable approach to capturing knowledge from organizational Subject Matter Experts (SMEs), documenting known dependencies, and prioritizing assets based on their criticality to mission [1].

THE CROWN JEWELS ANALYSIS (CJA) PROCESS PROVIDES A REPEATABLE APPROACH TO CAPTURING KNOWLEDGE FROM ORGANIZATIONAL SUBJECT MATTER EXPERTS (SMES), DOCUMENTING KNOWN DEPENDENCIES, AND PRIORITIZING ASSETS BASED ON THEIR CRITICALITY TO MISSION.

Understanding Crown Jewels and Mission Dependencies

A crown jewel is a logic-bearing or non-logic bearing device (i.e., a device that may contain a microelectronic component) whose failure—or failure to perform as intended—can cause mission failure. While a mission may have many dependencies on varied devices and components, crown jewels are considered devices and components whose failure to perform as expected or intended can result in failure of one or more mission objectives. Different levels of mission impacts have been identified by the Defense Acquisition Guidebook, as identified below [2].

- **Level I:** Total Mission Failure (Failure)
- **Level II:** Significant Degradation (Degradation)
- **Level III:** Partial Capability Loss (Workaround)
- **Level IV:** Negligible or No Loss (Nominal)

While the CJA process focuses on the identification of mission dependencies on assets whose failure can create conditions for possible mission failure (Level I), it also more broadly identifies significant dependencies that create conditions for possible mission degradation (Level II).

A control system whose technology can cause failure of a mission objective if compromised aligns to CJA's definition of a crown jewel. The effects of compromise of an OT asset and the potential mission impacts from that compromise may be well-known by personnel operating in Operational Technology (OT) environments. For example, a Supervisory Control and Data Acquisition (SCADA) server may be a critical asset well-known to operational SMEs, or a security architect may understand that a firewall is key to enforcing security-focused segmentation across networking domains. However, knowledge about which assets are crown jewels is often distributed across multiple organizational roles and responsibilities. Furthermore, in many cases no single individual or organization will fully understand the broader mission or business system dependencies on an asset. Lack of understanding of mission or business dependencies on assets relates to how an asset may be supporting functions across multiple organizational units. Therefore, the process of identifying crown jewels should include the following:

- Leveraging diverse expertise across mission/ business functions
- An understanding of organizational mission/ business goals or objectives
- Knowledge of key operational processes and functions
- Inputs from network administrators and cybersecurity analysts
- An understanding of operational dependencies on key cyber terrain (i.e., assets)

Data required in the crown jewels information gathering phase results from conversations with mission/business owners, managers, administrators, operators, engineers, and technicians.

Understanding OT Dependencies

The CJA process provides a repeatable approach to identifying mission objectives, operational tasks, system functions, and the assets that directly provide, support, or enable functions. Functions support operational tasks, whose performance supports missions. A CJA can be applied to different critical infrastructure sectors to identify assets critical to supporting a mission. For example, CJA has been applied to an oil refinery for determining systems used to acquire crude oil. The criticality analysis revealed systems most critical to sustaining refinery operations [3].

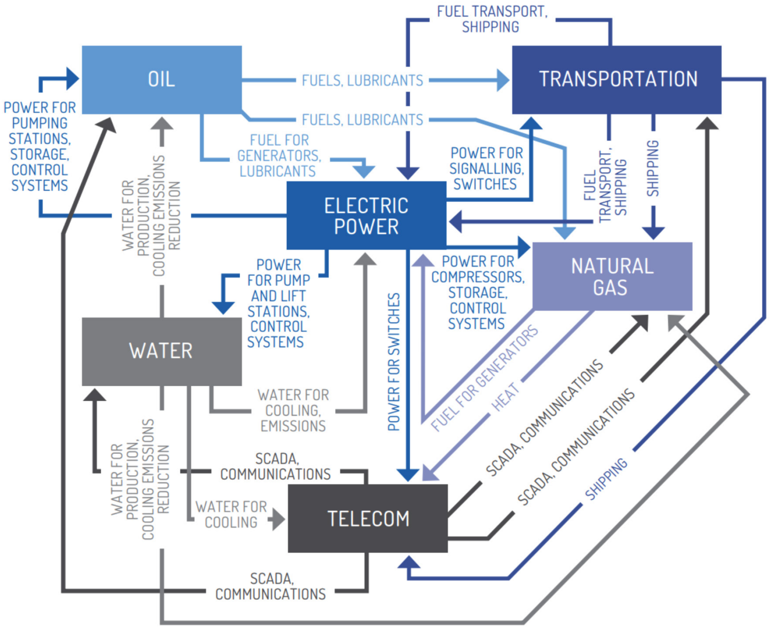

FUEL TRANSPORT, SHIPPING
OIL
FUELS, LUBRICANTS
TRANSPORTATION
FUELS, LUBRICANTS
POWER FOR PUMPING STATIONS, STORAGE, CONTROL SYSTEMS
FUEL FOR GENERATORS, LUBRICANTS
POWER FOR SIGNALLING, SWITCHES
FUEL TRANSPORT, SHIPPING
SHIPPING
WATER FOR PRODUCTION COOLING EMISSIONS REDUCTION
ELECTRIC POWER
POWER FOR COMPRESSORS, STORAGE, CONTROL SYSTEMS
NATURAL GAS
POWER FOR PUMP AND LIFT STATIONS, CONTROL SYSTEMS
WATER
POWER FOR SWITCHES
FUEL FOR GENERATORS
HEAT
WATER FOR COOLING, EMISSIONS
SCADA, COMMUNICATIONS
SCADA, COMMUNICATIONS
SCADA, COMMUNICATIONS
SHIPPING
WATER FOR PRODUCTION, COOLING EMISSIONS REDUCTION
WATER FOR COOLING
TELECOM
SCADA, COMMUNICATIONS

FIGURE 1. UNDERSTANDING OPERATIONAL DEPENDENCIES ACROSS KEY CRITICAL INFRASTRUCTURE SECTORS [4].

CJA is a process for understanding the dependencies of mission objectives on operational tasks, system functions, and diverse technologies in support of OT services. OT services can include providing electrical power, potable water, heating, ventilation, air conditioning (HVAC), etc. Often, organizations performing missions understand which of their assets are critical; however, there are instances where organizations lack understanding of the significance of people and supporting OT services.

Performing a Mission Impact Analysis (MIA)

MIA is a feature of the CJA process that allows for the automated simulation of asset failure and its effect on mission. The ability to simulate the failure of one or more assets, simultaneously, is important for developing an understanding of mission dependencies on assets and what impact a failed asset can have on achievement of mission objectives. Mission dependencies on assets are determined by mapping mission objectives to the operational tasks that support them; mapping operational tasks to the system functions that enable them; and finally, mapping system functions to the assets they are dependent on. Each layer in the analysis is described below.

Mission Objectives

The first step toward revealing critical assets is to identify the organization's mission objectives associated with the operational environment. Mission objectives reflect goals or desired outcomes involving the purpose of the operational environment. Mission objectives relying on operational technology can include safety and environmental security needs. For OT, an example is the ability to provide energy services via oil, natural gas, water, etc. Examples of mission objectives include:

- Provide uninterrupted power to mission critical systems
- Provide cooling/heating to essential assets
- Provide Fire Suppression

Mission Objectives
M1
M2
M3
MJ

FIGURE 2. EXAMPLE IDENTIFICATION OF MISSION OBJECTIVES.

Operational Tasks

The second step, after mission objectives have been determined, is to identify the various operational tasks whose performance supports achievement of mission objectives. In the OT domain, operational tasks are the activities of personnel and/or capabilities of technology needed for actuating, monitoring, and controlling physical processes. Examples of operational tasks include:

- Collecting telemetry to monitor processes
- Maintaining/providing situational awareness
- Performing maintenance on end devices

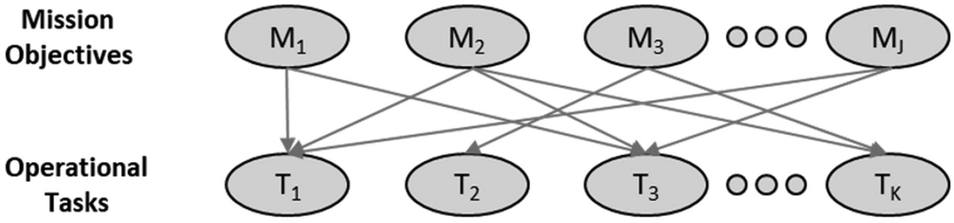


FIGURE 3. EXAMPLE DEPENDENCY OF MISSION OBJECTIVES ON OPERATIONAL TASKS

System Functions

The third step toward revealing critical assets is to identify system functions whose availability supports performance of operational tasks. While operational tasks rely on information and control functions needed for executing the mission (e.g., collecting data and sending control signals), they also depend on implementation of control algorithms in devices such as Programmable Logic Controllers (PLCs) and Distributed Control Systems (DCSs). Additionally, supporting performance of operational tasks requires numerous management functions of various systems and devices. Examples of system/management functions include:

- Poll devices for operations related data
- Archive configuration settings and states of devices
- Capture ICS events and anomalies

System functions also include various indirect services and functions needed to support the operation of networks and hosts. From a network perspective, this could include protocols that support timing (Network Time Protocol - NTP), addressing (Domain Name System - DNS), reliability (Spanning Tree Protocol - STP), and security (Virtual Private Network - VPNs). Examples of higher-level system functions include:

- Identity and access management
- User and device authentication
- Configuration management

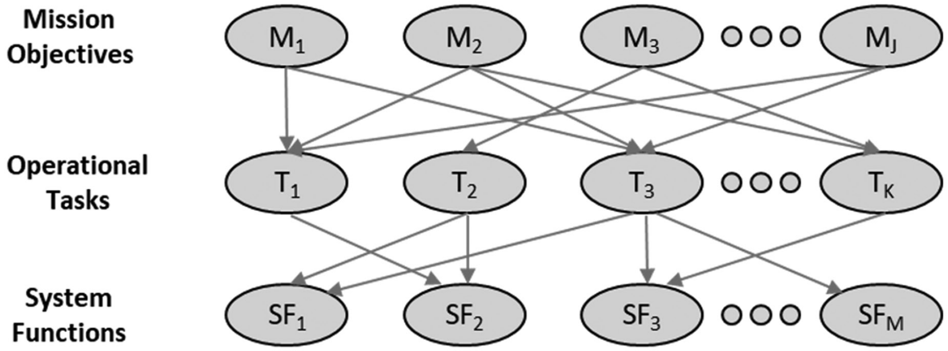


FIGURE 4. EXAMPLE SHOWING DEPENDENCY OF OPERATIONAL TASKS ON SYSTEM FUNCTIONS

Assets

Assets are the broad set of OT, IT and infrastructure devices that provide or enable system functions. The range of OT devices includes cyber-physical systems (where a processor monitors/controls a mechanism), low-level controllers, and communications components. Examples of OT assets include:

- Programmable Logic Controller (PLC)
- Direct Digital Controller (DDC)
- Remote Terminal Unit (RTU)

IT devices are primarily higher-level hardware/software platforms that perform or support monitoring and control functions remotely. Examples of IT assets include:

- SCADA server
- Historian database
- Operator workstation

Assets can also be network infrastructure components that provide the IT/OT connectivity that allows both local and remote monitoring and control to be performed. Examples of infrastructure assets include:

- Network backbone devices (e.g., switches, routers, gateways)
- Security devices (e.g., firewalls, gateways)
- Management systems (e.g., jump hosts, engineering workstations)

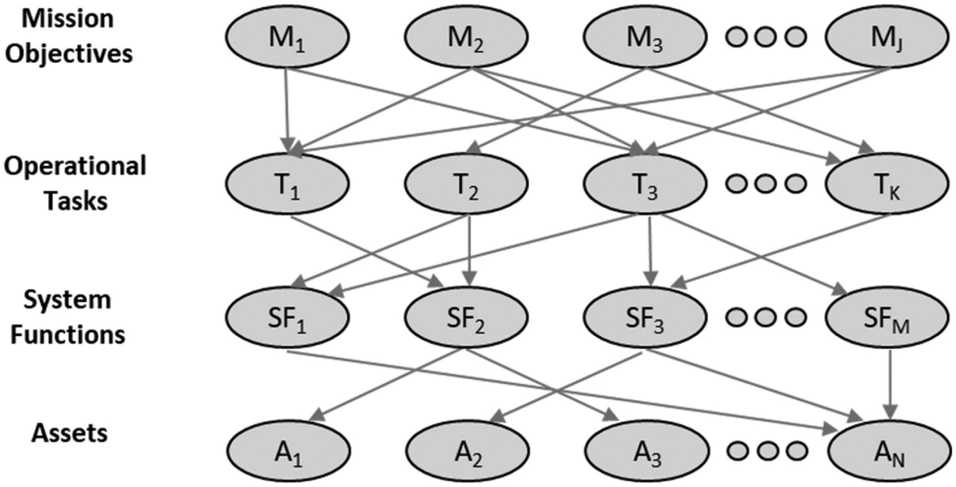


FIGURE 5. EXAMPLE SHOWING DEPENDENCY OF SYSTEM FUNCTIONS ON ASSETS

Figure 6 below, A Representational Dependency Map, illustrates mission dependency relationships among the multiple tiers of a dependency model. Examples are given of the types of mission elements that could be represented at each tier of the model.

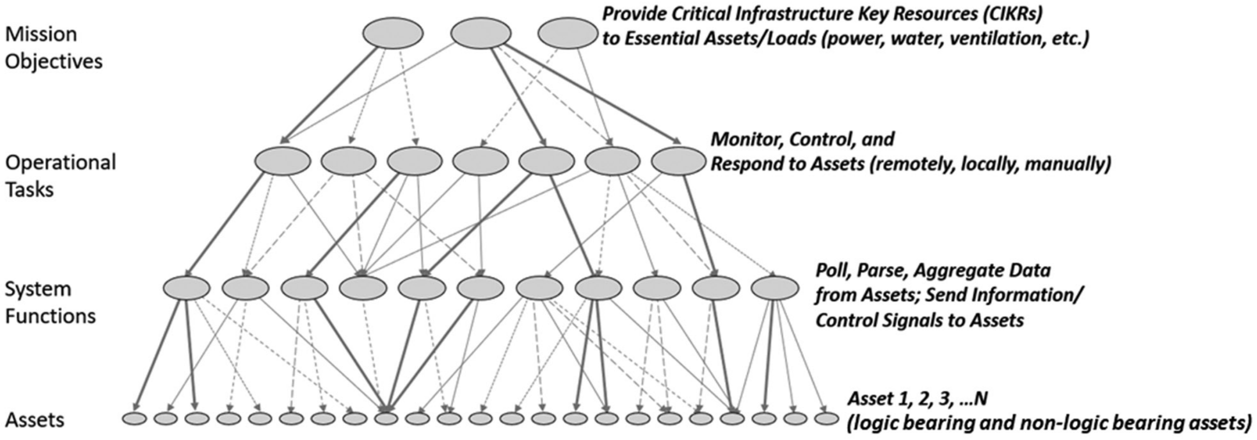

Mission Objectives
Provide Critical Infrastructure Key Resources (CIKRs) to Essential Assets/Loads (power, water, ventilation, etc.)
Operational Tasks
Monitor, Control, and Respond to Assets (remotely, locally, manually)
System Functions
Poll, Parse, Aggregate Data from Assets; Send Information/ Control Signals to Assets
Assets
Asset 1, 2, 3, …N (logic bearing and non-logic bearing assets)

FIGURE 6. A REPRESENTATIONAL DEPENDENCY MAP

Understanding Mission Dependencies

In performing the CJA Mission Impact Analysis for the system being assessed, organizational SMEs help define the degree of criticality of dependences between each layer or tier of the CJA dependency model. Figure 6 is an illustration and example of a mission dependency mapping structure. In practice, each dependency will be assigned a weight (i.e., a criticality score) to indicate how critical each child node is to its parent. Criticality of a dependency of a parent node on a child node can be informed by assessing the extent to which loss of the child would impact the parent, where that extent is expressed in terms of the four-level impact scale described above.

Once mission dependencies have been mapped from top tier down through to the bottom tier, the analytic techniques of Analytic Hierarchy Process (AHP), Quality Function Deployment (QFD) and Failure Modes and Effects Analysis (FMEA) are used to rank order tier elements, for each tier, based on their relative importance to achievement of all mission objectives. With the use of the Mission Impact Analysis technique, tier four assets are evaluated for their individual criticality to mission accomplishment. Highly critical assets are flagged for further analysis and assessment. See reference [1] for details on how tier elements and their dependencies are determined and how criticality scores are determined and assigned to dependencies.

Figure 7 below, Example Impact on Mission of a Crown Jewel Failure, illustrates how failure of an asset can impact a mission objective. The failed asset can no longer provide a necessary system function to an operational task that relies on that function being available. Because the operational task can now not be performed, any dependent mission objective can now not be achieved.

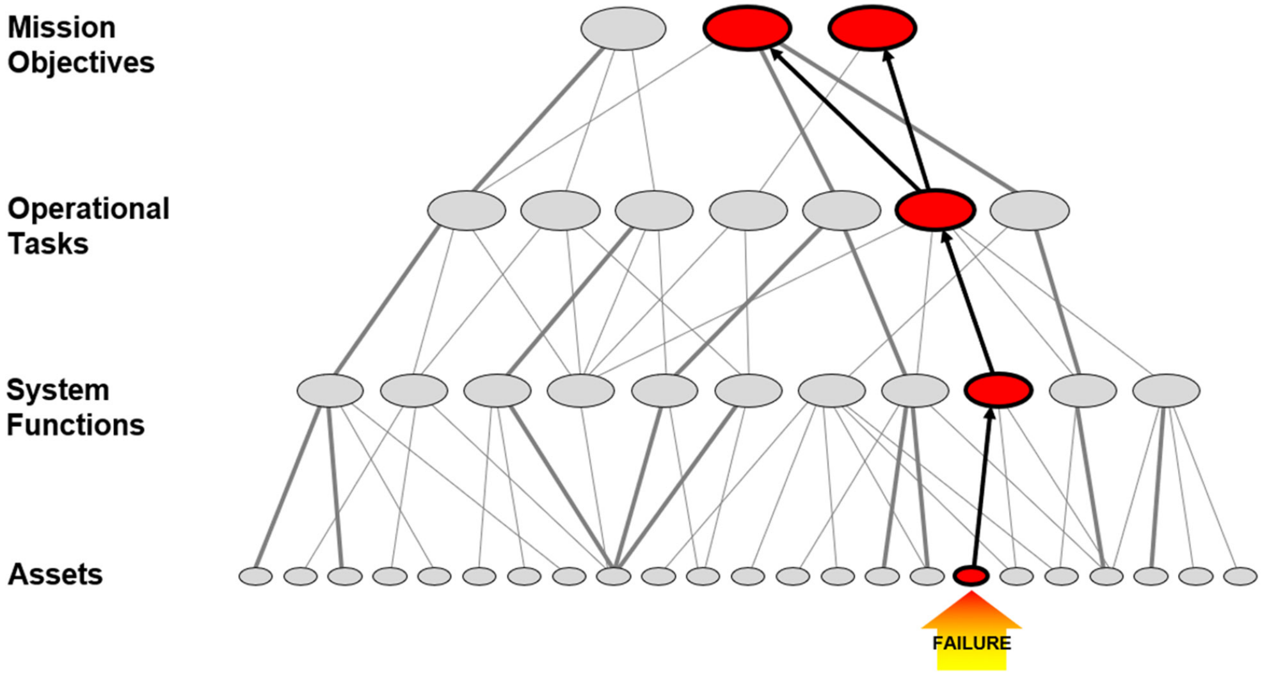


FIGURE 7. EXAMPLE IMPACT ON MISSION OF A CROWN JEWEL FAILURE

Figure 8 below illustrates how in a mission architecture containing a high level of dependency, failure of a single asset can severely impact a mission

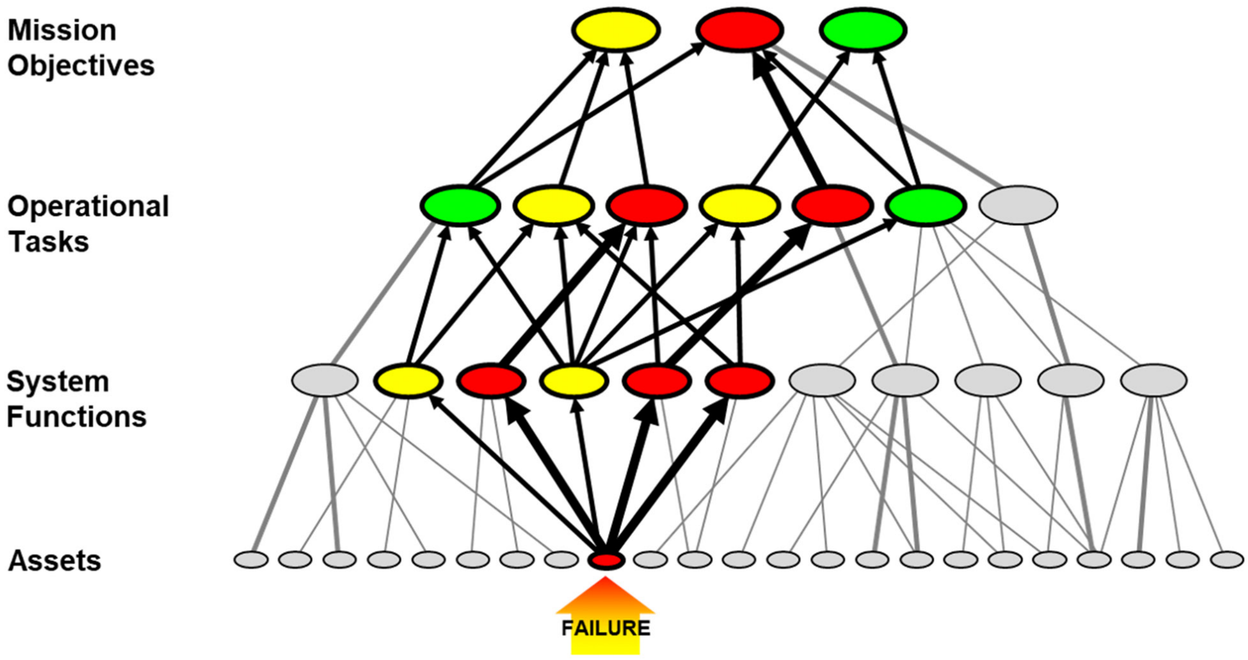


FIGURE 8. GREATER DEPENDENCY RESULTS IN GREATER IMPACT FROM ASSET FAILURE

Figure 9 below is a notional representation of dependencies for a mission of providing electrical power and services to a customer. In this example, if the OT/IT gateway were to fail, OT/IT connectivity would not be available. This failure would impact the ability to monitor the distribution of electricity, which could degrade the ability to provide electrical power safely.

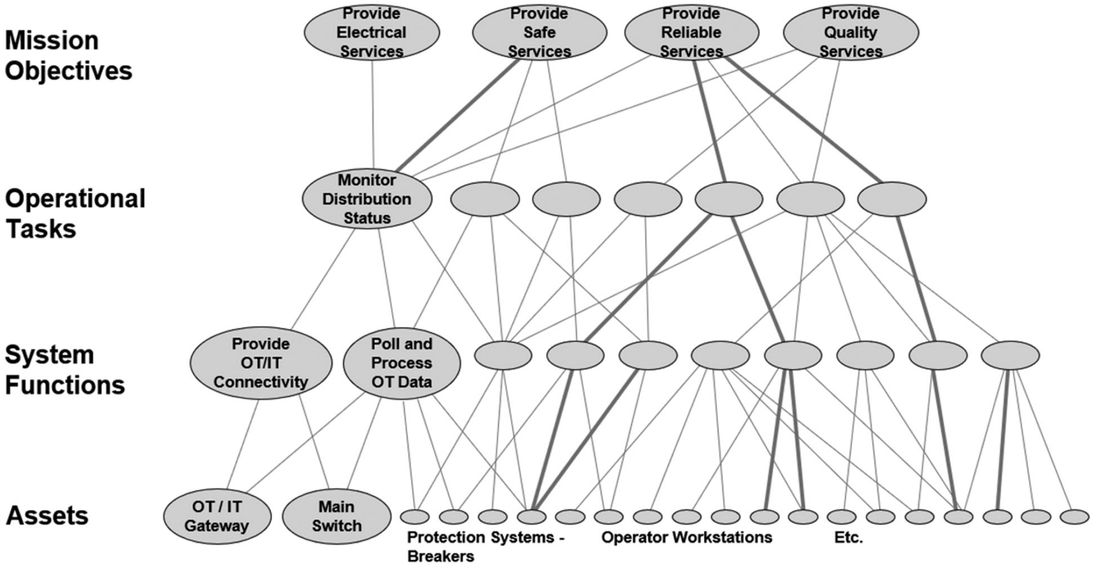


FIGURE 9. DEPENDENCY EXAMPLE FOR ELECTRICAL POWER DISTRIBUTION

Figure 10 below is a notional representation of dependencies for a mission of cooling essential mission assets. In this example, if operator workstations were to fail, control devices could become unmanageable, which would impact the ability to control cooling locally, which could degrade the ability to cool essential missio

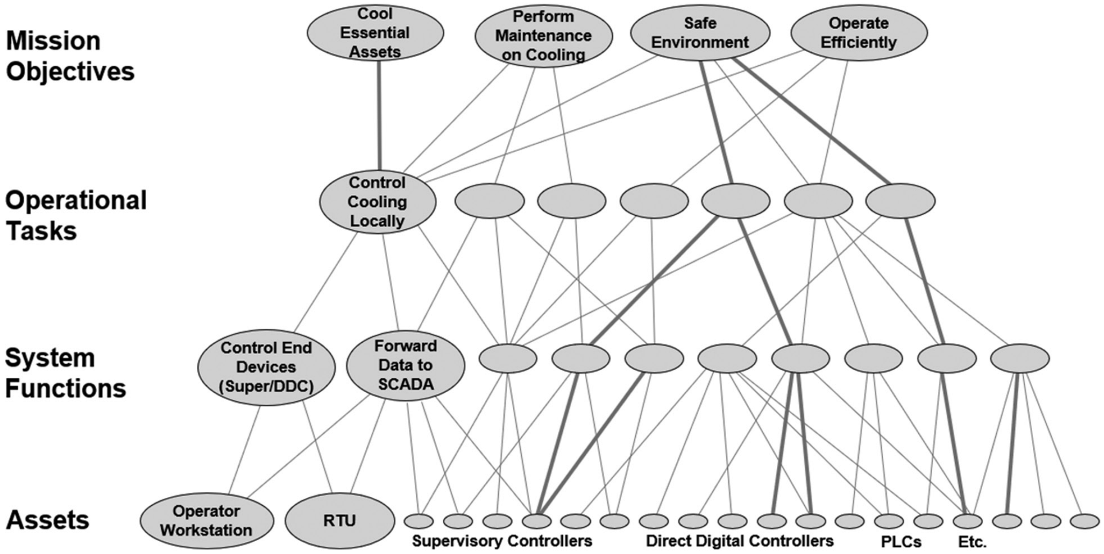


FIGURE 10. DEPENDENCY EXAMPLE FOR BUILDING AUTOMATION CONTROL SYSTEM

Conclusion

Crown Jewels Analysis (CJA) is used to identify where to focus device/asset level security assessments in environments where the number of devices/assets are too numerous to assess. Assets revealed to be crown jewels can then be made the initial focus of device/asset level security audits. Serving as input to threat susceptibility assessments, crown jewels can play a role in assessing both cyber and physical threats to the system. Other benefits gained through performance of CJA include:

- **Shows where to emphasize operator training**—Mission critical systems likely support mission critical functions, or tasks, indicating where increased training for operators would provide mission assurance/ mission resiliency benefits.
- **Lays groundwork for developing survivability focused “Fight Through” TTPs for dealing with cyber-attacks on ICSs**—,CJA informs TTP development.
- **Shows where to design for robustness/redundancy**—Becoming aware of design weaknesses provides opportunity for improving robustness and redundancy for critical functions and systems.
- **Shows where to prioritize equipment updates**—Critical IT/OT devices often benefit from technology refreshes, which include improved capability, performance, and security.
- **Shows how to schedule or sequence software updates or enhancements**—Software modules developed by contractors can be prioritized based on need factors for mission-critical assets.

Crown Jewels Analysis is a methodical, logical, and transparent approach to discovering mission components critical to mission success.

Acronyms

AHP	Analytic Hierarchy Process
CIKR	Critical Infrastructure Key Resources
CJA	Crown Jewels Analysis
DCS	Distributed Control System
DDC	Direct Digital Controller
DoD	Department of Defense
FMEA	Failure Modes and Effects Analysis
HVAC	Heating Ventilation and Air Conditioning
ICS	Industrial Control System
IT	Information Technology
MIA	Mission Impact Analysis
NTP	Network Time Protocol
OT	Operational Technology
PLC	Programmable Logic Controller
QFD	Quality Function Deployment
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SME	Subject Matter Expert
STP	Spanning Tree Protocol
TTP	Tactics Techniques and Procedures
VPN	Virtual Private Network

References

1. Watters, Chalton J. (Jim), Morrissey, Shaun P., ScD, Crown Jewels Analysis (CJA) Process. MITRE Technical Report MTR180005, November 2018
2. Defense Acquisition Guidebook Chapter 9 – Program Protection, CH 9–3.1.3.1 Criticality Analysis. URL: https://www.dau.edu/pdfviewer?Guidebooks/DAG/DAG-CH-9-Program-Protection.pdf
3. Kertzner, P. Watters, J., Bodeau, D., Hahn, A., Process Control System Security Technical Risk Assessment Methodology & Technical Implementation, Institute for Information Infrastructure Protection (I3P) Research Report No. 13, March 2008.
4. Young, Celeste, et al., Risk Ownership Framework for Emergency Management Policy and Practice. Bushfire and Natural Hazards CRC. Melbourne, Australia (2017). URL: https://www.vu.edu.au/sites/default/files/risk-ownership-framework-for-emergency-management-policy-and-practice.pdf

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

The views, opinions, and/or findings contained herein are those of the author(s) and should not be construed as an official government position, policy, or decision unless designated by other documentation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®