Crown Jewels Analysis (CJA)

A Mission Criticality Analysis Technique Using Dependency Maps

A Presentation and Demonstration for Boston SPIN

20 February 2018

Jim Watters

Approved for Public Release: Cases 08-0490, 11-2827, 14-1906, 16-0777
© 2018 The MITRE Corporation. All rights reserved

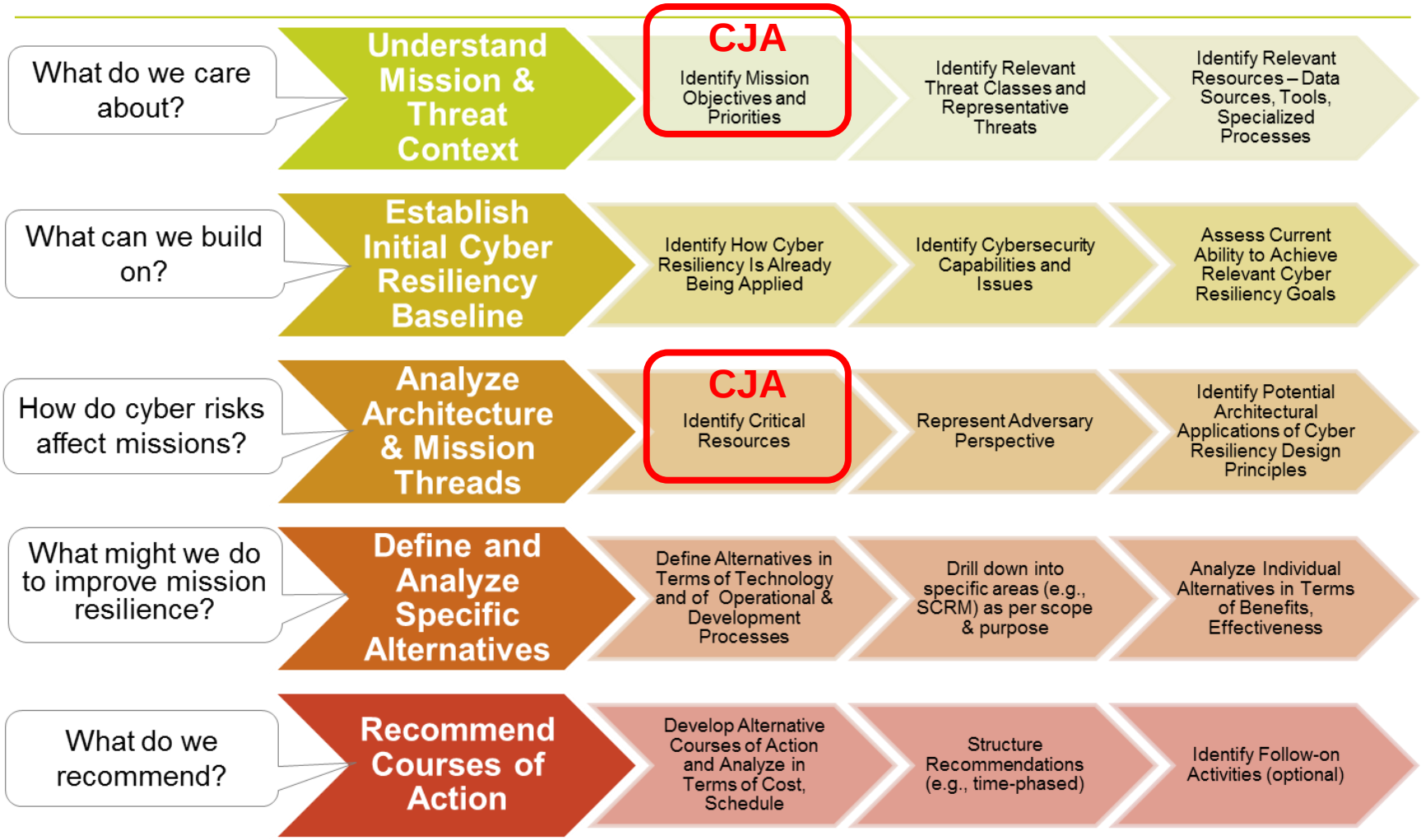
MITRE

Background

- Advanced Persistent Threats (APT) use sophisticated capabilities to attack, and maintain a presence in, our mission systems
- As a result, it is not realistic to use a defensive strategy based on stopping all threats at the boundary
- Instead, we must assume that the APT can penetrate, deny, and/or degrade our Cyber Assets (CA)
- A defensive strategy based on that assumption is to harden mission-critical CA so we can operate through an APT attack
- Cyber resiliency techniques help us identify the mission-critical CA, evaluate the risks facing those CA, and develop mitigation strategies

Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

CJA As a Cyber Resiliency Technique



Ref: Structured Cyber Resiliency Analysis Methodology (SCRAM), by D. Bodeau and R. Graubart

Approved for Public Release: Case 16-0777
© 2018 The MITRE Corporation. All rights reserved

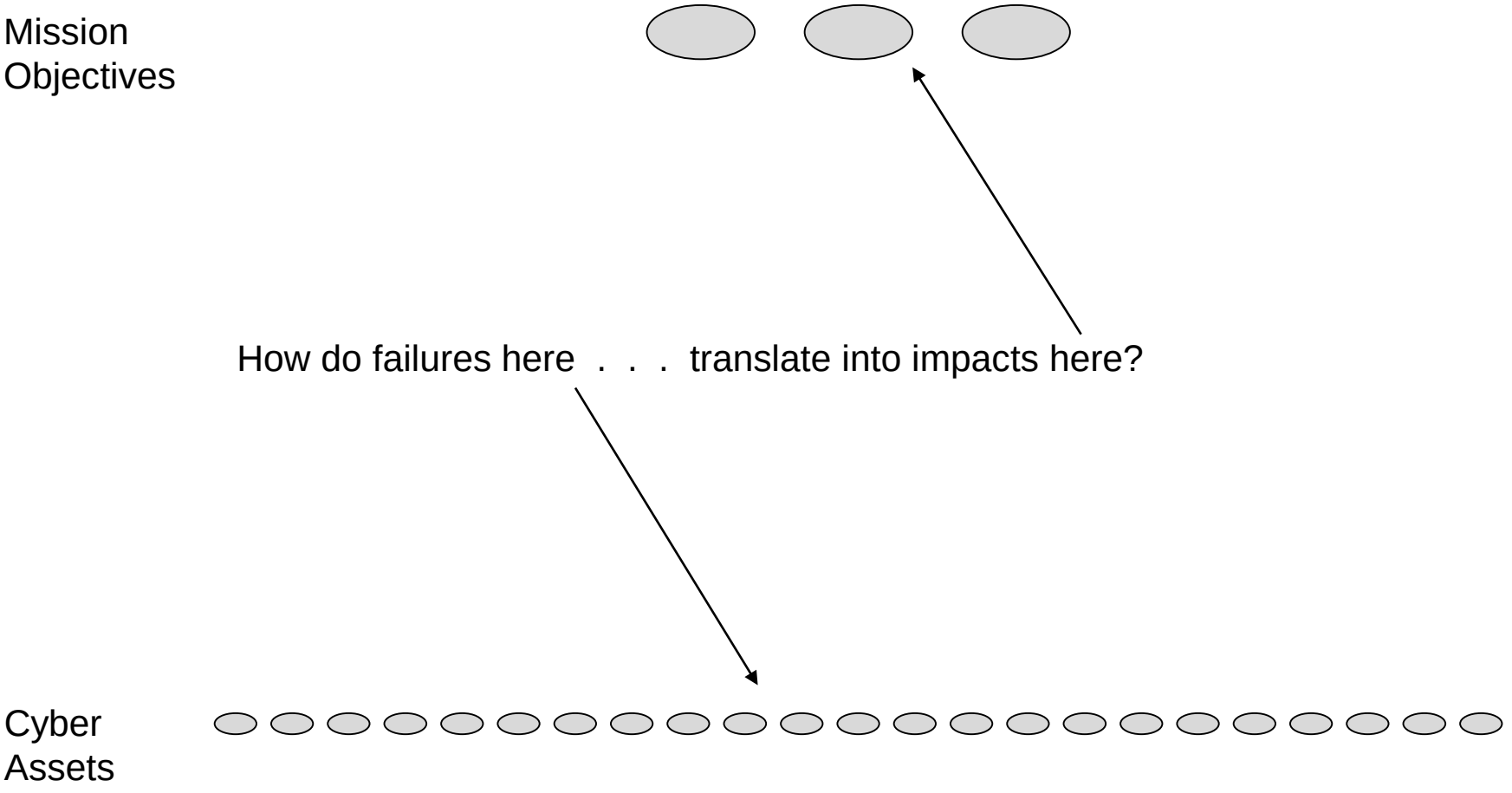
MITRE

What is CJA?

- **MITRE-developed Mission Criticality Analysis technique**
  - *First used during Operations Without Space deep-dive at 613th Air and Space Operations Center (AOC) in 2009*
- **CJA's Dependency Map approach combines expert input with established techniques:** *AHP, QFD, and FMEA*
- **Definitions when applied to Cyber/IT systems**
  - *"Cyber Asset" = A logic-bearing device including its hardware, firmware, software, and initialization/configuration data*
    - *We have also included non-logic bearing devices; e.g. comm links*
  - *"Mission-Critical Cyber Asset" = A Cyber Asset whose failure or degradation causes mission failure; a "Crown Jewel"*

Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

CJA Helps Us Answer a Key Question

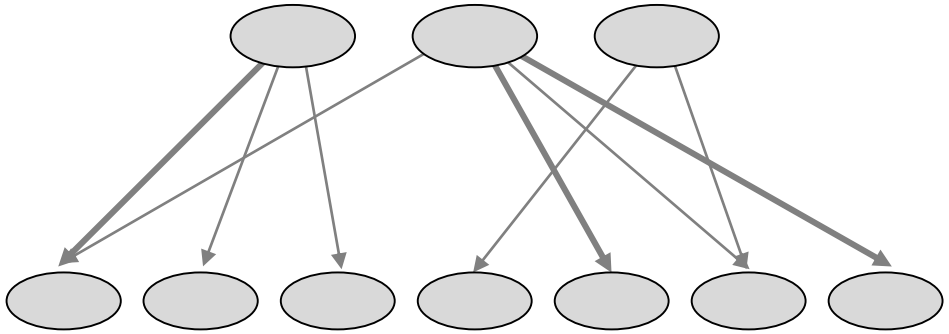


Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

We Start by Identifying the Tasks That Support Each Mission Objective

Mission Objectives

Operational Tasks

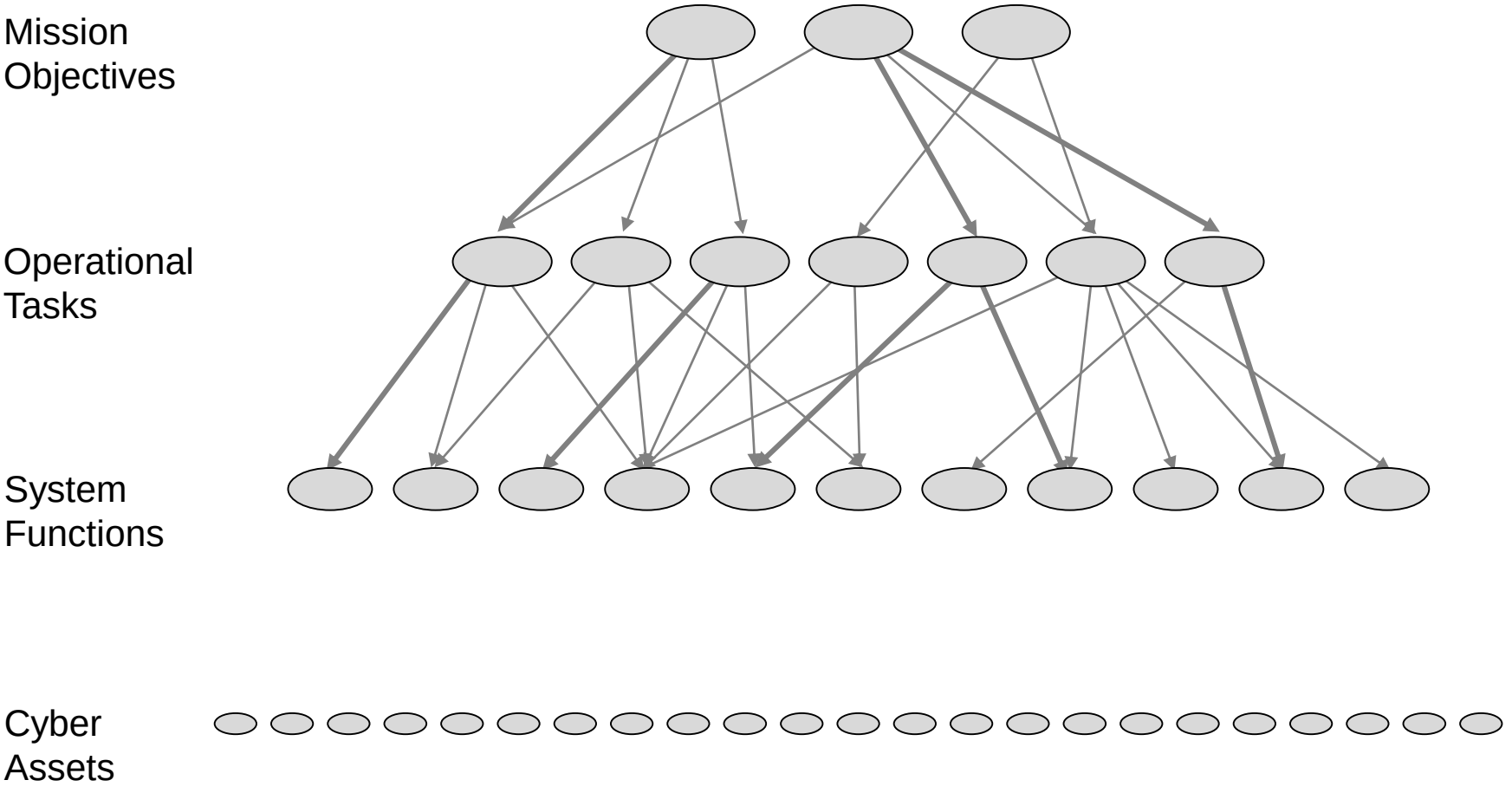


Cyber Assets

Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

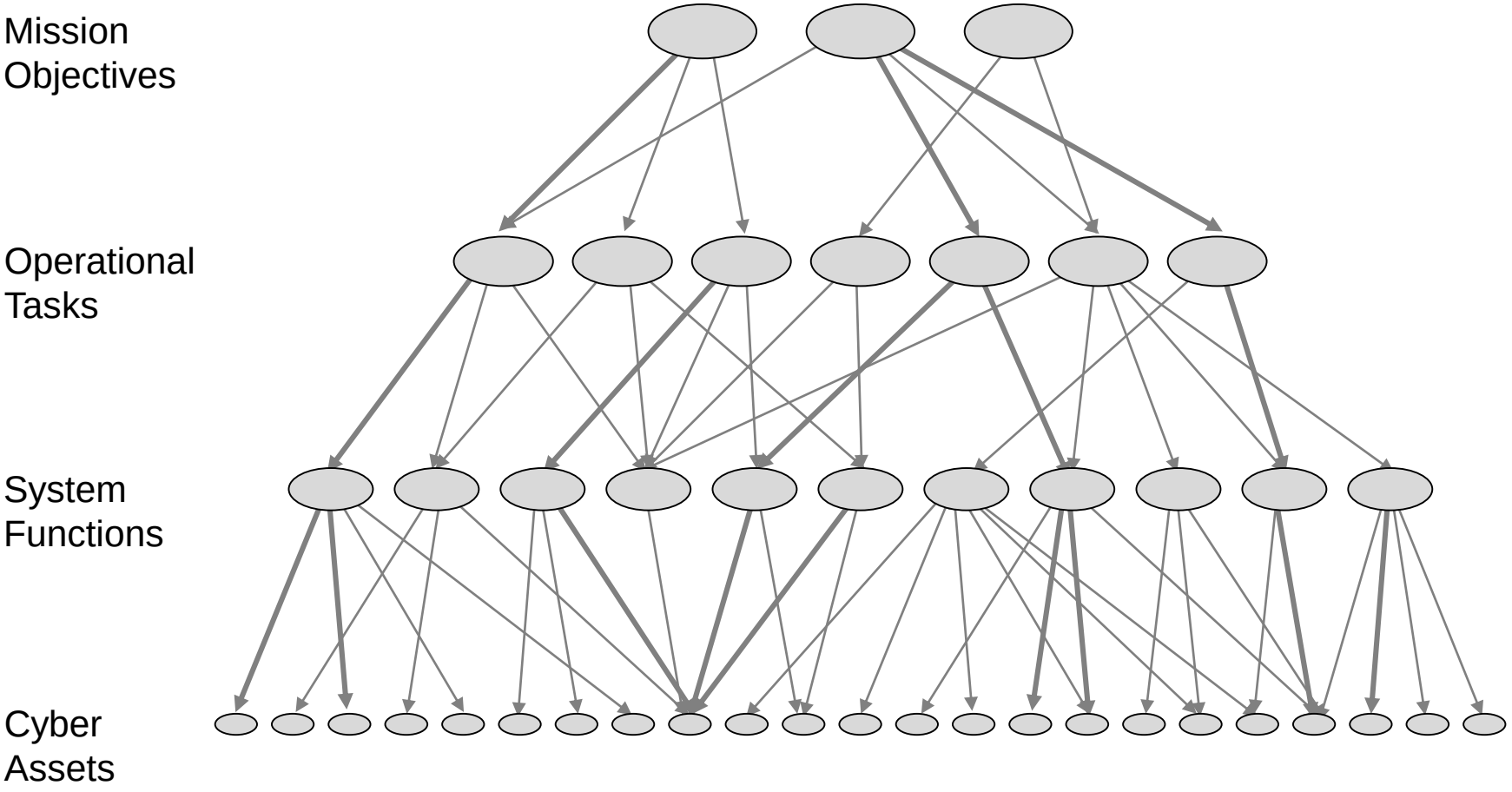
MITRE

Next, We Identify the System Functions That Support Each Task



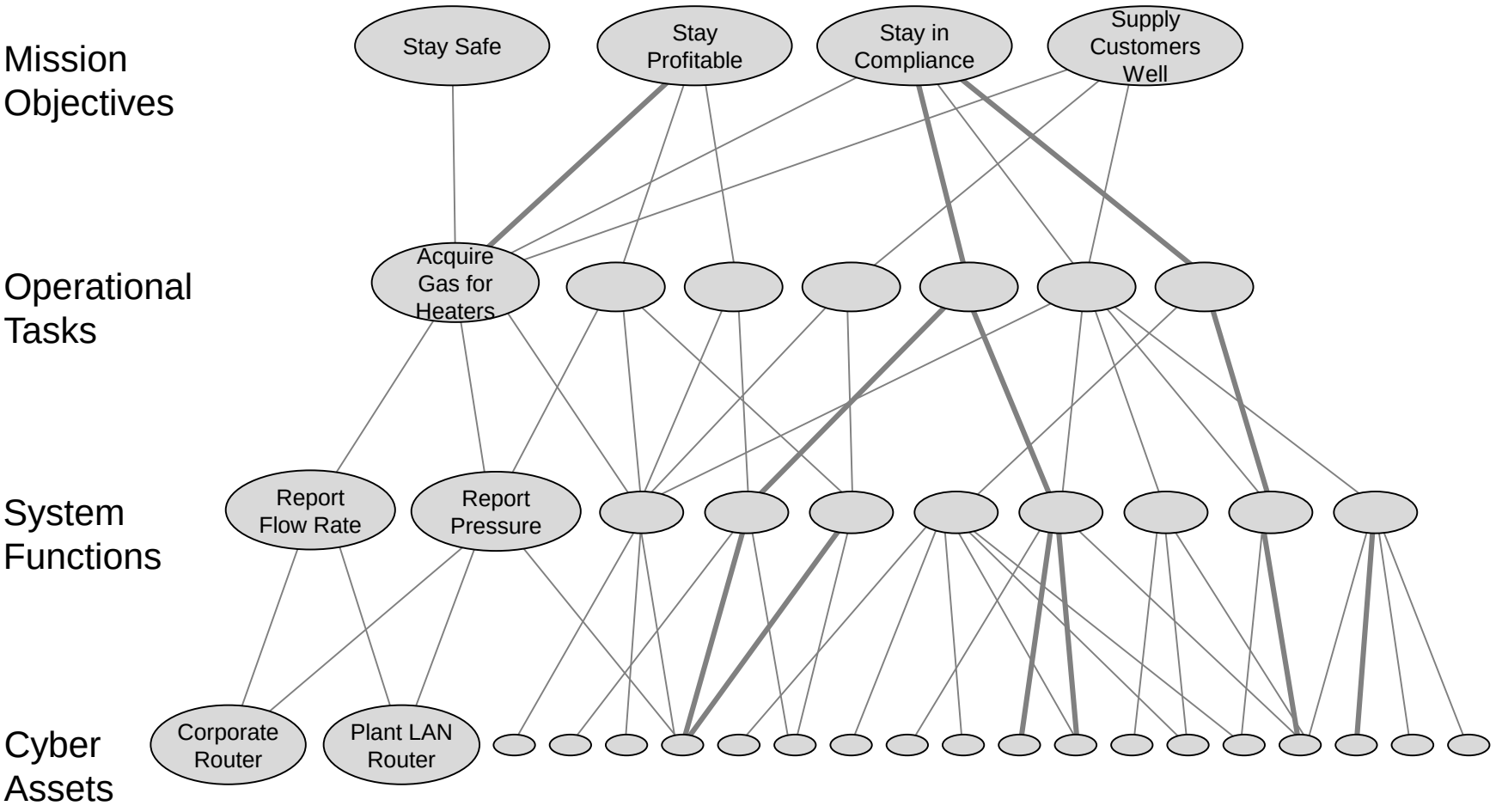
Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

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



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

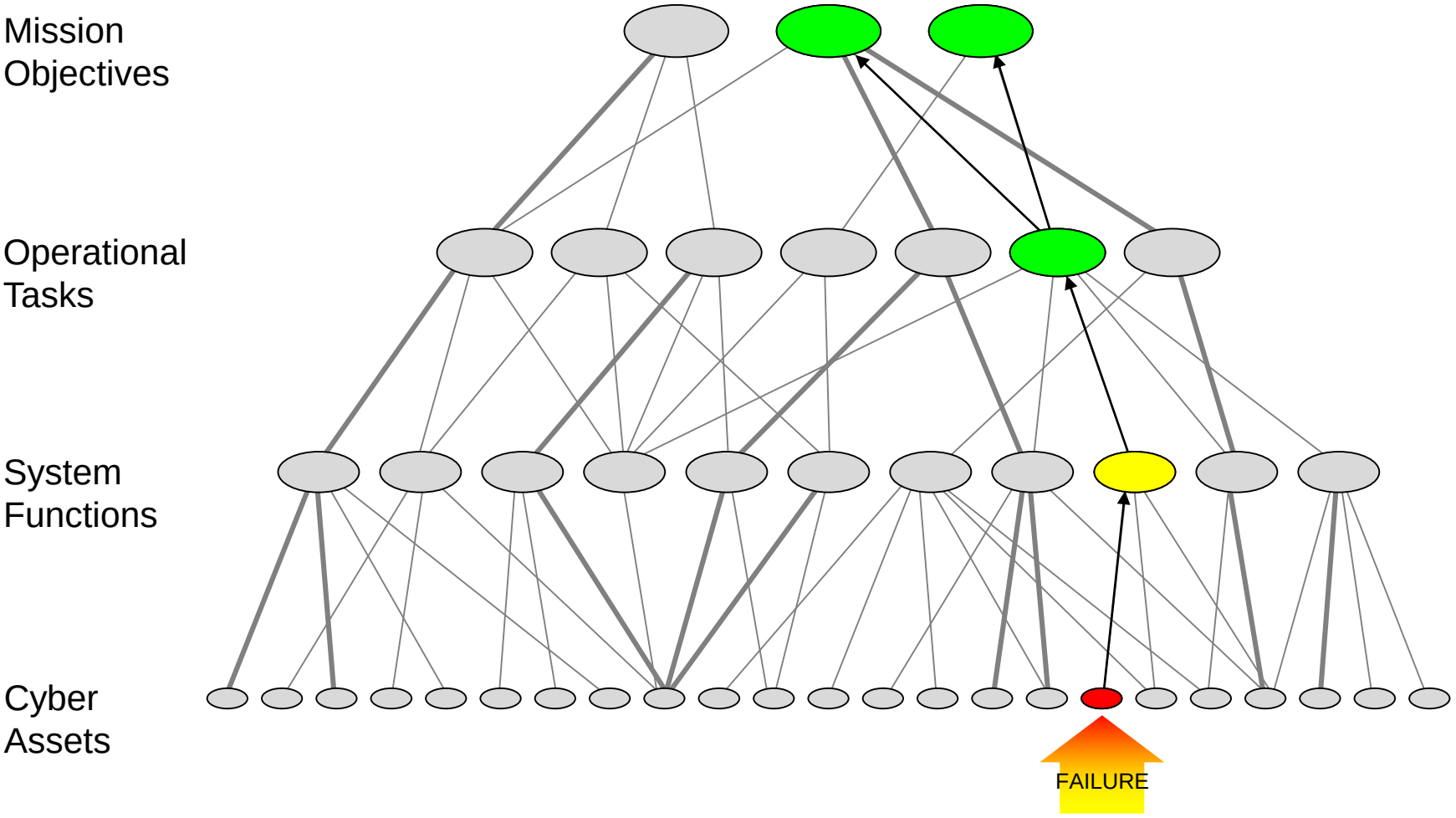
Dependency Mapping - Refinery Example



Approved for Public Release: Case 08-0490
© 2018 The MITRE Corporation. All rights reserved

MITRE

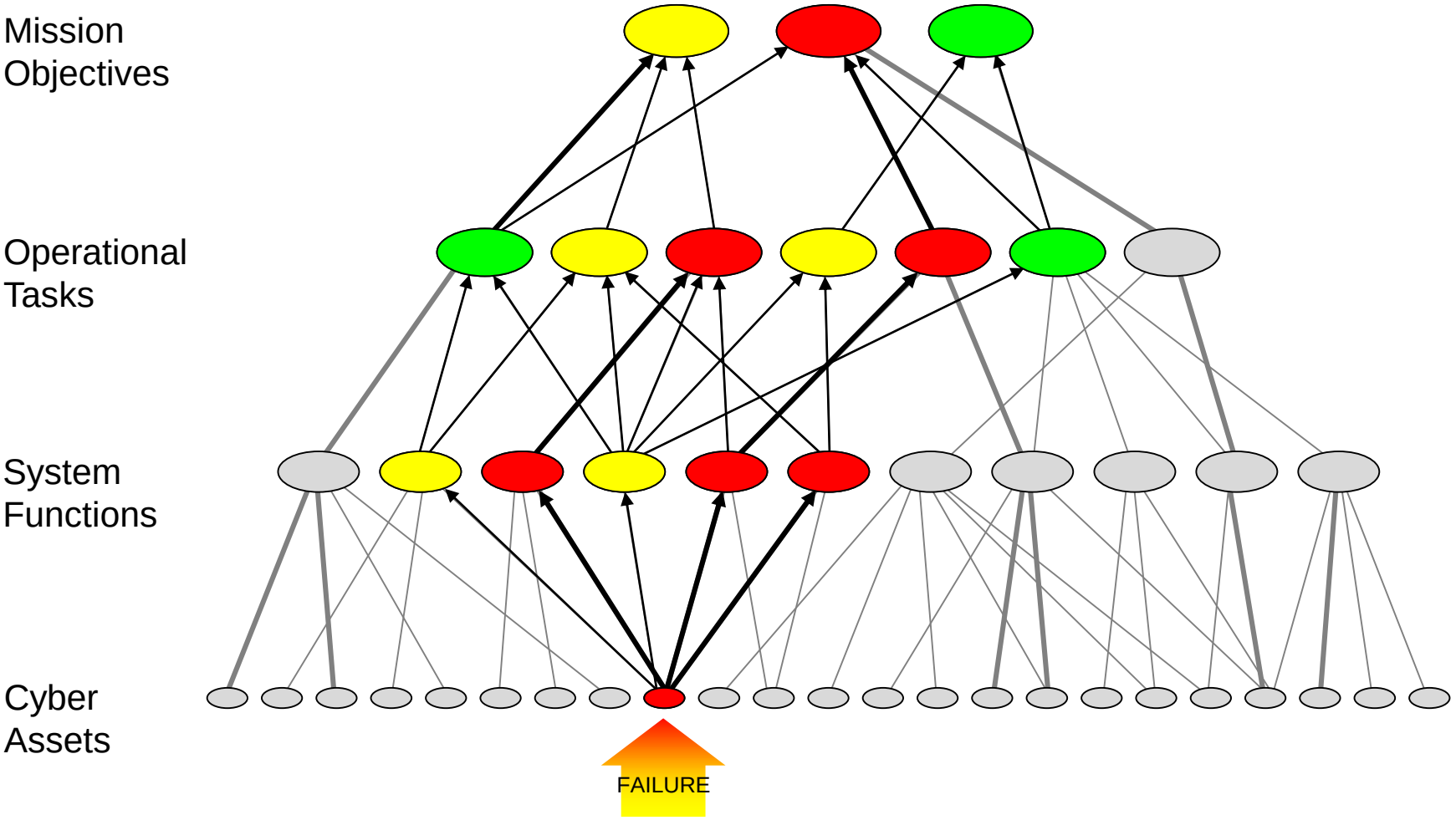
We Use the Dependencies to Predict the Impact of Cyber Asset Failures



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

Greater Dependency Means Greater Impact from Cyber Asset Failure



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

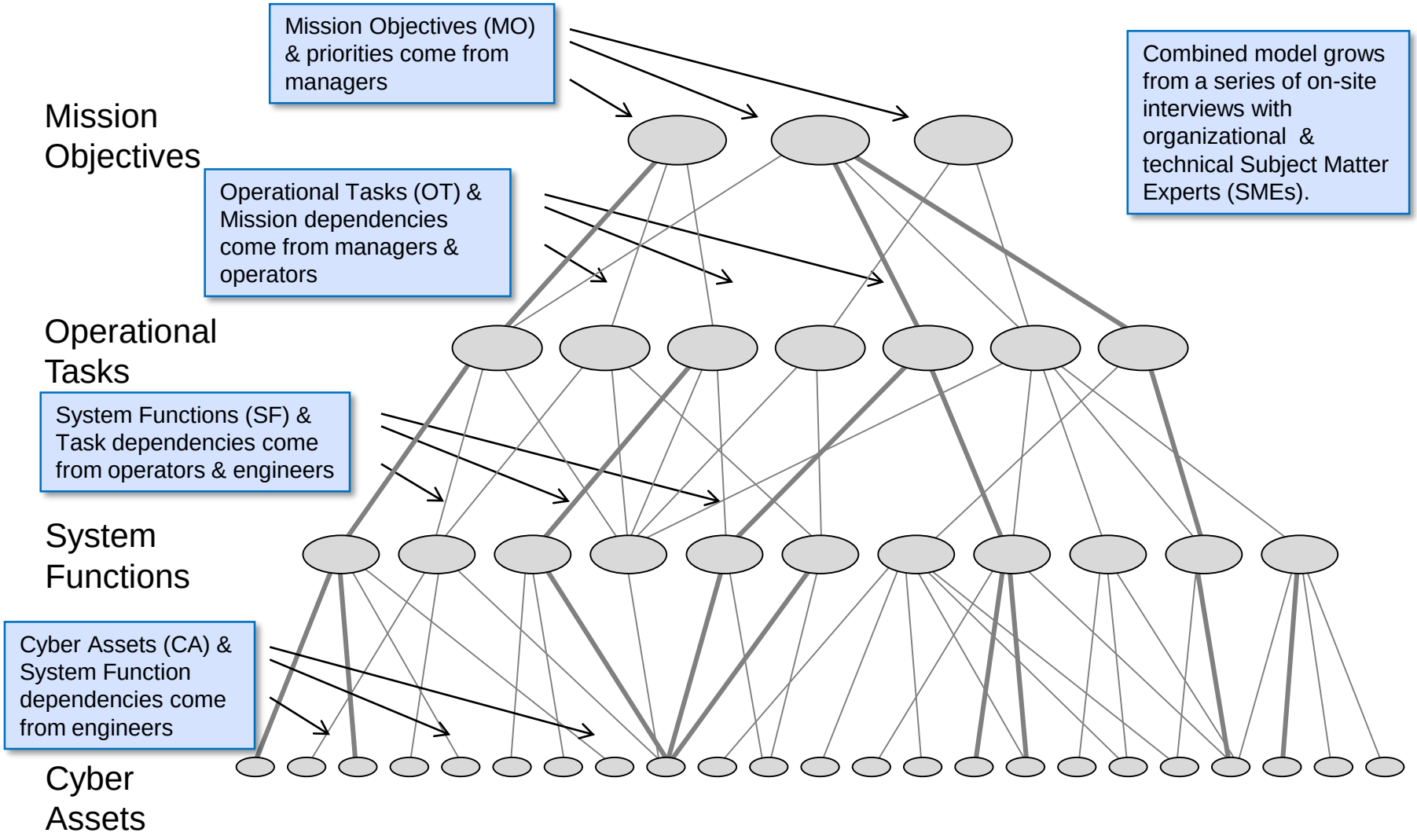
How Do We Evaluate a Dependency?

- **For our purposes, a dependency is a need**
  - *Achieving a Mission Objective depends on one or more Tasks being performed as intended*
  - *Performance of a Task depends on one or more System Functions executing as intended*
  - *Execution of a System Function depends on one or more Cyber Assets operating as intended*

- **We express the degree of dependency in terms of criticality**
  - *Criticality describes the impact of loss of an asset, based on the effect the loss would have on operations and the ability to fulfill the mission*
  - *We define four levels of impact: Failure, degradation, a work-around is required, and none*

Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

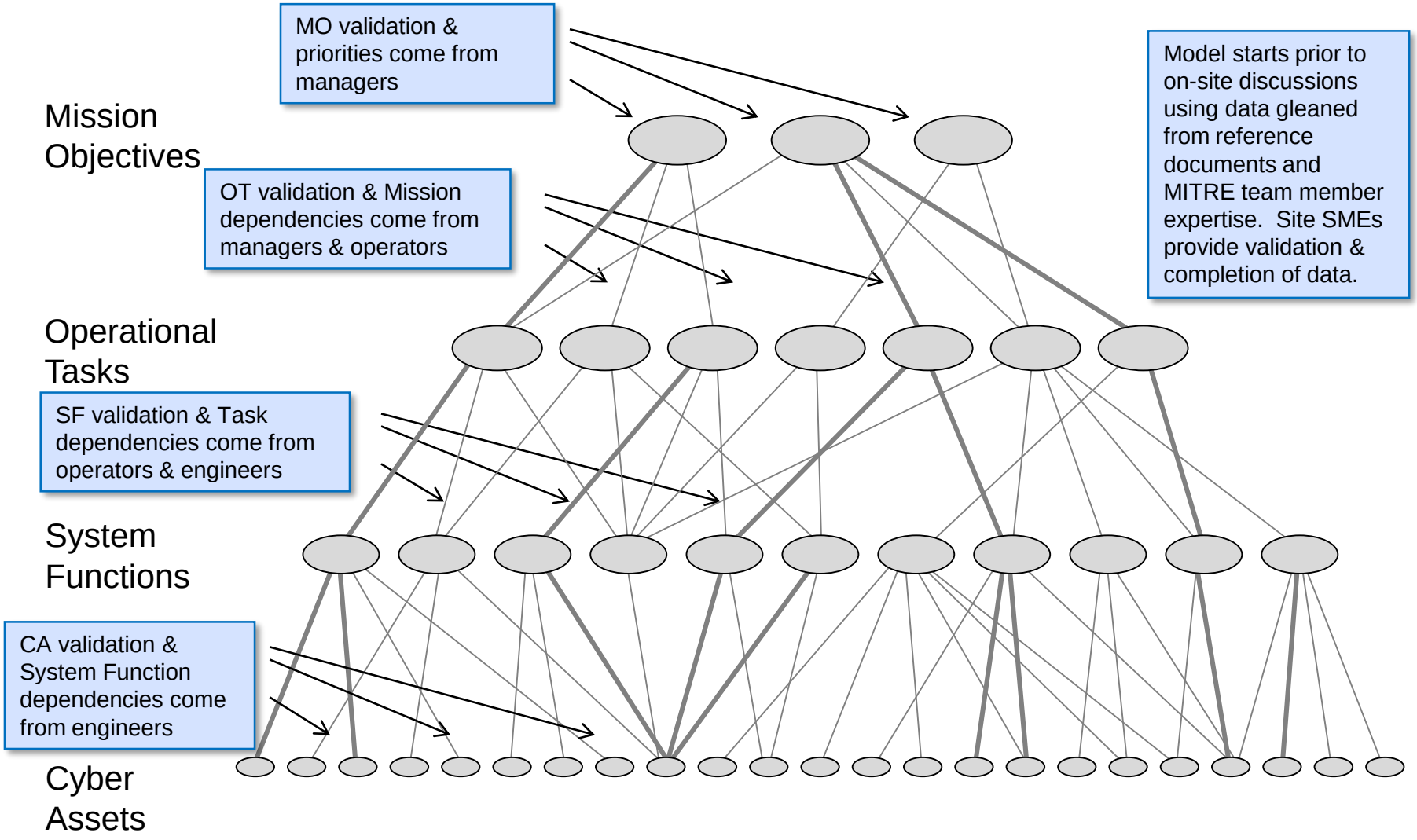
Where Does the Information Come From? (Option 1)



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

Where Does the Information Come From? (Option 2)



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

How Do We Limit Subjectivity?

1. **We use structured question-and-answer sessions with the operational and technical experts on the system**

   a. *Managers/Operators: What is the impact on Mission Objective "MO1" if Task "T1" is not performed as intended?*

      – *No impact? Work-Around Required? Degradation? Failure?*

   b. *Operators/Engineers: What is the impact on Task "T1" if System Function "SF1" does not execute as intended?*

      – *No impact? Work-Around Required? Degradation? Failure?*

   c. *Engineers/Administrators: What is the impact on System Function "SF1" if Cyber Asset "CA1" is not operating as intended?*

      – *No impact? Work-Around Required? Degradation? Failure?*

2. **Scoring tables provide a reference, to ensure consistency**

   – *We define "as intended" to mean no failures and no degradation*

Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

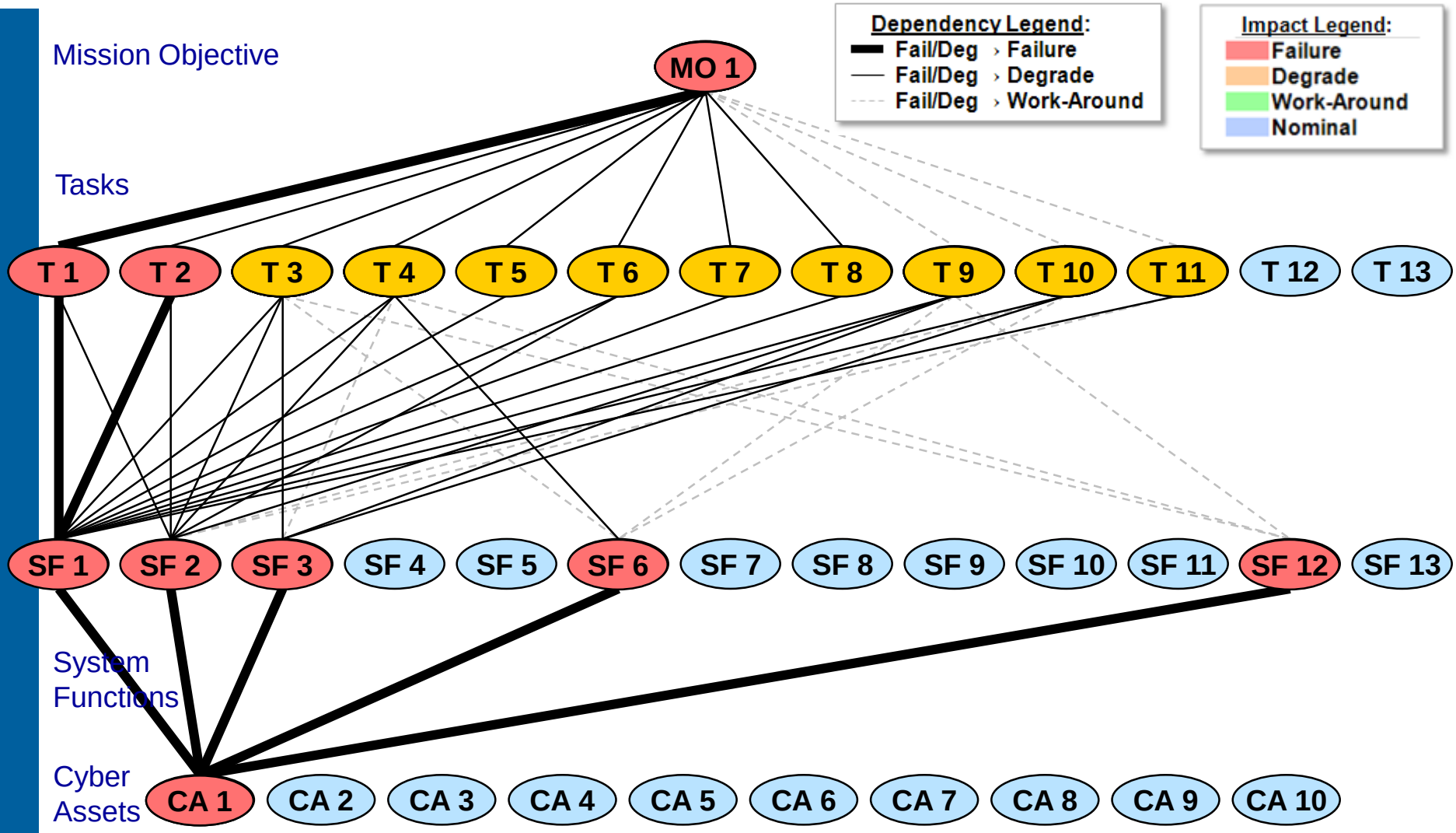
MITRE

How Do We Identify the Mission-Critical Cyber Assets?

1. **From the dependency identification, we know the following:**
   a. *If Task "T1" fails, the impact on achieving Mission Objective "MO1" is one of the following:*
      - *No impact, work-around required, mission degradation, or mission failure*
   b. *If System Function "SF1" fails, the impact on performing Task "T1" is one of the following:*
      - *No impact, work-around required, task degradation, or task failure*
   c. *If Cyber Asset "CA1" fails, the impact on the performance of System Function "SF1" is one of the following:*
      - *No impact, work-around required, function degradation, or function failure*
2. **We can use these "if-then" statements to predict the impact at each level in the dependency map**
   – *We call this step in the CJA the Mission Impact Analysis (MIA)*

Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

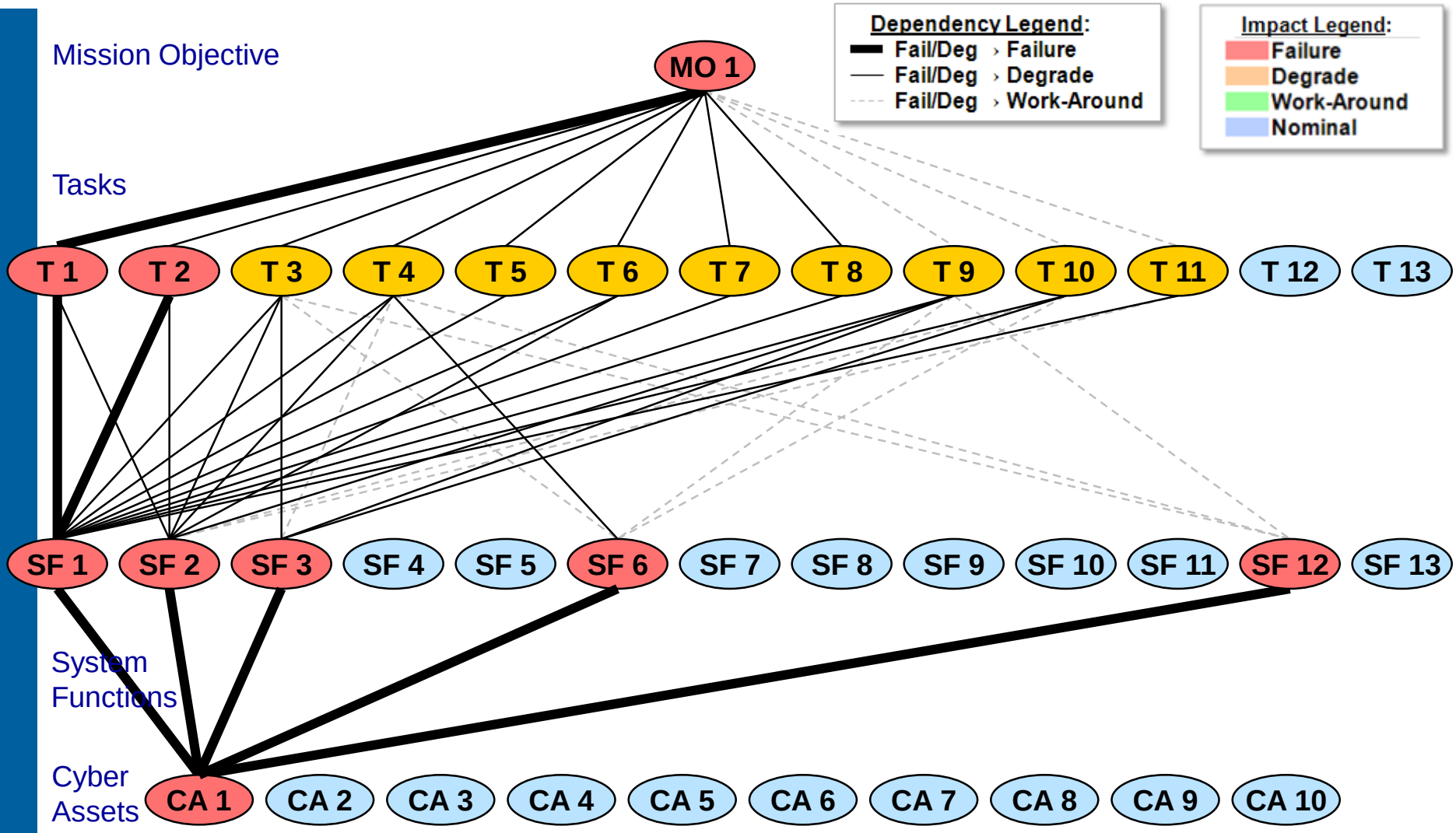
In the MIA We Consider Each CA As Failed, Starting with CA1



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

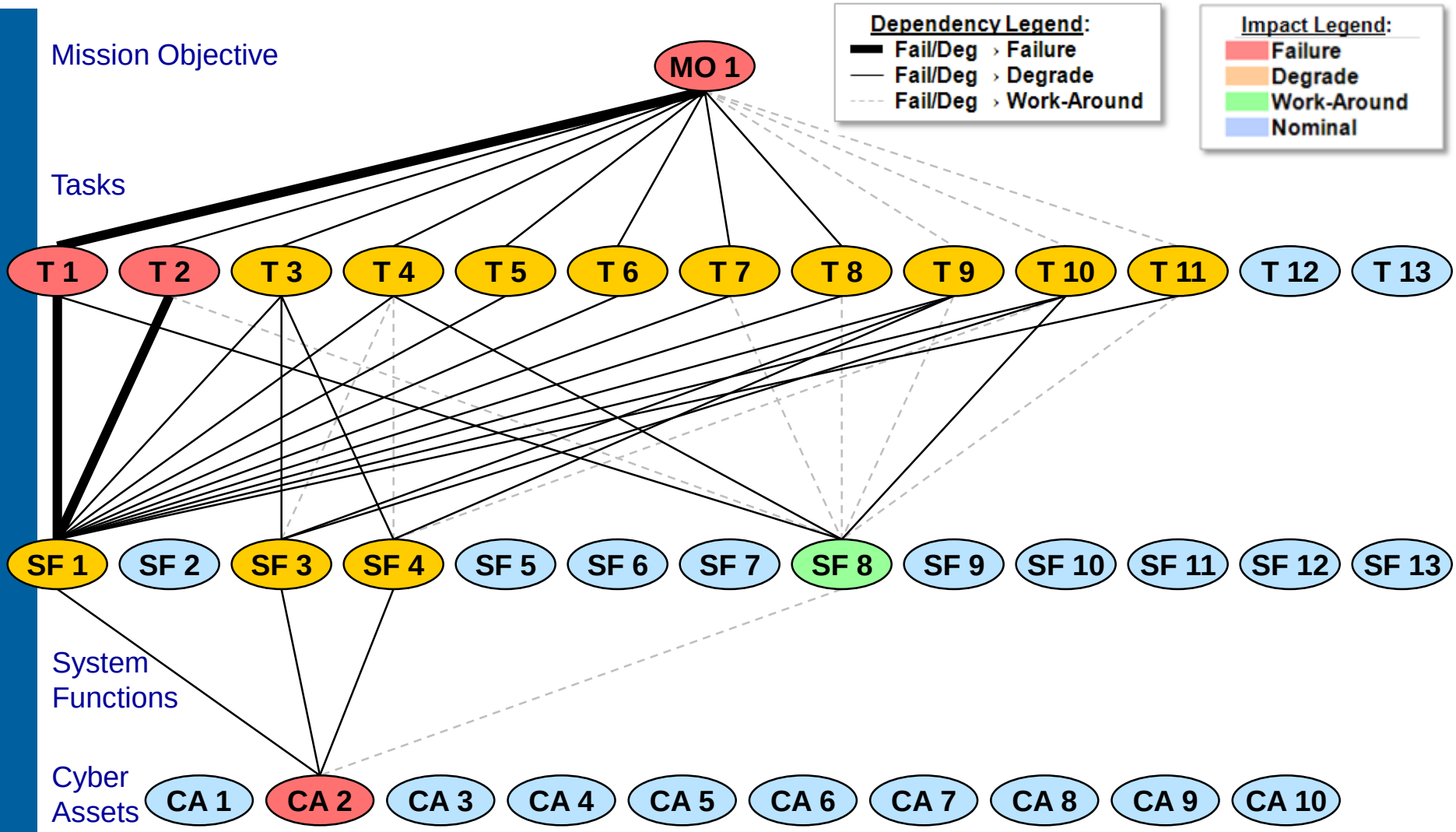
CA1's Failure Causes Several SF and Tasks to Fail, Causing MO1 Failure



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

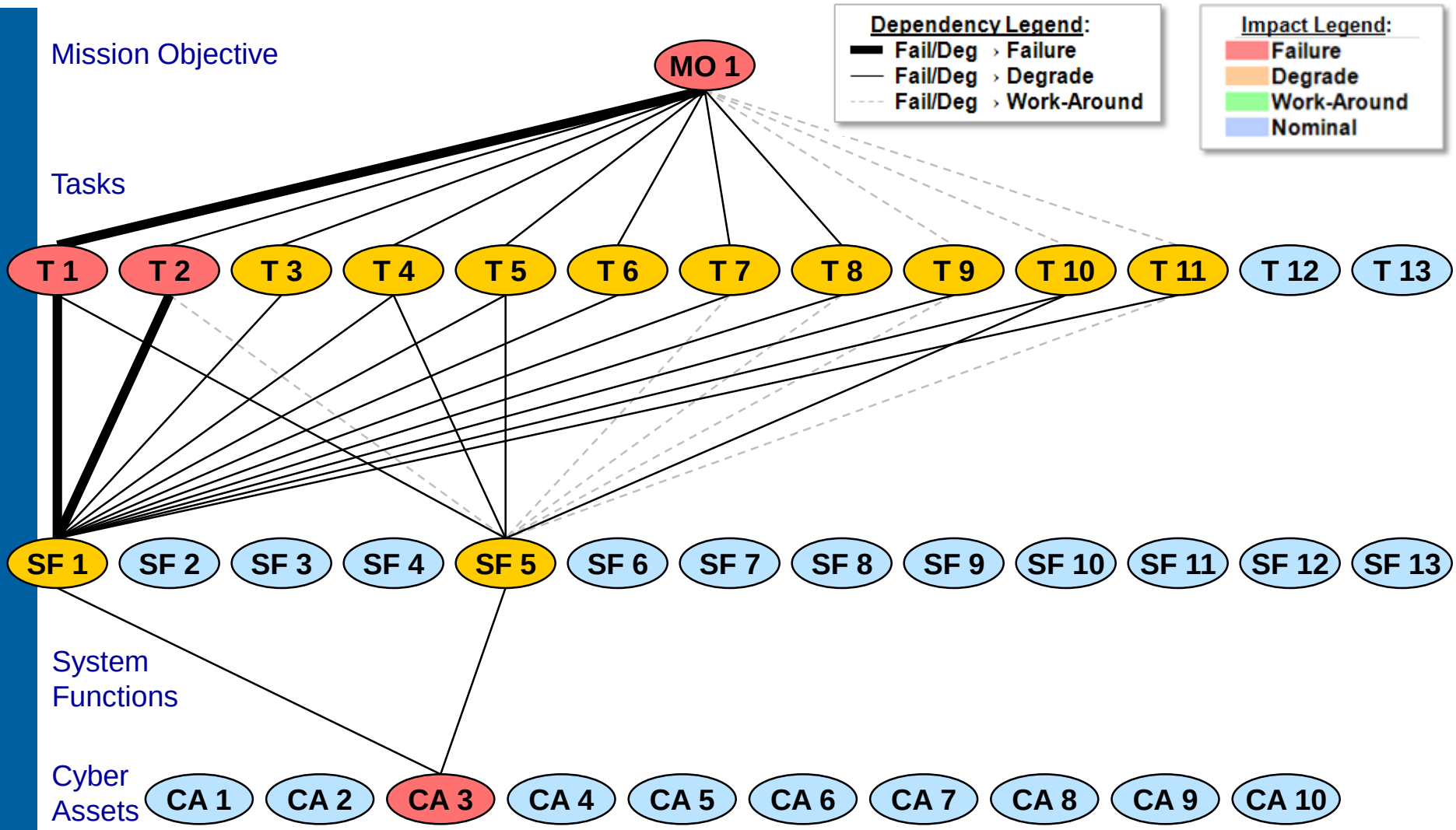
CA2's Failure Degrades SF1, Causing Task T1 to Fail, Causing MO1 Failure



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

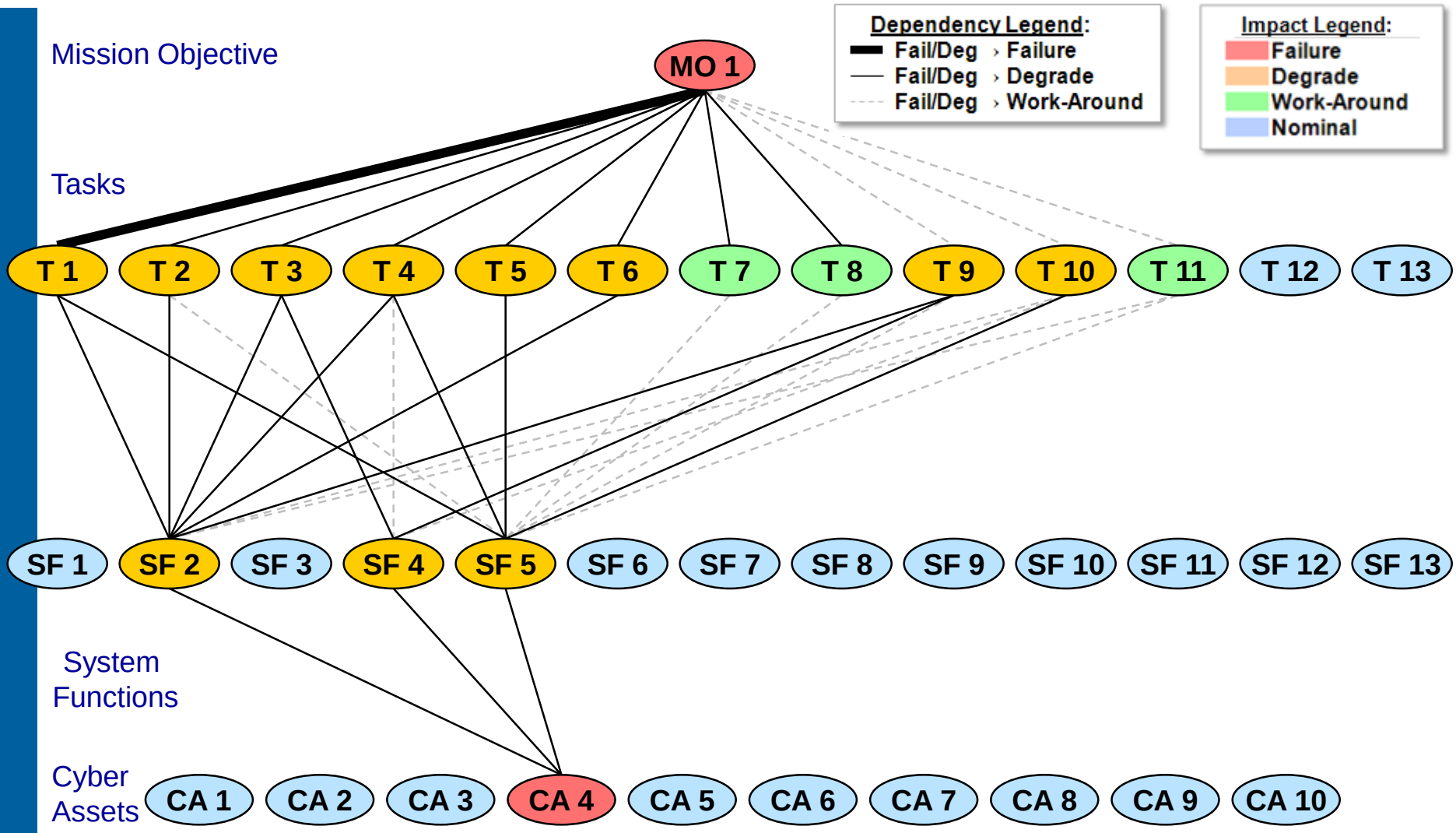
CA3's Failure Has an Effect Like That of CA2's Failure – Causing MO1 Failure



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

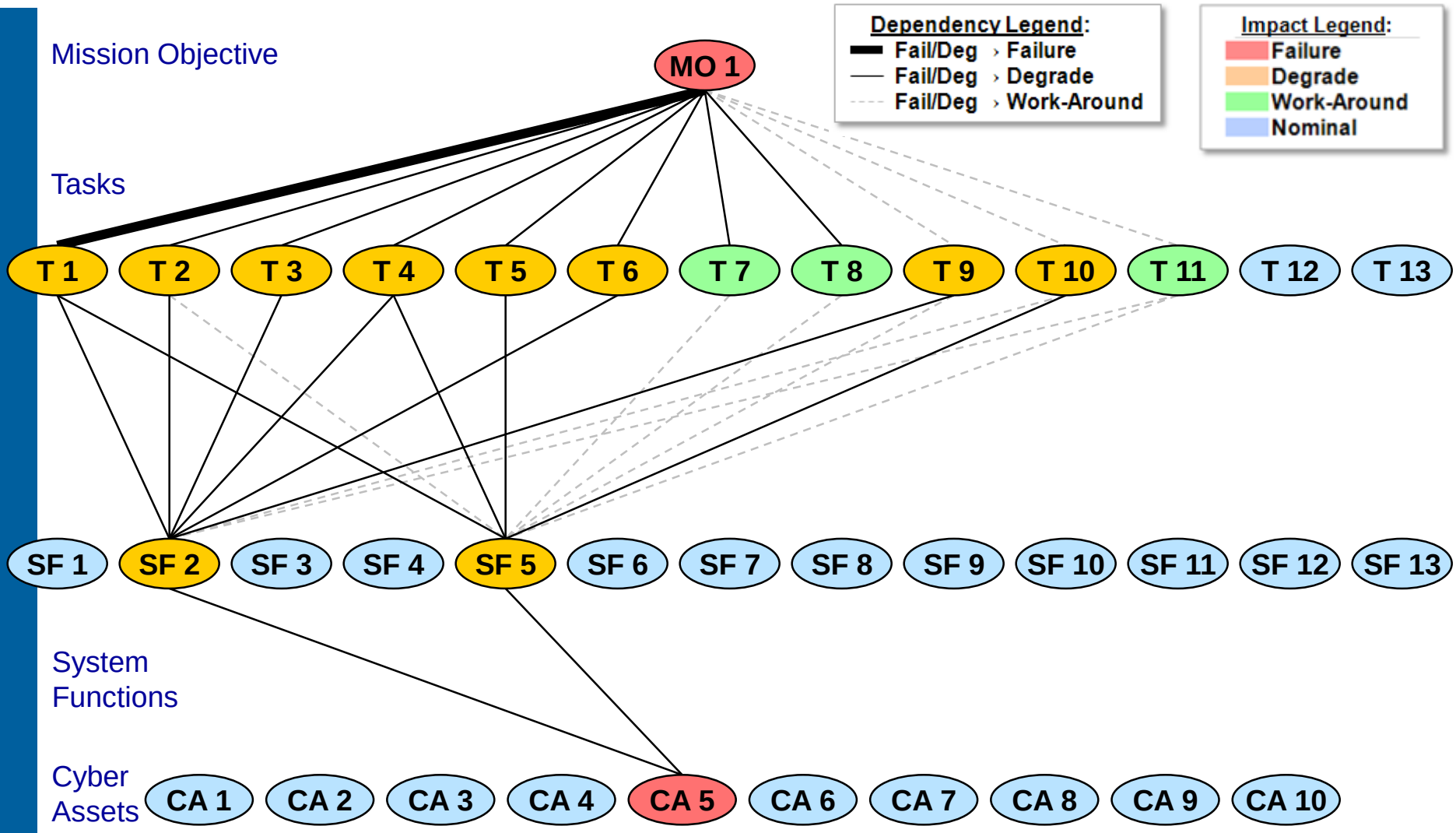
Because CA4's Failure Degrades SF2 and T1, It Causes MO1 Failure



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

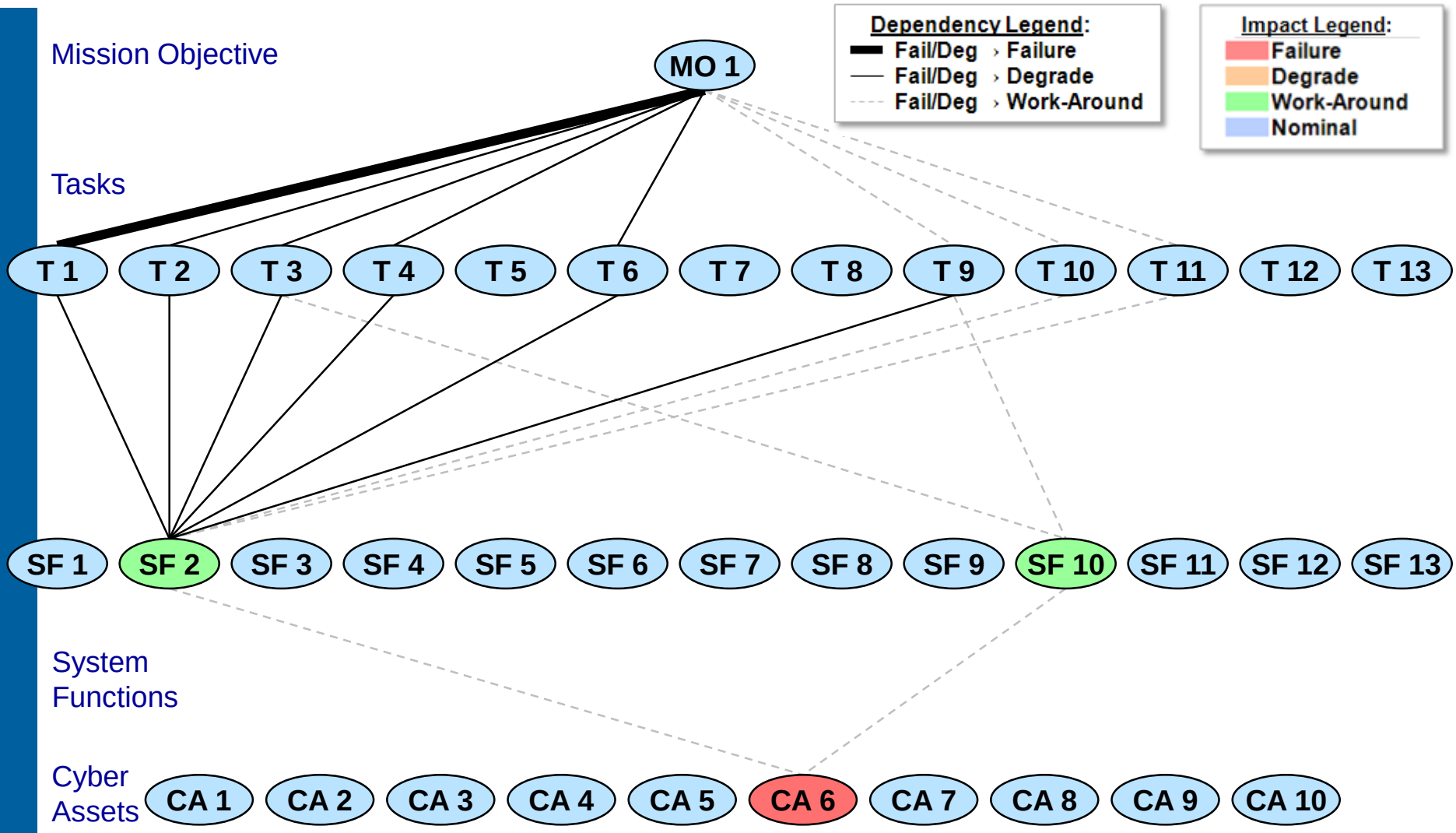
CA5's Failure Has an Effect Like That of CA4's Failure – Causing MO1 Failure



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

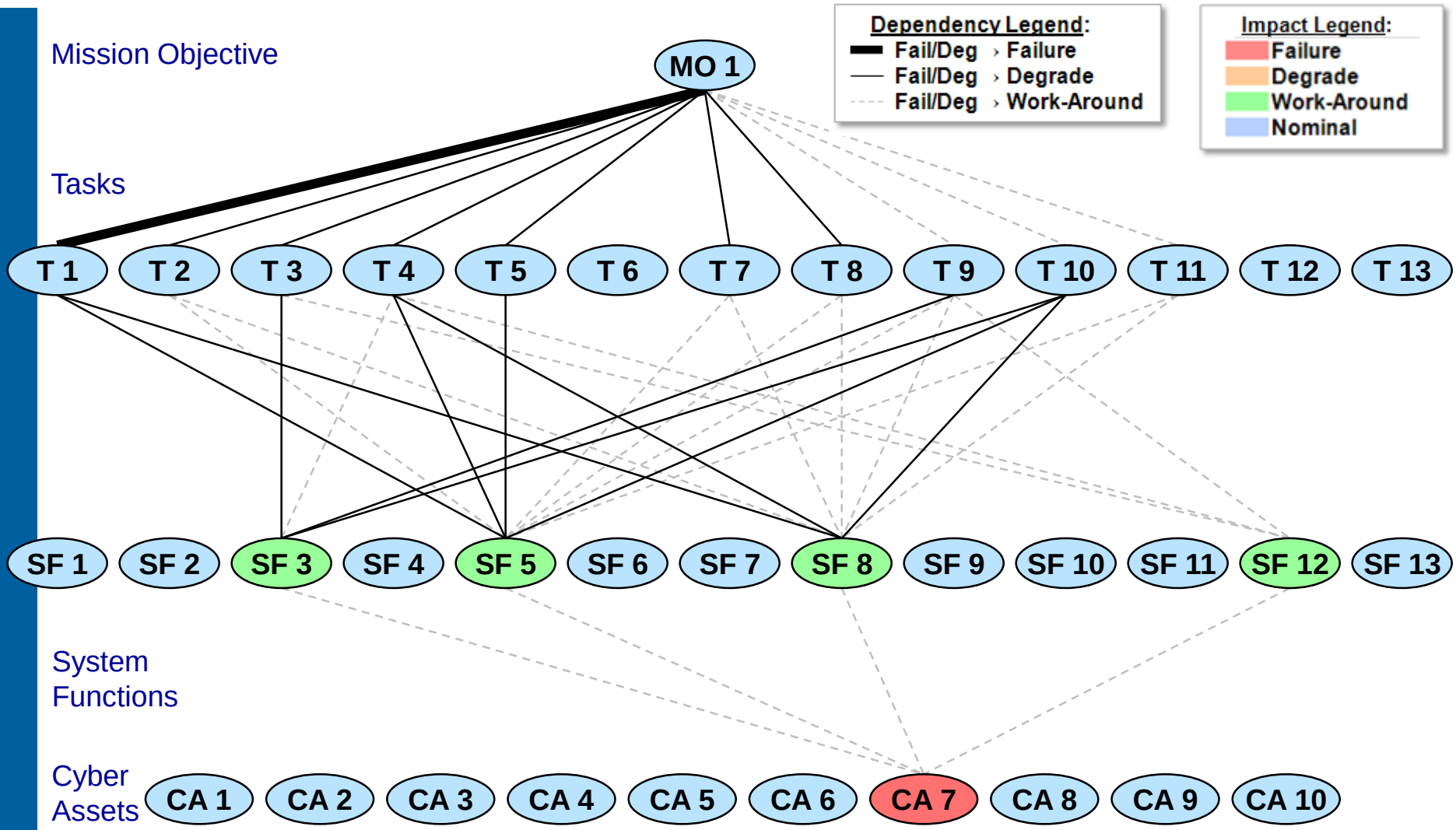
CA6's Failure Requires a Work-Around for SF2 and SF10 – No MO1 Impact



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

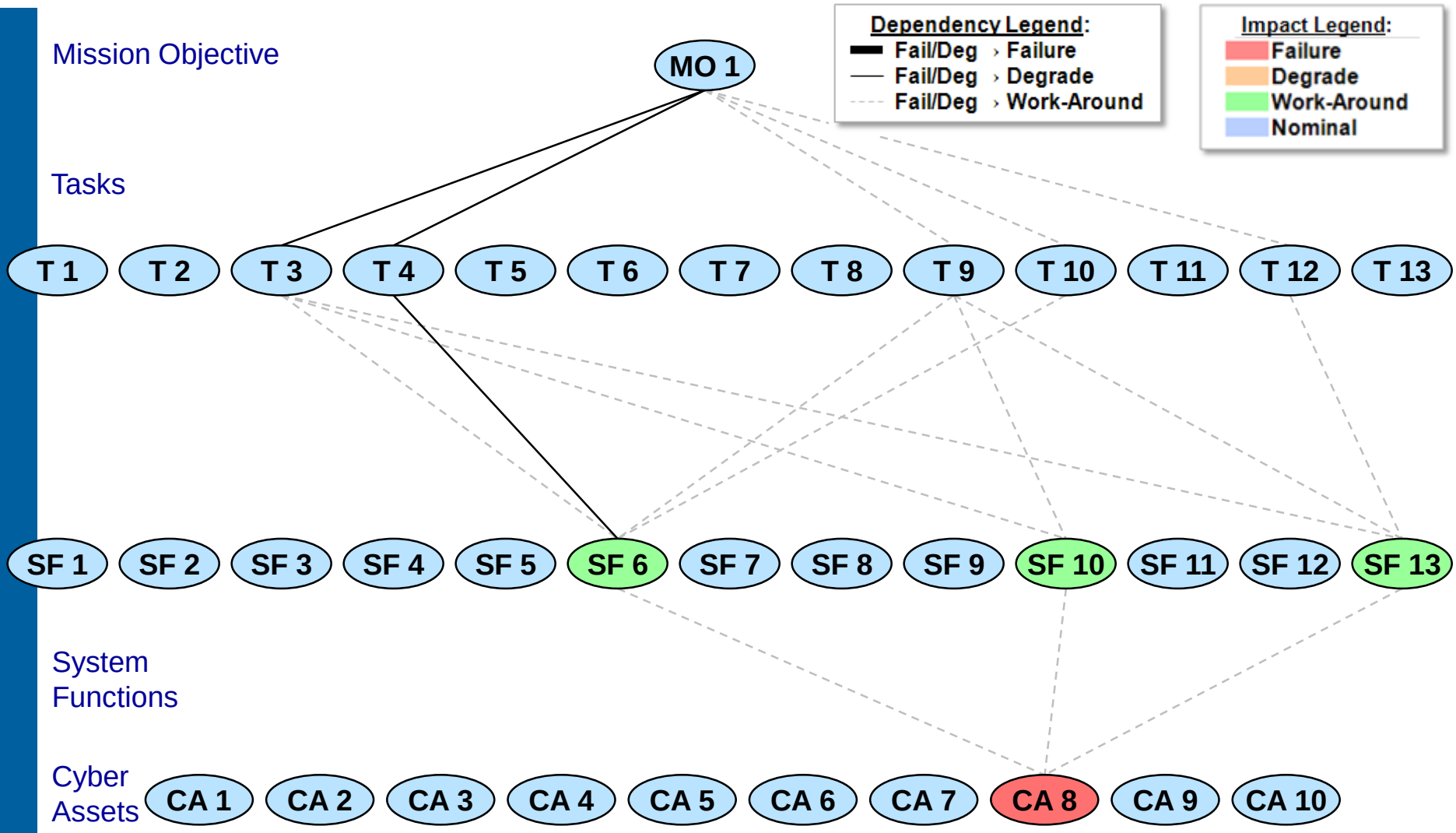
CA7's Failure Has an Effect Like That of CA6's Failure – No MO1 Impact



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

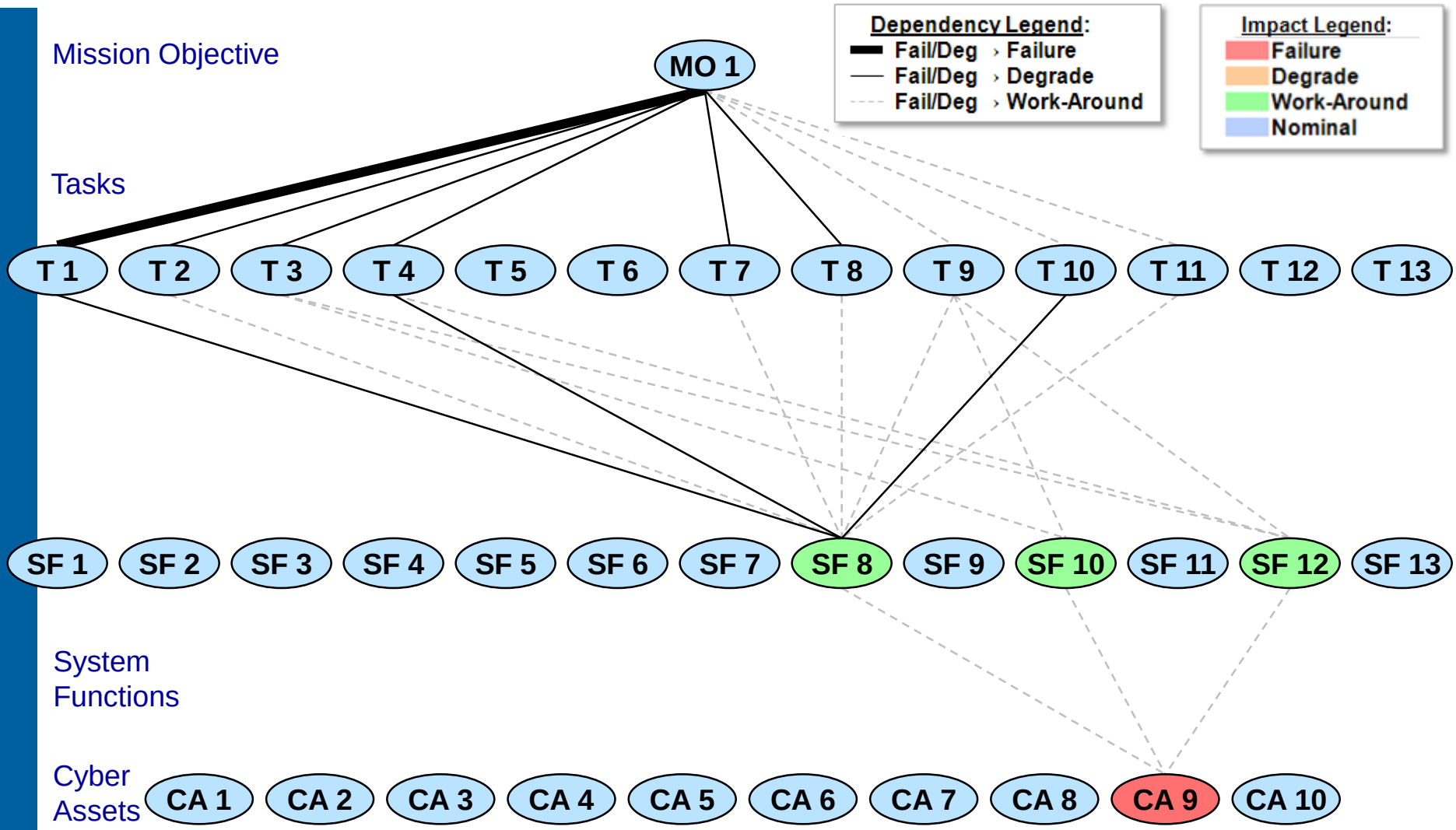
CA8's Failure Has an Effect Like That of CA6's Failure – No MO1 Impact



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

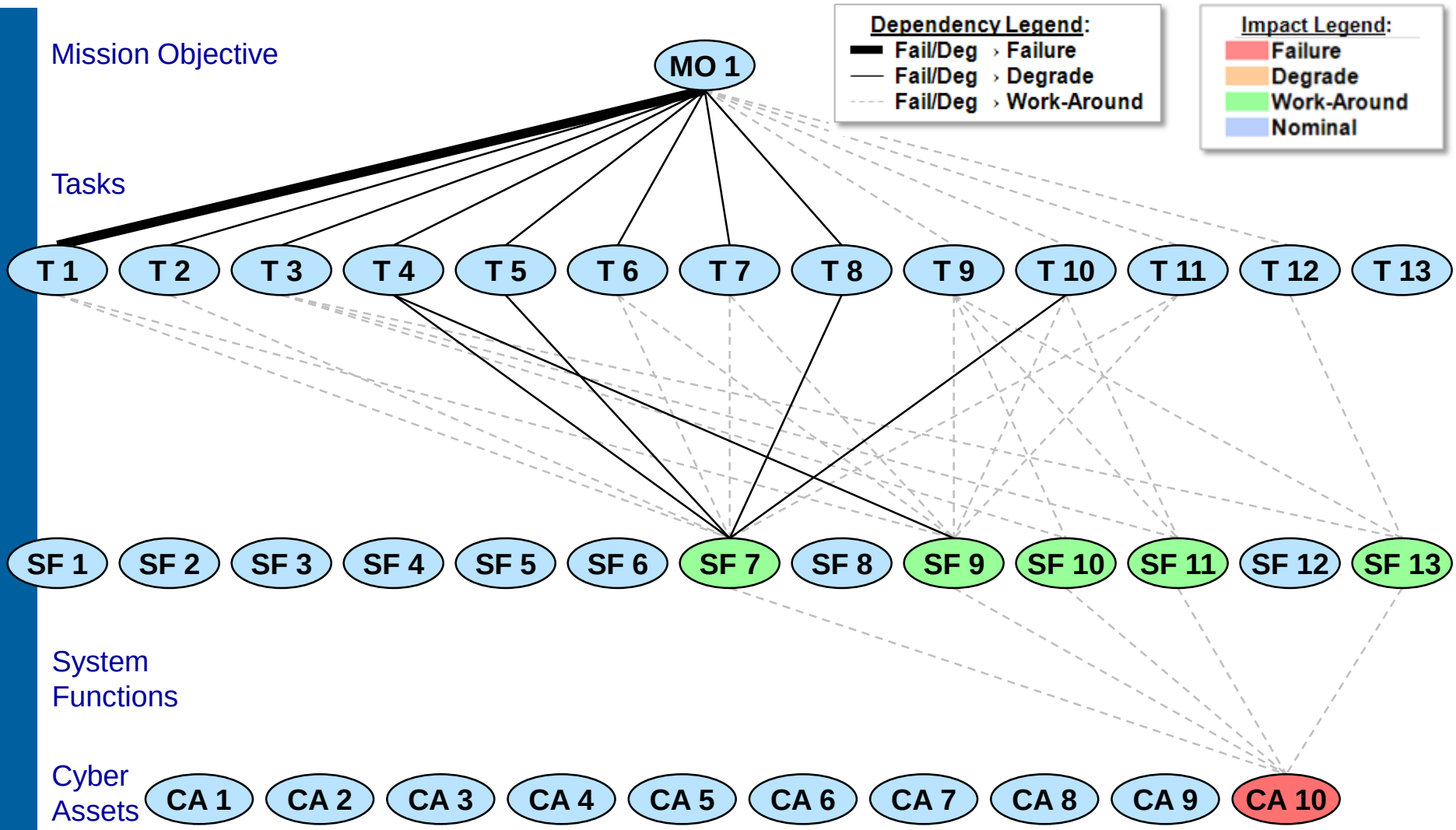
CA9's Failure Has an Effect Like That of CA6's Failure – No MO1 Impact



Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

CA10's Failure Has an Effect Like That of CA6's Failure – No MO1 Impact

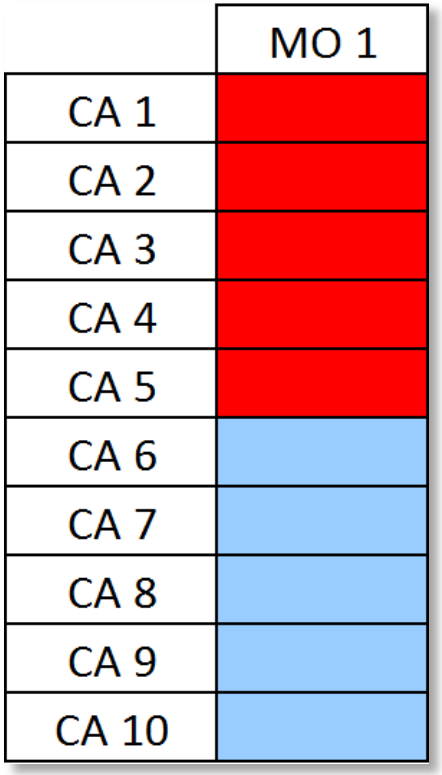


Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved

MITRE

The Results Can Be Compacted For Easy Viewing

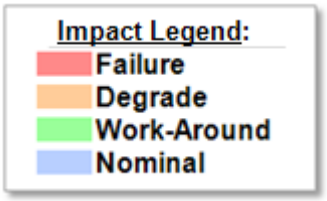
- **Cell color indicates the Mission Objective's Impact resulting from each CA failure**
- **Red means that MO1 fails, and Blue means that MO1 is nominal**
- **In this example, CA1 through CA5 are Mission-Critical Cyber Assets since their failure would cause MO1 to fail**
- **Cyber Assets CA1 through CA5 are Mission-Critical Cyber Assets – the "Crown Jewels"**



Approved for Public Release: Case 14-1906
© 2018 The MITRE Corporation. All rights reserved

A Typical Case Shows Mission-Critical CA for Several Mission Objectives

Result of CA Failure/Degrade: Blue = Mission Nominal Green = Mission Work Around Yellow = Mission Degrade Red = Mission Failure	Mission Objective 1	Mission Objective 2	Mission Objective 3	Mission Objective 4	Mission Objective 5	Mission Objective 6	Mission Objective 7	Mission Objective 8	Mission Objective 9	Mission Objective 10
Cyber Asset 1										
Cyber Asset 2										
Cyber Asset 3										
Cyber Asset 4										
Cyber Asset 5										
Cyber Asset 6										
Cyber Asset 7										
Cyber Asset 8										
Cyber Asset 9										
Cyber Asset 10										
Cyber Asset 11										
Cyber Asset 12										
Cyber Asset 13										
Cyber Asset 14										
Cyber Asset 15										
Cyber Asset 16										
Cyber Asset 17										
Cyber Asset 18										
Cyber Asset 19										
Cyber Asset 20										
Cyber Asset 21										
Cyber Asset 22										
Cyber Asset 23										
Cyber Asset 24										
Cyber Asset 25										
Cyber Asset 26										
Cyber Asset 27										
Cyber Asset 28										
Cyber Asset 29										
Cyber Asset 30										



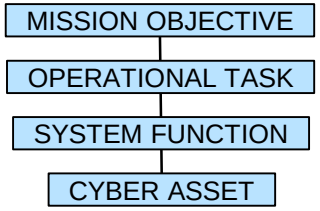
- **A single CA in a highly integrated infrastructure will affect more than one MO**
- **The total mission impact of each CA is shown across each row**
- **For each MO, the column below it shows the CA that are critical to its achievement**

Approved for Public Release: Case 14-1906
© 2018 The MITRE Corporation. All rights reserved

MITRE

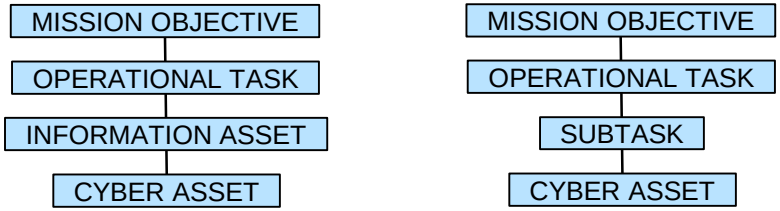
The CJA Methodology Allows For Flexibility

- **The preceding slides show a CJA based on the 4-tier model shown here:**



  - *Different models are also used, depending on the reference information available to the CJA team*

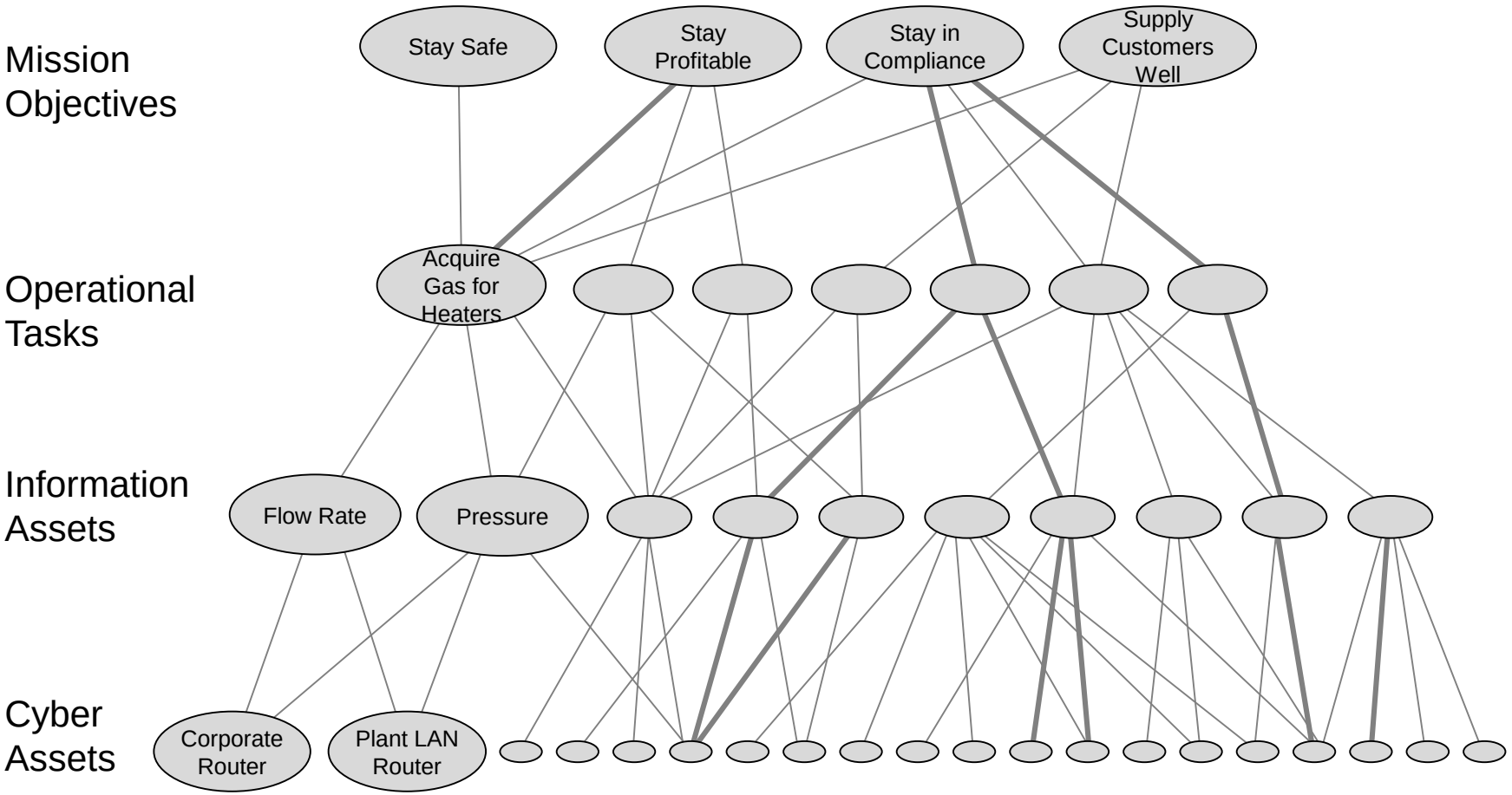
- **Alternative 4-tier models:**



  - *An Information Asset is operational information needed to perform a task*

Approved for Public Release: Case 08-0490
© 2018 The MITRE Corporation. All rights reserved

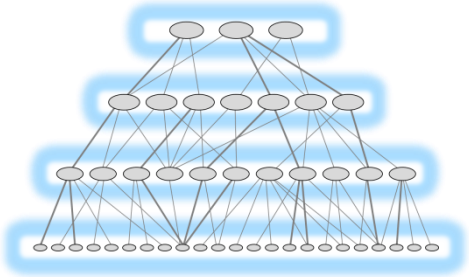
Alternative Model Using Information Assets - Refinery Example



Approved for Public Release: Case 08-0490
© 2018 The MITRE Corporation. All rights reserved

MITRE

We Use the CJA Tool to Help Build the Dependency Map



Cyber Asset Weights

Info Asset/ Sys Funct Weights

Task Weights

Objective Weights

Mission-Critical CA Candidates

4 CA

IA / SF

3 IA / SF

Tasks

2 Tasks

Object's

1 Object's

Object's

Identify Dependencies on Tasks

… and on Info Assets or System Functions

… and on Cyber Assets

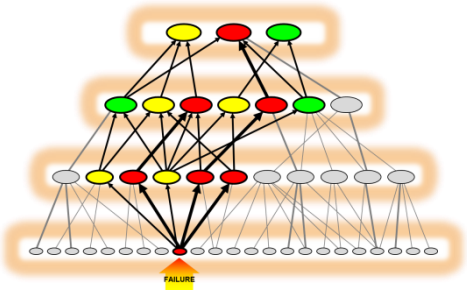
Prioritize Mission Objectives

Approved for Public Release: Case 08-0490

© 2018 The MITRE Corporation. All rights reserved

MITRE

Next, The CJA Tool Automatically Completes the Mission Impact Analysis (MIA)



Propose
CA Failures/
Degrades

CA
Criticality

IA/SF
Criticality

Task
Criticality

5 Scenarios
CA's

4c CA
IA/SF

3c IA/SF
Tasks

2c Tasks
Object's

CA
Impact

IA/SF
Impact

Task
Impact

Roll-Up Rules Utilize User-Input
Criticality Scores

Mission
Impact

Approved for Public Release: Case 14-1906
© 2018 The MITRE Corporation. All rights reserved

MITRE

Tool Demonstration

© 2018 The MITRE Corporation. All rights reserved

MITRE

For More Information:

CJA article in MITRE's Systems Engineering Guide:

- http://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis

Contact the following at MITRE Bedford:

- Jim Watters - jwatters@mitre.org
- Peter Kertzner - kertzner@mitre.org

Approved for Public Release: Case 14-1906

© 2018 The MITRE Corporation. All rights reserved

MITRE