



Sponsor: Brookhaven National Laboratory
(BNL), under contract with Department of
State
Dept. No.: T886
Contract No.: 355358
Project No.: 14198021-AE

The views, opinions and/or findings
contained in this report are those of The
MITRE Corporation and should not be
construed as an official government position,
policy, or decision, unless designated by
other documentation.

Approved for Public Release; Distribution
Unlimited, Case 20-0021.

©2020 The MITRE Corporation.
All rights reserved.

Bedford, Massachusetts

Critical Infrastructure Cyberspace Analysis Tool (CICAT)

Capability Description

**Jackson Wynn
Joseph Whitmore
William Coconato
Samuel McCracken**

January 2020

Abstract

Critical Infrastructure Cyberspace Analysis Tool (CICAT) is a modeling and simulation tool for evaluating how an adversary might conduct a cyber attack on a system. MITRE developed CICAT to automate production of cyber attack scenarios in conjunction with participation in International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) J02008: *"Enhancing Computer Security Incident Analysis at Nuclear Facilities"* [1], which is an international research project to improve capabilities to prevent, detect and respond to cyber security incidents at nuclear facilities. The CICAT tool can be easily applied to other critical infrastructures or cyber physical systems through development of an infrastructure model to represent the target environment. Potential applications of CICAT include cyber threat modeling for acquisition programs, as well as defensive cyber operations (DCO) incident analysis, planning, and decision support in a production environment. This paper provides a capability description of the CICAT tool.

This page intentionally left blank.

Executive Summary

Critical Infrastructure Cyberspace Analysis Tool (CICAT) is a modeling and simulation tool for evaluating how an adversary might conduct a cyber attack on a system. MITRE developed CICAT to automate production of cyber attack scenarios in conjunction with participation in International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) J02008: *"Enhancing Computer Security Incident Analysis at Nuclear Facilities"* [1], which is an international research project to improve capabilities to prevent, detect and respond to cyber security incidents at nuclear facilities.

The CICAT data model integrates an infrastructure model representing the target environment with a threat model that includes vulnerability and threat actor capabilities data. The infrastructure model represents an enterprise or cyber physical system as a hierarchical set of mission capabilities containing functions, systems, components and attack surfaces. The threat model characterizes threat actor capabilities and component vulnerabilities based on open source ATT&CK™[2] and CVE™[3].

CICAT uses the infrastructure and threat models to generate cyber attack scenarios. A cyber attack scenario is defined as a targeted cyber attack by a known threat actor. Scenario generation simulates threat actor activities within the infrastructure and produces a variety of reports. CICAT can be easily adapted to generate cyber attack scenarios for a variety of critical infrastructures and cyber physical systems. Automated production of cyber attack scenarios using CICAT compares favorably to cyber attack scenarios produced through manual analysis.

CICAT generates cyber attack scenarios using a 2-stage approach. The first stage performs attack path analysis to identify a component pathway connecting an entry point to the scenario target based on the infrastructure topology. The second stage applies a pattern of adversary objectives to each component in an attack path, using objectives defined by the Office of the Director of National Intelligence (ODNI) Common Cyber Threat Framework [4] mapped to ATT&CK™ tactics and techniques.

Scenario generation produces a detailed report of the attack path and ATT&CK™ TTPs selected. CICAT utilities provide command line options to generate alternative mitigation or forensic reports. A web-based GUI is available to initiate scenario generation and view scenario reports.

Potential applications of scenario generation include cyber assessments, Cyber Table Top (CTT) activities, defensive cyber operations, and cyber awareness training. Additionally, CICAT provides a platform for threat modeling and experimentation through its ability to import supplemental TTP and threat actor capability data.

Acknowledgments

We gratefully acknowledge the collaboration with Dr. Sukesh Aghara and graduate students from the University of Massachusetts Lowell (UML) Nuclear Engineering department, the guidance and support provided by Mr. Christopher Spirito with Idaho National Laboratory (INL), by Mr. Mike Rowland, Mr. Mitchell Hewes, and Mr. Trent Nelson with International Atomic Energy Agency (IAEA), by Mr. David Trask with Canadian Nuclear Laboratories (CNL), and the support of organizations participating in CRP J02008. We also wish to thank Daryl Hild and Nathan Edwards with MITRE for their thoughtful review and feedback on this document.

Table of Contents

1	Introduction	1
1.1	IAEA CRP J02008	1
1.1.1	Participating Member States and US Organizations.....	1
1.1.2	MITRE's Role in CRP J02008	2
1.1.2.1	MITRE Contributions to CRP J02008.....	2
1.1.3	Asherah Reference Architecture	2
1.1.3.1	CICAT Infrastructure Model	3
1.1.4	Asherah Hardware-in-the-Loop (HIL) Simulation	3
1.1.4.1	Scenario Development Workshop	3
2	Critical Infrastructure Cyber Analysis Tool (CICAT)	5
2.1	Concept of Operation	5
2.2	CICAT Data Model.....	5
2.2.1	Infrastructure Model	5
2.2.2	Threat Model.....	6
2.2.3	Cyber Attack Scenarios.....	6
2.3	CICAT Functional Capabilities	7
2.3.1	Scenario Generation.....	7
2.3.2	Use of Open Source CVE™ and ATT&CK™	9
2.3.3	Applied Cyber Analytics.....	9
2.3.3.1	Impact Scores	10
2.3.3.2	Threat Actor Sophistication.....	11
2.3.3.3	Analytics-based Mitigation Selection.....	11
2.3.4	CICAT Utilities.....	12
2.3.4.1	Support for Standalone Operation	12
2.3.5	Report Generation.....	13
2.3.5.1	Scenario Detail Reports	13
2.3.5.1.1	Example Scenario Detail Report	13
2.3.6	CICAT User Interface.....	16
2.3.6.1	The Scenarios View.....	16
2.3.6.2	Performing Scenario Generation through the User Interface	16
2.3.6.3	Viewing Scenario Details through the User Interface	17
3	Comparison with other MITRE-developed Tools	20
4	Applications of CICAT Scenario Generation.....	21
4.1	Cyber Assessments	21

4.2	Cyber Awareness Training	21
4.3	Defensive Cyber Operations	21
4.4	Threat Modeling and Experimentation	22
5	Summary.....	23
6	References/Bibliography	24
Appendix A	Comparison with Manually Developed Scenarios.....	26
	Hand Crafted Scenarios	26
	CDBT-001: Boiler Level / Pressure Control System DoS.....	26
	CDBT-002: Malicious PHTS PLC Configuration.....	27
	CDBT-003: Malicious Turbine High Pressure Oil System Configuration.....	27
	CDBT-004: Theft of Sensitive Corporate Data	27
	CDBT-005: Plant Data Historian Ransomware Infection	27
	CDBT-006: In-Transit Theft of Nuclear Fuel.....	28
	CDBT-007: Remote Access Tool Implantation.....	28
	CDBT-008: Insider Attack on Boiler Level / Pressure Control System.....	28
	CDBT-009: Primary Heat Transport System Pressure Control DoS.....	29
	CDBT-010: Electrical Protection Equipment DoS	29
	CDBT-011: Theft of Sensitive Operational Data	29
	CDBT-012: Theft of Operational Data for Political Purposes.....	30
	CDBT-013: Turbine Governing System DoS.....	30
	CDBT-014: Turbine Governing System DoS.....	30
	Comparison of Hand Crafted and CICAT-Generated Scenarios.....	30
Appendix B	Design Basis Threat Considerations	32
	Application of ATT&CK™.....	32
Appendix C	Abbreviations and Acronyms	33

List of Figures

Figure 1 CRP J02008 3rd Research Coordination Meeting Daejeon, Korea	1
Figure 2 IAEA Headquarters, Vienna, Austria	2
Figure 3 CNL Integration Lab	4
Figure 4 CICAT Data Model	5
Figure 5 Lateral Movement within an Infrastructure.....	7
Figure 6 ODNI Cyber Threat Framework and ATT&CK™	8
Figure 7 TTP Filtering	9
Figure 8 Asherah Heat Management Capability.....	11
Figure 9 Scenario Metadata	12
Figure 10 CICAT Scenarios View	16
Figure 11 CICAT Scenario Generation Page.....	17
Figure 12 Scenario Detail View (Attack Paths).....	18
Figure 13 Scenario Detail View (ATT&CK™ TTPs and CVEs).....	19
Figure 14 MITRE / UML scenario team, with visiting IAEA and INL members.....	26

List of Tables

Table 1 CICAT Analytics	9
Table 2 CICAT Utilities.....	12
Table 3 Comparison of CICAT with other MITRE-developed Tools.....	20
Table 4 Supplemental ATT&CK™ TTPs	22

This page intentionally left blank.

1 Introduction

Critical Infrastructure Cyber Analysis Tool (CICAT) is a modeling and simulation tool for evaluating how an adversary might conduct a cyber attack on a system. CICAT is being developed in conjunction with MITRE participation in an international Collaborative Research Program (CRP) on cyber incident analysis and response hosted by International Atomic Energy Agency (IAEA). MITRE support to the CRP commenced in 2017 and was originally scheduled to end June 2019. It has been extended until June 2020. This section provides an overview of the CRP and MITRE's supporting role in cyber threat model and scenario development.

1.1 IAEA CRP J02008

International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) J02008: *"Enhancing Computer Security Incident Analysis at Nuclear Facilities"* [1] is a 3-year, international research project to improve capabilities at nuclear facilities to prevent, detect and respond to cyber security incidents that have potential to directly or indirectly adversely affect nuclear safety and nuclear security. J02008 explores good practices, technology, analytical methods, and recommended procedures for evaluating and responding to cyber security incidents in four (4) areas:

- Operator support for computer security incident recognition and response
- Analysis and technology support for computer security incident response
- Computer security information exchange
- Forensic analysis and cybercrime investigation

1.1.1 Participating Member States and US Organizations

The CRP is an international collaboration of the following member states: Argentina, Australia, Austria, Brazil, Canada, China, Germany, Ghana, Hungary, Mexico, Pakistan, Poland, Republic of Korea, and the United States (US).



Figure 1 CRP J02008 3rd Research Coordination Meeting Daejeon, Korea

A total of 17 organizations participate in CRP J02008. US-based organizations participating in the CRP include: Idaho National Labs (INL), MITRE, Underwriter Labs (UL), University of Massachusetts Lowell (UML), and University of Tennessee Knoxville (UTK).

1.1.2 MITRE's Role in CRP J02008

MITRE's role in CRP J02008 focuses on providing technical leadership in development of cyber threat models and scenarios to assist other CRP participating organizations perform cybersecurity analysis and develop cyber attack scenarios to evaluate engineering testbeds being developed to represent Pressurized Water Reactor (PWR) systems. To provide this support, MITRE partnered with University of Massachusetts Lowell (UML) Nuclear Engineering department to leverage their deep technical knowledge of nuclear power generation and plant operations, and collaborated with UML staff to develop cyber attack scenarios. As a follow-on activity, the CICAT tool is being developed to automate scenario production.

1.1.2.1 MITRE Contributions to CRP J02008

MITRE's contributions to CRP J02008 since 2017 included the following.

2017: MITRE partnered with the Nuclear Engineering department at University of Massachusetts Lowell (UML) to leverage their expertise in nuclear technology and power plant operations.

MITRE deployed an online ICS/SCADA repository of CAPEC-based [5] attack vectors to assist CRP participants in their development of cyber attack scenarios.

2018: MITRE collaborated with UML to manually develop cyber attack scenarios targeting selected PWR subsystems. Examples of these scenarios are provided in Appendix A.

MITRE participated in an IAEA-hosted technical review of NSS 10, "Deployment, Use, and Maintenance of the Design Based Threat"[6], which is discussed in Appendix B.

2019: MITRE developed the CICAT tool to automate production of cyber attack scenarios and tested it at an IAEA-sponsored Scenario Development Workshop.



Figure 2 IAEA Headquarters, Vienna, Austria

1.1.3 Asherah Reference Architecture

CRP J02008 developed a reference architecture of a pressurized water reactor (PWR) called Asherah [7] to support IAEA research and training objectives. The Asherah reference architecture is a hypothetical representation that captures technical aspects of a PWR, but is not based on commercial reactor designs and does not incorporate sensitive details from commercial PWRs.

Cyber attack scenarios discussed in this paper outline broad classes of cyber exploitation, but are based on the IAEA-developed, Asherah reference architecture to ensure that they contain no sensitive information and cannot be used for nefarious purposes.

1.1.3.1 CICAT Infrastructure Model

An infrastructure model was developed as input to the CICAT tool based on the Asherah reference architecture. This model is implemented as a spreadsheet containing tabs that list PWR capabilities, functions, systems, components, attack surfaces, connections, and locations.

The infrastructure model includes a components tab that lists commercial Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA) and Information Technology (IT) components, e.g., Programmable Logic Controllers (PLCs), Human Machine Interfaces (HMIs), servers, routers, workstations, etc. These components are not defined in Asherah, but instead are based in part on engineering testbeds developed by CRP participating organizations for a Hardware-in-the-Loop (HIL) simulation of the Asherah reference architecture.

1.1.4 Asherah Hardware-in-the-Loop (HIL) Simulation

CRP J02008 also developed a Hardware-in-the-Loop (HIL) simulation of the Asherah reference architecture in support of IAEA research and training objectives. Participating CRP organizations implemented engineering testbeds to emulate selected PWR reactor components. These testbeds are integrated with a neutron transport model developed by University of Sao Paulo (USP) to emulate neutron flux within a reactor core. The USP model is implemented in Simulink and MATLAB, and provides interfaces through which PWR component models can be replaced by engineering testbeds that emulate those components. Engineering testbeds developed and integrated with the HIL simulation include a pressurizer, condenser, turbine and electrical distribution network, feedwater system, and other PWR components.

1.1.4.1 Scenario Development Workshop

In July 2019 Canadian Nuclear Laboratories (CNL), another CRP-participating organization, hosted a Scenario Development Workshop to evaluate cyber attack scenarios targeting engineering testbeds integrated with the reactor model in order to generate and collect anomalous behaviors and indicators of compromise (IoCs). The CNL test facility is pictured in Figure 3 below.



Figure 3 CNL Integration Lab

The Scenario Development Workshop provided an opportunity to evaluate CICAT capabilities for generating scenarios for selected CRP-developed engineering testbeds. This CICAT testing involved creating infrastructure model representations and generating scenarios for engineering testbed available at the workshop. These testbeds consisted of a single controller and HMI operating within a single zone, and were significantly less complicated than the infrastructure model developed for the full Asherah reference architecture. Scenarios generated during the workshop did not evaluate multiple entry points or span multiple zones.

2 Critical Infrastructure Cyber Analysis Tool (CICAT)

The Critical Infrastructure Cyber Analysis Tool (CICAT) is a modeling and simulation capability for evaluating how an adversary might conduct a cyber attack on a system. It uses technical details about the target environment, vulnerabilities, and threat actor capabilities to generate cyber attack scenarios that simulate threat actor activities within that target environment. This section discusses the CICAT concept of operation, data model, and function capabilities.

2.1 Concept of Operation

At startup CICAT imports information on the target infrastructure, threat actor capabilities and component vulnerabilities, which it uses to generate cyber attack scenarios. The scenario generation process identifies attack paths between specified entry points and a designated target, and then selects adversary tactics and techniques used to gain access to the targeted component and deliver effects. Each scenario run may identify several attack paths depending on the connectivity of the target and the number of entry points. Threat actor capability information is used to select tactics and techniques along the attack path.

A scenario run produces a detailed scenario report listing the tactics and techniques selected for each component in the attack path. Mitigation and forensic reports can also be produced that provide mitigation and detection information based on the tactics and techniques selected. These reports can be used to make recommendations and select potential courses of action.

2.2 CICAT Data Model

The CICAT data model includes details about the target infrastructure and possible threat actors. A cyber attack scenario specifies a target and one or more entry points, from the infrastructure, a threat actor, and an intended effect, either disruption or exfiltration. This data model is depicted in Figure 4.

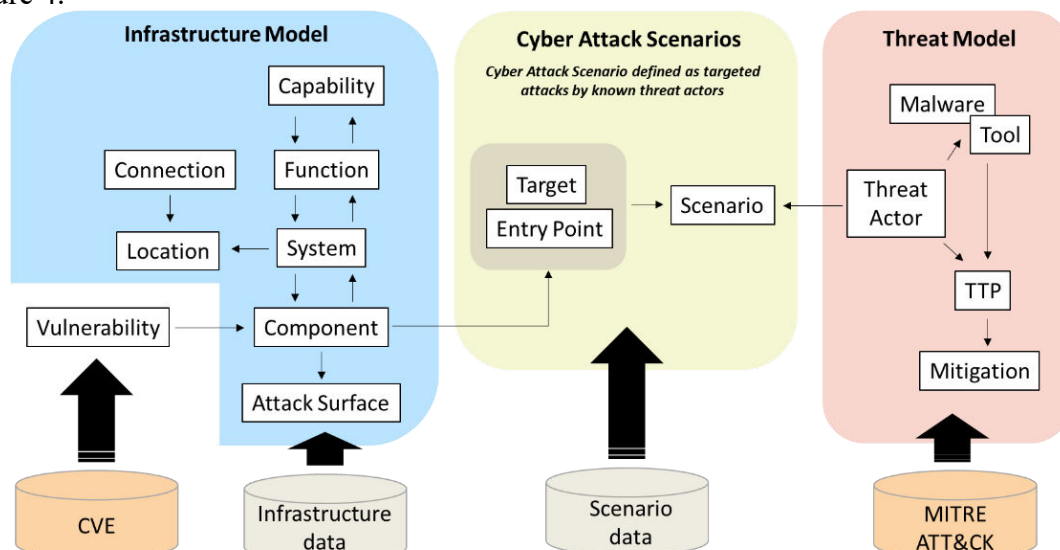


Figure 4 CICAT Data Model

2.2.1 Infrastructure Model

The infrastructure model represents an enterprise or cyber physical system as a hierarchical set of mission capabilities containing functions, systems, components and attack surfaces. A system in

the infrastructure model is comprised of components and supports multiple functions. At the lowest level in the hierarchy, each component is identified by its unique IP address and device type, and one or more attack surfaces. Example attack surfaces include hardware, software, firmware, interfaces, protocols, etc. Each Commercial Off the Shelf (COTS) component includes supply chain as an attack surface. The infrastructure model also provides network connectivity information between infrastructure components.

2.2.2 Threat Model

The threat model characterizes the intent and capability of different cyber threat actors. Intent is characterized in terms of the industries the threat actor is known to attack. Examples include industrial sectors, e.g., energy, transportation, etc., as well as military units and government agencies. Threat actor capabilities are defined by the range of tactics and techniques the threat actor is known to employ. Reconnaissance, privilege escalation, and lateral movement are commonly used tactics, while more sophisticated threat actors may also employ defensive evasion and persistence.

CICAT uses a threat model that leverages open source cyber threat actor and capabilities data provided by MITRE ATT&CK™. This use of ATT&CK™ is a departure from the IAEA-standard approach for characterizing adversary capabilities discussed in Nuclear Security Series (NSS) 10, “Deployment, Use, and Maintenance of the Design Based Threat”[6]. Appendix B provides discussion on use of the ATT&CK™ threat model for DBT development.

2.2.3 Cyber Attack Scenarios

Conceptually, a cyber attack scenario is a targeted cyber attack by a known threat actor. A scenario specification is defined for each scenario to identify the threat actor, from the list of approximately 80 threat actors represented in ATT&CK™, the target, and one or more entry points from the infrastructure model. Lateral movement within the infrastructure is the assumed objective of the adversary seeking to gain access to the targeted component, subject to network connectivity within the infrastructure model. As Figure 5 illustrates, a given target may be accessible from multiple entry points, just as an entry point may provide direct or indirect access to multiple targets.

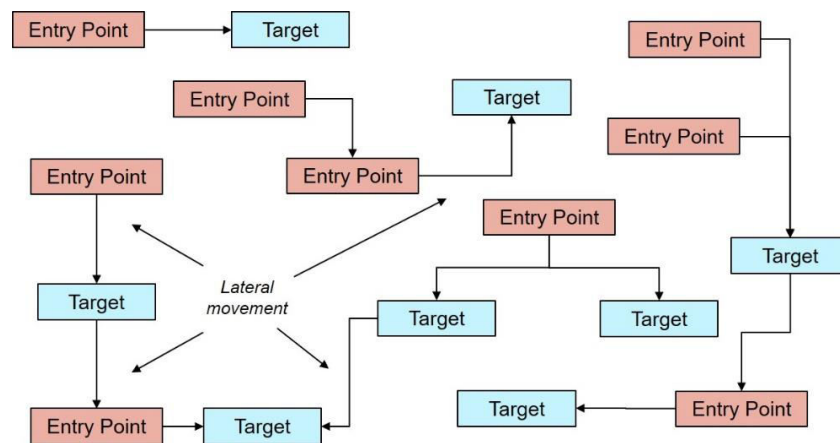


Figure 5 Lateral Movement within an Infrastructure

A scenario specification also characterizes the adversary's intended effect, either exfiltration or disruption, which is used in the selection of tactics and techniques when the scenario is simulated.

2.3 CICAT Functional Capabilities

CICAT provides capabilities for generating cyber attack scenarios based on analytics developed using infrastructure data combined with open source vulnerability and threat actor data. MITRE CVE™ and ATT&CK™, respectively, are used as open source data. CICAT was developed to generate a variety of reports and is currently being integrated with a web-based interactive user interface. This section discusses CICAT functional capabilities.

2.3.1 Scenario Generation

CICAT generates cyber attack scenarios based on an imported infrastructure model and open source, threat actor, TTP, and vulnerability data. CICAT applies a 2-stage generation approach. During the first stage, an attack path is identified based on the zone(s) in which the component entry point and target are located. A shortest path algorithm is applied to prevent cycles. A component is selected from each zone along the attack path based on its assessed susceptibility relative to other components within the zone. The component susceptibility metric is computed for each component based on the number of attack surfaces and reported vulnerabilities. The attack path analysis yields a sequence of IP addresses that include the entry point, the target, and components selected along the attack path.

During the second stage, an attack pattern is applied to each component in the attack path and used to construct a sequence of ATT&CK™ TTPs to compromise that component. Attack patterns are based on the ODNI Common Cyber Threat Framework[4], which decomposes adversary activities into stages, objectives and actions. The ODNI framework is illustrated in Figure 6 below.

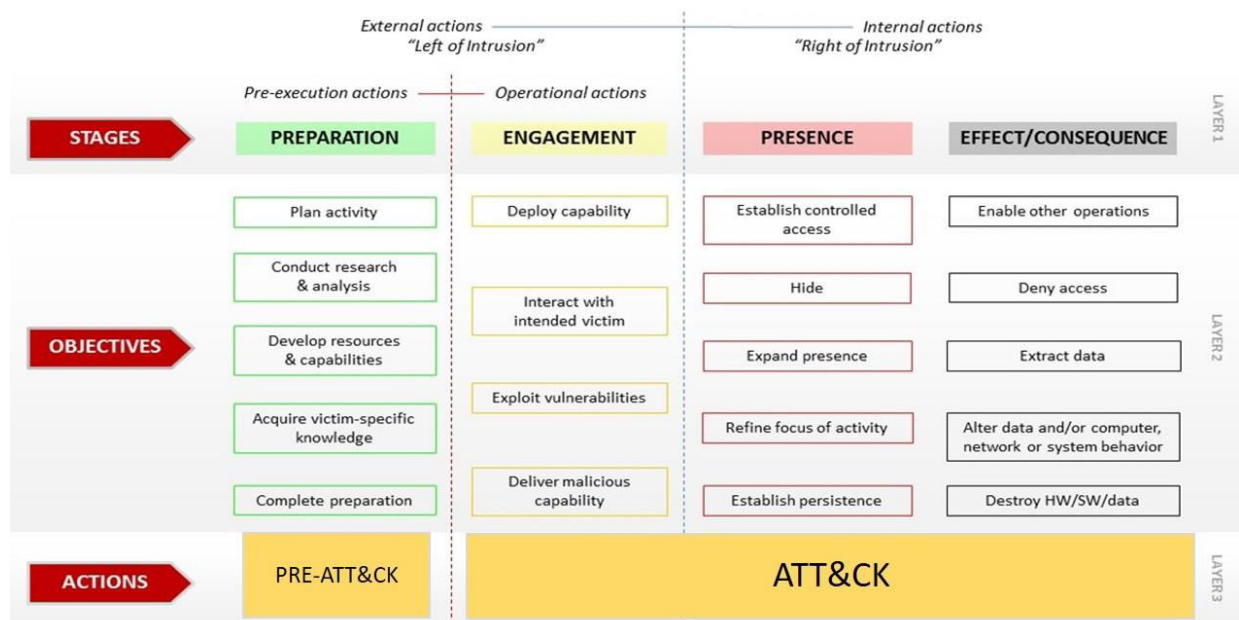


Figure 6 ODNI Cyber Threat Framework and ATT&CK™

CICAT pattern attacks specify a sequence of objectives from the ODNI Engagement, Presence and Effects stages. These objectives are mapped to ATT&CK™ tactics and TTPs. The ODNI Preparation stage is not supported in the current implementation of the CICAT tool.

CICAT defines several pattern attacks. Pattern attacks to achieve exfiltration or disruptive effects are applied to targets, while pattern attacks for lateral movement are applied to component along the attack path, including the entry point. There are patterns specific to Windows and Linux platforms. There are simple patterns with minimal objectives, and advanced patterns that include sophisticated or optional objectives, such as defensive evasion, command and control, persistence, etc. CICAT can be configured to apply patterns to emulate a variety of adversary behaviors during scenario generation. CICAT can also be configured with additional tactics and TTPs, which is discussed in section 4.4

The selection of ATT&CK™ TTPs applies a series of filters based on the threat actor, pattern tactic and platform. In the TTP filtering example in Figure 7, out of 448 Enterprise ATT&CK™ TTPs, 25 TTPs are attributable to the APT34 threat actor, 8 TTPs of those are associated with the Discovery tactic, and 3 TTPs of those are applicable to Linux platforms. If more than 1 TTP is selected by the TTP filtering process, random selection is used to pick a TTP for the scenario. That is, successive runs of the CICAT tool may yield different TTP selections for the same scenario specification.

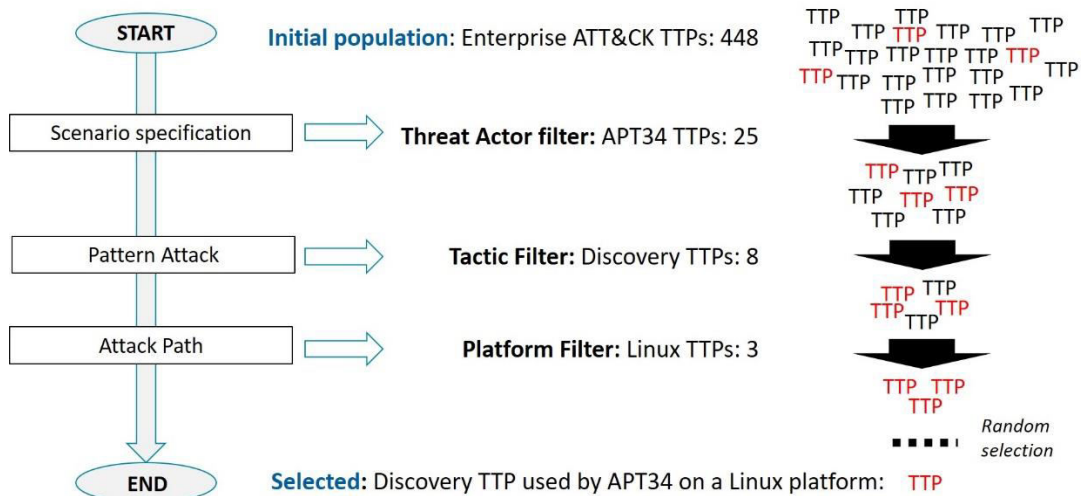


Figure 7 TTP Filtering

2.3.2 Use of Open Source CVE™ and ATT&CK™

CICAT utilizes open source ATT&CK™ and CVE™, which it imports at startup. CVE™ vulnerability data is imported from eXtensible Markup Language (XML) files and associated with components in the infrastructure model using keyword matching on component vendor and model information. CVE™ data is used to evaluate component susceptibility during attack path analysis. ATT&CK™ threat actor data is used as a filter in the selection of TTPs during the second stage of scenario generation. This ensures that TTPs selected for a generated scenario are attributable to the scenario threat actor. Importation of ATT&CK™ data from locally stored XML and JSON files allows CICAT to be deployed on non-network systems.

2.3.3 Applied Cyber Analytics

CICAT produces and applies a variety of analytics during scenario generation.

Table 1 CICAT Analytics

Analytic	Description	Applies to
Component CVEs	The number of component CVEs.	Component
Component Attack Surfaces	The number of component attack surfaces.	Component
Component Susceptibility	Sum of Component CVEs and attack surfaces.	Component
Component Impact Score	Assessed impact of component based on the criticality of the system, function and capability the component supports.	Component
Zone Component Count	Number of components in a zone.	Zone

Attack path length	The number of IP addresses in an attack path.	Attack path
Number of entry points	Number of infrastructure model components designated as entry points.	Infrastructure model
Number of attack paths	Number of attack paths identified for a scenario.	Scenario
Target exposure	Ratio of attack paths to entry points.	Scenario
Scenario Target Impact Score	Component impact score of targeted component.	Scenario
Scenario Breadcrumbs	Sum of breadcrumb scores for TTPs selected for an attack path.	Scenario
Actor sophistication	Number of TTPs attributed to a threat actor.	Threat Actor

The component susceptibility analytic, discussed previously, is used to select which component in a zone to include in an attack path. Impact scores are used to assess impact from disruption based on the criticality of components within the infrastructure model. The threat actor sophistication analytic is calculated based on attribution of ATT&CK™ TTPs, malware, and cyber tools to various threat actors. Other analytics are captured in scenario metadata, which can be used in the selection of mitigations.

2.3.3.1 Impact Scores

Criticality[8] refers to the impact of temporary or permanent loss of an asset on the ability to perform a mission or maintain a capability. In this context, an asset is lost when its availability or integrity is compromised. An asset is mission critical (MC) if its loss results in mission failure. An example of a mission critical asset is the axle of car. A broken axle will render the car undrivable. An asset is mission essential (ME) if a workaround would allow the mission to continue. An example of a mission essential asset is a car tire. A flat tire will disrupt the operation of the car. However the journey can resume once the flat is replaced with the spare. An asset is mission support (MS) if its loss has no impact on successful completion of the mission. An example of a mission support asset is the car's radio. Loss of the radio would not render the car undrivable.

A criticality attribute is associated with each capability, function, system, and component in the infrastructure model, and used to calculate an impact score for each component based on the systems, functions, and capabilities supported. These impact scores are calculated when the infrastructure model is loaded.

Figure 8 depicts the functional decomposition of the Heat Management PWR capability in the Asherah reference architecture in terms of its constituent functions, systems and components. Criticality scores assigned at each level are used to calculate impact scores for all supporting components.

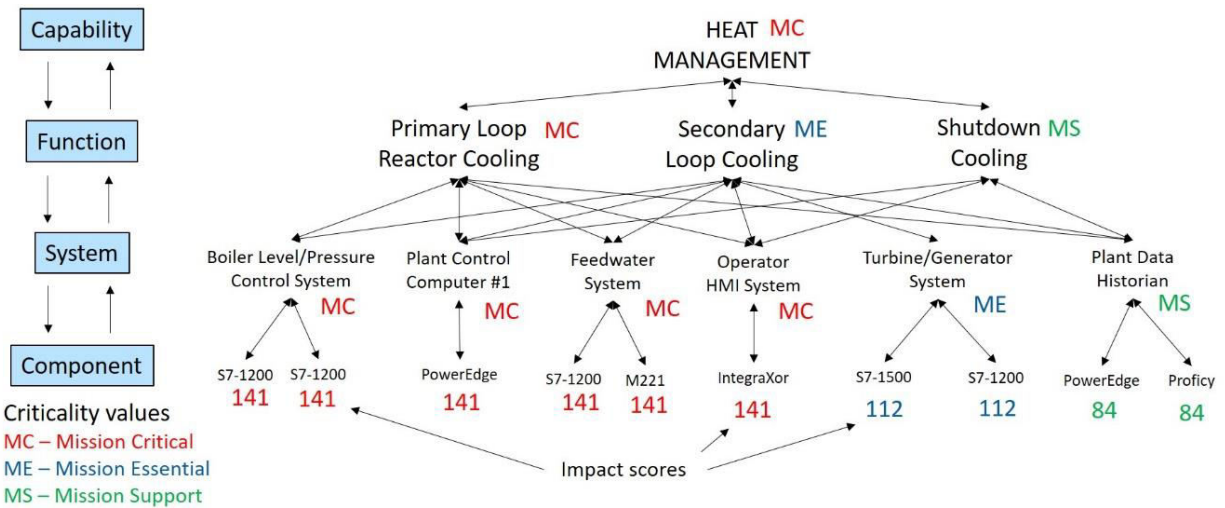


Figure 8 Asherah Heat Management Capability

In this example, the heat management capability is provided through primary loop, secondary loop, and shutdown cooling functions. The primary loop cooling function is mission critical as it is responsible for removing heat from the reactor core. Disruption of the primary loop cooling function, even for a short period, can result in a core meltdown. The secondary loop cooling function converts heat to mechanical energy that turns a turbine and generates electricity. This is a mission essential function because heat is still managed through the primary cooling loop when the turbine goes offline, i.e., as a result of a turbine trip. In this example, shutdown cooling is represented as a mission support function as it is engaged only when a reactor shutdown is performed.

CICAT uses a simple weighted sum to calculate impact scores based on criticality information imported from the infrastructure model. These impact scores are incorporated into scenario detail reports and can be used to set priorities for applying defensive mitigations. This simple capability is a place holder for more sophisticated and nuanced consequence scoring approaches, e.g., Crown Jewel Analysis (CJA) [9], etc.

Note that scenario detail reports also identify the 1st, 2nd and 3rd order effects of a disruptive cyber attack based on functional dependencies between capabilities, functions, systems, and components in the infrastructure model. This information is necessary to understand the consequent effects of a targeted disruption regardless of context – a single numeric impact score does NOT adequately characterize mission impact.

2.3.3.2 Threat Actor Sophistication

The ATT&CK™ dataset captures the relationship between threat actors and the TTPs, malware, and tools each threat actor is attributed to using. CICAT uses the length of this list to characterize the level of sophistication of each threat actor. Some threat actors are significantly more capable than other threat actors – this analytic can be used to select which threat actor(s) to evaluate.

2.3.3.3 Analytics-based Mitigation Selection

Each scenario run produces metadata describing viable attack paths and TTP sequences over a range of entry points. This metadata includes analytics that can be used in the selection of mitigations.

actor	str	1	APT16
effect	str	1	disrupt
name	str	1	SCN0003EP192.168.43.65
path	list	2	['192.168.43.65', '192.168.126.24']
score	int	1	126
target	str	1	192.168.126.24
ttps	list	2	[['T1199', 'T1057', 'T1210'], ['T1078', 'T9904']]

Figure 9 Scenario Metadata

Figure 9 depicts the metadata representation of a simple, 2-node scenario. This metadata includes the impact score of the target, the attack path listing of IP addresses, its length, and the distribution of ATT&CK™ TTPs for each node in the attack path. The compilation of this metadata over multiple scenario targets and entry points can be analyzed to identify “hot spots” in an infrastructure where an adversary is likely to transit or dwell. Attack path length also provides context for applying mitigations that segment the network. The frequency distribution of TTPs over the range of entry points may help set priorities for mitigations applied across subsystems.

2.3.4 CICAT Utilities

CICAT was initially designed as a collection of Python utility programs. These utilities perform scenario generation, housekeeping functions and provide basic troubleshooting. Table 2 lists CICAT utility programs.

Table 2 CICAT Utilities

Utility name	Description
scenGEN.py	The CICAT scenario generation tool. Optional command line arguments are used to generate different scenario reports.
actorGEN.py	Utility to generate a report on threat actor capabilities.
atk2xl.py	Utility to export ATT&CK™ data into a spreadsheet.
dbload.py	Utility to export Infrastructure model, ATT&CK™ and CVE™ data to MySQL database.
zoneCrawl.py	Interactive utility used to examine zone topology.

The CICAT user interface (see section 2.3.6) was developed to provide users with a web-based capability to initiate scenario generation and to navigate and view generated scenarios. The user interface functions by invoking scenGEN.py and dbload.py utilities.

2.3.4.1 Support for Standalone Operation

CICAT is designed to operate in both network connected and standalone modes. In network connected mode, CICAT imports MITRE ATT&CK™ data from a hosted STIX/TAXII service

accessible on the Internet. In standalone mode, CICAT imports MITRE ATT&CK™ data from a locally-stored JSON file. This allows CICAT to be used on classified systems where access to the STIX/TAXII service may be unavailable.

2.3.5 Report Generation

CICAT generates scenario reports that enumerate all attack paths identified for the scenario target. By default, a scenario detail report includes CVE™ vulnerability information for each component in the attack path, and detailed information for all ATT&CK™ TTPs used in the scenario. Other report formats can be selected through command line options. A mitigation report can be generated that provides ATT&CK™ TTP mitigation details for each TTP referenced in a scenario. A forensics report can be generated that provides ATT&CK™ TTP detection details for each TTP referenced in a scenario. In each case, scenario reports are “terrain following” by providing open source ATT&CK™ and CVE™ details specific to identified attack paths in the infrastructure model.

2.3.5.1 Scenario Detail Reports

CICAT produces a scenario detail report by default. Each report includes a header that identifies the scenario, threat actor, system target, intended effect, and a summary of affected systems, enterprise functions, and capabilities.

The next section of the report identifies attack path(s) based on entry point(s) and target. Each attack path is represented as a sequence of IP addresses that connect an entry point to the target. If five (5) entry points are specified for the scenario, then up to five (5) attack paths will be included in the report depending on accessibility of the target from those entry points. Following an attack path, this section will provide a detailed description of each component and a list of CVE™ vulnerabilities with matching vendor and model information. Detail reports include URLs to vulnerability reporting for each CVE™.

The last section of the report identifies the sequence of ATT&CK™ TTPs generated by CICAT during the TTP filtering stage for each IP address in the attack path. Note that if the intended effect of the scenario is disruption, the sequence of TTPs for the targeted component, i.e., the final IP address in attack path, will be a disruption sequence. If the intended effect is exfiltration, the sequence of TTPs for the targeted component will be an exfiltration sequence. The sequence of TTPs selected for non-targeted components in an attack path will be a lateral movement sequence. The detail report provides URLs to referenced ATT&CK™ TTPs.

2.3.5.1.1 Example Scenario Detail Report

An example scenario detail report is provided below. Note that ATT&CK™ TTP descriptions are omitted for the sake of brevity.

Scenario: SCN0001EP192.168.121.32

Group ID: G0007 | Name: APT28 | Sophistication: 66

Target: 192.168.122.15 | Intended Effect: disrupt | Impact score: 122

Effects:

1st order / System Affected: Feedwater System

2nd order / Function(s) Affected: ['Primary Loop Reactor Cooling', 'Secondary Loop Cooling']

3rd order / Capabilities Affected: {'HEAT MANAGEMENT'}

Attack path: ['192.168.121.32', '192.168.122.15']

192.168.121.32 | System: Boiler Level/Pressure Control System | CVE count: 9 | Impact Score: 117 | Component Description: Schneider M221 PLC

*CVE-2018-7792 URL: <https://www.schneider-electric.com/en/download/document/SEVD-2018-235-01/>
CVE-2018-7789 URL: <https://ics-cert.us-cert.gov/advisories/ICSA-18-240-02>
CVE-2018-7798 URL: <https://www.schneider-electric.com/en/download/document/SEVD-2018-270-01/>
CVE-2017-6030 URL: <https://ics-cert.us-cert.gov/advisories/ICSA-17-089-02>
CVE-2018-7791 URL: <https://www.schneider-electric.com/en/download/document/SEVD-2018-235-01/>
CVE-2018-7790 URL: <https://www.schneider-electric.com/en/download/document/SEVD-2018-235-01/>
CVE-2019-6820 URL: <https://www.schneider-electric.com/en/download/document/SEVD-2019-134-02/>
CVE-2017-7575 URL: <https://os-s.net/advisories/OSS-2017-01.pdf>
CVE-2017-7574 URL: <https://os-s.net/advisories/OSS-2017-02.pdf>*

192.168.122.15 | System: Feedwater System | CVE count: 5 | Impact Score: 122 | Component Description: Siemens S7-1200 PLC

*CVE-2018-13800 URL: <https://cert-portal.siemens.com/productcert/pdf/ssa-507847.pdf>
CVE-2017-12741 URL: <https://cert-portal.siemens.com/productcert/pdf/ssa-346262.pdf>
CVE-2017-2680 URL: <https://ics-cert.us-cert.gov/advisories/ICSA-18-023-02>
CVE-2017-2681 URL: https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-293562.pdf
CVE-2016-2846 URL: <https://ics-cert.us-cert.gov/advisories/ICSA-16-075-01>*

ATT&CK TTPs:

IP 192.168.121.32:

*T1190: Exploit Public-Facing Application
Tactic(s): ['initial-access']
URL: <https://attack.mitre.org/techniques/T1190>*

*T1018: Remote System Discovery
Tactic(s): ['discovery']
URL: <https://attack.mitre.org/techniques/T1018>*

*T1111: Two-Factor Authentication Interception
Tactic(s): ['credential-access']
URL: <https://attack.mitre.org/techniques/T1111>*

T1166: Setuid and Setgid
Tactic(s): ['privilege-escalation']
URL: <https://attack.mitre.org/techniques/T1166>

T1014: Rootkit
Tactic(s): ['defense-evasion']
URL: <https://attack.mitre.org/techniques/T1014>

T1210: Exploitation of Remote Services
Tactic(s): ['lateral-movement']
URL: <https://attack.mitre.org/techniques/T1210>

IP 192.168.122.15:

T1078: Valid Accounts
Tactic(s): ['initial-access']
URL: <https://attack.mitre.org/techniques/T1078>

T1078: Valid Accounts
Tactic(s): ['privilege-escalation']
URL: <https://attack.mitre.org/techniques/T1078>

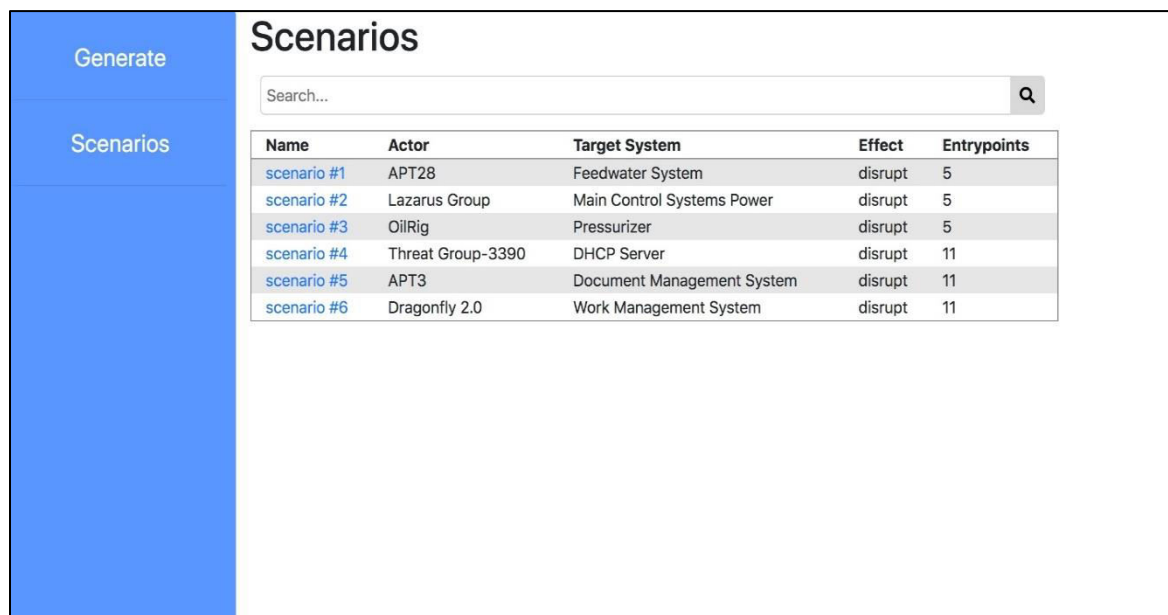
T9909: Modify device logic/programming
Tactic(s): ['deny']
URL: <https://not-your-standard-attack.com>

2.3.6 CICAT User Interface

The CICAT user interface provides users with a web-based capability to initiate scenario generation and to navigate and view generated scenarios. The user interface organizes generated scenarios by scenario and targeted component, and allows the user to drill-down to access all levels of scenario data. The user interface also provides capabilities to search for specified TTPs, IP addresses, systems, etc. which can be used to group scenarios that have common features. This web-based user interface supports remote access, which allows multiple users to simultaneously view the same scenario data.

2.3.6.1 The Scenarios View

The CICAT user interface can store scenario details for multiple scenarios. The Scenarios View illustrated in Figure 10 is accessed by clicking “Scenarios” in the sidebar menu. This view displays all scenarios currently in the database in a searchable table structure.



Name	Actor	Target System	Effect	Entrypoints
scenario #1	APT28	Feedwater System	disrupt	5
scenario #2	Lazarus Group	Main Control Systems Power	disrupt	5
scenario #3	OilRig	Pressurizer	disrupt	5
scenario #4	Threat Group-3390	DHCP Server	disrupt	11
scenario #5	APT3	Document Management System	disrupt	11
scenario #6	Dragonfly 2.0	Work Management System	disrupt	11

Figure 10 CICAT Scenarios View

Listed scenario details include Scenario Name, Threat Actor, Target System, Intended Effect, and number of identified Attack Paths. The Scenario Name is an active URL link to the Scenario Detail View (see below). The Threat Actor is assigned from threat actor details provided in ATT&CK™. Targets represent systems in the Infrastructure model. Adversary intended effects supported by CICAT include disruption of operations and exfiltration of data. The number of entry points corresponds to the number of attack paths to the target. Consideration should be given to targets with many attack paths.

2.3.6.2 Performing Scenario Generation through the User Interface

Figure 11 illustrates the CICAT scenario generate page, which is used to initiate scenario generation.

The screenshot shows a web interface for scenario generation. On the left is a blue sidebar with two buttons: 'Generate' at the top and 'Scenarios' below it. The main content area has a title 'Scenario Generation'. Below the title are two input fields. The first is labeled 'Infrastructure Model ⓘ' and contains the text '/cicat/cicat2/data/ASHERAH.xlsx'. The second is labeled 'Scenario Specification ⓘ' and contains the text '/cicat/cicat2/data/THREAT.xlsx'. Below these fields is a warning message: 'WARNING: Generating scenarios will replace existing scenarios.' At the bottom of the main content area is a blue button labeled 'Generate'.

Figure 11 CICAT Scenario Generation Page

The scenario generation page contains input fields used to enter path and filenames for the infrastructure and scenario spreadsheets to generate scenarios for. These fields are prepopulated with default filenames. Help buttons provide details for each input field.

Pressing the Generate button causes the user interface to invoke the CICAT utility (scenGEN.py) to generate a scenario detail report for the specified infrastructure and scenario spreadsheets. Generated report data is stored in an SQL database, replacing previously generated scenario data.

2.3.6.3 Viewing Scenario Details through the User Interface

The Scenario Details View is illustrated by Figures 12 and 13 below. Figure 12 shows a scenario with multiple traces, which detail each attack path to the scenario target from one of the designated entry points. To reduce visual clutter, trace details can be collapsed using a toggle caret.

Scenarios
Generate

scenario #1

ID: SCN0001

Description: Disruption of Feedwater System by Actor G0007

Actor: G0007

Intent: disrupt

Target: TGT00012 (192.168.122.15)

Traces:

Entry IP: 192.168.121.32

Path:

1. IP: 192.168.121.32

Zone: 2A

Platform: Linux

Vendor: Schneider

Description: M221

Type: PLC

Entry IP: 192.168.123.20

Path:

1. IP: 192.168.123.20

2. IP: 192.168.122.15

Entry IP: 192.168.126.23

Entry IP: 192.168.127.38

Entry IP: 192.168.43.65

Path:

1. IP: 192.168.43.65

Zone: 2A

Platform: Linux

Vendor: Siemens

Description: S7-1200

Type: PLC

Score: 126

Figure 12 Scenario Detail View (Attack Paths)

Figure 13 below shows the GUI display of ATT&CK™ TTPs and CVEs for each component in an attack path. A toggle caret allows the user to expand TTP and CVE™ entries to show additional details. A path tracker at the top of the view reminds the user where they are in the report as they scroll up and down. If internet connectivity is available, embedded hyperlinks can be used to access TTP data on the MITRE ATT&CK™ portal as well as URLs included in CVE™ descriptions.

Tree: Entry IP: 192.168.121.32 / IP: 192.168.121.32
TTPs and CVEs

- HEAT MANAGEMENT
- ▼ TTPs:
 - ^ 1. ID: T1200
Name: Hardware Additions
 - ^ 2. ID: T1201
Name: Password Policy Discovery
 - ^ 3. ID: T1111
Name: Two-Factor Authentication Interception
 - ^ 4. ID: T1176
Name: Browser Extensions
 - ^ 5. ID: T1205
Name: Port Knocking
 - ^ 6. ID: T1105
Name: Remote File Copy
- ▼ CVEs:
 - ^ ID: CVE-2017-7575
 - ^ ID: CVE-2017-7574
 - ^ ID: CVE-2018-7791
 - ^ ID: CVE-2018-7792
 - ^ ID: CVE-2018-7798
 - ^ ID: CVE-2019-6820
 - ^ ID: CVE-2018-7789
 - ^ ID: CVE-2017-6030
 - ^ ID: CVE-2018-7790

Figure 13 Scenario Detail View (ATT&CK™ TTPs and CVEs)

3 Comparison with other MITRE-developed Tools

This section compares CICAT with three (3) MITRE-developed tools for cyber threat modeling, analysis and assessment: CALDERA[10], TRACE/ECHO, and TARA[11]. Additional information about these MITRE tools can be found in the reference section.

Table 3 Comparison of CICAT with other MITRE-developed Tools

	MITRE Capability			
	CALDERA	TRACE / ECHO	TARA	CICAT
Capability description	CALDERA is used to test and evaluate network security posture and endpoint security solutions <u>on systems in operation</u> , and provides automated red teaming and adversary emulation based on MITRE ATT&CK.	Traversal-driven Risk Assessment of Composite Effects (TRACE) is a modeling and simulation toolset for analyzing probabilistic zero-day attack path models within a <u>digitally defined system architecture</u> . The ECHO model is a version of TRACE that incorporates ATT&CK tactics and techniques.	Threat Assessment and Remediation Analysis (TARA) is an engineering methodology used to identify and assess cyber vulnerabilities and select countermeasures effective at mitigating those vulnerabilities for a <u>digitally defined system design</u> . TARA uses a catalog of stored attack vector and countermeasure data.	Critical Infrastructure Cyber Analysis Tool (CICAT) provides capabilities for generating cyber attack scenarios based on analytics developed for a <u>digitally defined system model representing critical infrastructure or a cyber physical system</u> , combined with open source vulnerability and threat actor data.
Tool implementation			The TARA catalog is implemented as a IIS web application with MySQL data storage	Python 3.x application with web-based, DJANGO user interface and MySQL data storage
Development timeframe			2010 - 2011	2019
Applications			Cyber assessments, cyber resiliency assessments, RMF control tailoring	Cyber assessments, cyber awareness training, defensive cyber operations, threat modeling and experimentation
References	https://www.mitre.org/research/technology-transfer/open-source-software/caldera		https://www.mitre.org/sites/default/files/publications/pr-11-4987-presentation-tara-overview.pdf	[CICAT brief]
	https://www.mitre.org/sites/default/files/publications/pr-18-0944-1-automated-adversary-emulation-planning-acting.pdf		https://www.mitre.org/publications/technical-papers/threat-assessment-and-remediation-analysis-tara	[This paper]
Source repository	https://github.com/mitre/caldera		N/A	TBD
Inputs				
Open source data			CAPEC, CVE, CWE, industry best practices, NIST 800-53, etc.	ATT&CK, CVE
Other			Catalog mapping data, e.g., attack surface/vector mappings, vector/ countermeasure mappings, etc.	Infrastructure model, scenario specifications, supplemental ATT&CK tactic and TTP data
Outputs				
Artifacts, products, reports, etc.			Threat susceptibility matrix, mitigation mapping table, solution effectiveness table	Attack path info, cyber attack scenarios, scenario detail, mitigation, forensic reports

4 Applications of CICAT Scenario Generation

Potential applications of CICAT scenario generation include cyber assessments, cyber awareness training, defensive cyber operations, and threat modeling and experimentation.

4.1 Cyber Assessments

Cyber attack scenario generation supports Systems Security Engineering (SSE) outcomes within a systems acquisition, and can be used to evaluate alternative system designs, use of commercial off-the-shelf (COTS) components, identification of cyber key terrain, adversary hot spots, security critical entry points and primary attack paths.

An assessment methodology using CICAT would require development of an infrastructure model representing the target environment, and scoping to select threat actors, targets, and entry points for assessment. Detail and mitigation reports produced by CICAT using the infrastructure model as input would be used to identify issues and develop recommendations. For DoD acquisition programs, CICAT-generated attack scenarios and subsequent analysis would nominally yield classified results, requiring CICAT to be used on a classified system.

4.2 Cyber Awareness Training

One objective in partnering with UML to develop cyber attack scenarios for J02008 was to help provide cybersecurity awareness to undergraduate and graduate students from the UML nuclear engineering program. Cybersecurity awareness training is essential for both current and future PWR plant operators.

Cyber awareness training could be developed around use of CICAT and the Asherah reference architecture, in which trainees learn to use CICAT to identify critical PWR systems and entry points that could provide adversary access. Forensic reports generated using CICAT could provide trainees with an understanding of where to look and what to look for when a cyber incident occurs. Students in the collegiate nuclear engineering programs could potentially use CICAT to help identify potential vulnerabilities in a PWR design course.

4.3 Defensive Cyber Operations

Cyber attack scenario generation supports identification of component vulnerabilities, which would help prioritize application of software updates and/or security patches. Scenario generation would help identify critical entry points, and components and network “hot spots”, where additional monitoring may be useful. CICAT-generated mitigation reports would help in development of contingencies and/or courses of action. CICAT-generated forensic reports would help identify what to look for when a cyber incident occurs.

A methodology using CICAT would require development of an infrastructure model representing the operational (target) environment, which would be used to perform “what if” analysis to evaluate specific targets over a range of potential entry points. Scenario detail reports would contain sensitive data and would need to be protected from unauthorized access.

4.4 Threat Modeling and Experimentation

The CICAT tool supports capabilities to import ATT&CK™ extensions, including new TTPs, new TTP attributes, and threat actor attribution data. The following table lists supplemental TTPs used in scenario generation at the IAEA Scenario Development Workshop in 2019. They include a range of disruptive effects a threat actor might attempt once access to the target system is obtained. MITRE is developing extensions to ATT&CK™ for ICS/SCADA components[12], which will replace or augment this list of supplemental TTPs.

Table 4 Supplemental ATT&CK™ TTPs

TTP ID	Tactic	TTP Name	TTP URL
T9901	deny	Modify device configuration	https://not-your-standard-attack.com
T9902	deny	Disable via crafted packet	https://not-your-standard-attack.com
T9903	deny	Initiate device reboot	https://not-your-standard-attack.com
T9904	deny	Disable SNMP agent	https://not-your-standard-attack.com
T9905	deny	Disable administrative access	https://not-your-standard-attack.com
T9906	deny	Spoof command message	https://not-your-standard-attack.com
T9907	deny	Exploit 0-day vulnerability	https://not-your-standard-attack.com
T9908	deny	Exploit unpatched vulnerability	https://not-your-standard-attack.com
T9909	deny	Modify device logic/programming	https://not-your-standard-attack.com

CICAT also supports a capability to import supplemental TTP attributes. This capability provides a framework for defining new analytics for cyber threat analysis. For example, one supplemental attribute added to each TTP is called “breadcrumbs”, which is used to characterize a TTP’s ease of detection. When aggregated over the sequence of TTPs selected during scenario generation, the breadcrumbs analytic can be used to rank scenarios in terms of relative noisiness.

Cyber threat actors become more capable over time as they develop and/or apply new cyber tradecraft. The ability to supplement threat actor attribution data in ATT&CK™ provides a means to model a threat actor behavior as they evolve over time. This capability could be used to perform predictive analysis of threat actor behavior 3-5 years into the future.

5 Summary

CICAT is a modeling and simulation tool for evaluating how an adversary might conduct a cyber attack on a system. CICAT incorporates a data model that integrates details about the target infrastructure and threat actor capabilities. The infrastructure model represents an enterprise or cyber physical system as a hierarchical set of mission capabilities containing functions, systems, components and attack surfaces, which it loads from a spreadsheet at start up. The threat model characterizes cyber threat actor intent and capability based on open source ATT&CK™, which can be extended with supplemental TTP and capability data.

MITRE developed CICAT to automate production of cyber attack scenarios in support of participation in International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) J02008: *"Enhancing Computer Security Incident Analysis at Nuclear Facilities"*, which is an international research project to improve capabilities at nuclear facilities to prevent, detect and respond to cyber security incidents.

CICAT generates cyber attack scenarios using a 2-stage approach. The first stage performs attack path analysis to identify a sequence of components connecting an entry point to the scenario target based on the infrastructure topology. The second stage applies a pattern to each component in the attack path based on the ODNI Common Cyber Threat Framework. Each pattern produces a sequence of ATT&CK™ TTPs for that component by applying filters that select TTPs appropriate for the platform and threat actor. Scenario generation produces a detailed report of the attack path and TTPs selected. Command line options can be used to generate alternative mitigation or forensic reports.

In addition to scenario generation CICAT functional capabilities include use of open source ATT&CK™ and CVE™ data, cyber analytics, and a web-based user interface for initiating scenario generation and reviewing scenario reports. Potential applications of scenario generation include cyber assessments, defensive cyber operations, cyber awareness training. Additionally, CICAT provides a framework for cyber threat modeling and experimentation through its ability to import supplemental TTP and threat actor capability data.

6 References/Bibliography

- [1] IAEA, "Enhancing Computer Security Incident Analysis at Nuclear Facilities, CRP J02008, <https://www.iaea.org/projects/crp/j02008>
- [2] MITRE, "Adversary Tactics, Techniques, and Common Knowledge (ATT&CK™)", <https://attack.mitre.org/>
- [3] MITRE, "Common Vulnerabilities and Exposures (CVE™)", <https://cve.mitre.org/>
- [4] Richberg, James, "A Common Cyber Threat Framework: A Foundation for Communication", ODNI, 2018, https://www.dni.gov/files/ODNI/documents/features/ODNI_Cyber_Threat_Framework_Overview_UNCL_20180718.pdf
- [5] MITRE, "Common Attack Pattern Enumeration and Classification (CAPEC)", <https://capec.mitre.org/>
- [6] IAEA, "Deployment, Use, and Maintenance of the Design Based Threat", Implementation Guide, NSS No. 10, 2009.
- [7] IAEA, Advanced PWR Simulator (Asherah), <https://www.iaea.org/topics/nuclear-power-reactors/nuclear-reactor-simulators-for-education-and-training/advanced-pwr-simulator>
- [8] DoD, "Mission Assurance Strategy", April 2012, https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf
- [9] MITRE, "Crown Jewel Analysis (CJA)", <https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis>
- [10] MITRE, CALDERA, <https://www.mitre.org/research/technology-transfer/open-source-software/caldera>
- [11] MITRE, "Threat Assessment and Remediation Analysis (TARA)", <https://www.mitre.org/publications/technical-papers/threat-assessment-and-remediation-analysis-tara>
- [12] Alexander, Otis, "ICS ATT&CK™", MITRE, December 2017, <https://www.acsac.org/2017/workshops/icss/Otis-Alexander-ICS,%20Adversarial%20Tactics,%20Techniques.pdf>

This page intentionally left blank.

Appendix A

Appendix A Comparison with Manually Developed Scenarios

In 2018 MITRE collaborated with University of Massachusetts (UML) Nuclear Engineering department to develop cyber attack scenarios. MITRE staff with expertise in cyber security and adversary tactics and techniques regularly met to discuss attack scenarios with graduate students from UML. This activity spanned several months and produced 24 scenarios in total. Interest in automating this activity was the impetus for developing CICAT.



Figure 14 MITRE / UML scenario team, with visiting IAEA and INL members

Hand Crafted Scenarios

Cyber attack scenarios developed manually by the MITRE / UML scenario team are discussed below. This section also provides comparison between manual and automated scenario production.

CDBT-001: Boiler Level / Pressure Control System DoS

An opportunist, financed by a Nation state, seeks to disrupt plant operations. The adversary achieves their goal by targeting the Boiler Level / Pressure Control System. The adversary enters through a temporary network connection and targets a Siemens S7-1200 PLC by exploiting ICSA-14-079-01. This causes the PLC to enter defect mode, a failure in the Boiler level/pressure control system, and an unscheduled plant shutdown to reset the PLC configuration and investigate. As a result, Primary and Secondary Loop Reactor Cooling Functions are degraded.

Because the consequences of the attack are Low and the likelihood of a successful attack is Moderate, the risk is Low. Possible mitigations include controls restricting temporary network connections and continuous network monitoring.

CDBT-002: Malicious PHTS PLC Configuration

A disgruntled employee, motivated by actual or perceived wrongdoing, seeks to exact revenge on their employer. The adversary achieves their goal by targeting the primary heat transport system. The adversary enters through an operator data entry field and targets a pressure relief valve by exploiting their legitimate employee privileges to push a malicious configuration to a PLC. This causes altered PLC setpoint(s), safety system actuation, and potentially a plant shutdown.

As a result, Primary Loop Reactor Cooling Functions are degraded. Because the consequences are low and the likelihood of a successful attack is low, the risk is very low. Possible mitigations include restoring PLC configuration from a baseline, enforcing the principle of least privilege, implementing a 2-person rule for critical operations, and insider threat awareness training for all staff.

CDBT-003: Malicious Turbine High Pressure Oil System Configuration

A single issue terrorist, motivated by their anti-nuclear views, seeks to negatively impact public sentiment on nuclear energy. The adversary achieves their goal by targeting the Turbine and turbine high pressure oil system. The adversary enters through a user account and targets a Siemens S7-300 or S7-400 PLC by exploiting ISCA-16-348-05D. This causes an unauthorized change to PLC configuration to over pressurize turbine oil, turbine trip, flash ignition of turbine oil, plant shutdown for repairs, and news that impacts public sentiment on plant security and safety. As a result, Secondary Loop Cooling Functions are degraded.

Indicators of compromise include unauthorized use of port 102/TCP (ISO-TSAP) or Profibus, excessively high turbine bearing oil pressure, and turbine trip. Because the consequences are high, and the likelihood of a successful attack is low, the risk is moderate. Possible mitigations include continuous network monitoring, applying software patches in a timely manner, and operator or manual mode intervention.

CDBT-004: Theft of Sensitive Corporate Data

An organized crime syndicate, motivated by financial gain, seeks to steal sensitive corporate data for resale. The adversary achieves their goal by attacking the Corporate IT Network. The adversary enters through compromised user credentials by installing a keylogger. This causes a keylogger to be inadvertently installed to a corporate laptop, theft of administrator credentials, exfiltration of sensitive corporate data, and the sale of sensitive data to a 3rd party or held for ransom.

Indicators of compromise include malware signatures on corporate network, bulk transfer of encrypted data to external IP addresses, and authorized user access during off hours. Because the consequences are moderate and the likelihood of a successful attack is moderate, the risk is moderate. Mitigations include antivirus and vulnerability scans, continuous network monitoring, security awareness training, and use of 2-factor authentication.

CDBT-005: Plant Data Historian Ransomware Infection

An organized crime syndicate, motivated by financial gain, seeks to extort money. The adversary achieves their goals by attacking the Plant Data Historian. The adversary enters through a

temporary network connection and targets the Cogent DataHub software by exploiting CVE-2014-3789. This causes a malware transfer from a maintenance laptop to the plant data historian, encryption of historical plant sensor data until the ransom is paid, and degraded plant operations.

Indicators of compromise include encrypted data, a ransom note, and malware signatures.

Because the consequences of a successful attack are low and the likelihood of a successful attack is moderate, the risk is low. Possible mitigations include segmenting the corporate network for the control network, regular data backups, and patching software in a timely manner.

CDBT-006: In-Transit Theft of Nuclear Fuel

A Nationalist/Separatist group, motivated by their lack of nuclear weapons capabilities, seeks to steal nuclear fuel in a complex attack. The adversary achieves their goal by targeting a nuclear fuel transport truck. The adversary enters through the On-Board Diagnostic (OBD) port and targets the vehicle control system by exploiting ICS-ALERT-17-209-01. This causes a denial of service on the CAN bus, renders the truck inoperable, and allows the adversary to intercept the fuel shipment outside the plant security perimeter.

Indicators of compromise include loss of vehicle functionality and loss of communication with the truck. Because the consequences of a successful attack are very high and the likelihood of a successful attack is very low, the risk is moderate. Possible mitigations include restricting and monitoring access to fuel transport trucks, ensuring maintenance laptops used to service the vehicles enforce cyber hygiene, and ensuring security forces provide adequate protection during transport.

CDBT-007: Remote Access Tool Implantation

A Nation State actor, motivated by the desire to achieve political, military, or espionage goals, seeks to establish clandestine monitoring of plant operations and establish persistent backdoor access. The adversary achieves their goal by targeting the corporate IT network. The adversary enters through a malicious software patch (watering hole attack) and targets a backup server by exploiting ICS-ALERT-14-176-02A. This causes a remote access tool (RAT) to be implanted during a routine software upgrade, allows the adversary to remotely monitor NPP networks and operations, and gives the adversary a staging point for future reconnaissance and/or sabotage.

Indicators of compromise include HAVEX malware signatures and encrypted traffic to known malicious IP addresses. Because the consequences are low and the likelihood of a successful attack is moderate, the risk is low. Possible mitigations include network monitoring, validation of software images, maintaining a trusted supply chain, and strong configuration management.

CDBT-008: Insider Attack on Boiler Level / Pressure Control System

A disgruntle employee, motivated by perceived or actual wrongdoing, seeks to exact revenge on their employer. The adversary achieves their goal through attacking the Boiler level/ pressure control system. The adversary enters through an engineering workstation and targets a Siemens S7-1200 PLC by exploiting CVE-2014-5074 and CVE-2016-2200. This causes a DoS on the targeted PLC, disrupts the ability to maintain proper boiler level, causes a reactor stepback, and causes an unscheduled plant shutdown.

As a result, Primary and Secondary Loop Reactor Cooling Functions are degraded. Indicators of compromise include crafted packets sent to the Boiler level/ pressure control system on TCP port 102 and irregular boiler level behavior. Because the consequences of a successful attack are low, and the likelihood of a successful attack is moderate, the risk is low. Possible mitigations include restricting access to engineering workstations, network monitoring, upgrading PLC firmware, and providing insider threat training for employees.

CDBT-009: Primary Heat Transport System Pressure Control DoS

A nation state actor, motivated to gain a military, political, or economic advantage, seeks to disrupt another country's power grid. The adversary achieves their goal by attacking the PHTS. The adversary enters through a temporary network connection and targets a Siemens S7-300/400 PLC by exploiting CVE-2016-9159. This causes unauthorized remote access and modifications to the PLC, disrupts PHT system pressure control, and ultimately causes an unscheduled plant shutdown.

Indicators of compromise include unexpected network access on PLC port 102/TCP and unauthorized changes to the PLC configuration. Because the consequences of a successful attack are moderate, and the likelihood of a successful attack is moderate, the risk is moderate. Possible mitigations include applying Protection-level 3 read/write protection and activating Field Interface Security in PCS 7 V9.0.

CDBT-010: Electrical Protection Equipment DoS

An organized crime syndicate, motivated by financial gain, seeks to disrupt plant operations. The adversary achieves their goal by targeting the electrical protection system. The adversary enters through a temporary network connection and targets a Siemens SIPROTEC 4 device by exploiting CVE-2015-5374. This causes a DoS on the affected device, removes the electrical protection offered by the device, and may cause electrical equipment damage.

Indicators of compromise include crafted packets on Port 50000/UDP. Because the consequences of a successful attack are high, but the likelihood of a successful attack is very low, the risk is low. Possible mitigations include upgrading firmware to V4.25, network monitoring for anomalous UDP packets, manual restart of the affected device, and implementing a failsafe design.

CDBT-011: Theft of Sensitive Operational Data

An opportunist, motivated by financial gain, seeks to conduct industrial espionage. The adversary achieves their goal by targeting the electrical system. The adversary enters through a compromise web page/application and targets a Siemens SIPROTEC 4 controller by exploiting CVE-2016-4784. This causes a sensitive data leak through the SIPROTEC 4 device, public disclosure of sensitive information, and loss of revenue during plant shutdown for investigation.

Indicators of compromise include unauthorized traffic on TCP Port 80, and sensitive information appearing in the public domain. Because the consequences are low and the likelihood of a successful attack is moderate, the risk is low. Possible mitigations include restricting network access via network segmentation, continuous monitoring of the process control network, and upgrading firmware to eliminate the vulnerability.

CDBT-012: Theft of Operational Data for Political Purposes

An opportunist, motivated by an environmentalist/anti-nuclear group, seeks to commit data theft to expose safety risks at the local NPP. The adversary achieves their goal by targeting the electrical system. The adversary enters through a remote vendor or partner VPN connection and targets Schneider Electric Telvent RTUs by exploiting CVE-2015-6485. This causes data exfiltration through the RTUs, strategic sensitive information release to show that plant security is “wide open,” and public opinion swayed in favor of shutting down the facility for security reasons.

Indicators of compromise include unauthorized outbound traffic from RTUs and sensitive information released to the public. Because the consequences of a successful attack are low and the likelihood of a successful attack is low, the risk is very low. Possible mitigations include minimizing network exposure for all control system devices, locate control system networks and remote devices behind firewalls, and upgrading the device firmware.

CDBT-013: Turbine Governing System DoS

A disgruntled employee, motivated by actual or perceived wrongdoing by their employer, seeks to disrupt plant operations. The adversary achieves their goals by attacking the turbine /generator system. The adversary enters through malware implanted on a USB thumb drive and targets a Siemens S7-1200 PLC by exploiting CVE-2013-2780. This causes a DoS on the PLC controlling turbine governing valves, loss of turbine governing control, activation of safety systems, and an unscheduled plant shutdown. As a result, Secondary Loop Cooling Functions are degraded.

Indicators of compromise include loss of turbine governing control and crafted packets on UDP port 161 (SNMP). Because the consequences of a successful attack are moderate and the likelihood of a successful attack is low, the risk is low. Possible mitigations include controls restricting use of removeable media, continuous network monitoring, and isolation of SNMP packets to separate device management network.

CDBT-014: Turbine Governing System DoS

A radicalized insider, motivated by their radical political/religious views, seeks to cause chaos and shutdown public services. The adversary achieves their goal by targeting the steam turbine governing system. The adversary enters through a temporary network connection and targets a Siemens S7-1500 PLC by exploiting CVE-2016-2200. This causes a DoS on the PLC responsible for turbine governing control, a loss of turbine governing functionality, an unscheduled plant shutdown, and unplanned safety system actuation. As a result, Secondary Loop Cooling Functions are degraded.

Indicators of compromise include crafted packets on Port 102/TCP (ISO-TSAP) and loss of turbine governing control. Because the consequences of a successful attack are low and the likelihood of a successful attack are moderate, the risk is low. Possible mitigations include controls restricting removeable media and continuous network monitoring.

Comparison of Hand Crafted and CICAT-Generated Scenarios

Similarities between hand crafted and CICAT-generated scenarios include identification of threat actor, targeted component, entry point, exploited vulnerability, and systemic effect(s) of

disruption. Differences include potential indicators of compromise (IOC), mitigations, and threat actor intent, which are absent in CICAT-generated scenarios. Other differences include:

- CICAT-generated scenarios provide impact scores rather than assessed risk.
- Hand crafted scenarios evaluate a single entry point. CICAT-generated scenarios evaluate multiple entry points.
- Hand crafted scenarios identify a single vulnerability of the targeted component. CICAT-generated scenarios list known CVEs associated with the target and each component in the attack path.
- Hand crafted scenarios provide no detail on the attack path or the tactics and techniques used by the adversary to gain access to and compromise the target. Generated scenarios identify attack paths and a sequence of ATT&CK™ TTPs based on threat actor capabilities and ODNI objectives.
- The MITRE and UML teams met regularly for several months to develop cyber attack scenarios manually. Using CICAT, the bulk of the activity is to prepare an infrastructure model for input to the CICAT tool. Scenario generation takes milliseconds once the infrastructure model is developed.

Hand-crafted cyber attack scenarios lack details found in CICAT-generated scenarios and take significantly more time to produce. Where generated scenarios lack details provided in hand-craft scenarios, efforts are planned to extend CICAT to support analytics-based mitigation selection and to leverage indicator data produced during the CNL Workshop in 2019.

Appendix B Design Basis Threat Considerations

In 2009 IAEA published NSS 10, “Development, Use and Maintenance of the Design Basis Threat”, as an implementation guide for member states regarding physical protection of nuclear materials and nuclear facilities. This document defines a Design Basis Threat (DBT) as a “comprehensive description of the motivation, intentions, and capabilities of potential adversaries against which protection systems are designed and evaluated.”[6]

NSS 10 focuses on preventing adversaries from removing nuclear materials or performing sabotage, and discusses the need for member states to enlist their national intelligence agencies to collect credible data on adversary intentions and capabilities as a basis for developing DBTs.

In February 2018, IAEA hosted a technical review of draft changes to NSS 10 that included an updated methodology for conducting threat assessments and development of DBTs covering cyber related threats in addition to physical threats. Draft NSS 10 considered blended attacks in which attacks on computer-based systems were conducted in conjunction with physical attacks.

The draft did not discuss cyber attacks specifically intended to achieve cyber effects, e.g., exfiltration of data, installation of malware (except through supply chain vectors), denial of service, etc. The draft also did not consider alternative sources of threat intelligence, e.g., open source, community based intelligence reporting, etc. A revised NSS 10 has yet to be published.

Application of ATT&CK™

CICAT’s use of ATT&CK™ suggests an alternative way to represent threat actor intent and capability in the context of DBT development. In the ATT&CK™ model, threat actor intent is represented in terms of the industry sector(s) a threat actor is known to target, without discussion of underlying motivations or specific (actionable) details. Threat actor capability is defined in terms of TTPs, malware, and tools each threat actor is attributed to using. This approach supports analytics, which can be used to characterize threat actor sophistication and other relevant metrics.

Use of ATT&CK™ in DBT development would leverage a standardized representation of adversary cyber capabilities in terms of the TTPs, malware, and tools a threat actor applies, regardless whether the adversary’s objective is to achieve physical or cyber effects.

Additionally, reliance on national intelligence agencies to provide credible threat information ignores other relevant sources, e.g., community based threat information sharing, etc. National intelligence agencies may not always provide high confidence reporting. Credible cyber threat intelligence, i.e., data validated by multiple, credible sources, may be available through commercial and open source reporting.

Several commercial and open source software tools for managing and analyzing cyber threat intelligence are available and use open source and/or community-based intelligence reporting. A DBT developed to characterize cyber threat actors, capabilities, etc. would benefit from use of software tools as well as exchange of community based, commercial, and open source cyber threat intelligence reporting.

Appendix C Abbreviations and Acronyms

ATT&CK™	Adversary Tactics, Techniques, and Common Knowledge
BLC	Boiler Level Control
BPC	Boiler Pressure Control
CAPEC	Common Attack Patterns Enumeration and Classification
CCW	Condenser Cooling Water
CICAT	Critical Infrastructure Cyber Analysis Tool
CJA	Crown Jewel Analysis
CNL	Canadian Nuclear Laboratories
COTS	Commercial Off-the-Shelf
CRP	Coordinated Research Program
CSW	Common Service Water
CVE™	Common Vulnerabilities Enumeration
DBT	Design Based Threat
DCO	Defensive Cyber Operations
DMZ	Demilitarized Zone
DoD	Department of Defense
DoS	Denial of Service
HMI	Human Machine Interface
HPRSW	High Pressure Recirculating Service Water
HIL	Hardware-in-the-Loop
IAEA	International Atomic Energy Agency
ICS/SCADA	Industrial Control Systems / Supervisory Control and Data Acquisition
INL	Idaho National Laboratories
IoC	Indicator of Compromise
IP	Internet Protocol
IT	Information Technology
JSON	JavaScript Object Notation
LAN	Local Area Network
LPSW	Low Pressure Service Water
MC	Mission Critical
ME	Mission Essential
MS	Mission Support
NMAC	Nuclear Materiel Accounting Control
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NSS	Nuclear Security Series
OBD	On-Board Diagnostic
ODNI	Office of the Director of National Intelligence
PHTS	Primary Heat Transport System

PLC	Programmable Logic Controllers
PWR	Pressurized Water Reactor
RAT	Remote Access Tool
RCP	Reactor Coolant Pump
RTU	Remote Terminal Unit
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSE	Systems Security Engineering
STIX/TAXII	Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information
TARA	Threat Assessment and Remediation Analysis
TCP	Transmission Control Protocol
TRACE	Traversal-drive Risk Assessment of Composite Effects
TTP	Tactics, Techniques, Procedures
UDP	User Datagram Protocol
UL	Underwriter Laboratories
UML	University of Massachusetts Lowell
URC	Unacceptable Radiological Consequences
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTK	University of Tennessee Knoxville
VPN	Virtual Private Connection
XML	eXtensible Markup Language