28th Annual INCOSE international symposium

Washington, DC, USA
July 7 - 12, 2018

Matthew Curreri.	Lockheed Martin Rotary and Mission Systems
Ambrose Kam.	Lockheed Martin Rotary and Mission Systems
Carl Hein.	XSIM LLC

Modeling Cyber Threats with SysML

Agenda

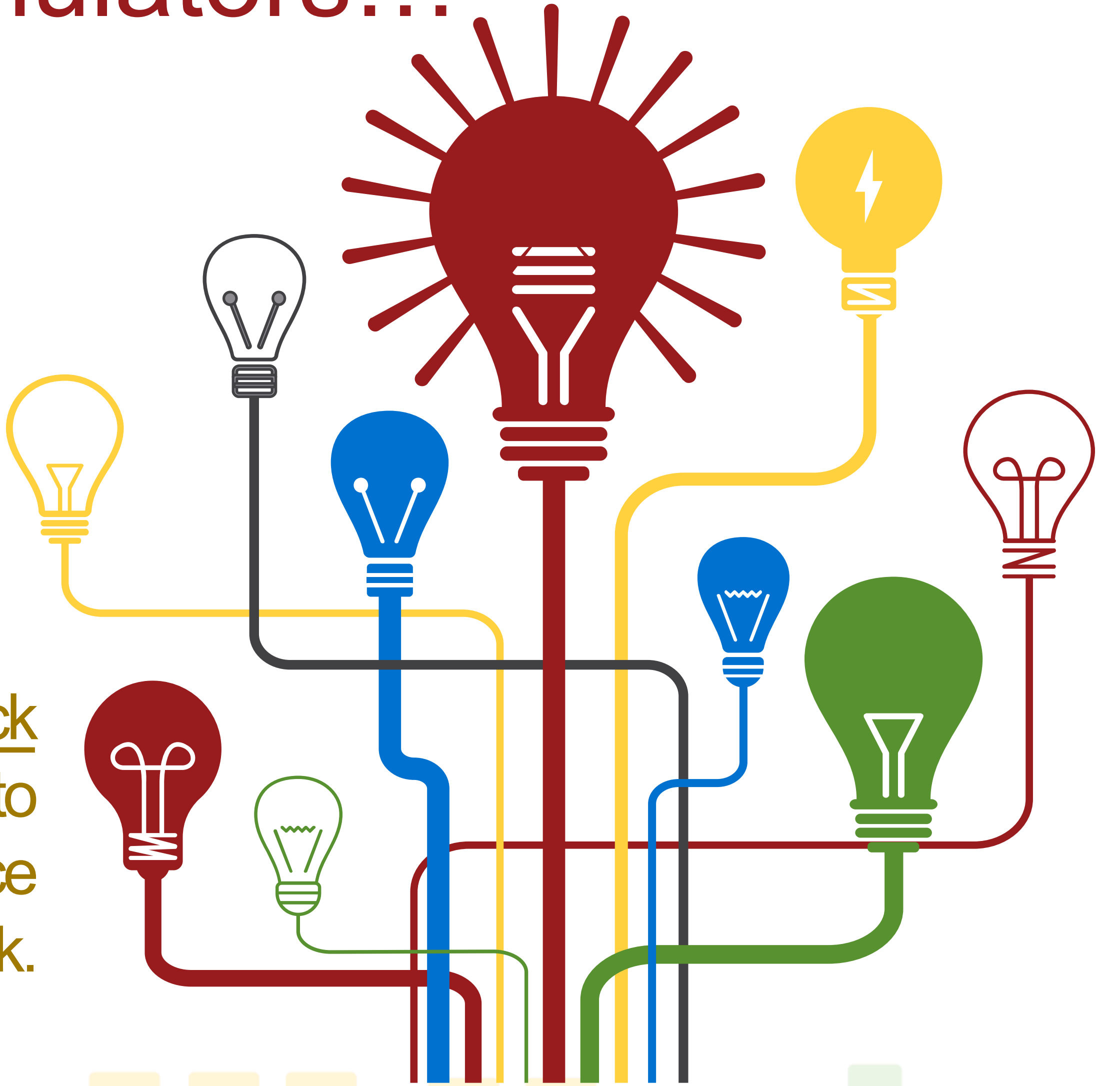
- System Modeling
- Cyber Effects Modeling
- Model Execution

Idea! Bridging the gap between SysML and External Simulators…

Doing More!

SysML Partnership (SysML to Cyber).

Use Internal Block Diagrams (IBD) to define an instance of a Cyber Network.



Jelly Framework for describing Network Topologies to support Cyber

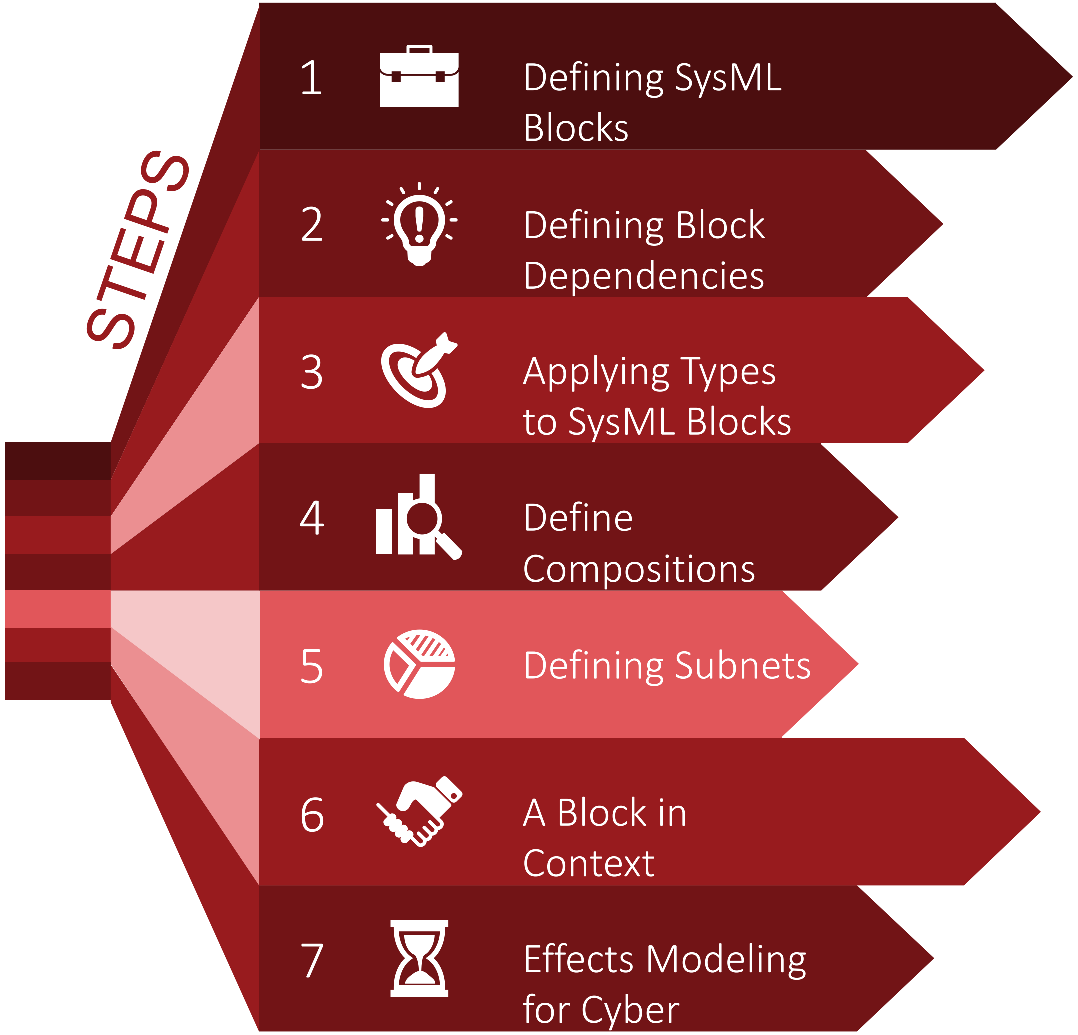
Develop an interface between SysML and External Simulation Tools (CSIM)

System Architecture Simulator.

System Modeling for Cyber Environment

SysML Cyber Environment

Developing a Network
Multi-Level
Cyber Topology.



STEPS

1 Defining SysML Blocks

2 Defining Block Dependencies

3 Applying Types to SysML Blocks

4 Define Compositions

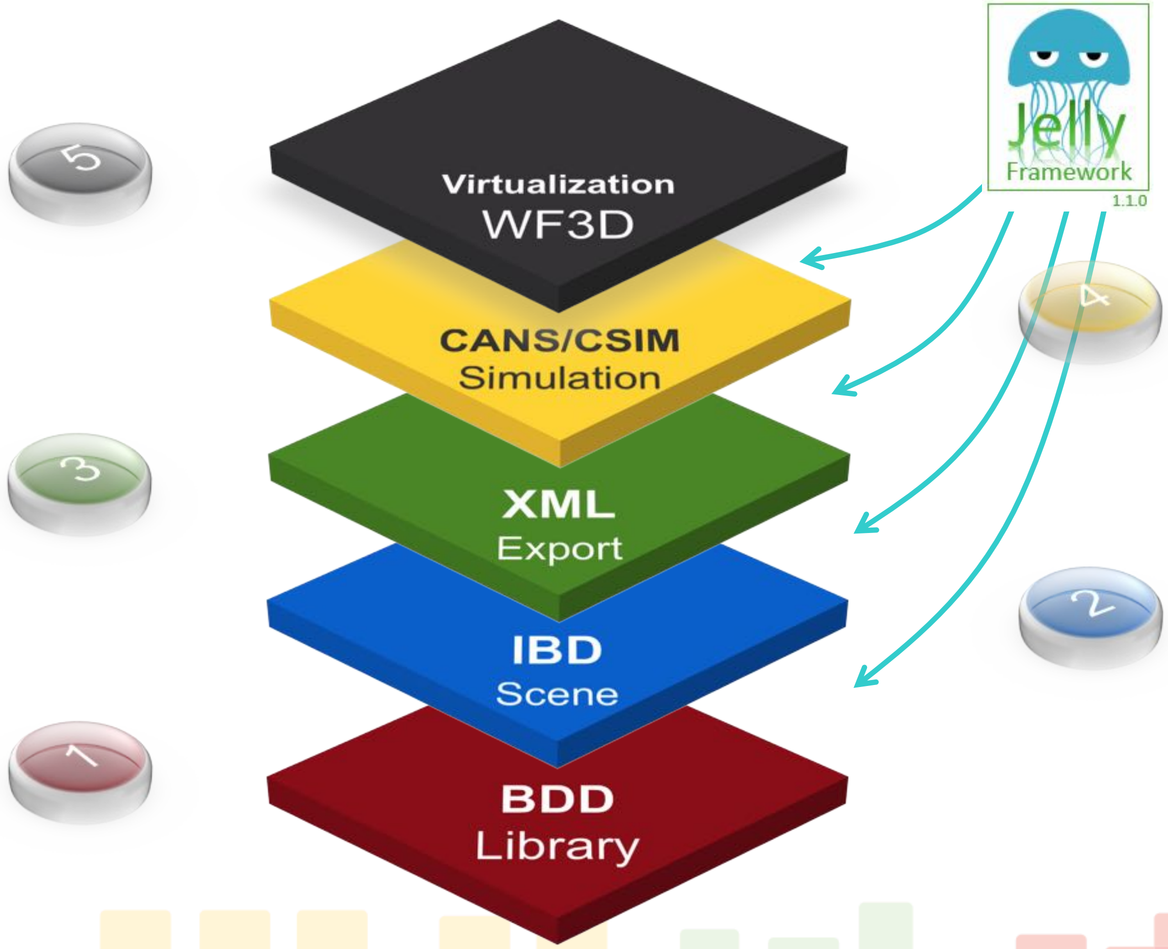
5 Defining Subnets

6 A Block in Context

7 Effects Modeling for Cyber

Jelly Framework Stack

Jelly fills in and bridges the gaps between the layers.



Virtualization of the Network and displaying the results of Simulation

Exporting your Network Topology to XML.

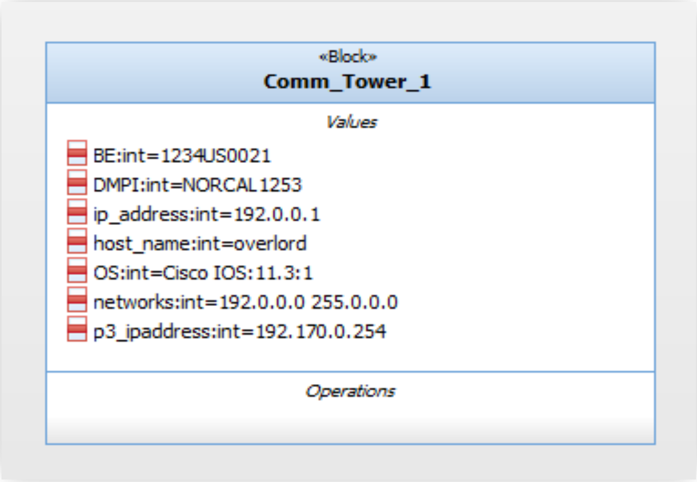
Block Definition Diagram (BDD) Library creation is entry point for your SysML design.

CANS (Cyber Attack Network Simulator) via CSIM runs the performance modeling algorithm.

Places your design in context using SysML IBD.

1. Defining SysML Blocks

- Using Structural SysML diagrams (BDD & IBD) to populate Blocks with Node attributes.
- Each platform is a computer with network capabilities.



«Block»
Comm_Tower_1

Values

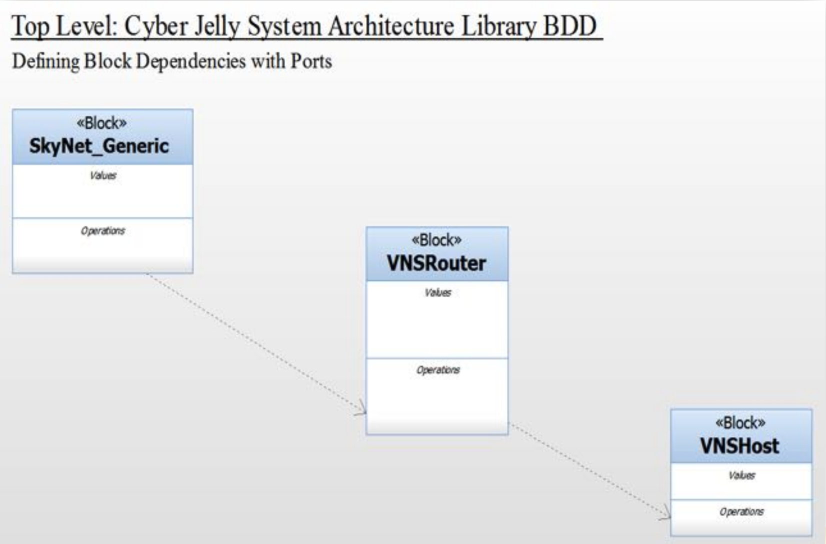
BE:int=1234US0021
DMPI:int=NORCAL1253
ip_address:int=192.0.0.1
host_name:int=overlord
OS:int=Cisco IOS:11.3:1
networks:int=192.0.0.0 255.0.0.0
p3_ipaddress:int=192.170.0.254

Operations

Lockheed Martin Image

2. Defining Block Dependencies

- Each network block or node is to be used as part of a VNS (Virtualized Network Service) which will be used to drive CSIM (Virtualized Network Simulator).
  - CSIM is a *re-useable general purpose discrete-event simulation* environment for modeling complex systems of interacting elements.
- A hierarchical dependency relationship is established to define the communication responsibilities:
  - Subnet *depends on* Router which *depends on* Host



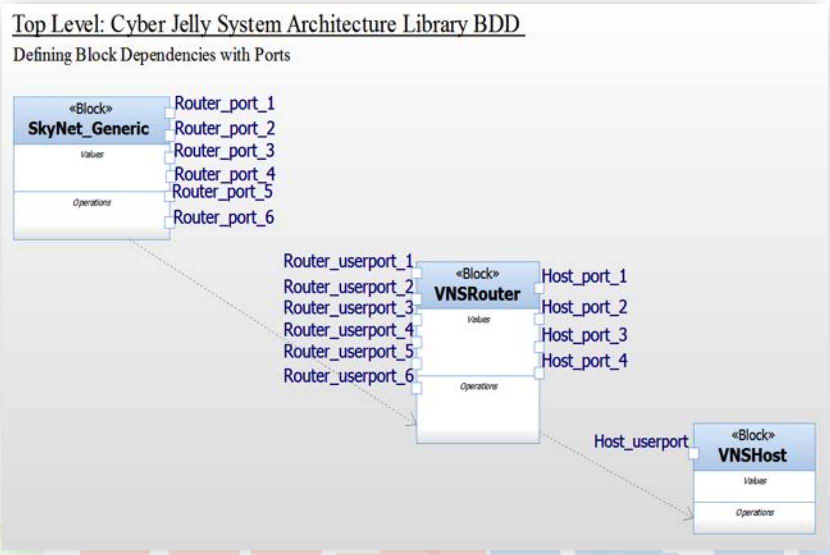
Top Level: Cyber Jelly System Architecture Library BDD

Defining Block Dependencies with Ports

Lockheed Martin Image

To create communication between SysML blocks a SysML port is applied.

SysML Blocks can have 1 to many ports each having 1 to many interfaces.



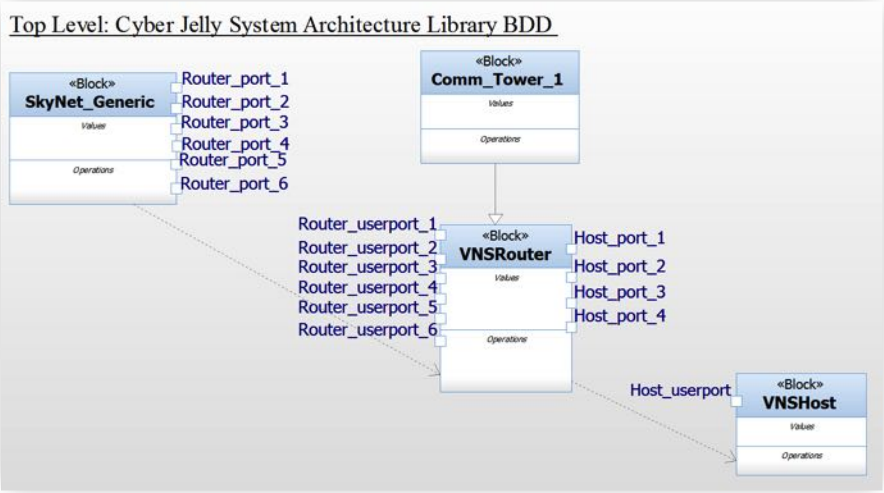
Top Level: Cyber Jelly System Architecture Library BDD

Defining Block Dependencies with Ports

Lockheed Martin Image

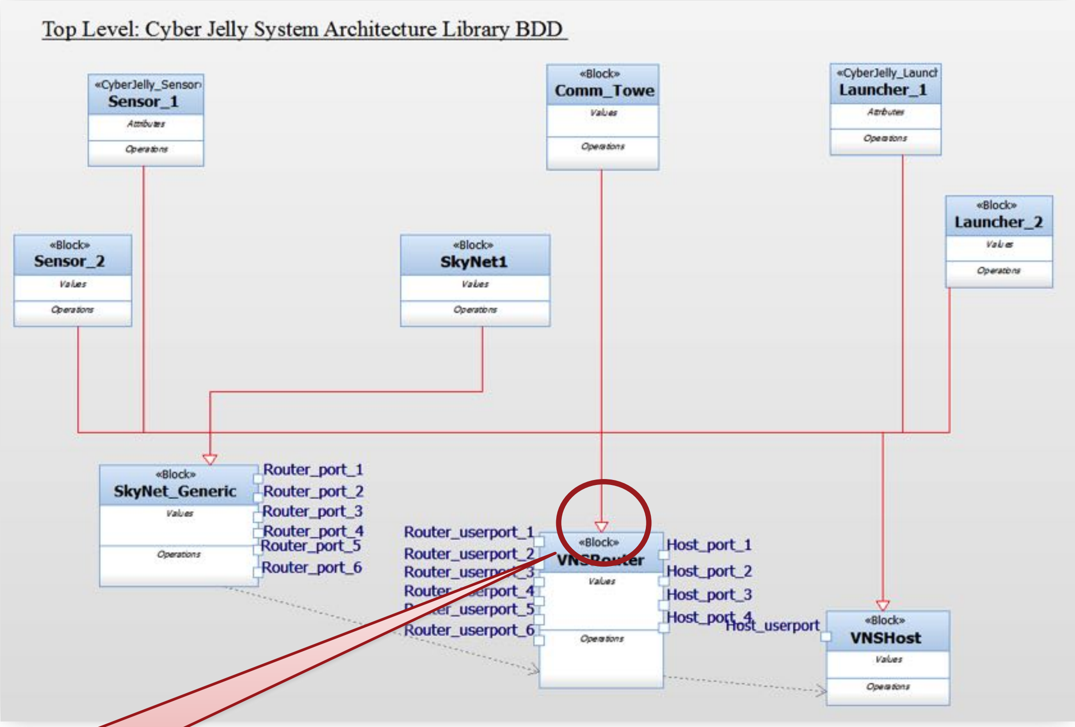
3. Applying Types to SysML Blocks

- Using Generalization or Inheritance relationships, associating types are applied to the SysML blocks, which the Child Block inherits all the contents of the Parent Block.



Lockheed Martin Image

Comm_Tower_1 inherits the VNSRouter contents



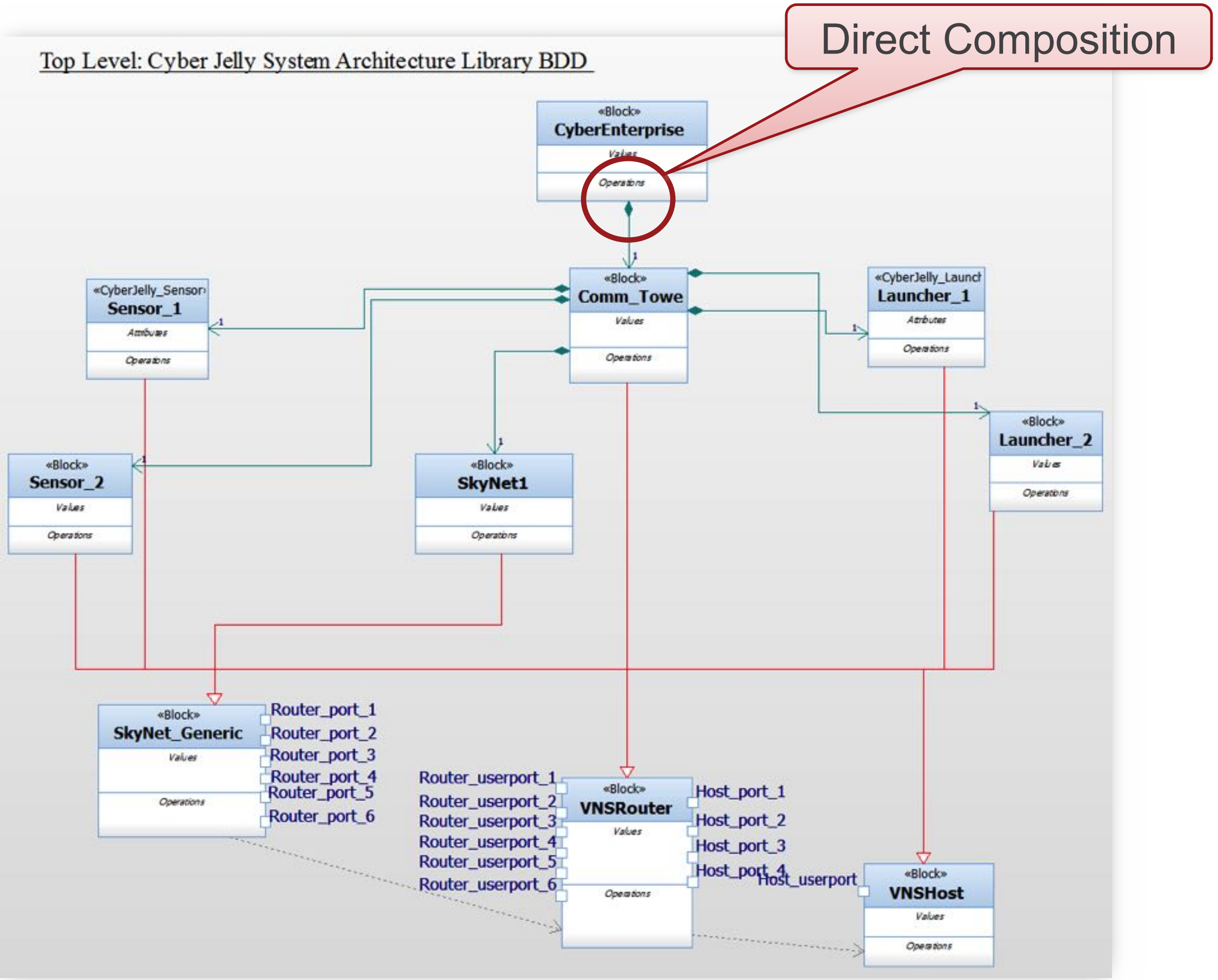
Generalization

Lockheed Martin Image

Applying to the rest of the Nodes

4. Define Compositions of SysML Blocks

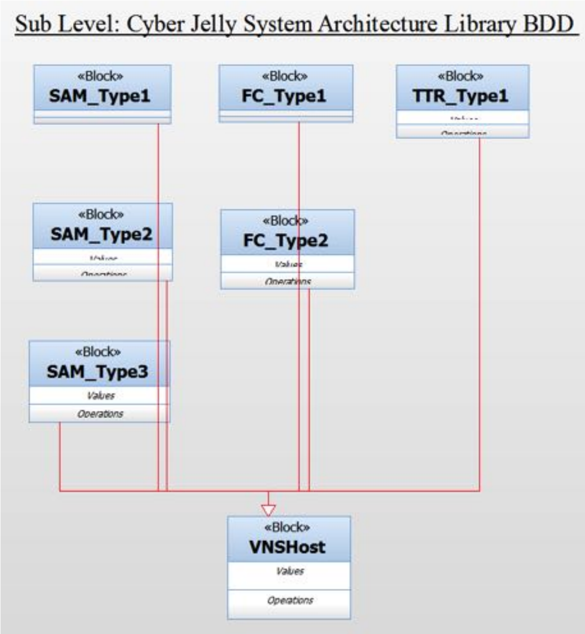
- Using Direct Composition relationship to grouping similar types of SysML Blocks into collections.
  - In the below example, all Network Nodes are parts of a Communication Tower which in turn constitutes a Cyber Enterprise.


Direct Composition

Lockheed Martin Image

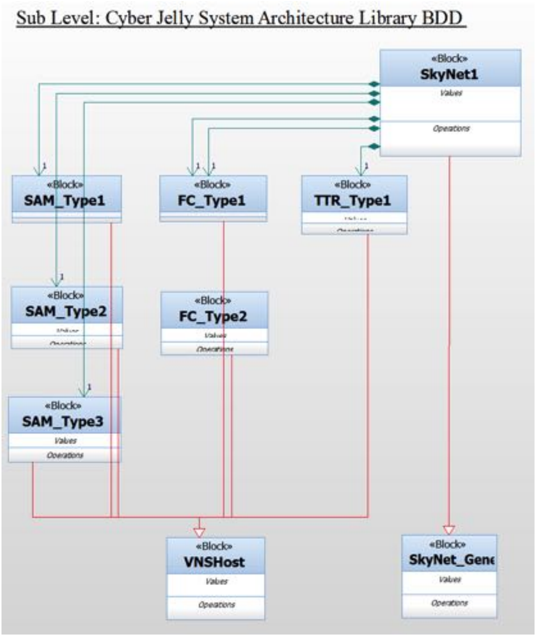
5. Defining Subnets

- If your network requires multiple levels or sub-networks, Jelly Framework can support these additional layers.
    - The same approach is used: Applying Inheritance and Direct Composition.



Lockheed Martin Image

Applying Inheritance

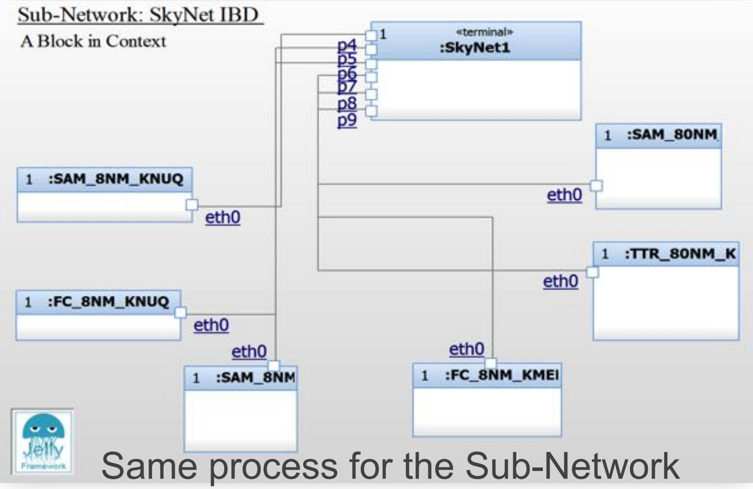


Lockheed Martin Image

Applying Direct Composition

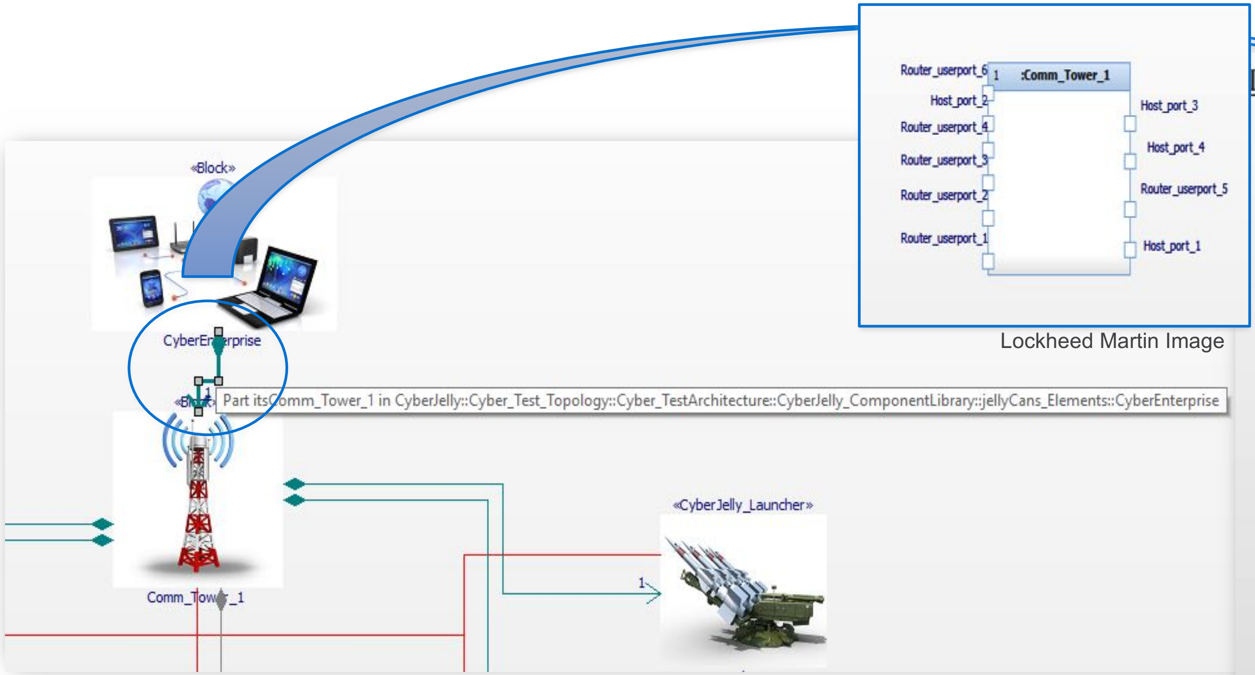
6. A Block in Context

- A IBD (Internal Block Diagram) is where the SysML block become parts or a Block in Context.



Same process for the Sub-Network

Lockheed Martin Image

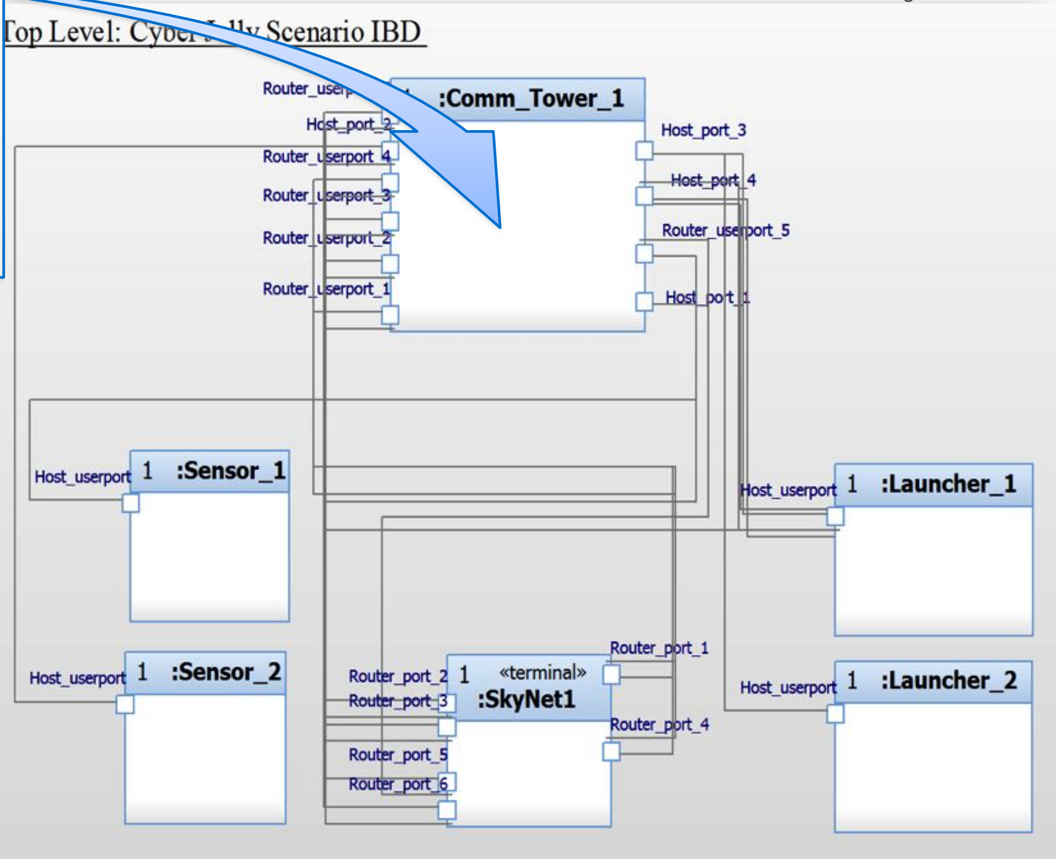


Part its Comm_Tower_1 in CyberJelly::Cyber_Test_Topology::Cyber_TestArchitecture::CyberJelly_ComponentLibrary::jellyCans_Elements::CyberEnterprise

Lockheed Martin Image

Lockheed Martin Image

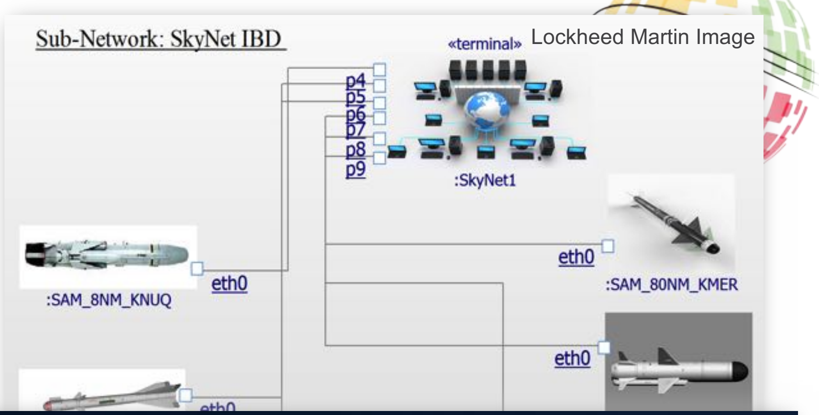
On the BDD, select the Direct Composition relationship

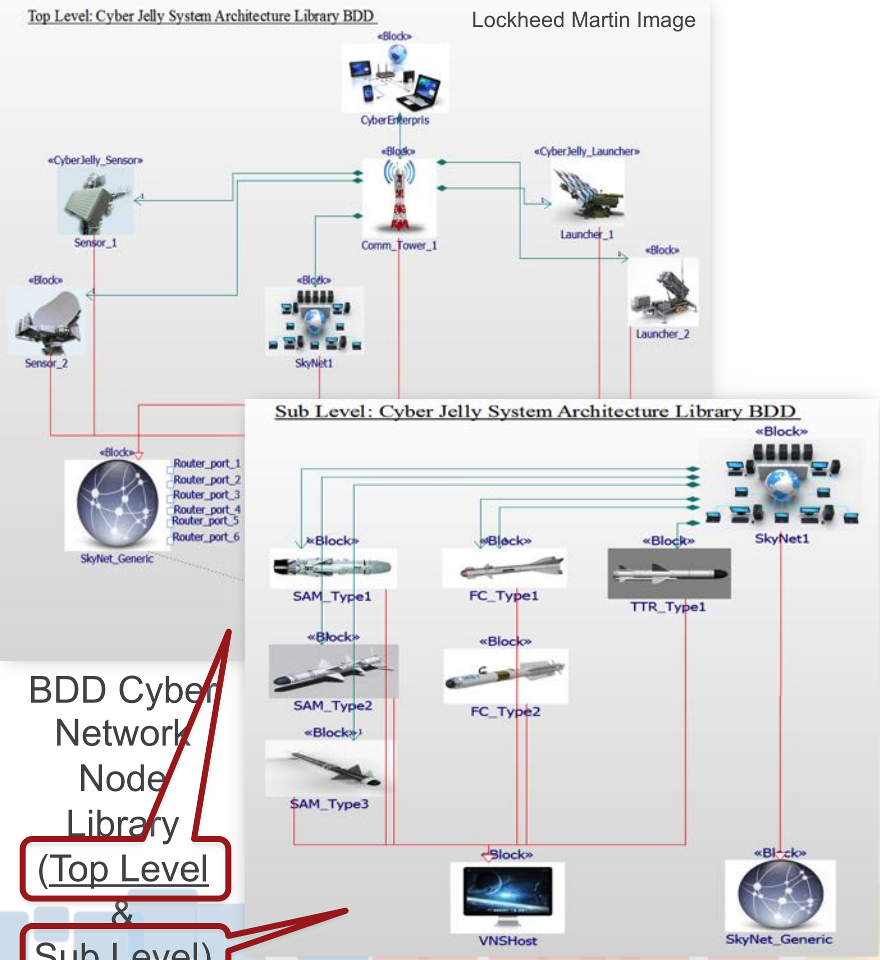


Lockheed Martin Image

A Touch of *Style*

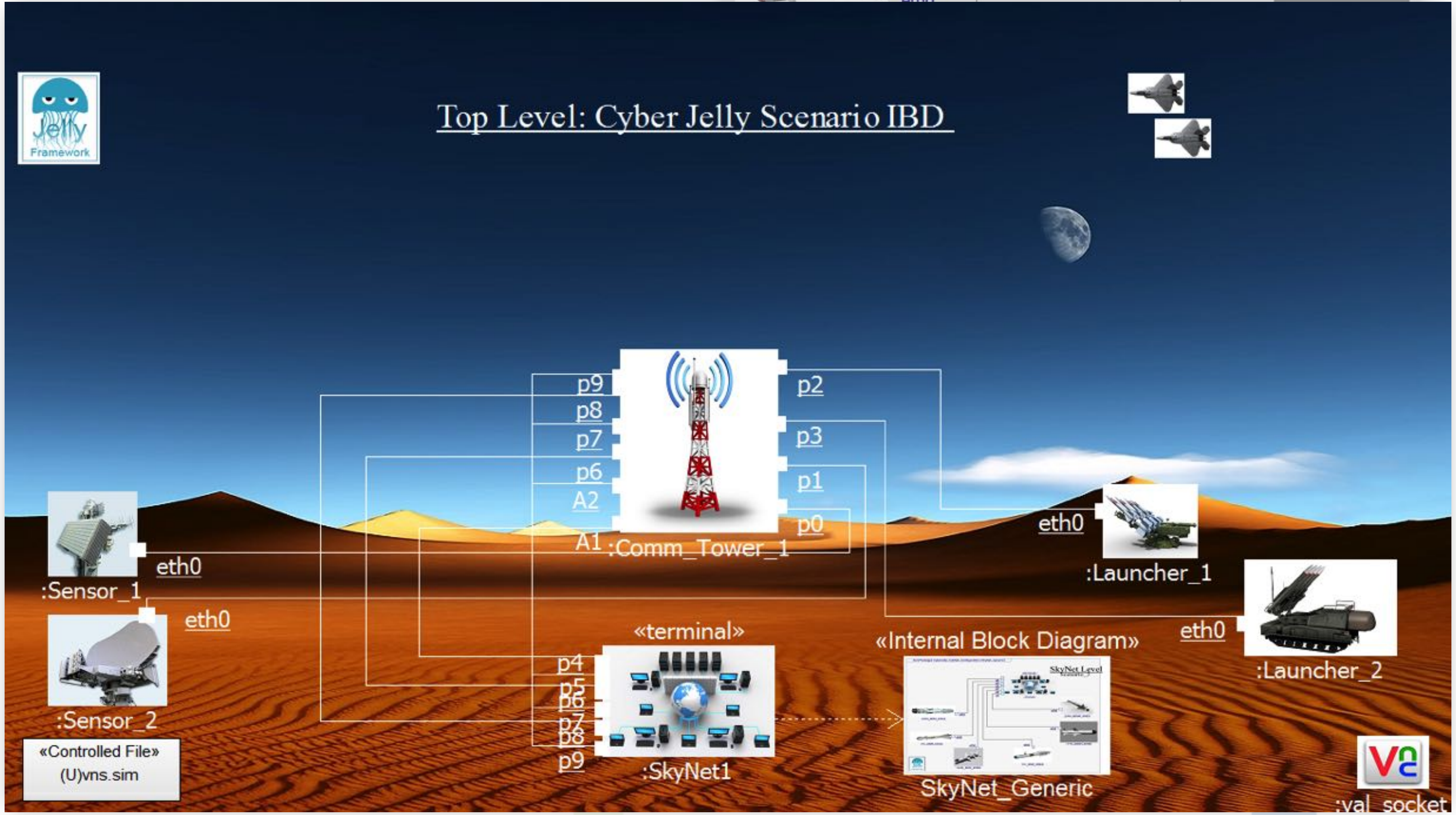
- Substituting the standard iconic Block images with realistic icons your audience or non SysML skilled client can get a more realistic understanding.





BDD Cyber Network Node Library (Top Level & Sub Level)

Lockheed Martin Image

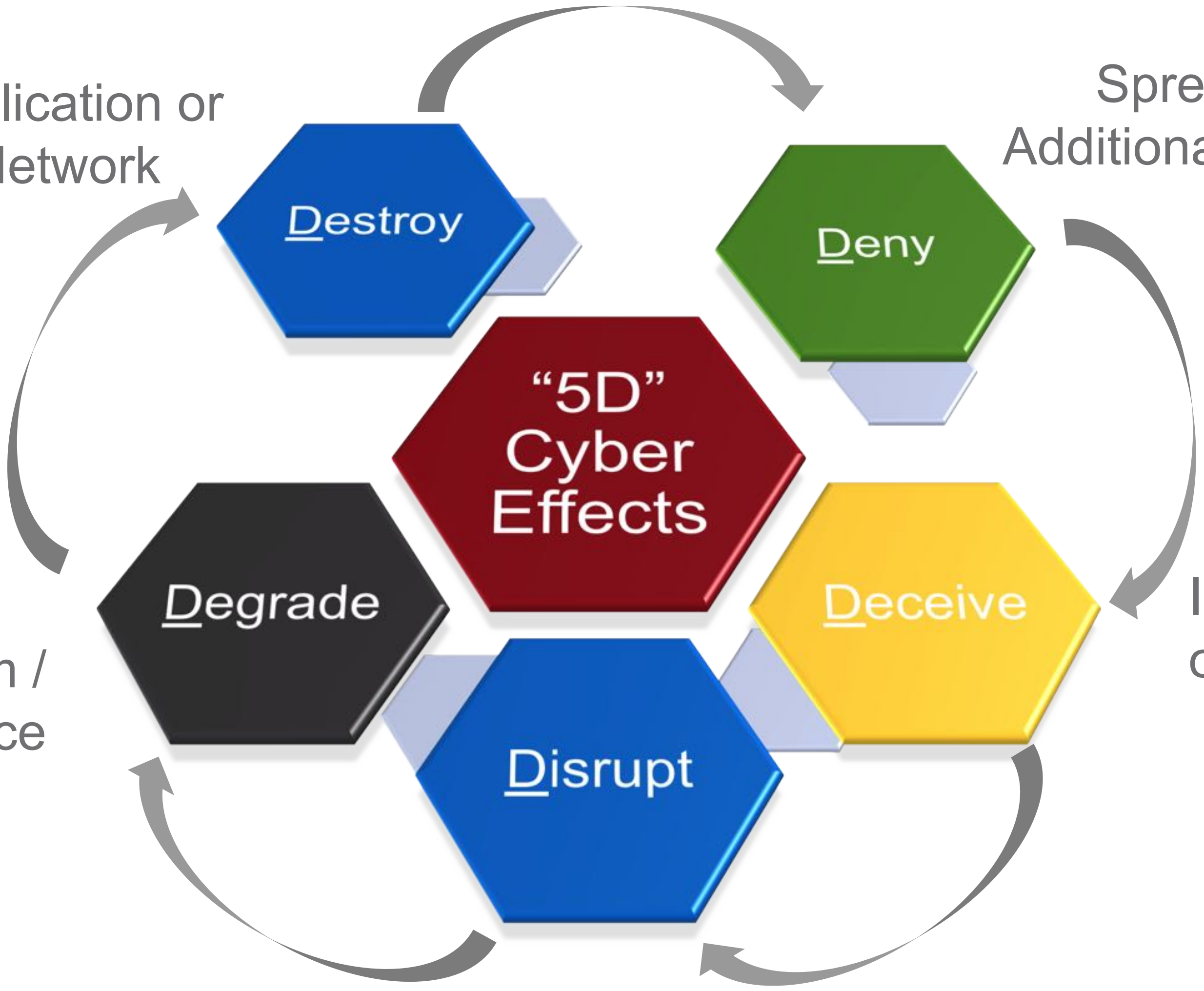


Lockheed Martin Image

Cyber Network Scenario IBD

Copyright © 2018 Lockheed Martin Corporation

7. Cyber Effects modeled by CANS



Disabling Application or Nodes or Network

Spreading Attack to Additional nodes on the Network

Inject False Information or Spoofing Data

Preventing Normal Operations

Reducing System / Node Performance

MODELING REPRESENTATIVE ATTACK PATTERNS

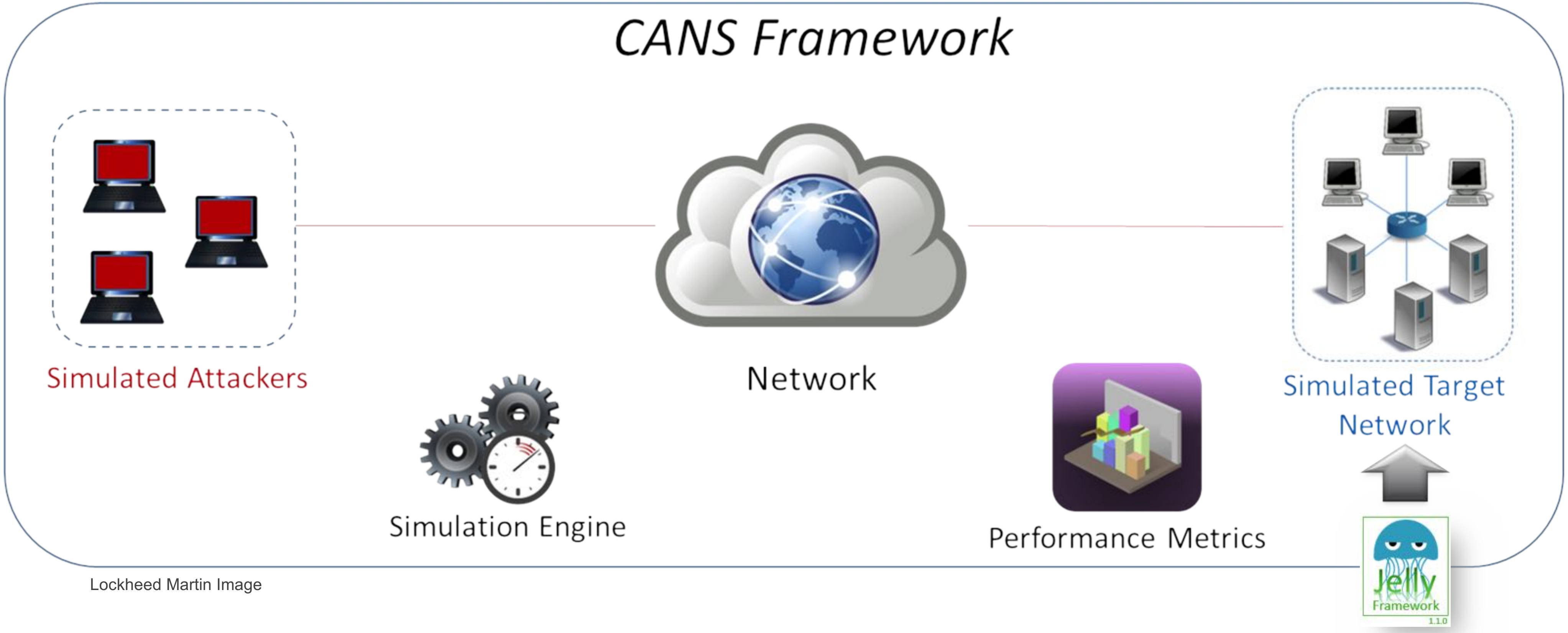
CAPEC Categories	Description*	Sample CAPEC ID*	Sample Exploits from NVD
Alter System Components	Alteration of components in a system to achieve a desired negative technical impact.	523 (Malicious Software Implanted), 532 (Altered Installed BIOS), 533 (Malicious Manual Software Update), 534 (Malicious Hardware Update), 538 (Open Source Libraries Altered), 578 (Disable Security Software)	CVE-2013-5364
Analyze Target	Analysis of system, protocol, message, or application to overcome protections, or as a precursor to other attacks. Dissecting applications, analysis of message patterns + protocols, or other methods. Discloses sensitive information / security configurations leading to further attacks to discover weaknesses.	28 (Fuzzing), 167 (White Box Reverse Engineering)	CVE-2017-2704
Deceptive Intervention	Malicious interactions to deceive and convince and take actions based on the level of trust. Often identified by the term "spoofing", these types of attacks rely on the falsification of the content and/or identify so target will incorrectly trust legitimacy of content.	145 (Checksum Spoofing), 194 (Fake the Source of Data), 195 (Principal Spoof), 473 (Signature Spoof)	CVE-2005-4437
Exploit of Authentication	Attacker exploits weaknesses, limitations, and assumptions in mechanisms used to manage identity and authentication. Leads to subversion of in the identify of all interacting entities. Exploits assumptions and overconfidence in strength of authentication mechanisms.	4 (Using Alternative IP Address Encodings), 16 (Dictionary-based Password Attack), 20 (Encryption Brute Forcing), 21 Exploitation of Trusted Credentials), 44 Overflow Binary Resource File), 50 Password Recovery Exploitation), 114 (Authentication Abuse), 115 Authentication Bypass)	CVE-2017-7905
Gathering Information	Gathering, collection, and theft of information through a variety of methods including active querying & passive observation. Aids adversary in inferences of weaknesses, vulnerabilities, or techniques assisting objectives. Prepares for other attacks, or info-collection as end goal.	158 (Sniff Network Traffic), 170 (Web Application Fingerprinting), 292 (Host Discovery), 300 (Port Scan), 309 (Network Topology Mapping), 310 (Scanning for Vulnerable Software), 312 (Active OS Fingerprinting, 315 (TCP/IP Fingerprinting Probes), 541 (Application Fingerprinting),	CVE-2017-7200

CANS has the capability to parse and extract threat metadata from the National Vulnerability Database (NVD) and Common Attack Pattern Enumeration and Classification (CAPEC)

*Extracted from capec.mitre.org/

**Extracted from https://nvd.nist.gov/vuln/search

Cyber Attack Network Simulator Features



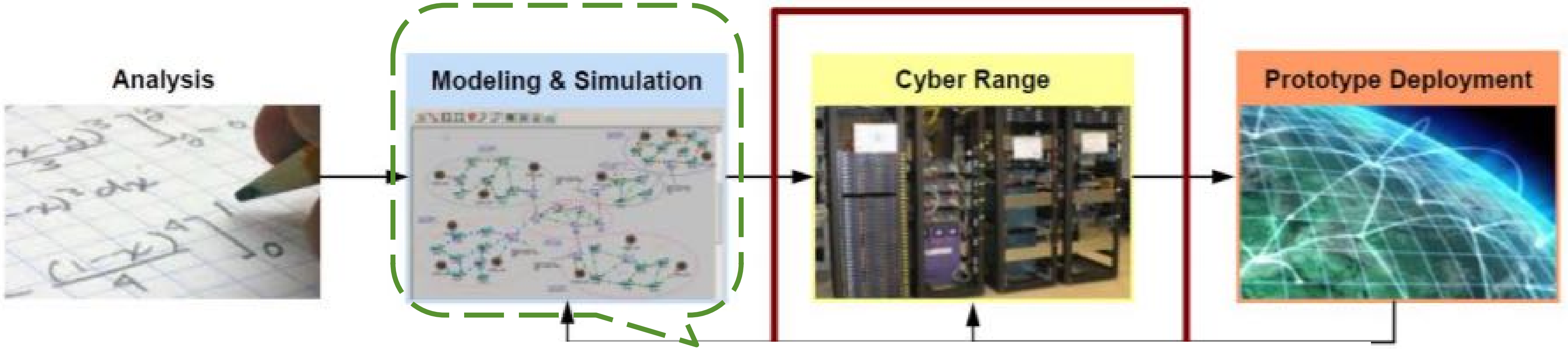
Lockheed Martin Image

JellyStudio SysML

Cyber Attack Network Simulator (CANS) is a discrete event simulation that allows analysts to study the effect of various cyber events against a model of a planned or operational network system.

CANS Models Cyber Events and Their Impacts to a System

Advantages using Modeling & Simulation for Cyber



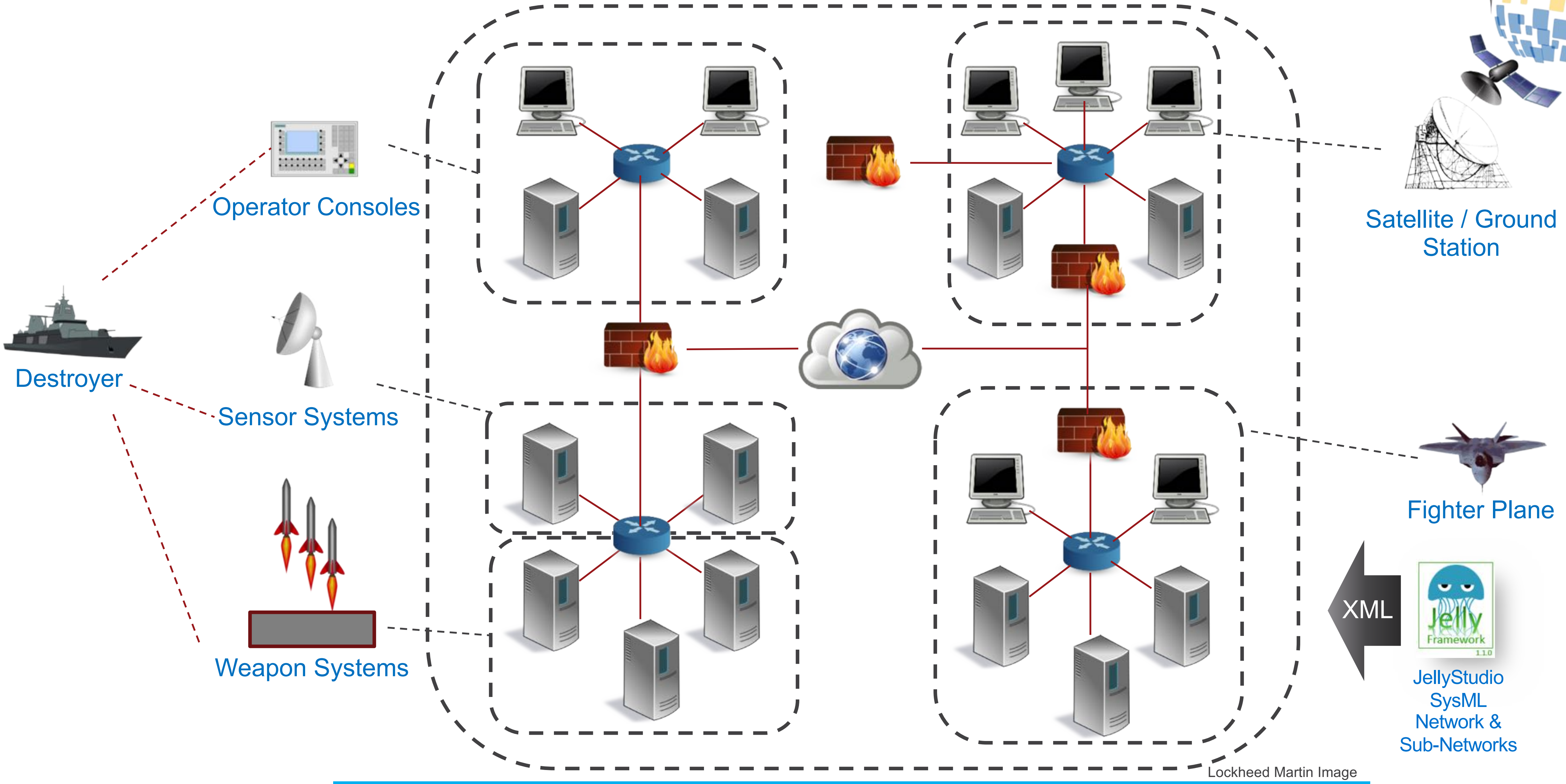
M&S Complements with lower Cost!

	Analysis	Modeling & Simulation	Cyber Range	Prototype Deployment
Fidelity	Low	Low	Moderate to High	High
Scalability	High	High	Moderate	Low
Cost	Low	Low	Moderate	High
Repeatability	N/A	High	Moderate to High	Low
Program Phase	Early	Early	Mid-term	Mid-term to Late

Lockheed Martin Image

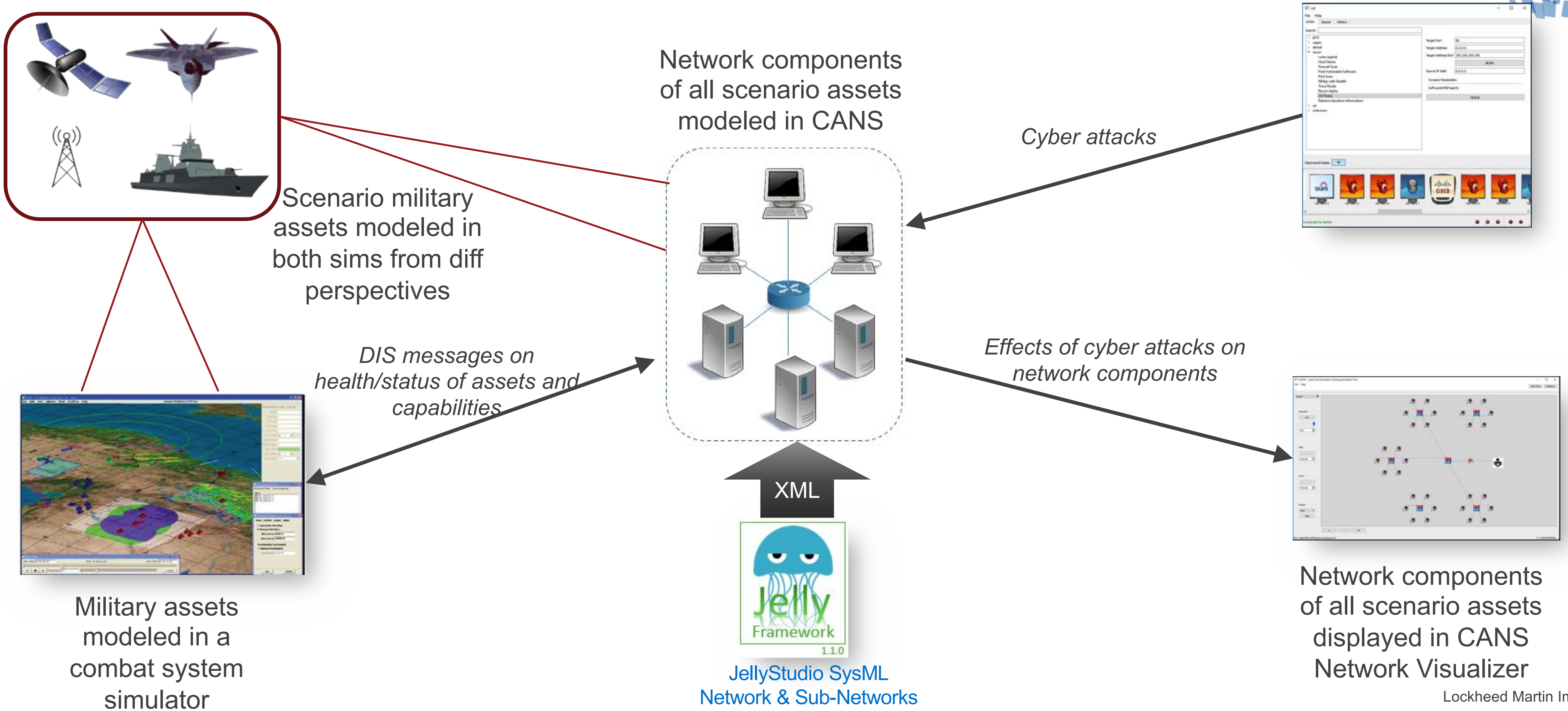
Effects-based Simulation <u>Complements</u> Higher Fidelity Cyber Range Equipment

CANS Network Types



CANS System Models are Highly Modular

Example Use Case: Degraded Sensor in a Combat System



Network components of all scenario assets modeled in CANS

Cyber attacks

Scenario military assets modeled in both sims from diff perspectives

DIS messages on health/status of assets and capabilities

Effects of cyber attacks on network components

XML

Military assets modeled in a combat system simulator

JellyStudio SysML Network & Sub-Networks

Network components of all scenario assets displayed in CANS Network Visualizer

Lockheed Martin Image

CANS helps simulate system effectiveness under cyber attack in combat scenarios

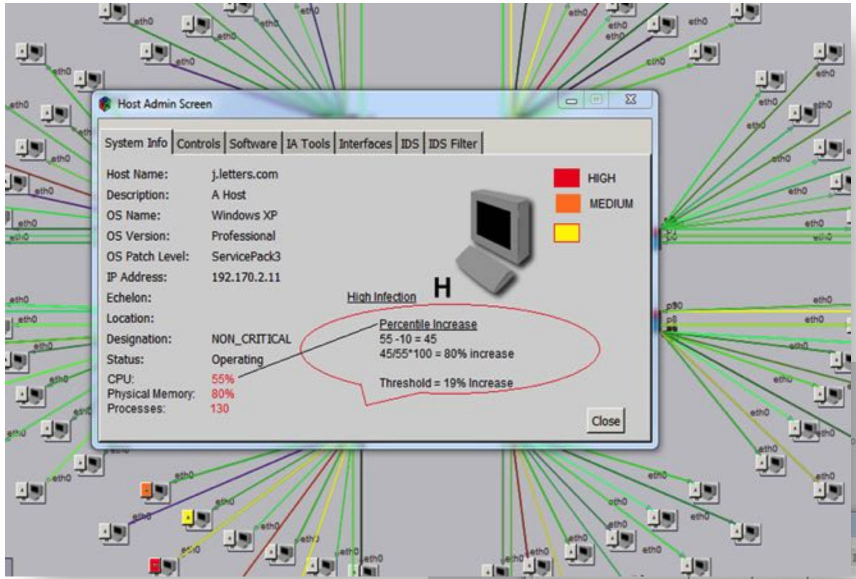
Cyber Attack Network Simulator (CANS) is a discrete event simulation that allows analysts to study the effect of various cyber events against a model of a planned or operational network system.

Host Node Modeling with SysML

- Easy of Use: Where the User can click on any node to visualize & manage the node's state

- Basic system info shows indicates OS and network information, obtained from the SysML model attributes!

- Users can manipulate these dynamically as the simulation runs.



Host Admin Screen

Host Name: j.letters.com
Description: A Host
OS Name: Windows XP
OS Version: Professional
OS Patch Level: ServicePack3
IP Address: 192.170.2.11
Echelon:
Location:
Designation: NON_CRITICAL
Status: Operating
CPU: 55%
Physical Memory: 80%
Processes: 130

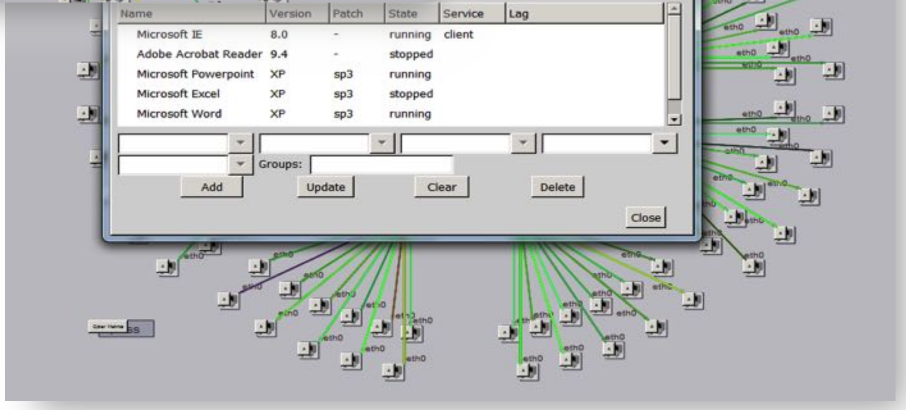
🟥 HIGH
🟧 MEDIUM
🟨

High Infection H

Percentile Increase
55 -10 = 45
45/55*100 = 80% increase

Threshold = 19% Increase

Lockheed Martin Image



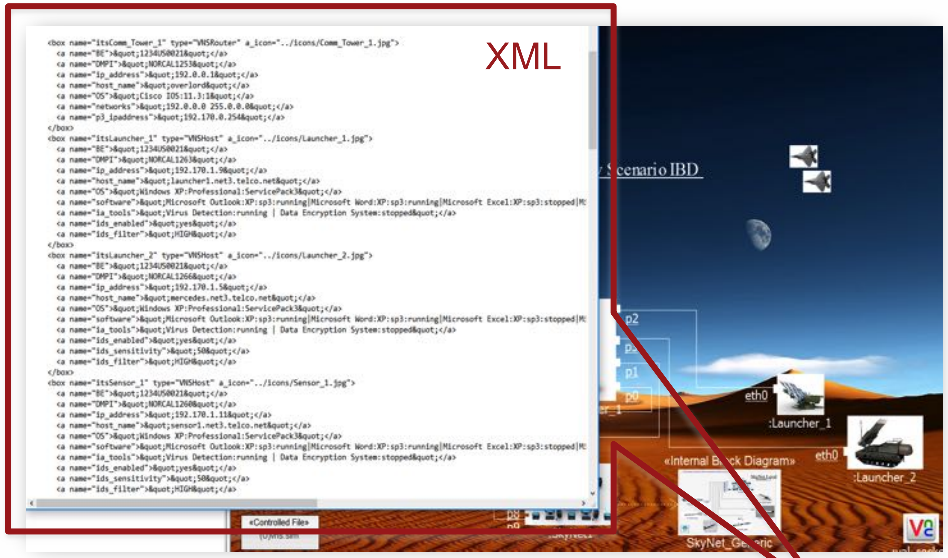
Name	Version	Patch	State	Service	Lag
Microsoft IE	8.0	-	running	client	
Adobe Acrobat Reader	9.4	-	stopped		
Microsoft Powerpoint	XP	sp3	running		
Microsoft Excel	XP	sp3	stopped		
Microsoft Word	XP	sp3	running		

Groups:

Lockheed Martin Image

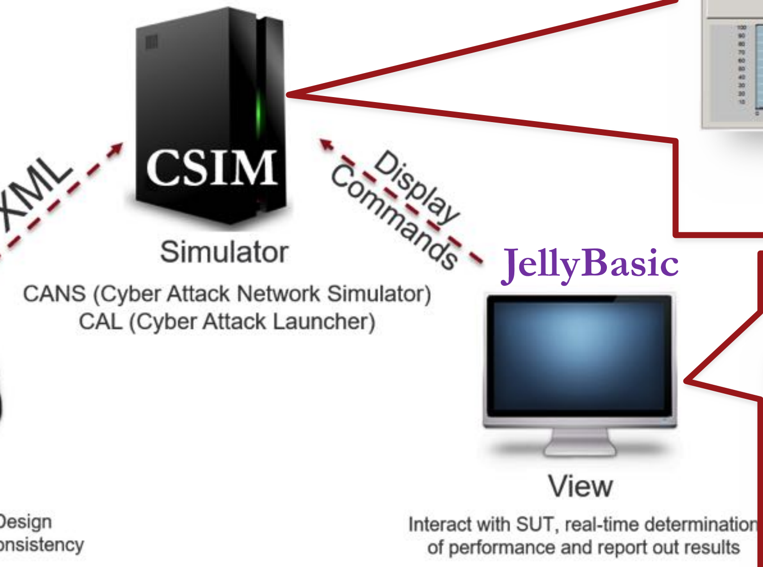
Driving SysML into Cyber Effect Simulation

- Once the IBD is created from the BDD, a companion IBM Rhapsody report generation tool call ReporterPLUS queries the model database to produce customized outputs in any format, including XML.



```
<box name="itsComm_Tower_1" type="VNSRouter" a_icon="../icons/Comm_Tower_1.jpg">
  <a name="BE">&quot;1234US0021&quot;</a>
  <a name="DMPI">&quot;NORCAL1253&quot;</a>
  <a name="ip_address">&quot;192.0.0.1&quot;</a>
  <a name="host_name">&quot;overlord&quot;</a>
  <a name="OS">&quot;Cisco IOS:11.3:1&quot;</a>
  <a name="networks">&quot;192.0.0.0 255.0.0.0&quot;</a>
  <a name="p3_ipaddress">&quot;192.170.0.254&quot;</a>
</box>
<box name="itsLauncher_1" type="VNSHost" a_icon="../icons/Launcher_1.jpg">
  <a name="BE">&quot;1234US0021&quot;</a>
  <a name="DMPI">&quot;NORCAL1263&quot;</a>
  <a name="ip_address">&quot;192.170.1.9&quot;</a>
  <a name="host_name">&quot;launcher1.net3.telco.net&quot;</a>
  <a name="OS">&quot;Windows XP:Professional:ServicePack3&quot;</a>
  <a name="software">&quot;Microsoft Outlook:XP:sp3:running|Microsoft Word:XP:sp3:running|Microsoft Excel:XP:sp3:stopped|M
  <a name="ia_tools">&quot;Virus Detection:running | Data Encryption System:stopped&quot;</a>
  <a name="ids_enabled">&quot;yes&quot;</a>
  <a name="ids_filter">&quot;HIGH&quot;</a>
</box>
<box name="itsLauncher_2" type="VNSHost" a_icon="../icons/Launcher_2.jpg">
  <a name="BE">&quot;1234US0021&quot;</a>
  <a name="DMPI">&quot;NORCAL1266&quot;</a>
  <a name="ip_address">&quot;192.170.1.5&quot;</a>
  <a name="host_name">&quot;mercedes.net3.telco.net&quot;</a>
  <a name="OS">&quot;Windows XP:Professional:ServicePack3&quot;</a>
  <a name="software">&quot;Microsoft Outlook:XP:sp3:running|Microsoft Word:XP:sp3:running|Microsoft Excel:XP:sp3:stopped|M
  <a name="ia_tools">&quot;Virus Detection:running | Data Encryption System:stopped&quot;</a>
  <a name="ids_enabled">&quot;yes&quot;</a>
  <a name="ids_sensitivity">&quot;50&quot;</a>
  <a name="ids_filter">&quot;HIGH&quot;</a>
</box>
<box name="itsSensor_1" type="VNSHost" a_icon="../icons/Sensor_1.jpg">
  <a name="BE">&quot;1234US0021&quot;</a>
  <a name="DMPI">&quot;NORCAL1260&quot;</a>
  <a name="ip_address">&quot;192.170.1.11&quot;</a>
  <a name="host_name">&quot;sensor1.net3.telco.net&quot;</a>
  <a name="OS">&quot;Windows XP:Professional:ServicePack3&quot;</a>
  <a name="software">&quot;Microsoft Outlook:XP:sp3:running|Microsoft Word:XP:sp3:running|Microsoft Excel:XP:sp3:stopped|M
  <a name="ia_tools">&quot;Virus Detection:running | Data Encryption System:stopped&quot;</a>
  <a name="ids_enabled">&quot;yes&quot;</a>
  <a name="ids_sensitivity">&quot;50&quot;</a>
  <a name="ids_filter">&quot;HIGH&quot;</a>
```

Lockheed Martin Image



JellyStudio

Model

System Design, Test Design
Data Storage, Integrity, Consistency

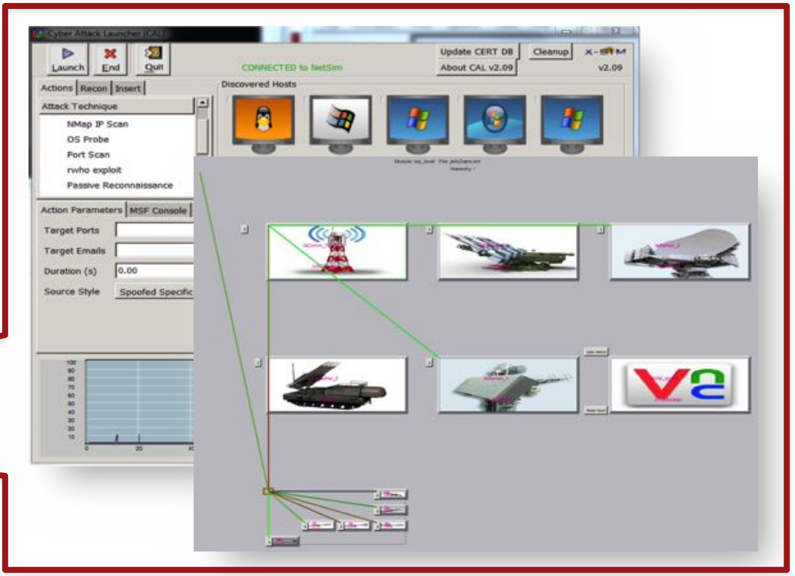
Simulator

CANS (Cyber Attack Network Simulator)
CAL (Cyber Attack Launcher)

View

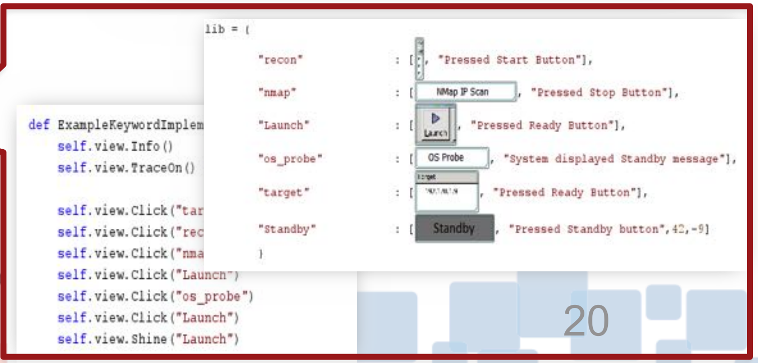
Interact with SUT, real-time determination of performance and report out results

Lockheed Martin Image



NMap IP Scan
OS Probe
Port Scan
rwho exploit
Passive Reconnaissance

Target Ports
Target Emails
Duration (s) 0.00
Source Style Spoofed Specific



```
def ExampleKeywordImplem
    self.view.Info()
    self.view.TraceOn()

    self.view.Click("tar
    self.view.Click("rec
    self.view.Click("nma
    self.view.Click("Launch")
    self.view.Click("os_probe")
    self.view.Click("Launch")
    self.view.Shine("Launch")
```

```
lib = (
        "recon"         : [ , "Pressed Start Button"],
        "nmap"          : [ NMap IP Scan , "Pressed Stop Button"],
        "Launch"        : [ Launch , "Pressed Ready Button"],
        "os_probe"      : [ OS Probe , "System displayed Standby message"],
        "target"        : [ , "Pressed Ready Button"],
        "Standby"       : [ Standby , "Pressed Standby button",42,-9]
        )
```

Lockheed Martin Image

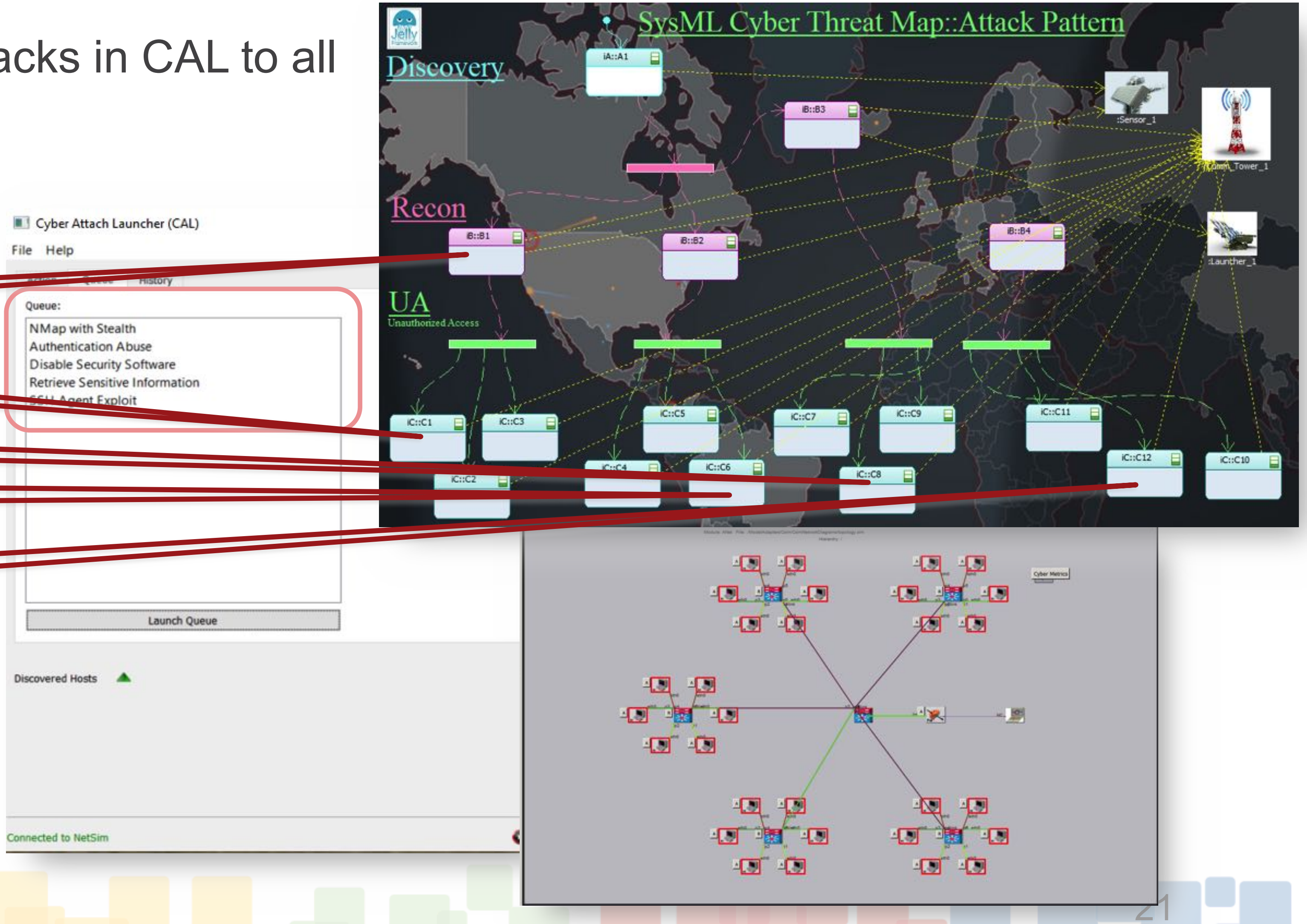
Automating Cyber Attack Launcher (CAL)

Simulated by launching multiple attacks in CAL to all network IP Addresses

0.0.0.0 to 255.255.255.255

1. NMAP with Stealth
2. Authentication Abuse
3. Disable Security Software
4. Retrieve Sensitive Information
5. SSH Agent Exploit

Lockheed Martin Image



Cyber Attach Launcher (CAL)

Queue:

NMap with Stealth
Authentication Abuse
Disable Security Software
Retrieve Sensitive Information
SSH Agent Exploit

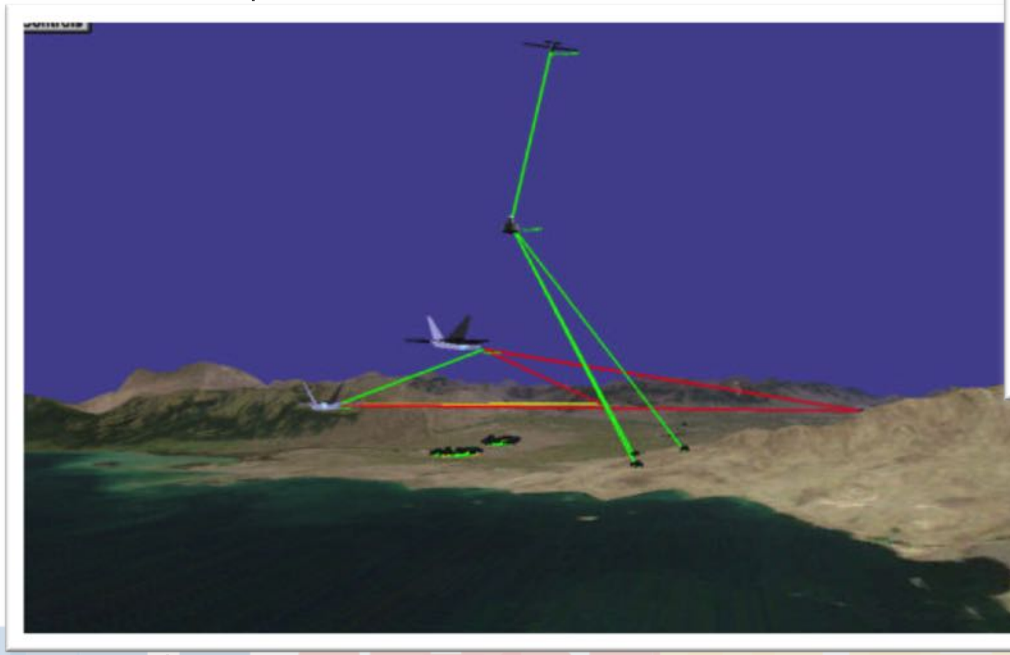
Connected to NetSim

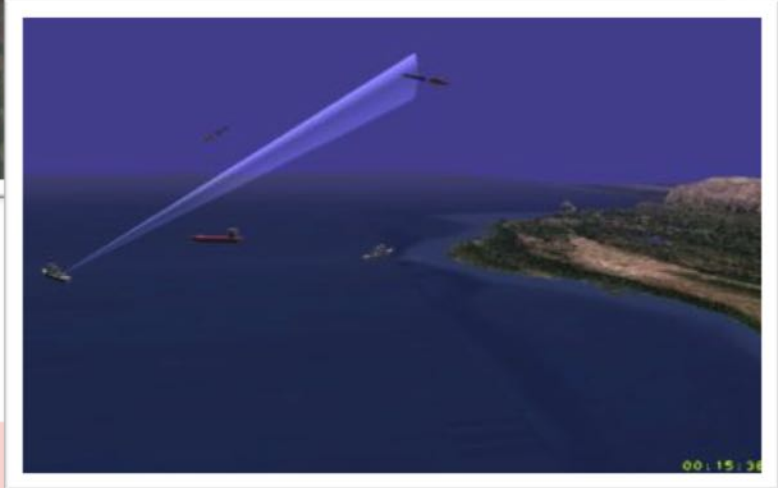
Virtualization (Future)

- Simulations drive scenario visualizations.
- Aides communication to all stake holders.
- Improves understanding of mission impacts.

Simultaneous Multiple Views

WinFrame Example





Lockheed Martin Image

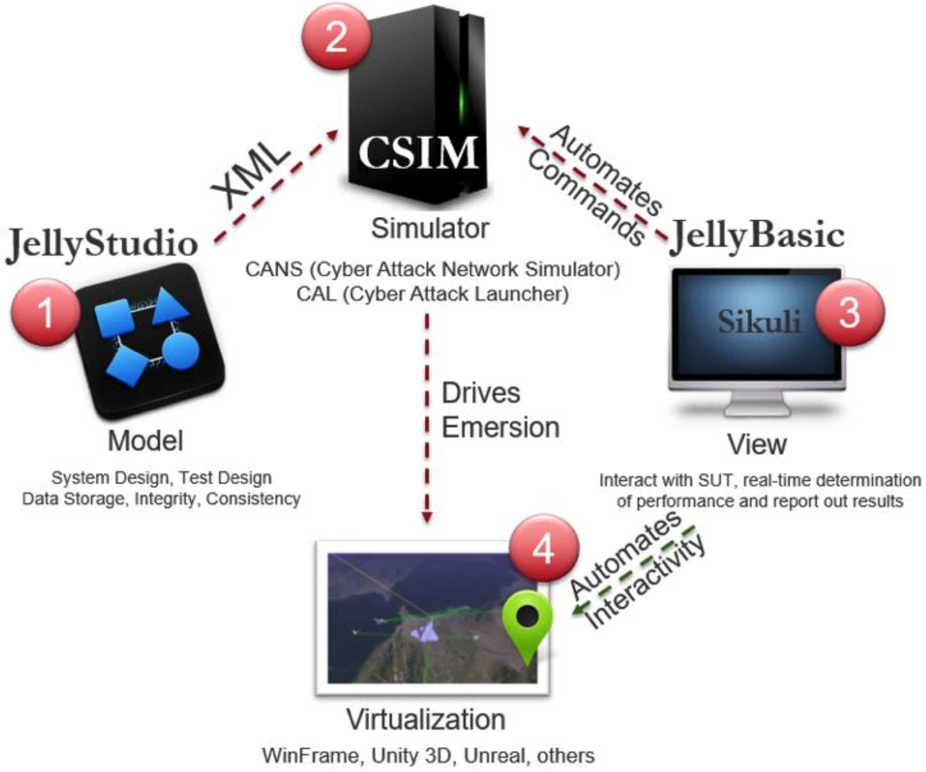
Summary (Complete End-to-End Solution)

1. Model System Engineering (MSE) with SysML accelerates cyber simulation development process, reduces software defects.
   - SysML offers flexibility in analysis
     - Network Topology Representation
     - Cyber Threat modeling

2. Simulation allows analysts to study event simulation effect of various cyber events that is Affortable and Increase Scalability.

3. Automation driven by SysML provides methods for performance modeling and I&T activities.

4. Virtualization allows for the Stakeholder to be immersed into the environment to gain a deeper understanding of the SysML Design.



JellyStudio
1
Model
System Design, Test Design
Data Storage, Integrity, Consistency
XML
2
CSIM
Simulator
CANS (Cyber Attack Network Simulator)
CAL (Cyber Attack Launcher)
Automates Commands
JellyBasic
Sikuli
3
View
Interact with SUT, real-time determination of performance and report out results
Drives Emersion
4
Automates Interactivity
Virtualization
WinFrame, Unity 3D, Unreal, others

Lockheed Martin Image

from…

SysML Model to Performance Model to Model Execution to Virtualization

28th Annual INCOSE
international symposium

Washington, DC, USA
July 7 - 12, 2018

www.incose.org/symp2018