COORDINATED SCIENCE LABORATORY

ENGINEERING AT ILLINOIS

ADVISE Meta – Alpha Tool Workshop

August 16, 2016

Andy Crapo, Brett Feddersen, Alfredo Galbadon, Ken Keefe, Carol Muehrcke, Michael Rausch, Bill Sanders, and Ron Wright

ITI.ILLINOIS.EDU

INFORMATION TRUST INSTITUTE

Agenda

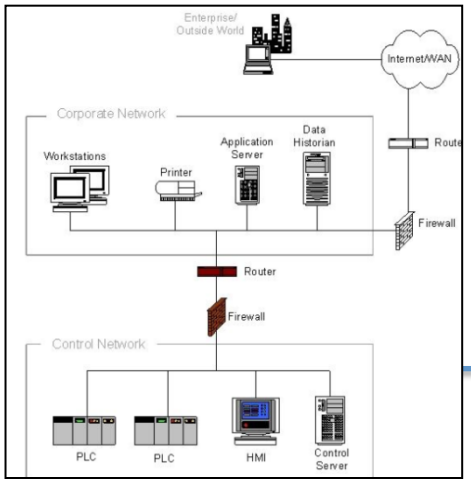
- Registration and Continental Breakfast
- Welcome
- Goals
  - Tool
  - Workshop
- Steps to Use ADVISE Meta
- Hands on Sessions
- Advanced Ontology: Selected Details and Customization
- Case Studies
- Wrap Up

ADVISE Meta Introduction

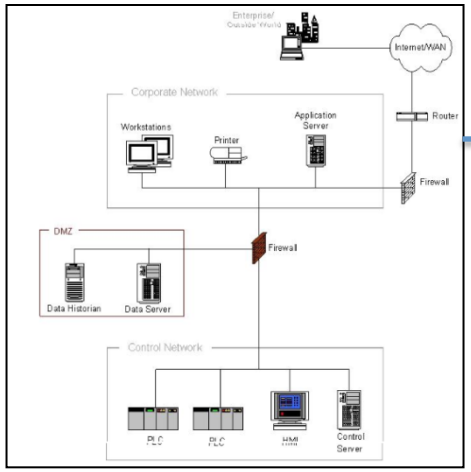
- Today: no scientific basis for designing security architectures
  - Follows from: no scientific basis for estimating effectiveness of security measures before deployment
- Today: security metrics
  - Before deployment, count countermeasures
    - Judge effectiveness based on experience, intuition
  - After deployment, count intrusions
- Purpose of ADVISE Meta
  - Provide scientific basis for design decisions by calculating security metrics at design time
  - Auditable results
  - No requirement for deep modeling or cybersecurity expertise

ADVISE Meta Tool on Möbius

Architecture 1



Architecture 2



Compare architecture metrics: common attack paths, time to compromise, probability of compromise, cost of attack,…

Möbius Tool

Attack simulation

Architecture 1 Security metrics

Architecture 2 Security metrics

Example architectures: NIST 800-82 Figures 5-2 and 5-3

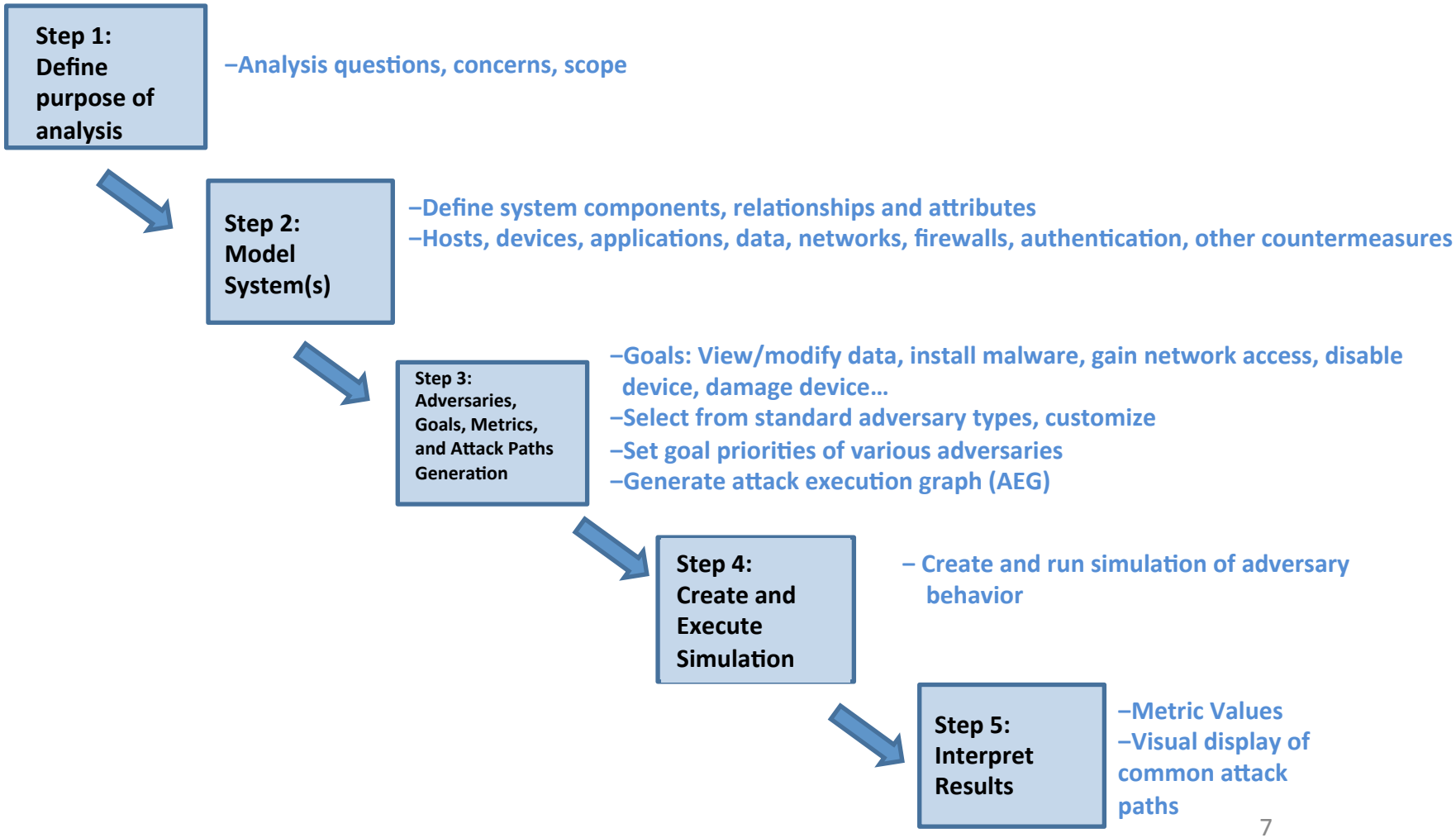
Workshop Goals

- Introduce the tool to the community
- Gather feedback about all aspects of the tool
  - High level concepts
  - Workflow
  - User Interface
  - Usability
- Feedback discussion at the end of each hands-on session

Agenda

- Registration and Continental Breakfast
- Welcome
- Goals
  - Tool
  - Workshop
- Steps to Use ADVISE Meta
- Hands on Sessions
- Case Studies and Custom Ontologies
- Wrap Up

Using ADVISE Meta

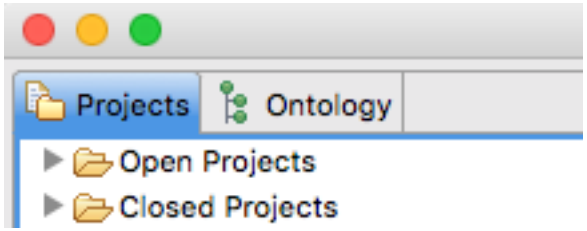


Agenda

- Registration and Continental Breakfast
- Welcome
- Goals
  - Tool
  - Workshop
- Steps to Use ADVISE Meta
- Hands on Sessions
- Case Studies and Custom Ontologies
- Wrap Up

Step 0 – Install and Ontology Overview

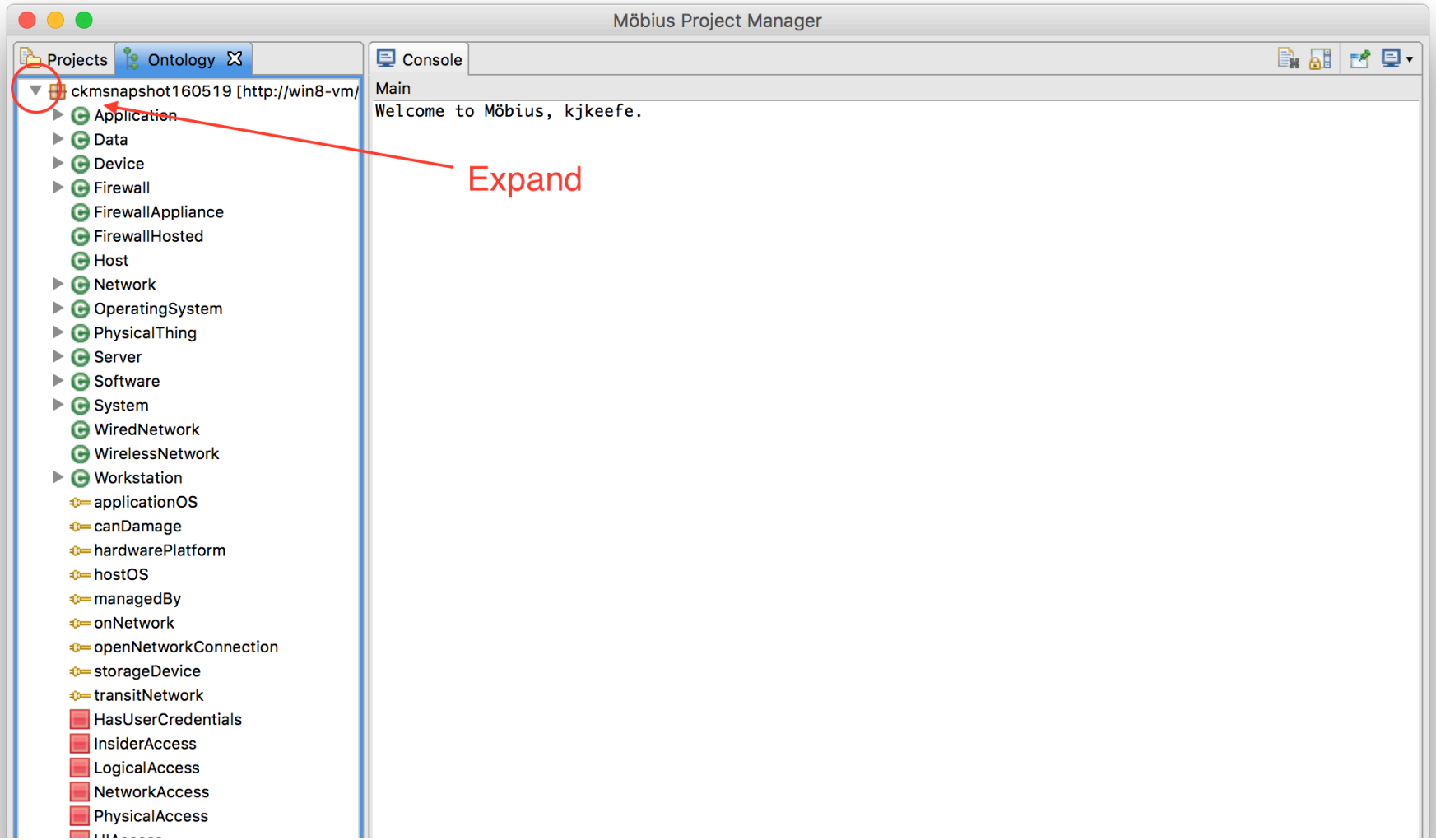
When you start Mobius, you will see two tabs in the upper left hand corner



- The Project tab contains projects with models of systems, attackers, and metrics.
- The Ontology tab is where individual system components, relationships, attributes, etc. are defined.

Step 0 – Install and Ontology Overview

1. On the ontology pane, click on the arrow to left of the ontology name, to expand the ontology



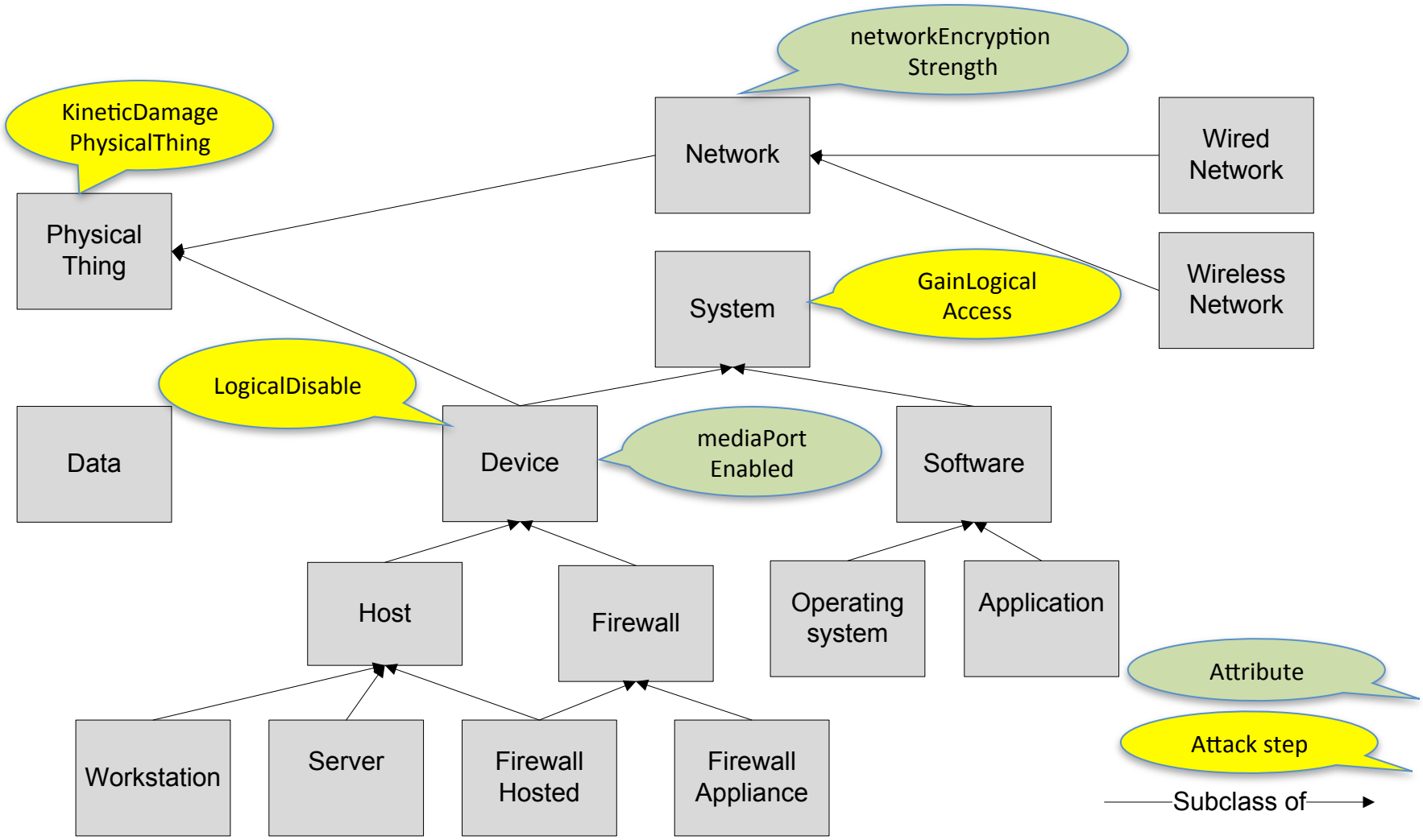
ADVISE Meta - Ontology

- Ontology (general definition): a particular theory about the nature of being or the kinds of things that have existence
- ADVISE Meta Ontology: types of things available to build a system model and simulate cyber attacks against it
- Concepts in tool ontology fall in these categories
  - Types of components 
  - Attributes of components by type 
  - Relationships between components 
  - Types of access,  skills,  and knowledge  an adversary may have
  - Types and characteristics of adversaries 
  - Attack steps 
  - State variables: other system, component, or adversary properties 

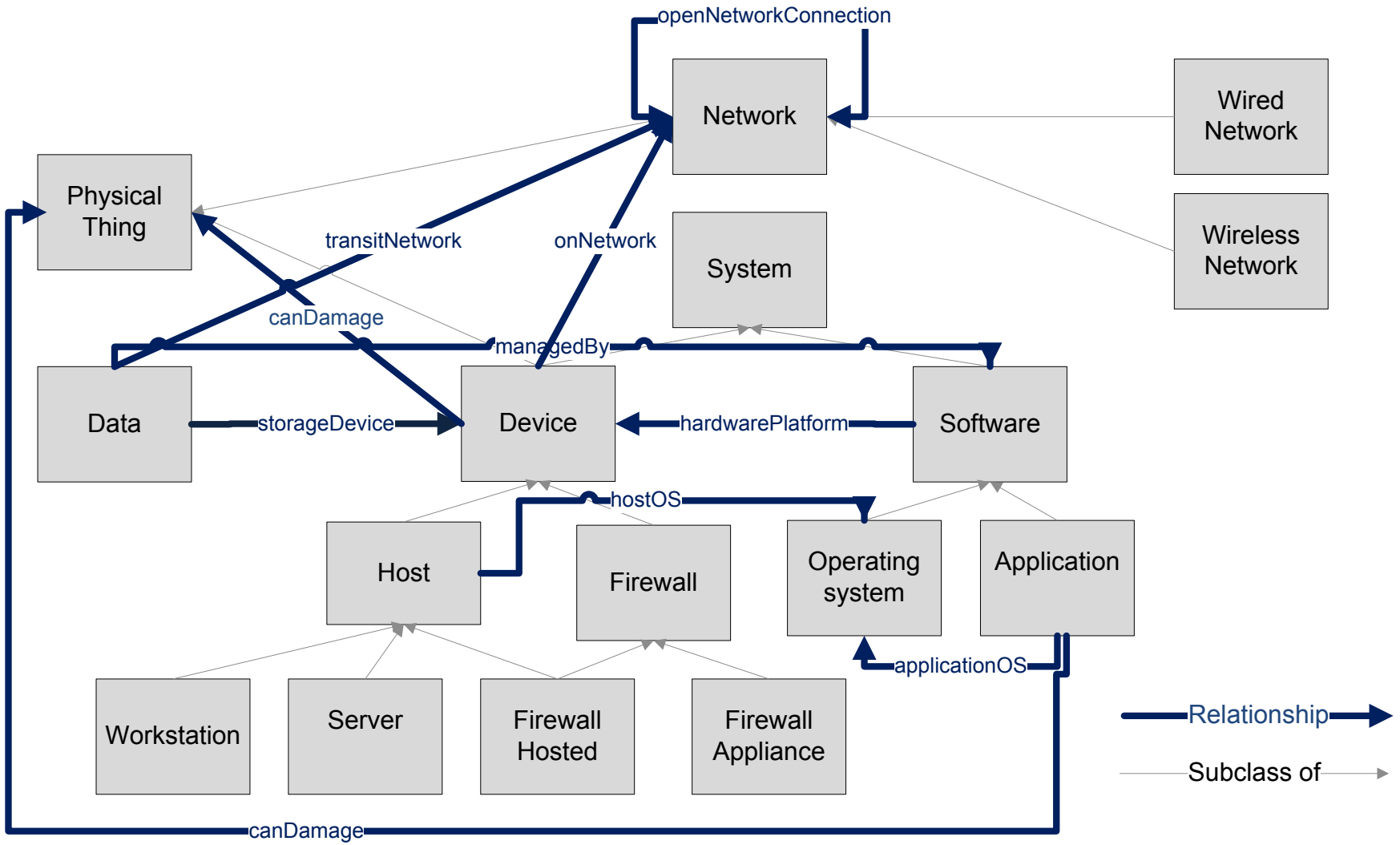
Base Ontology

- Base ontology used for hands-on exercise
- Representative of tool capabilities
- Grounded by:
  - Research on attack methods
  - Study of example analysis previously done with hand-created AEG
- Not yet a "complete" or vetted dataset
- Modifiable, replaceable (more on this later)

Base Component Ontology and Inheritance



Base Ontology Relationships



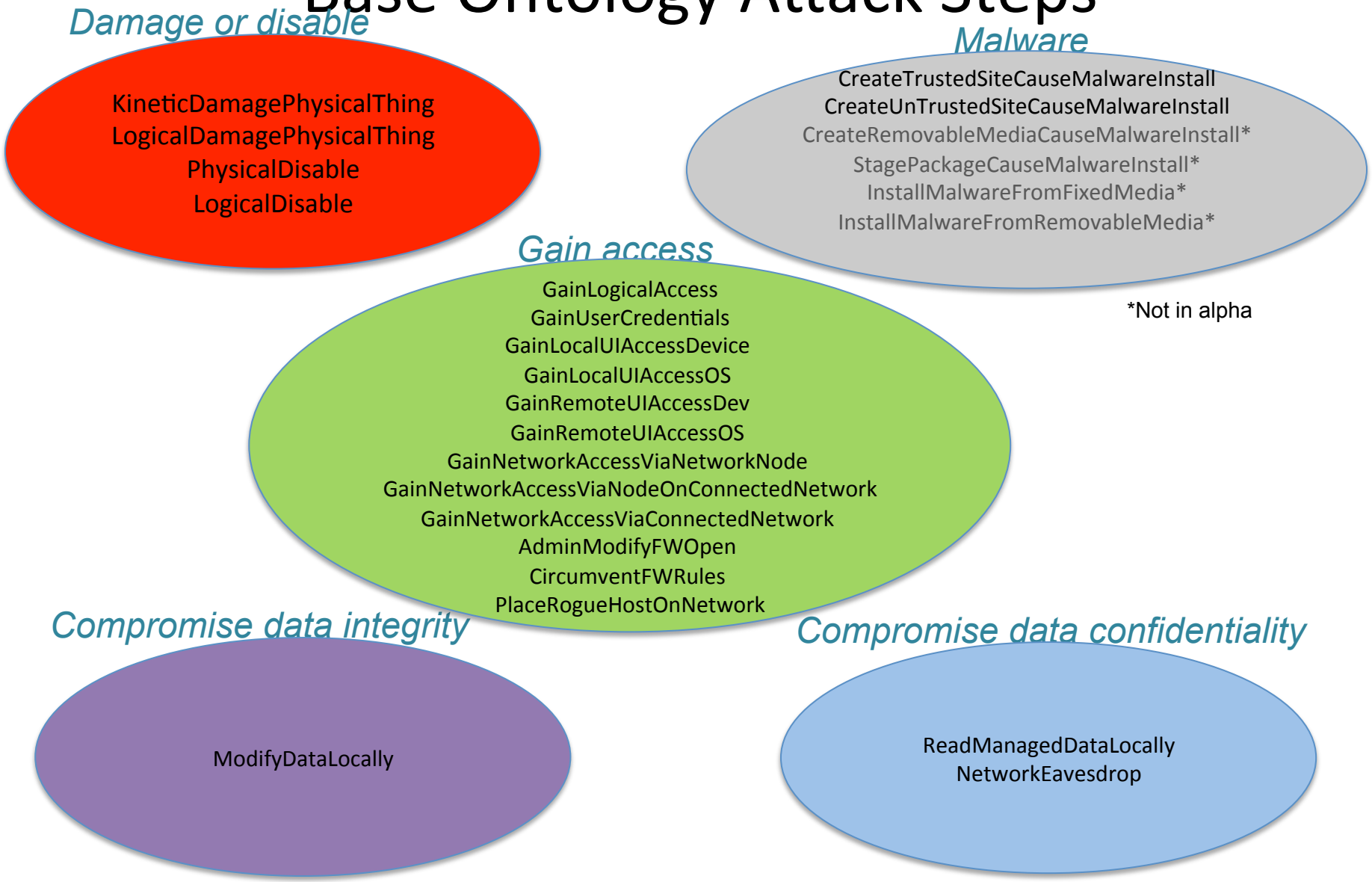
Base Ontology Types of Access

- PhysicalAccess(X), where X is a PhysicalThing
  - Not achievable via any attack step, must be given as initial condition
- NetworkAccess(X), where X is a Network
  - Able to read and write bits on the network
- UIAccess(X), where X is a Device or Software
  - Able to touch the login function (if any)
- HasUserCredentials(X), where X is a Device or Software
  - Has the password, token, key, or other credential required to access user functions provided by X
- LogicalAccess(X), where X is a Device or Software
  - Able to access user functions provided by X

Base Ontology Skills

- See list of skills on ontology tab with symbol 
- Adversary templates define default skill proficiencies
- Most skills are generic
- Reason for adding system specific skills ("Specialized")
  - Model the tremendous advantage they provide to adversary
- Reason for using broad skill categories
  - Represents how real adversaries accumulate skills
  - Fine grained skill proficiencies (e.g. at stealing passwords or breaking VPNs) unlikely to be known or even guessable in an actual case
  - Haven't seen reason yet for increasing data input requirements and complexity in attack step models

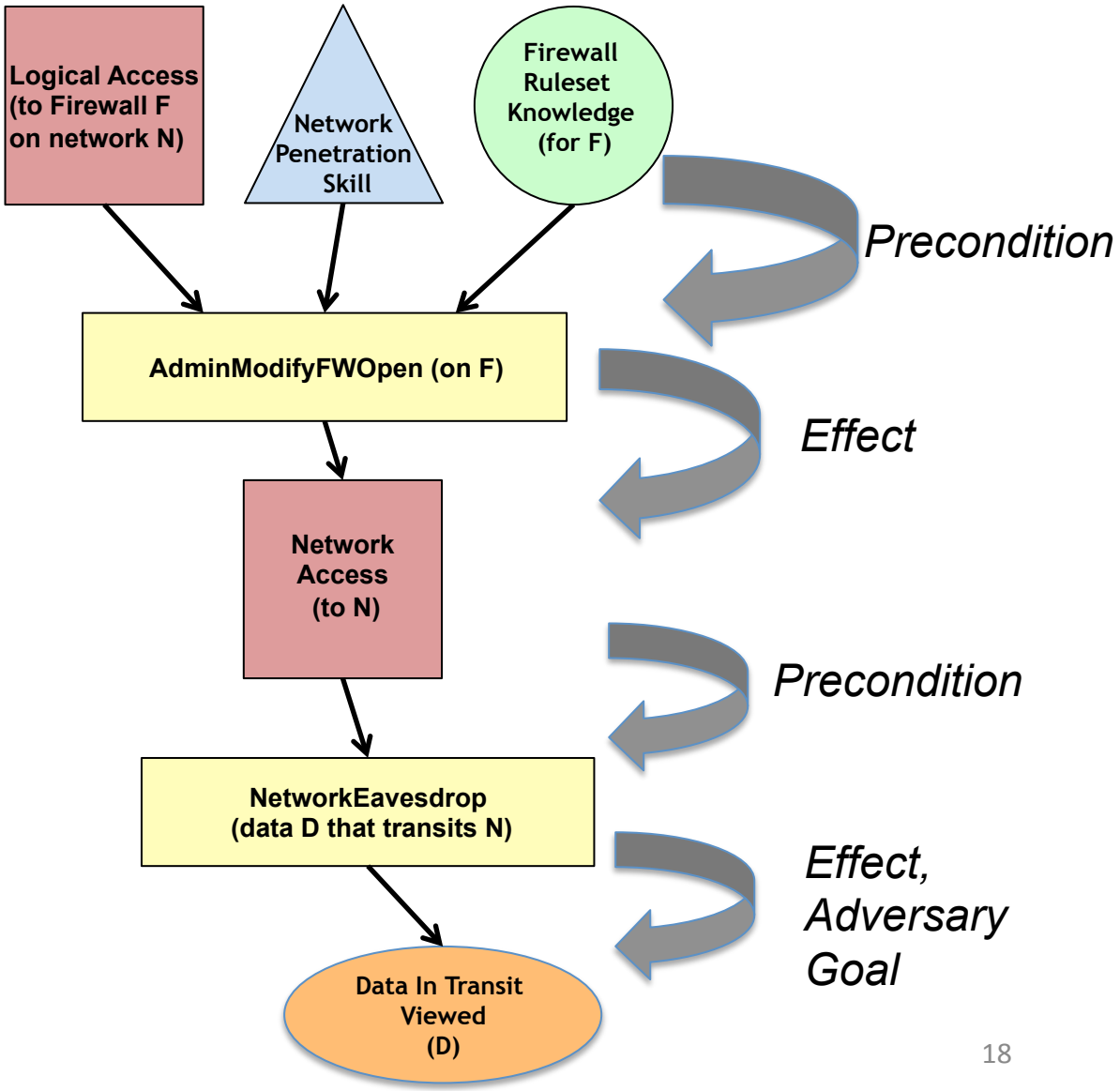
Base Ontology Attack Steps



*Not in alpha

Fragment of Attack Execution Graph (AEG)

- AEG describes potential attack paths from attacker viewpoint
- Attack step attempt requires certain *access*, *skills*, *knowledge* and/or *system state conditions*
- Attack outcome can affect any of these elements
- Any of these elements may be selected as an adversary goal



Hands-on Example Step 1 – Define Purpose of Analysis

What kinds of systems can be analyzed?

- With the base ontology: Enterprise system architectures that may have:
  - Networks hosting cyber and cyber-physical devices
  - Applications, data
  - Internet connections
  - Boundary protections and other common countermeasures
  - Design phase or existing
- With arbitrary ontology:
  - In theory, any system built of components, where attacks are constructed by linking attack steps against components

Example Enterprise Systems

- Architecture to support stock trading
- SCADA architecture supporting an electric utility
- Control systems in a water treatment plant
- Operations and administration systems for a telecommunications provider
- 911 computer systems architecture
- Reactor safety architecture for a nuclear power plant
- Systems in a hospital that process patient information
- Air traffic or train control systems
- Computer infrastructure for a research and development facility
- Computer infrastructure for an ISP

Step 1 – Define Purpose of Analysis (cont.)

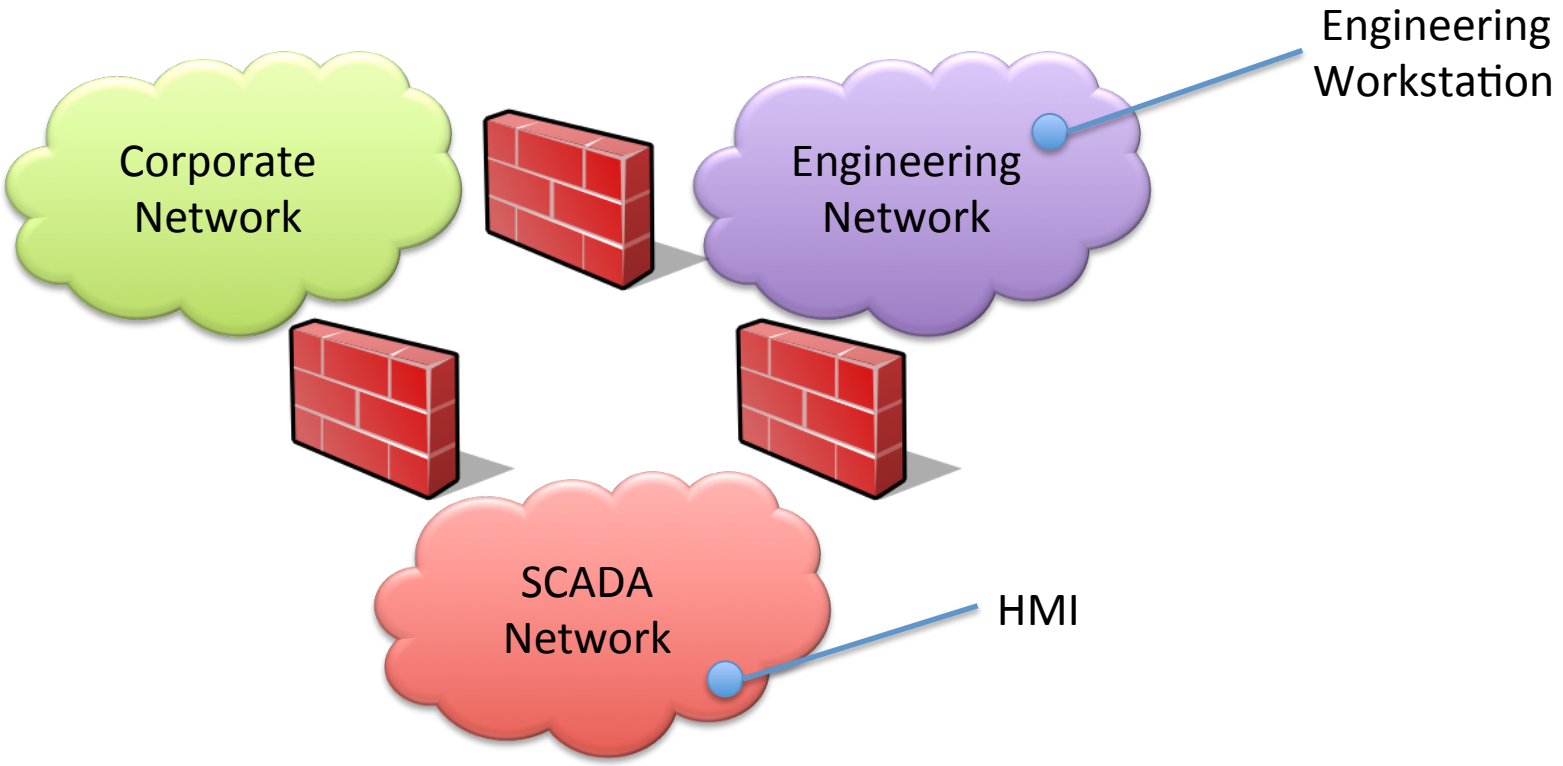
What kinds of questions can be answered?

- How susceptible is a system to cyber attacks?
- What can be done to decrease susceptibility?

Typical examples of analyses

- Which among alternative architectures should be recommended?
- What are security weak points of an architecture?
- Is a proposed countermeasure worthwhile?
- How will proposed functional architecture changes impact security?
  - If security decreases, how can decrease be minimized?

Step 1 – Define Purpose of Analysis – Small SCADA Networks



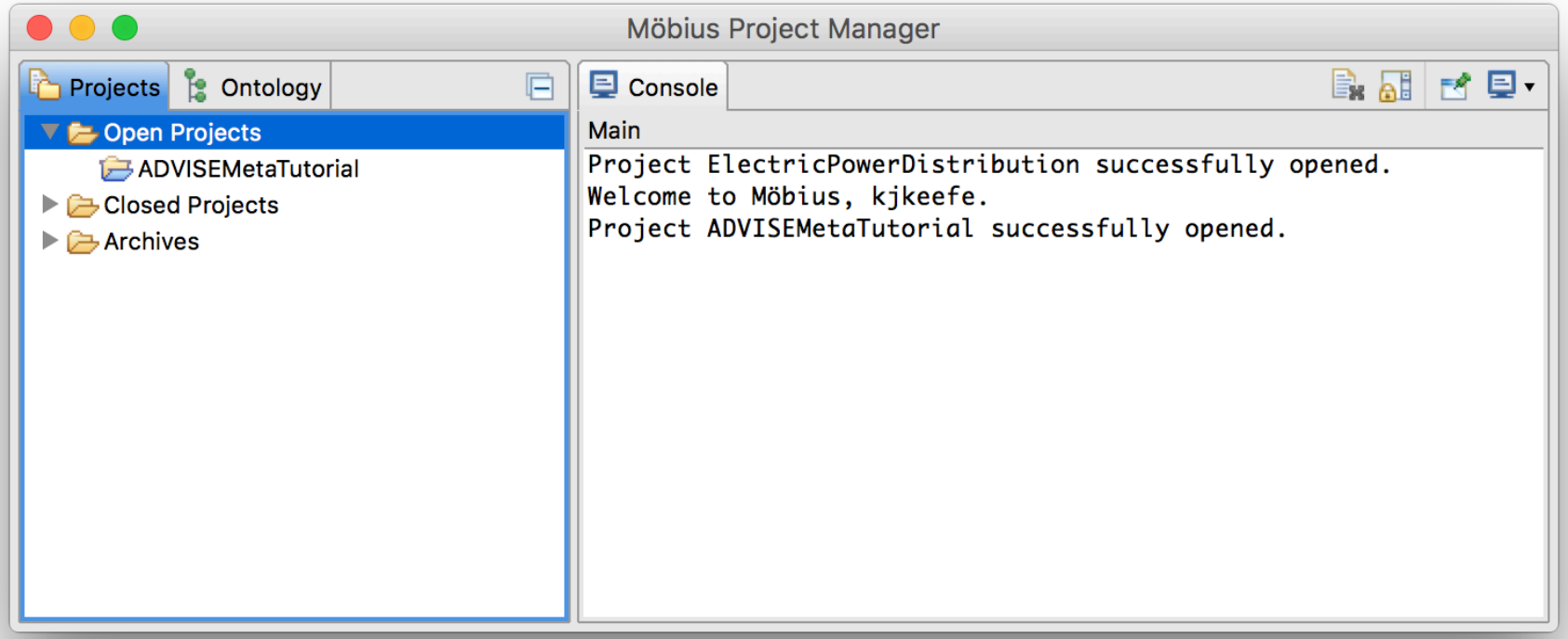
•Predicted electricity demand data stored on the SCADA LAN is found on the desk of an engineer not authorized to view this data. This data can be sold to competing electricity vendors to aid in their pricing.
•How could the engineer even gain access to the SCADA LAN?
•The engineer has physical access to all networks shown and to the HMI, and is an authorized user of the engineering workstation.
•What changes to the architecture would make this less likely to happen again?

Step 1 – Define Purpose of Analysis - Feedback

- Open questions/discussion on Step 1
- Questions for group:
  - What are some typical security architecture decisions for which rationale is hard to come by?
  - Are there specific systems that don't fall under enterprise systems, but that might benefit from this type of analysis?

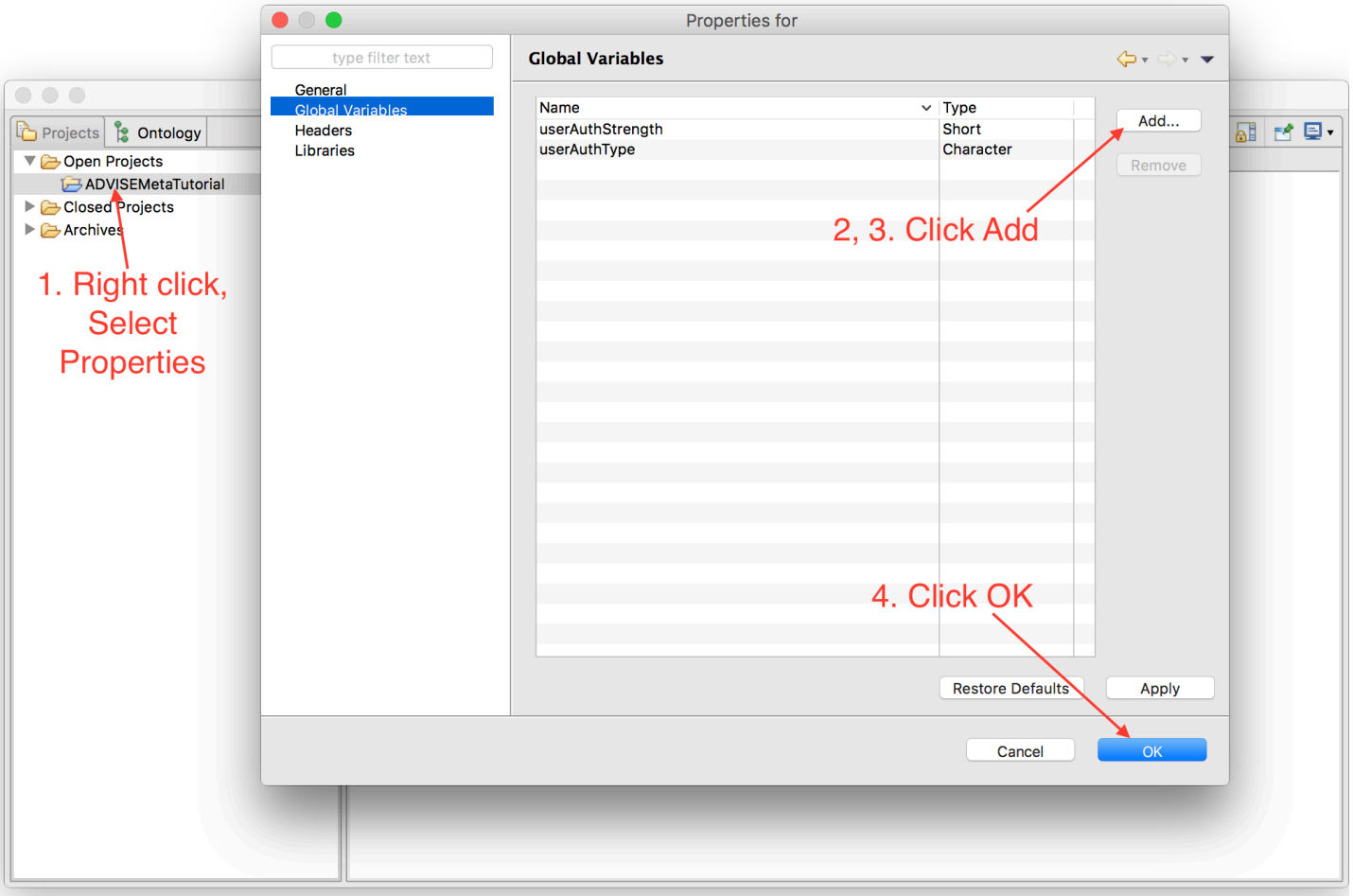
Step 2 – Model Systems

1. Select the Projects tab.
2. Right click Open Projects and select New Project…
3. Name the project **ADVISEMetaTutorial** and click Finish



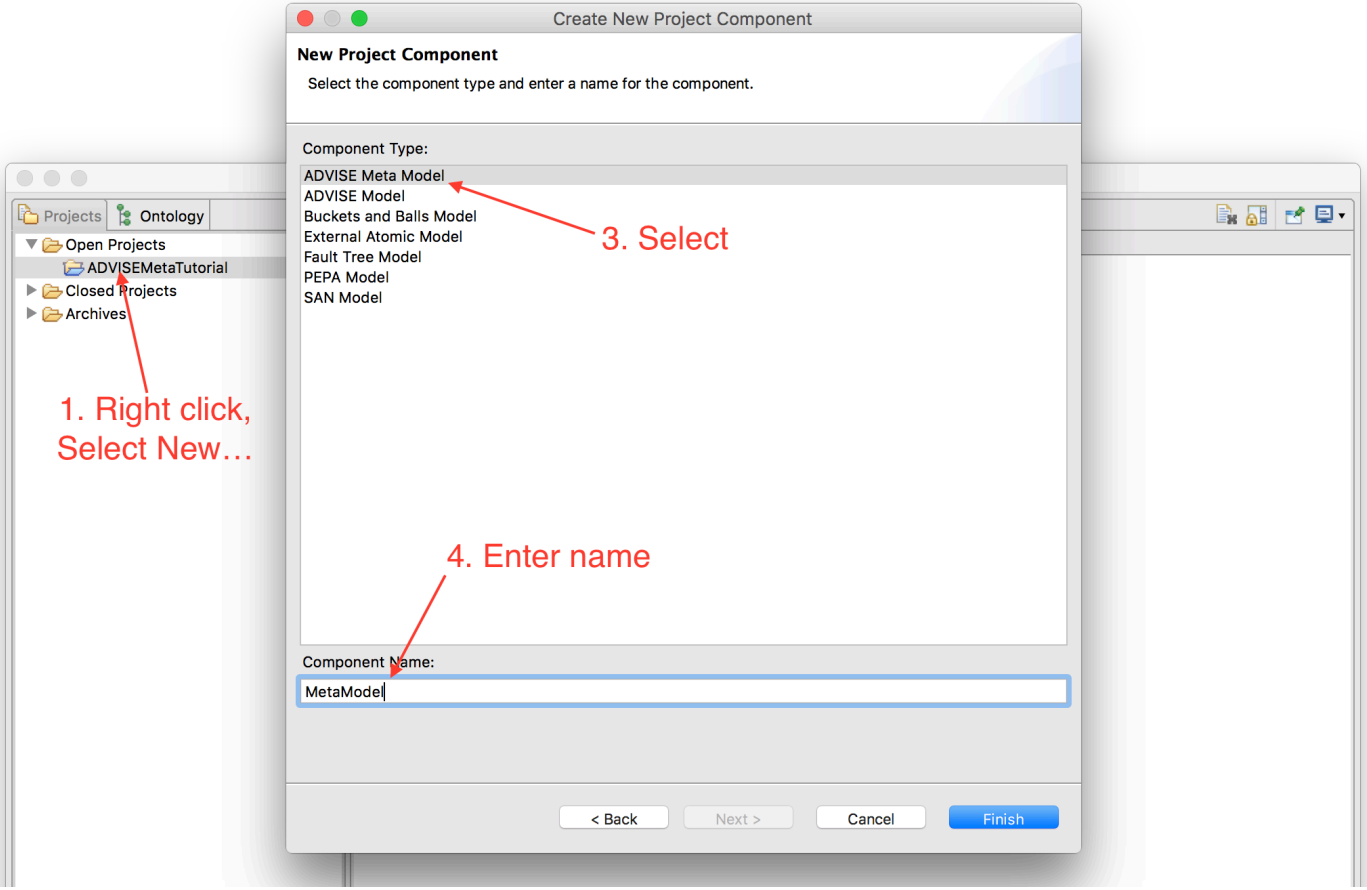
Step 2 – Model Systems

1. Right click the ADVISEMetaTutorial project, select Properties…
2. Add a global variable called **userAuthStrength** with type **Short**.
3. Add a global variable called **userAuthType** with type **Character**.
4. Click OK

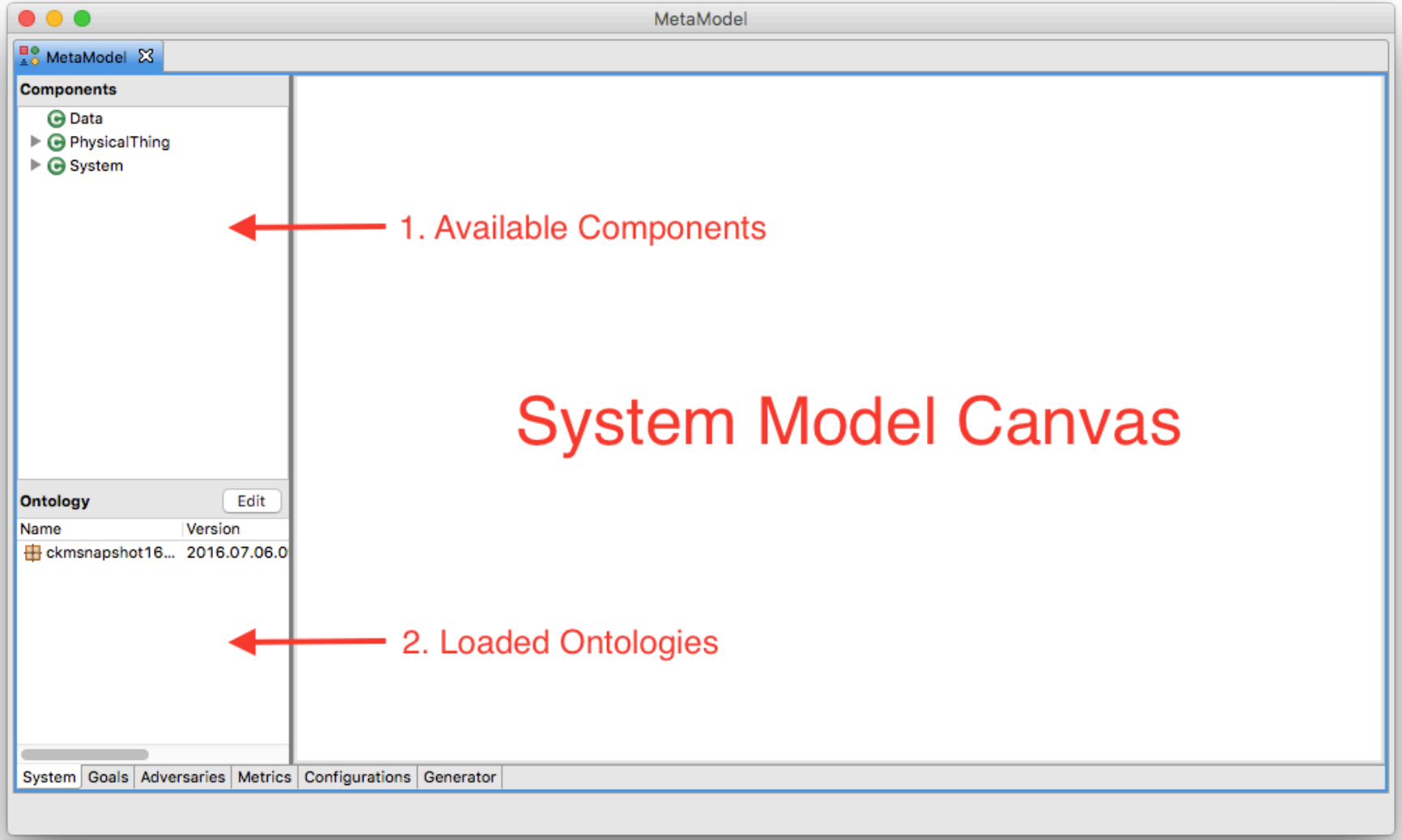


Step 2 – Model Systems

1. Right click the ADVISEMetaTutorial project, select New…
2. Select **Atomic** in the bottom pane and click Next.
3. Select **ADVISE Meta Model** in the list.
4. Enter the name **MetaModel** and click Finish.

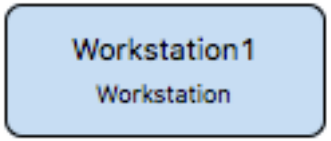


Step 2 – Model Systems

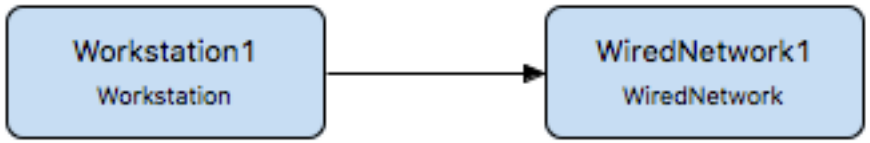


Step 2 – Model Systems

- Component
  - Part or element of the system
  - Physical objects, e.g., computer, firewall, building, etc.
  - Logical objects, e.g., data, software, etc.
  - Components are represented as blue rectangles on the system diagram

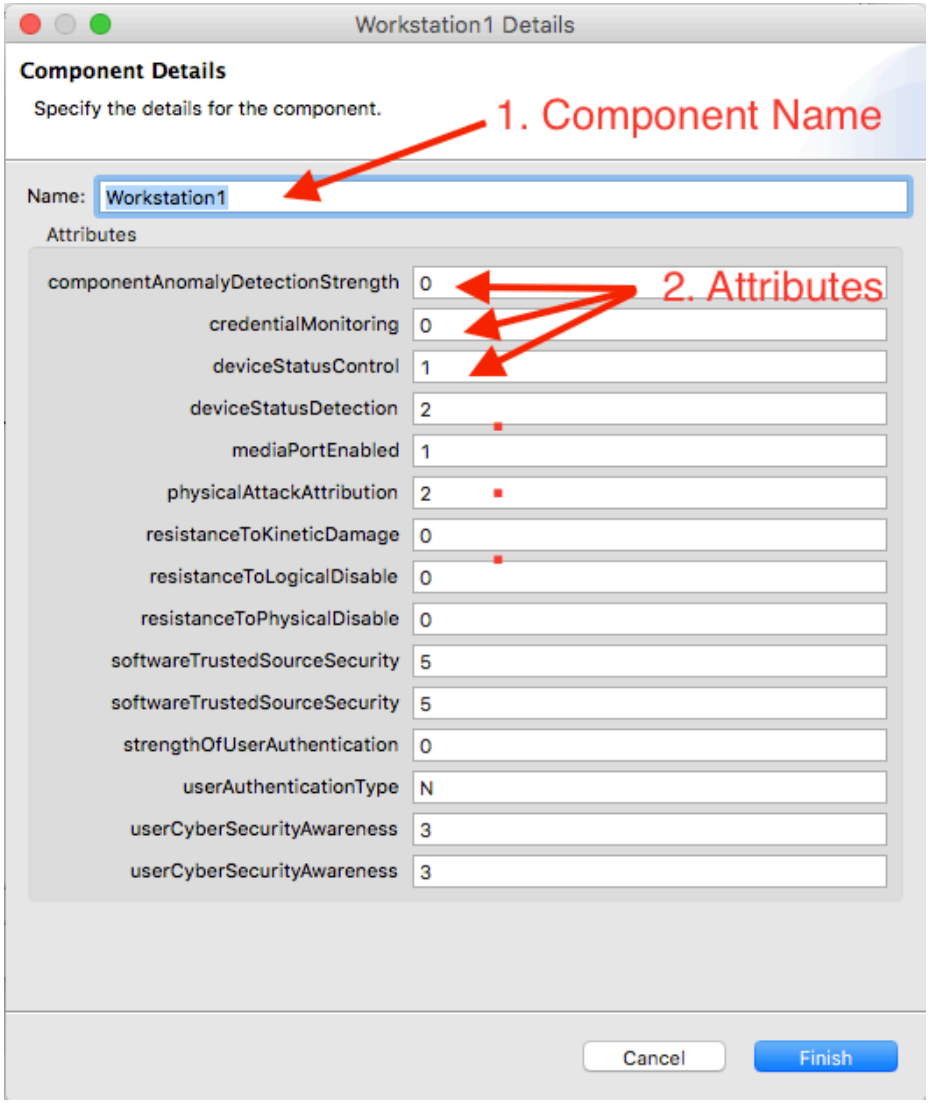


- Relationship
  - A semantic connection between two components.
  - For example, a computer is connected to a network through a **onNetwork** relationship, or data is managed by a software application through a **managedBy** relationship.
  - Relationships are represented as arcs on the system diagram.



Step 2 – Model Systems

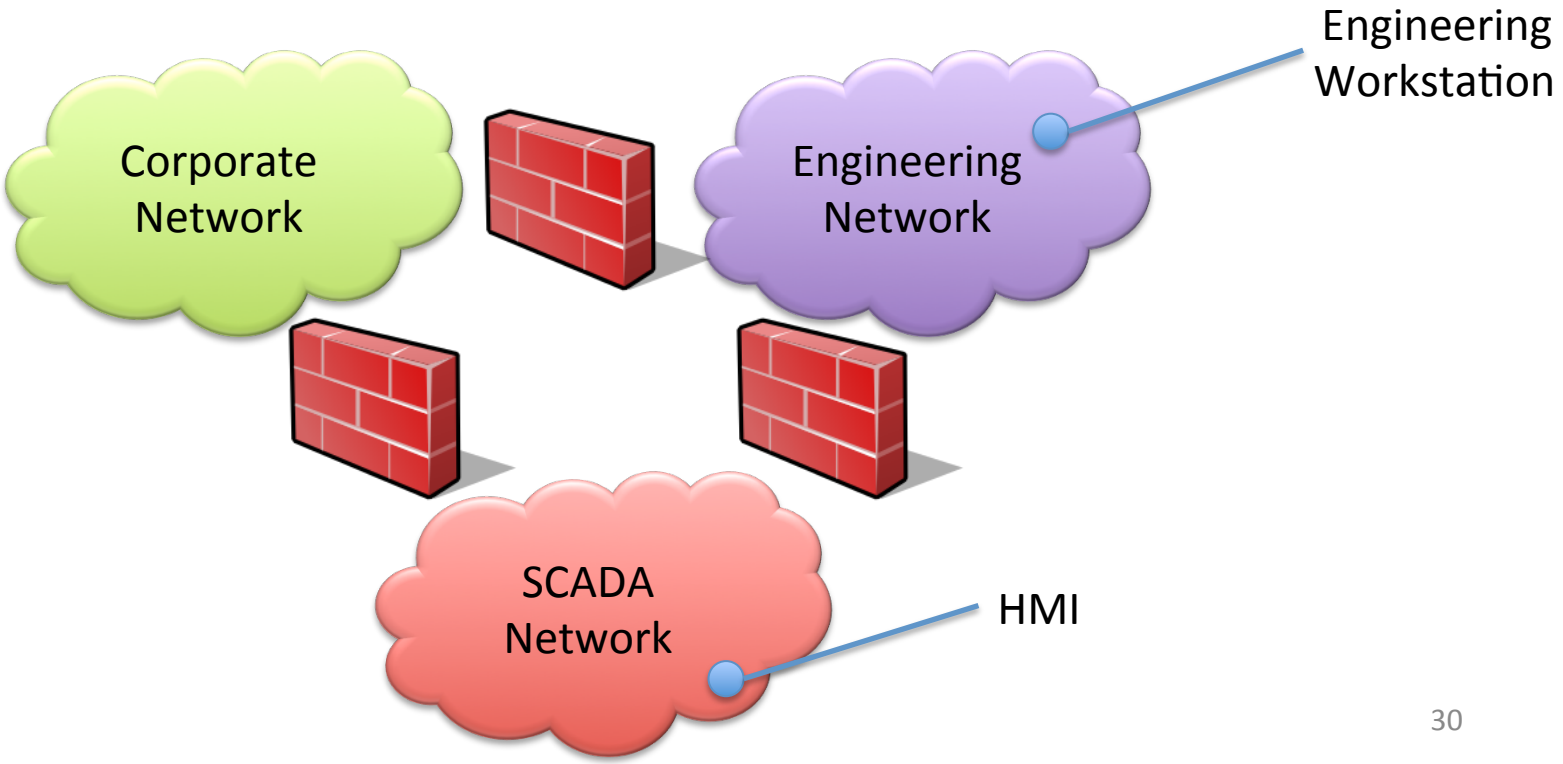
- Attributes
  - Security relevant properties associated with a component
  - For example, a component might use a specific type of authentication mechanism
  - Listed in the “Details” of the component



Step 2 – Model Systems

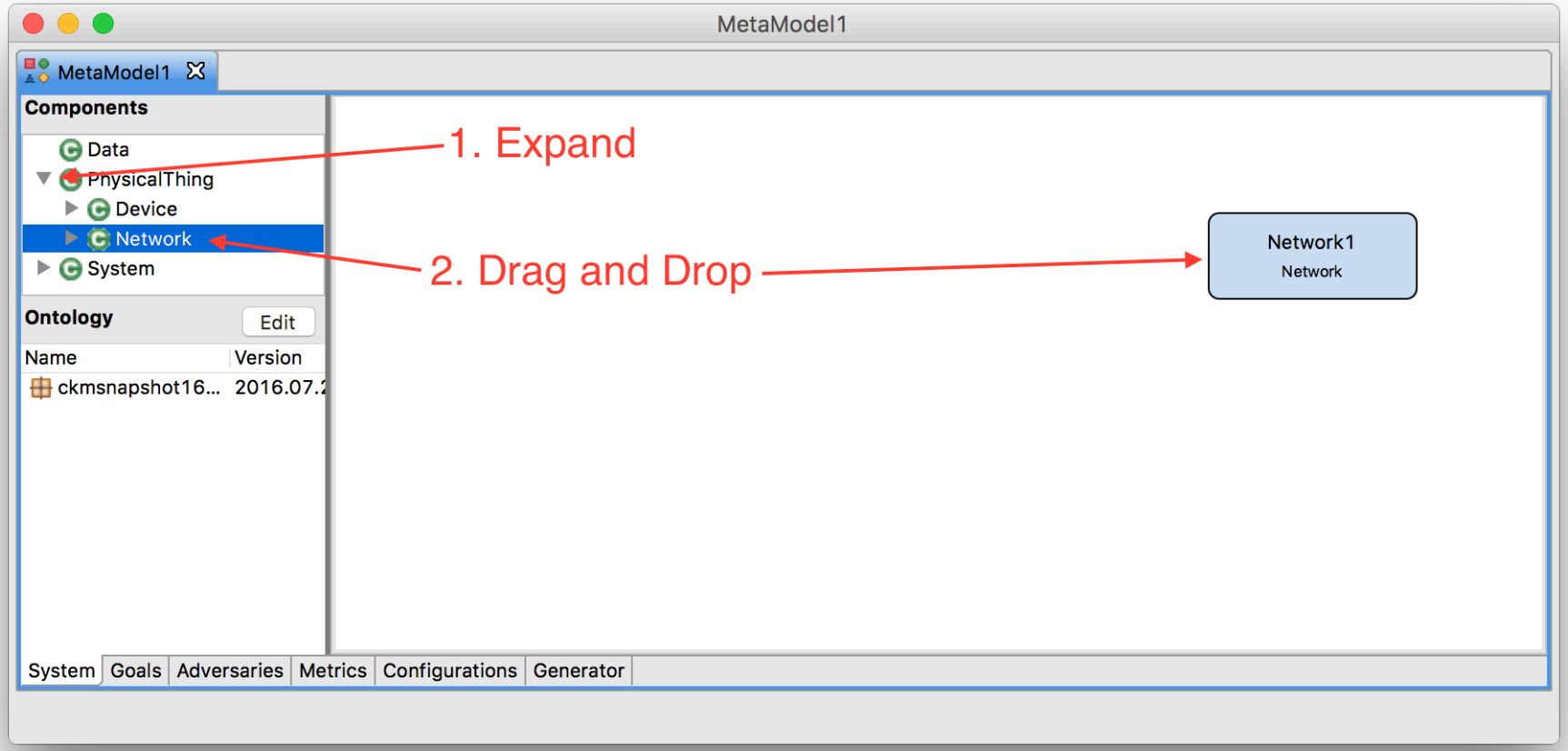
Our simple example consists of:

- SCADA Network with a local terminal (HMI)
- Engineering Network with a local Linux workstation running an SSH server
- Corporate LAN
- All networks are interconnected through firewalls



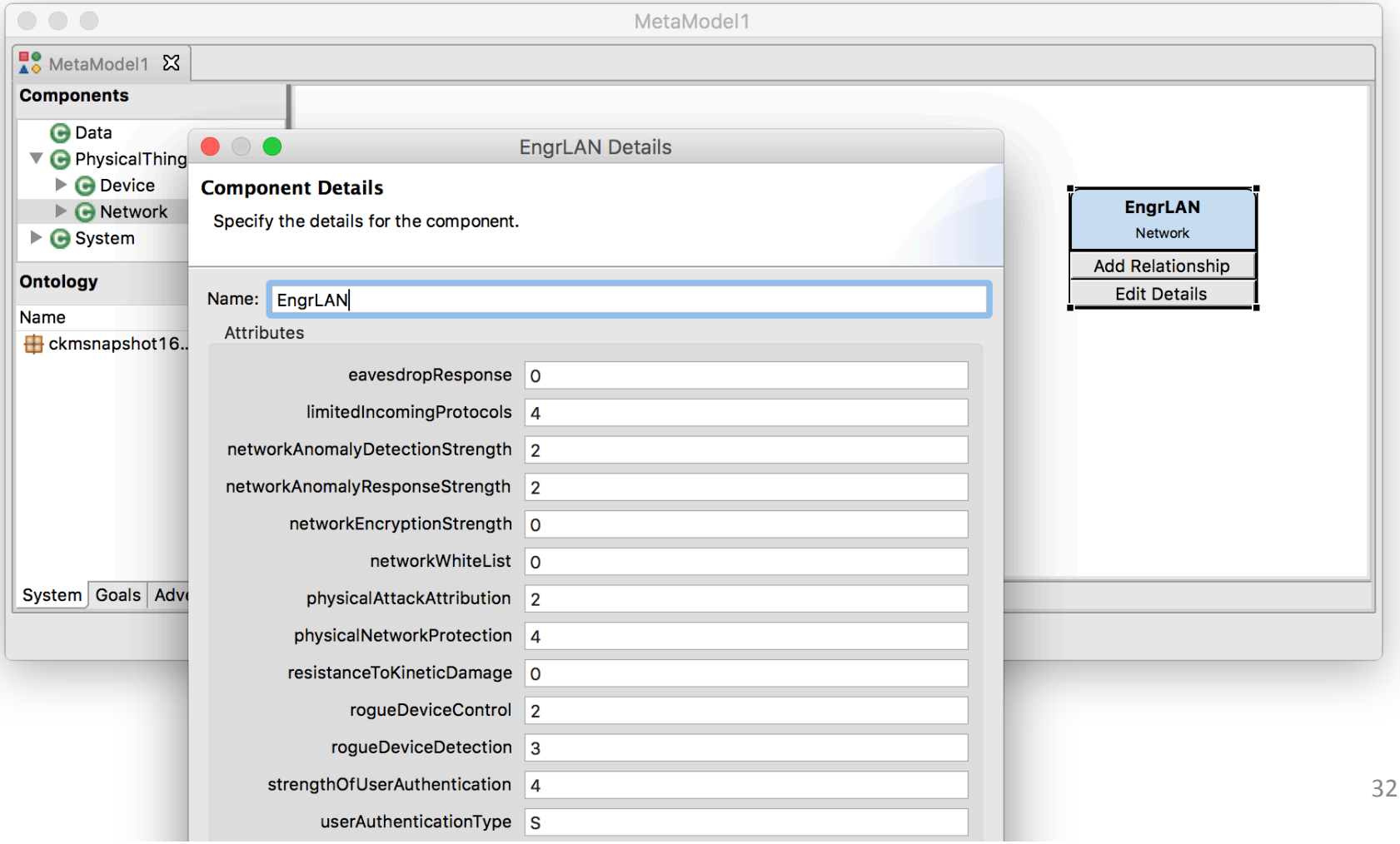
Step 2 – Model Systems

1. Expand the **PhysicalThing** node in the available components tree.
2. Drag and drop an instance of a **Network** onto the canvas.



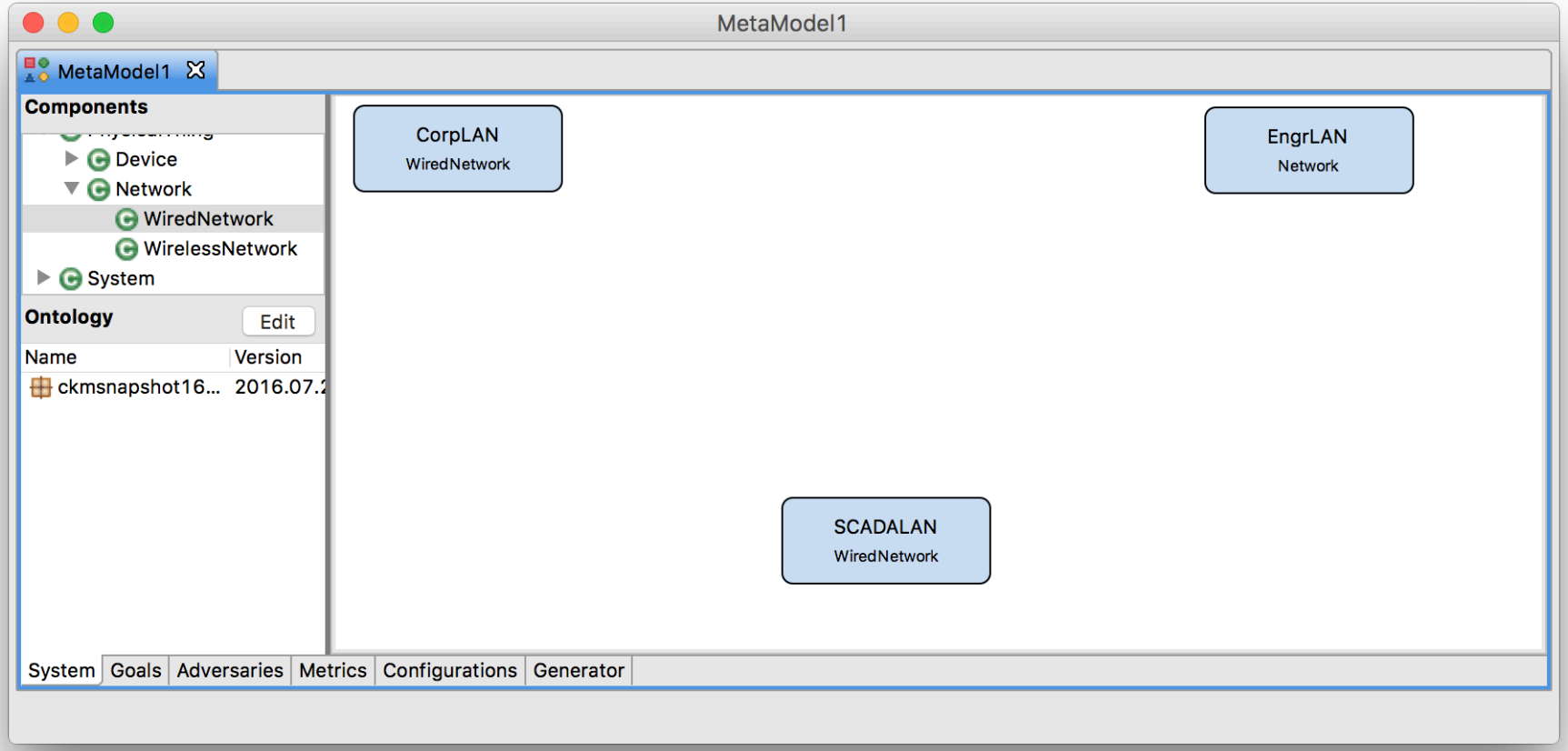
Step 2 – Model Systems

1. Select the **Network1** component and click the Edit Details button.
2. Change the name to **EngrLAN** and click Finish.



Step 2 – Model Systems

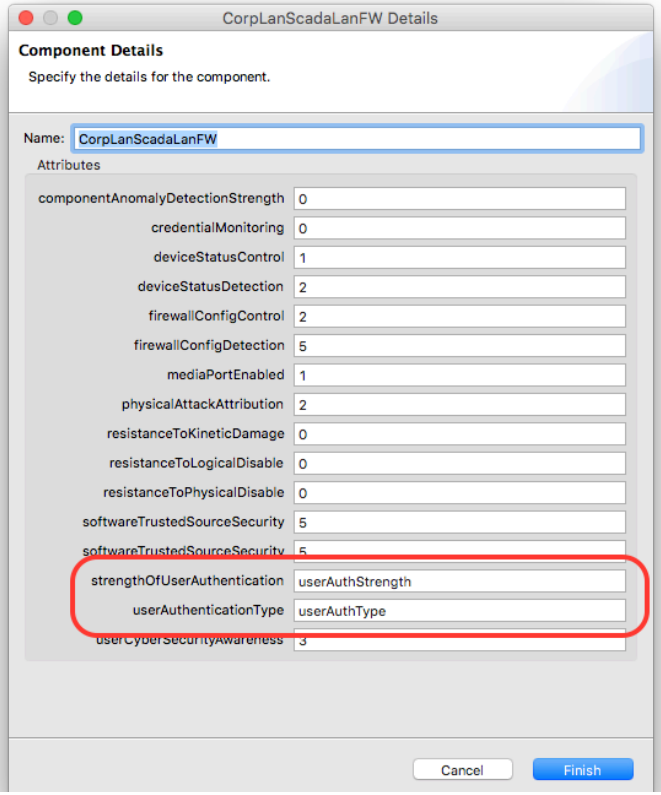
1. Create a **WiredNetwork** called **CorpLAN**
2. Create a **WiredNetwork** called **SCADALAN**



Step 2 – Model Systems

1. Create a **FirewallHosted** and define its attributes like so:

Attribute	Value
Name	CorpLanScadaLanFW
strengthOfUserAuthentication	userAuthStrength
userAuthenticationType	userAuthType



Step 2 – Model Systems

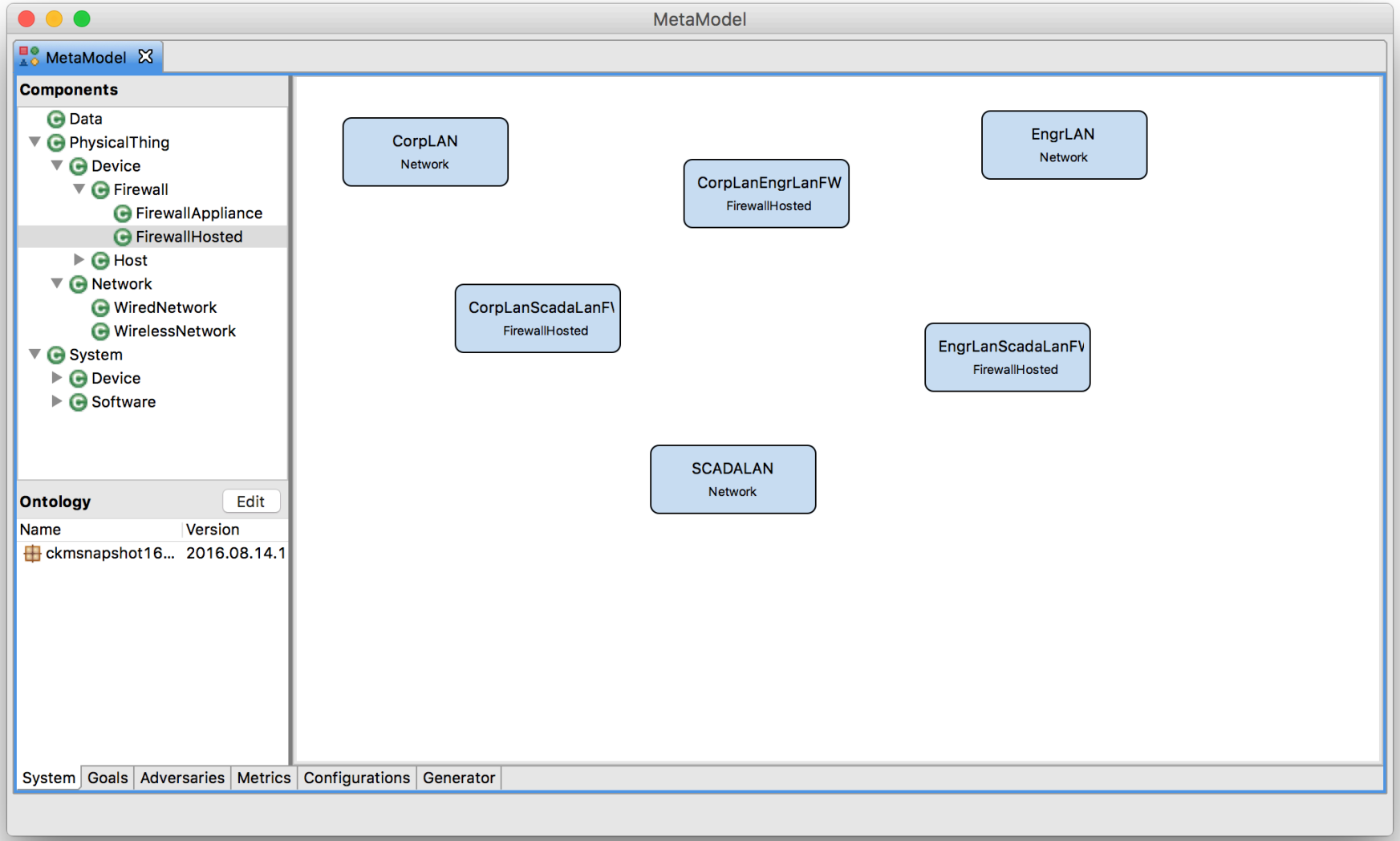
1. Create another **FirewallHosted**

Attribute	Value
Name	CorpLanEngrLanFW
strengthOfUserAuthentication	userAuthStrength
userAuthenticationType	userAuthType

2. Create another **FirewallHosted**

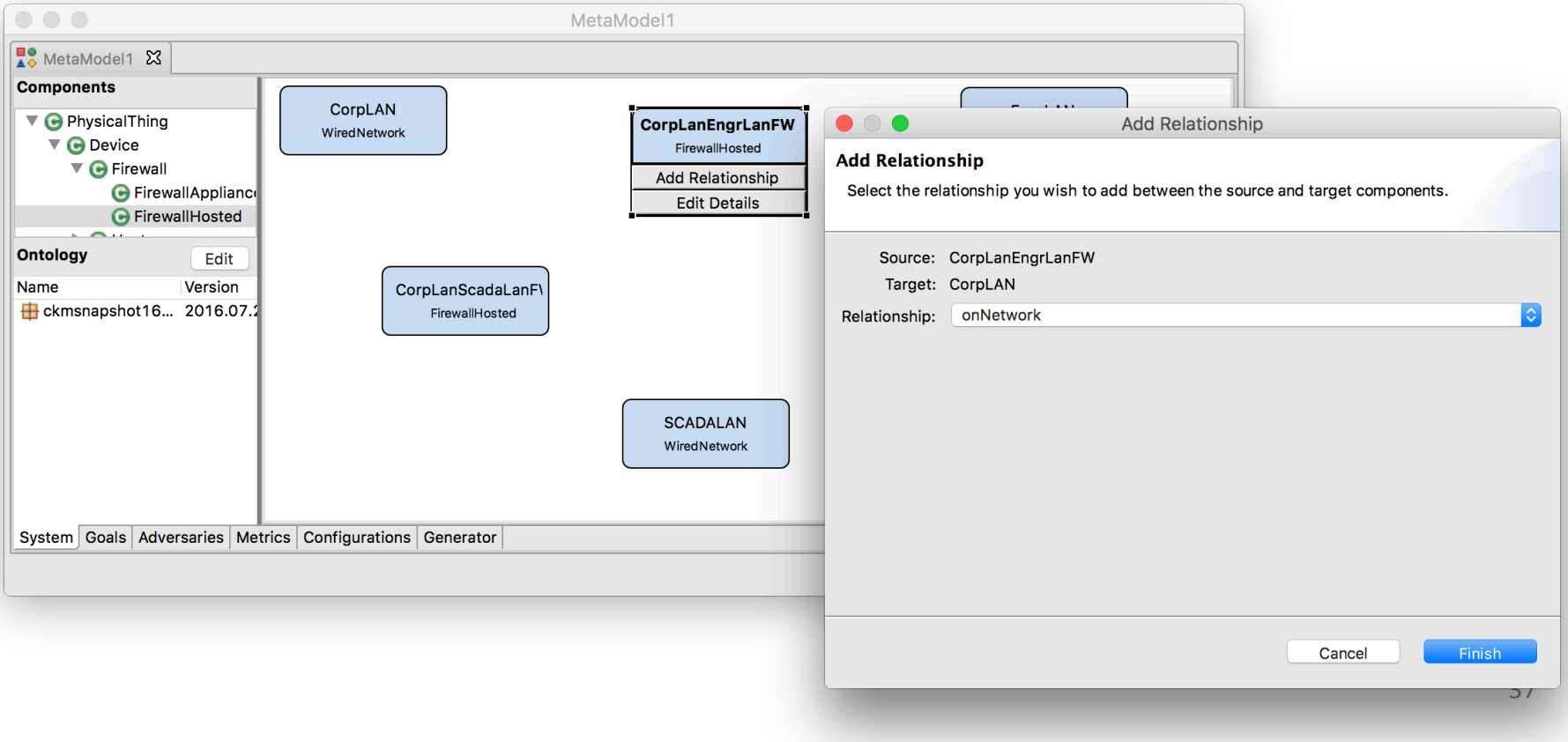
Attribute	Value
Name	EngrLanScadaLanFW
strengthOfUserAuthentication	userAuthStrength
userAuthenticationType	userAuthType

Step 2 – Model Systems



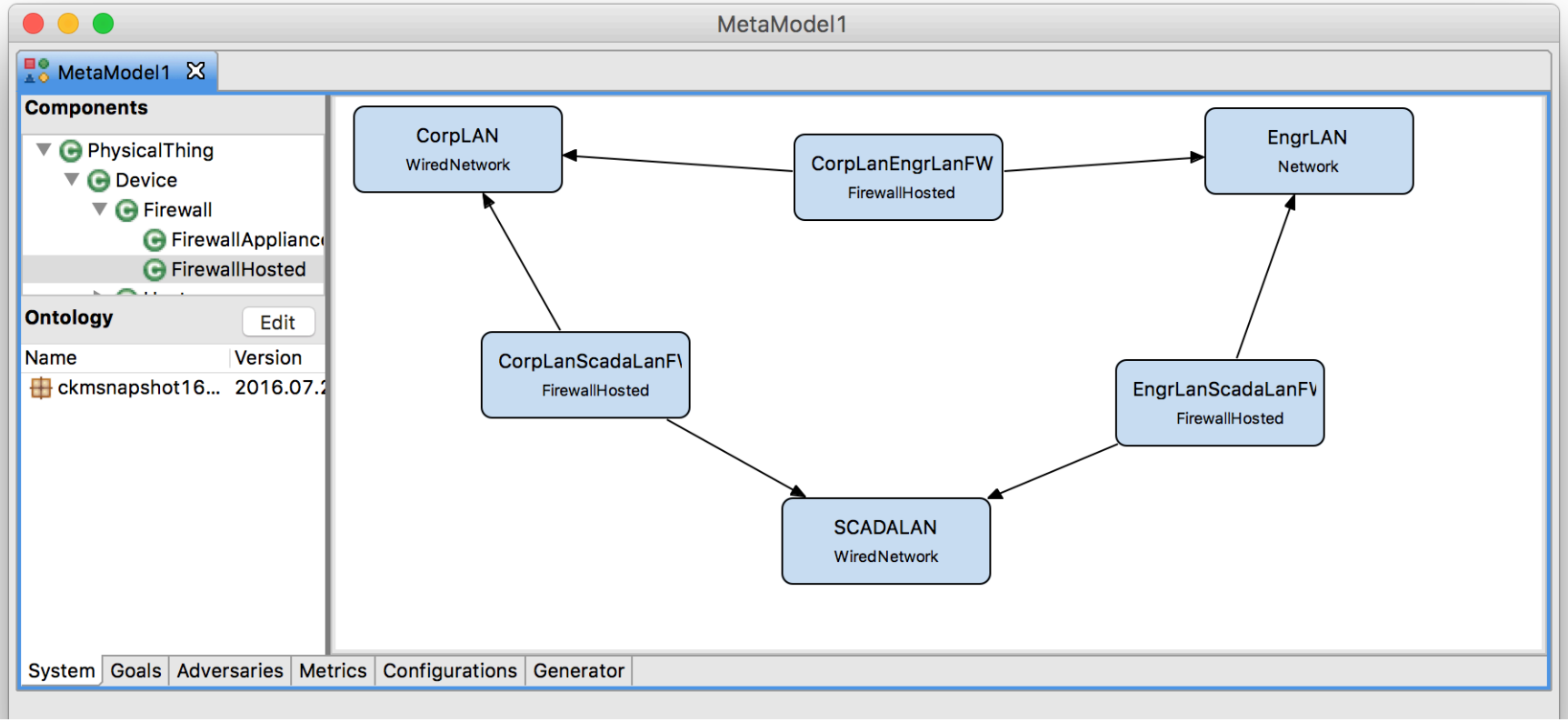
Step 2 – Model Systems

1. Select the **CorpLanEngrLanFW** component and click the Add Relationship button.
2. Select the **CorpLan** component.
3. Select the **onNetwork** relationship and click Finish.



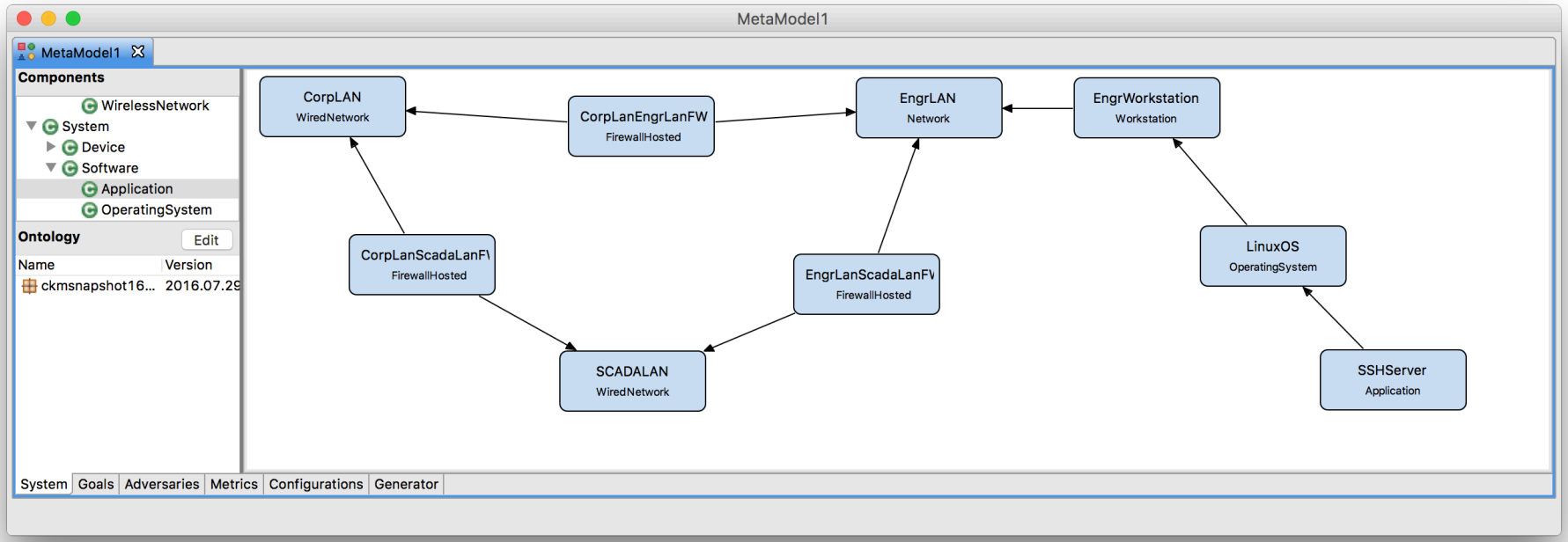
Step 2 – Model Systems

1. Create additional **onNetwork** relationships between:
   - **CorpLanEngrLanFW** to **EngrLAN**
   - **CorpLanScadaLanFW** to **CorpLAN**
   - **CorpLanScadaLanFW** to **SCADALAN**
   - **EngrLanScadaLanFW** to **EngrLAN**
   - **EngrLanScadaLanFW** to **SCADALAN**



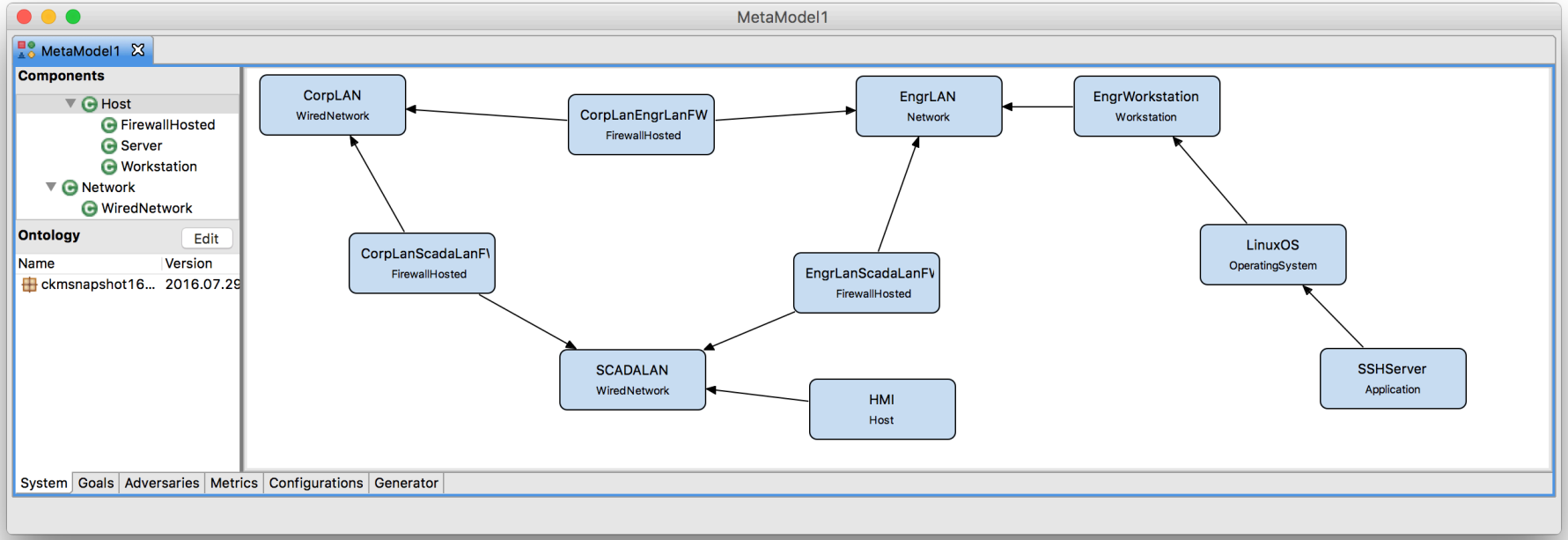
Step 2 – Model Systems

1. Create a **Workstation** called **EngrWorkstation**
2. Define an **onNetwork** relationship from **EngrWorkstation** to **EngrLAN**.
3. Create an **OperatingSystem** called **LinuxOS**.
4. Define a **hardwarePlatform** relationship from **LinuxOS** to **EngrWorkstation.**
5. Create an **Application** called **SSHServer**.
6. Define an **applicationOS** relationship from the **SSHServer** to **LinuxOS**.



Step 2 – Model Systems

1. Create a **Host** called **HMI**.
2. Define an **onNetwork** relationship from **HMI** to **SCADALAN**



Step 2 – Model Systems – Feedback

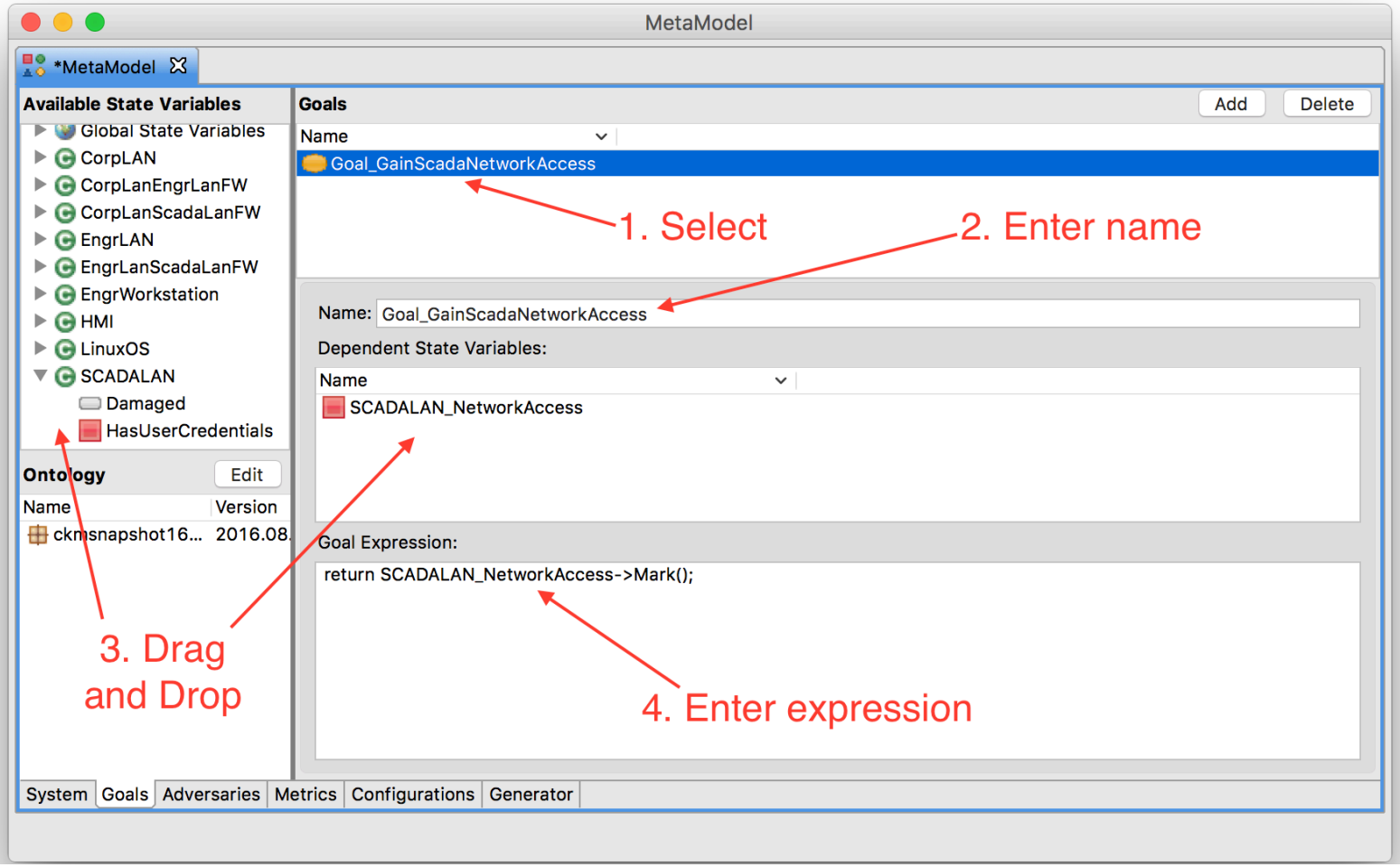
- How challenging was this step?
- Was adding components, creating relationships, and defining attributes easy?
- Could this part of the tool be useful for designing system diagrams for uses outside of the tool?
- How would you handle larger, more complex models? How would you expect the tool to help you with those models?
- Was the available components tree intuitive?

Step 3 – Attack Goals, Adversaries, Metrics, and Generation

- Possible attack goals are dependent on the system diagram
  - Choose a set of state variables (Access, Skill, Knowledge, SSV) the goal state is a function of.
  - Define the functional expression that indicates whether the goal has been achieved.

Small SCADA Networks – Step 3

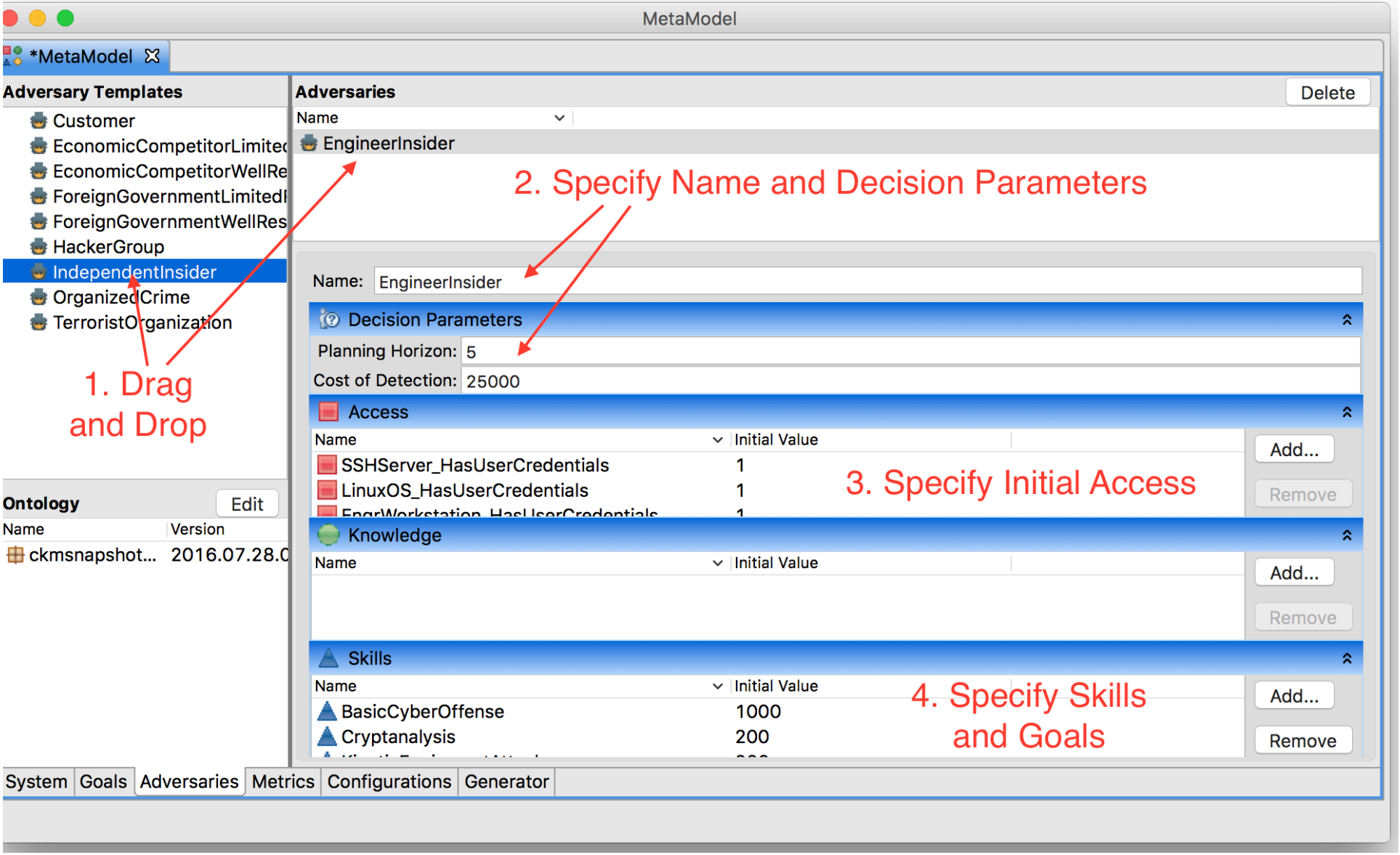
```
return SCADALAN_NetworkAccess->Mark();
```



Step 3 – Attack Goals, Adversaries, Metrics, and Generation

- Adversaries are created from Adversary Templates (defined in the ontology)
  - Attributes are customizable
  - Possible initial state depends on system diagram

Small SCADA Networks – Step 3



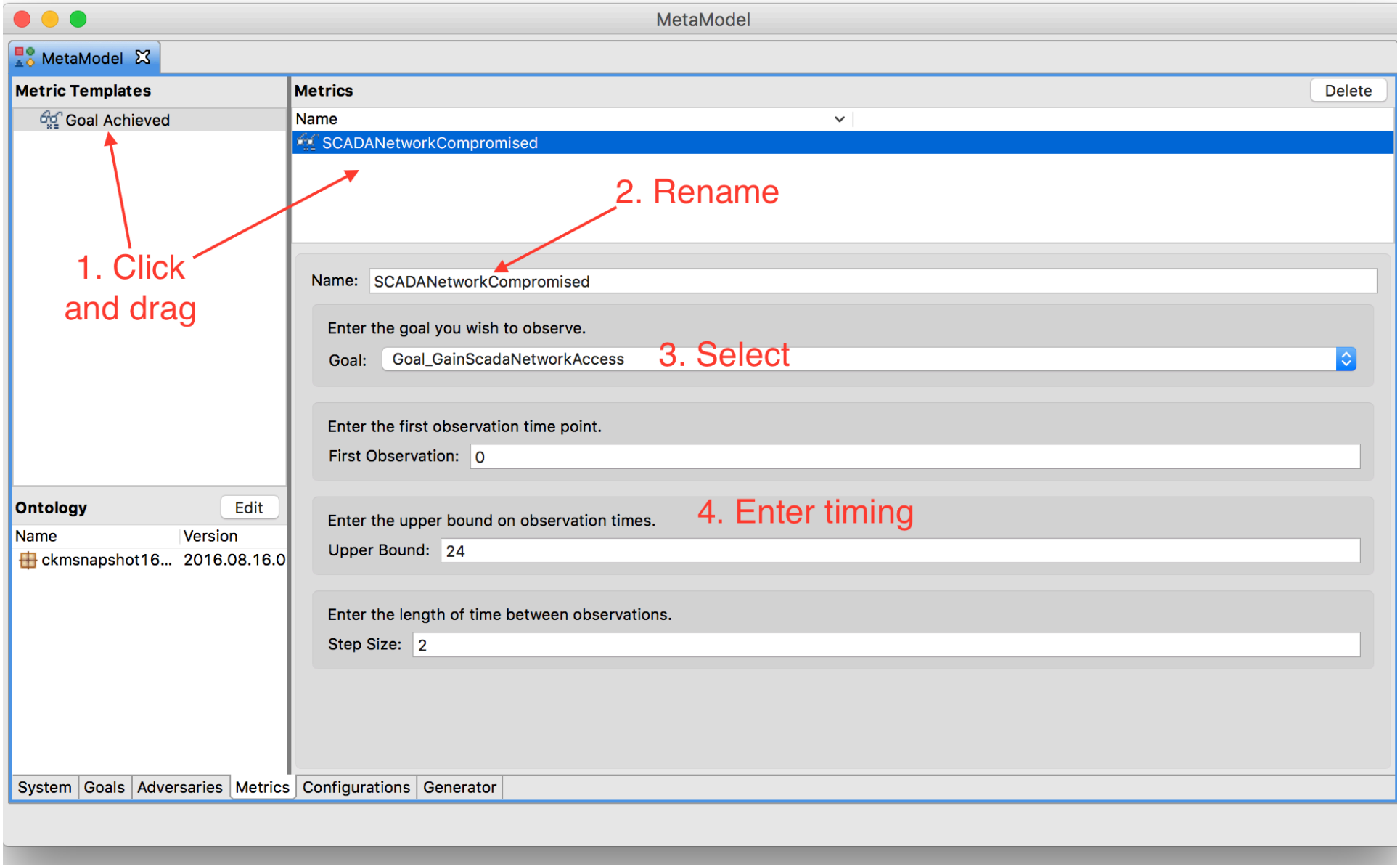
Small SCADA Networks – Step 3

1. Independent Insider
2. Name: EngineerInsider
   Cost of Detection: 100,000
3. Access: CorpLAN_PhysicalAccess
   CorpLanEngrLanFW_PhysicalAccess
   CorpLanScadaLanFW_PhysicalAccess
   EngrLAN_NetworkAccess
   EngrLAN_PhysicalAccess
   EngrLanScadaLanFW_PhysicalAccess
   EngrWorkstation_HasUserCredentials
   EngrWorkstation_LogicalAccess
   EngrWorkstation_PhysicalAccess
   EngrWorkstation_UIAccess
   HMI_PhysicalAccess
   LinuxOS_HasUserCredentials
   LinuxOS_LogicalAccess
   LinuxOS_UIAccess
   SCADALAN_PhysicalAccess
   SSHServer_HasUserCredentials
   SSHServer_LogicalAccess
   SSHServer_UIAccess
4. Goal: Goal_GainNetworkAccessOnScadaNetwork 50,000

Step 3 – Attack Goals, Adversaries, Metrics, and Generation

- Metrics are created from Metric Templates (defined in the ontology)
  - Input parameters are defined in the ontology
  - Input values specified by the user

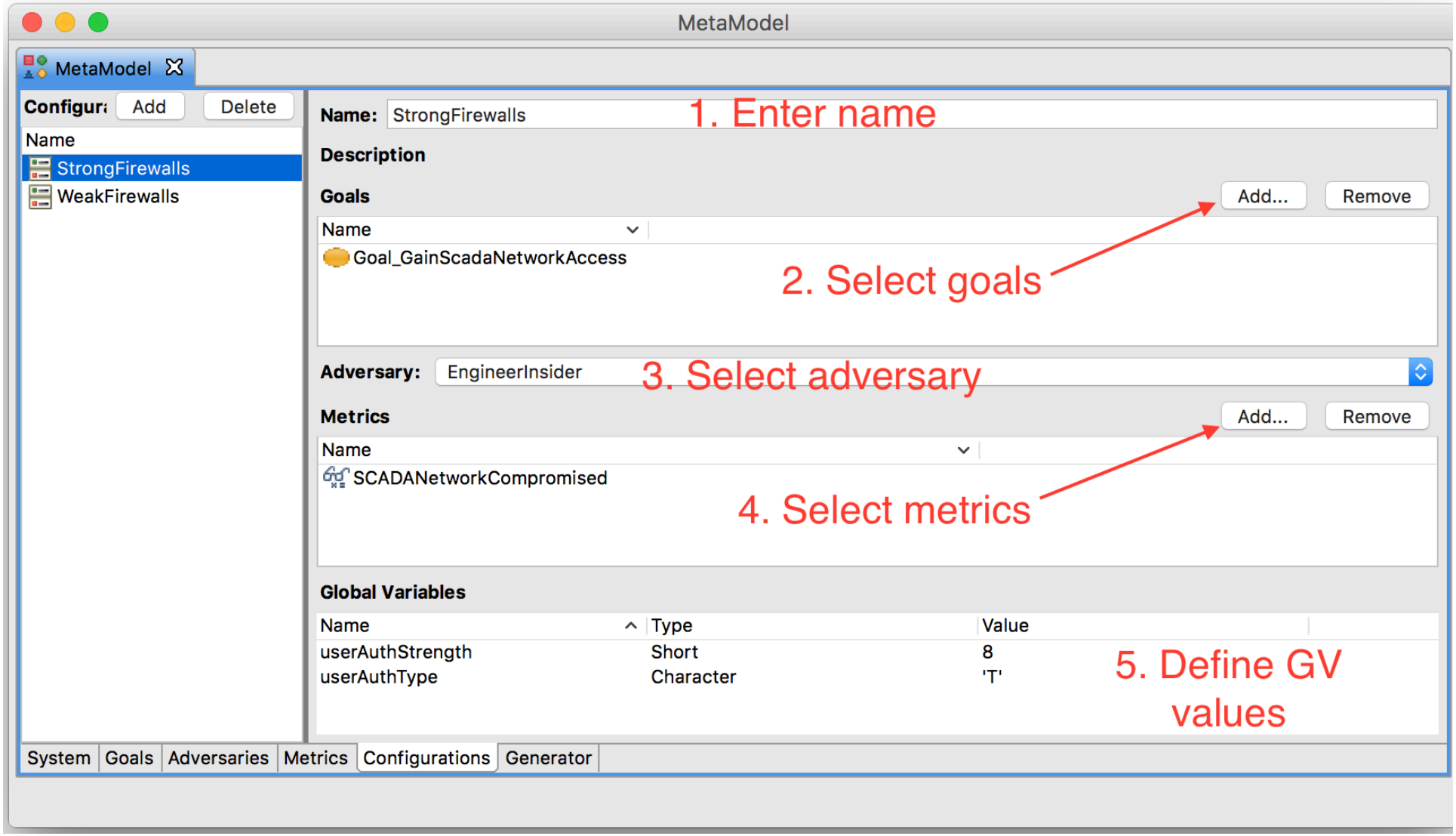
Small SCADA Networks – Step 3



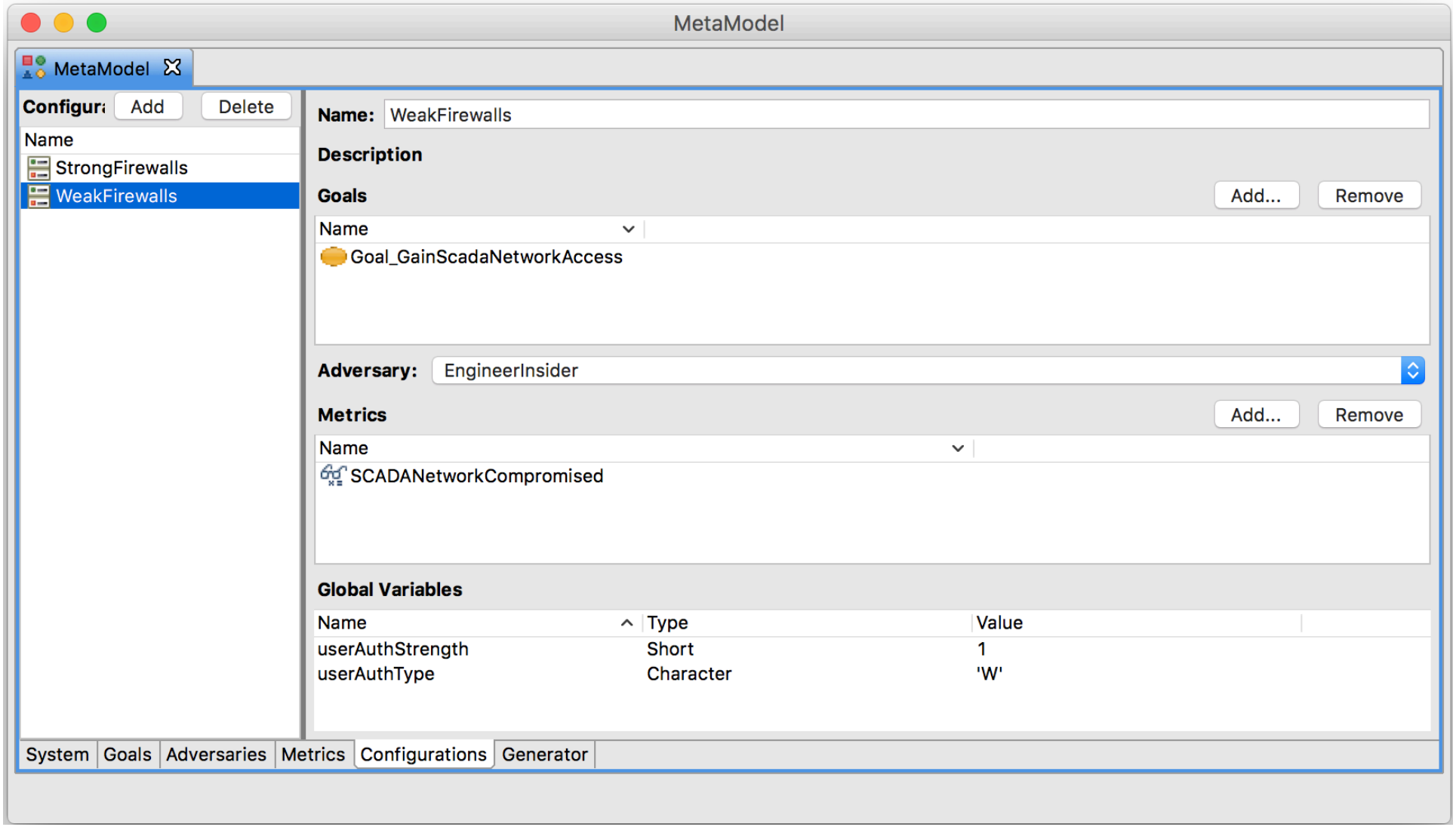
Step 3 – Attack Goals, Adversaries, Metrics, and Generation

- Configurations bring together a goal set, an adversary, and a metric set.
  - Multiple configurations will generate as one model
  - Each configuration will be an experiment
  - Simulator will run each experiment separately and report results

Small SCADA Networks – Step 3



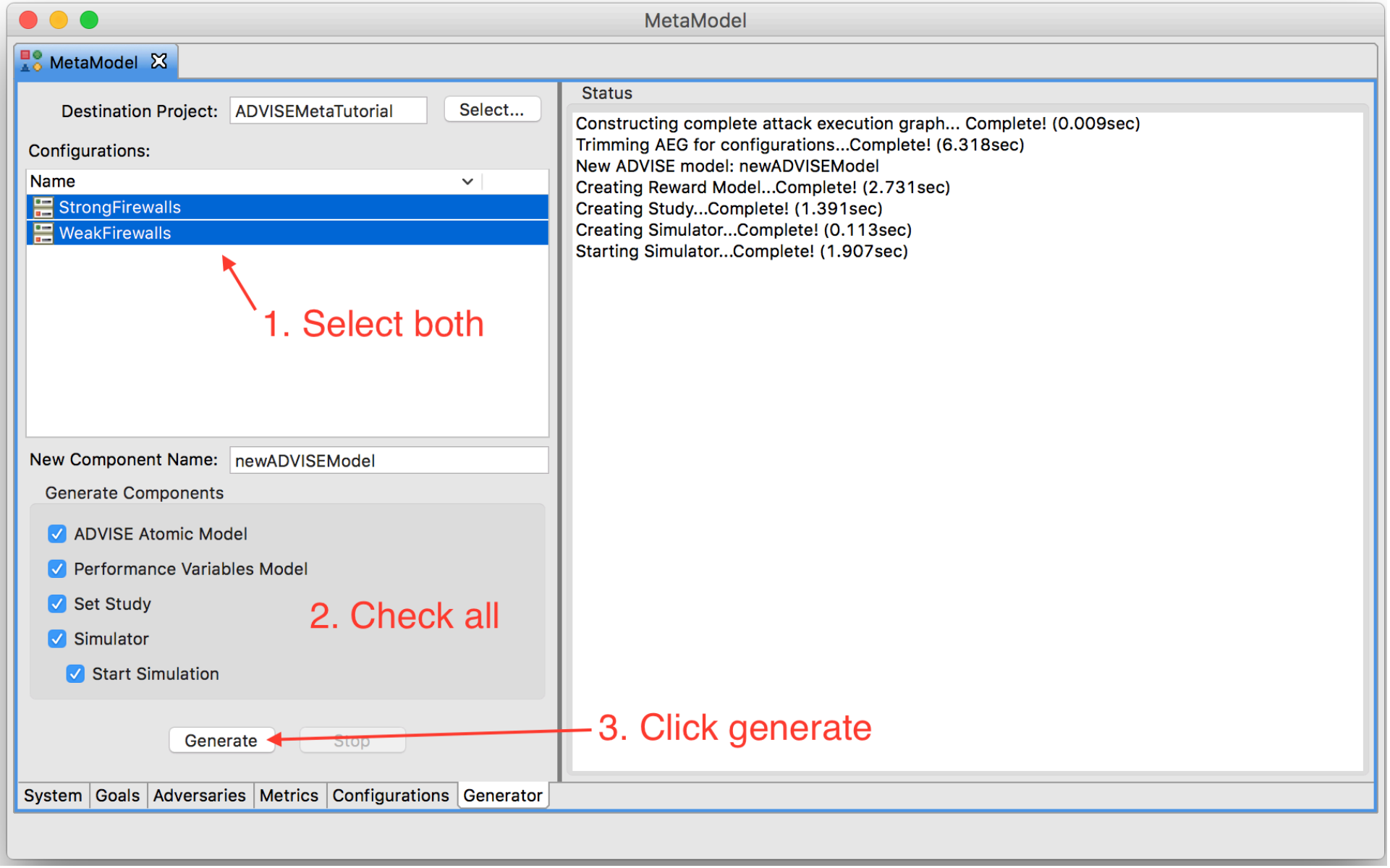
Small SCADA Networks – Step 3



Step 3 – Attack Goals, Adversaries, Metrics, and Generation

- The generator creates multiple components in the Mobius Modeling Tool and begins simulation.
  - The components are an ADVISE model, a Performance Variables model, a Set study, and a Discrete Event Simulator.
  - Simulation should take about a minute.
  - Numerical results are show once completed.

Small SCADA Networks – Step 3

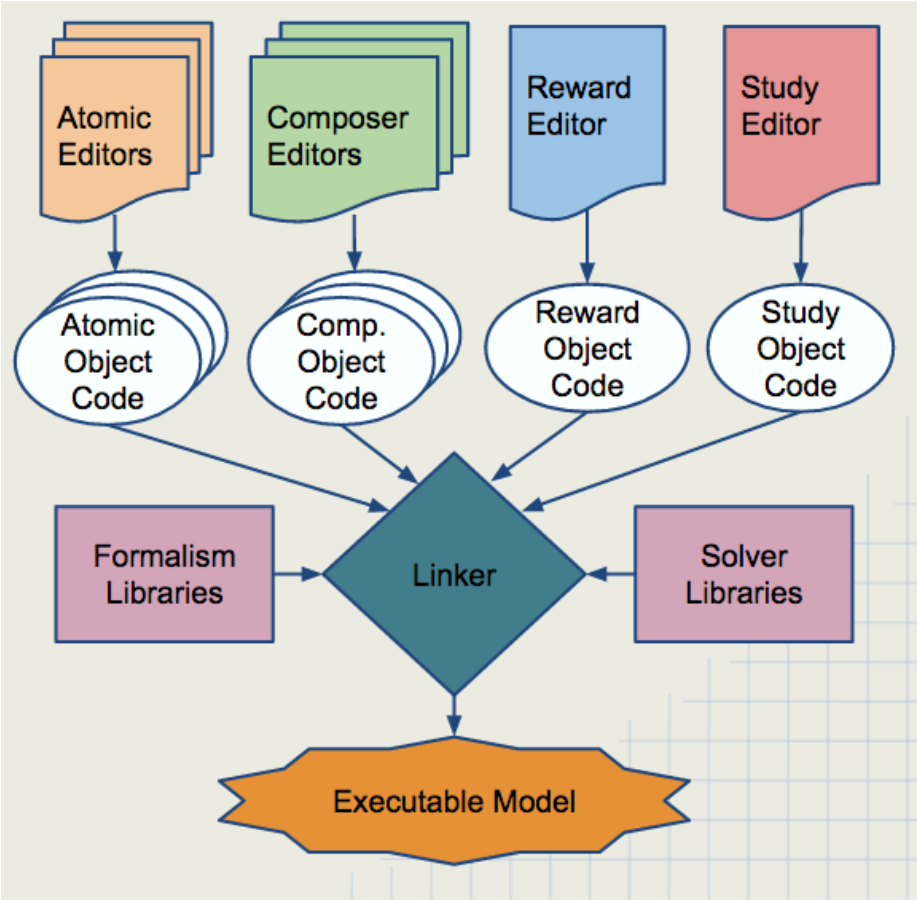


Step 3 – Attack Goals, Adversaries, and Generation – Feedback

- How challenging was this step?
- Did the goal definition seem intuitive?
- What other adversary templates would you look for?
- Does the configuration of an adversary's attributes make sense?

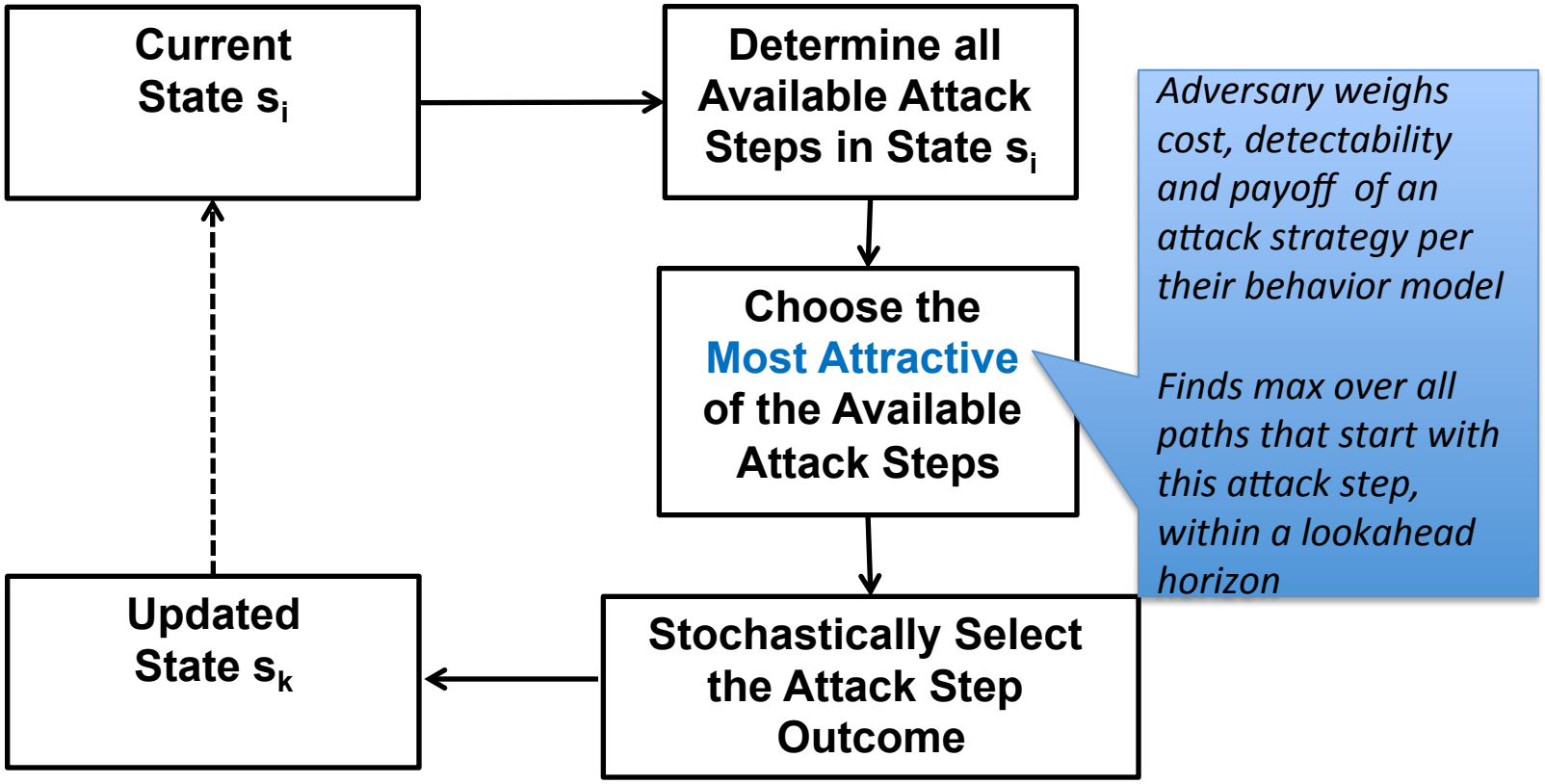
Step 4 – Execute Models

- Möbius creates an executable model by:
  - Generating C++ code representations of project models
  - Compiling the code and linking formalism and solver libraries
  - Executing the binary to gather observations and calculate statistics



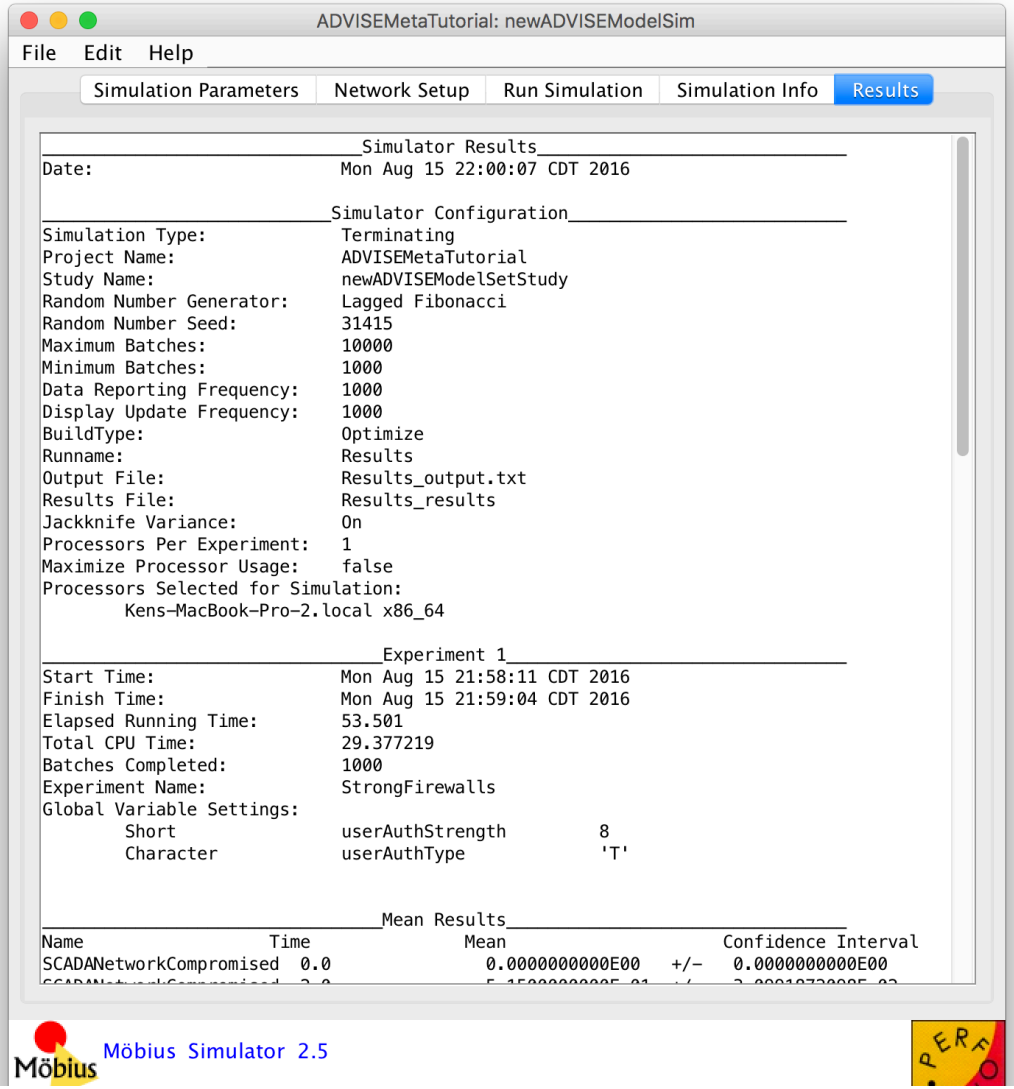
Step 4 Execute Models - Adversary Decision Cycle

- Adversary selects most attractive available attack step in AEG, repeats
- State transitions determined by outcome of selected attack step



Small SCADA Networks – Step 4

Simulation Is Complete



Step 5 – Interpret Results

- We will examine…
  - Numerical results from the simulation
  - A visual presentation of the model's behavior

Small SCADA Networks – Step 5

Numerical Results

- Adversary was more successful, more quickly when firewalls were hardened.

```
Experiment Name:                WeakFirewalls
Global Variable Settings:
        Short                   userAuthStrength        1
        Character               userAuthType            'W'


_____________________________________Mean Results_____________________________________
Name                    Time                Mean                        Confidence Interval
SCADANetworkCompromised  0.0                  0.0000000000E00   +/-   0.0000000000E00
SCADANetworkCompromised  2.0                  0.0000000000E00   +/-   0.0000000000E00
SCADANetworkCompromised  4.0                  3.0000000000E-03  +/-   1.0719782991E-03  (*)
SCADANetworkCompromised  6.0                  3.6300000000E-02  +/-   3.6660807717E-03  (*)
SCADANetworkCompromised  8.0                  1.6290000000E-01  +/-   7.2381403552E-03
SCADANetworkCompromised  10.0                 3.4830000000E-01  +/-   9.3385271315E-03
SCADANetworkCompromised  12.0                 4.9200000000E-01  +/-   9.7992354937E-03
SCADANetworkCompromised  14.0                 5.8290000000E-01  +/-   9.6648453634E-03
SCADANetworkCompromised  16.0                 6.6230000000E-01  +/-   9.2698070620E-03
SCADANetworkCompromised  18.0                 7.3310000000E-01  +/-   8.6702911980E-03
SCADANetworkCompromised  20.0                 7.8630000000E-01  +/-   8.0347836302E-03
SCADANetworkCompromised  22.0                 8.2660000000E-01  +/-   7.4207881630E-03
```

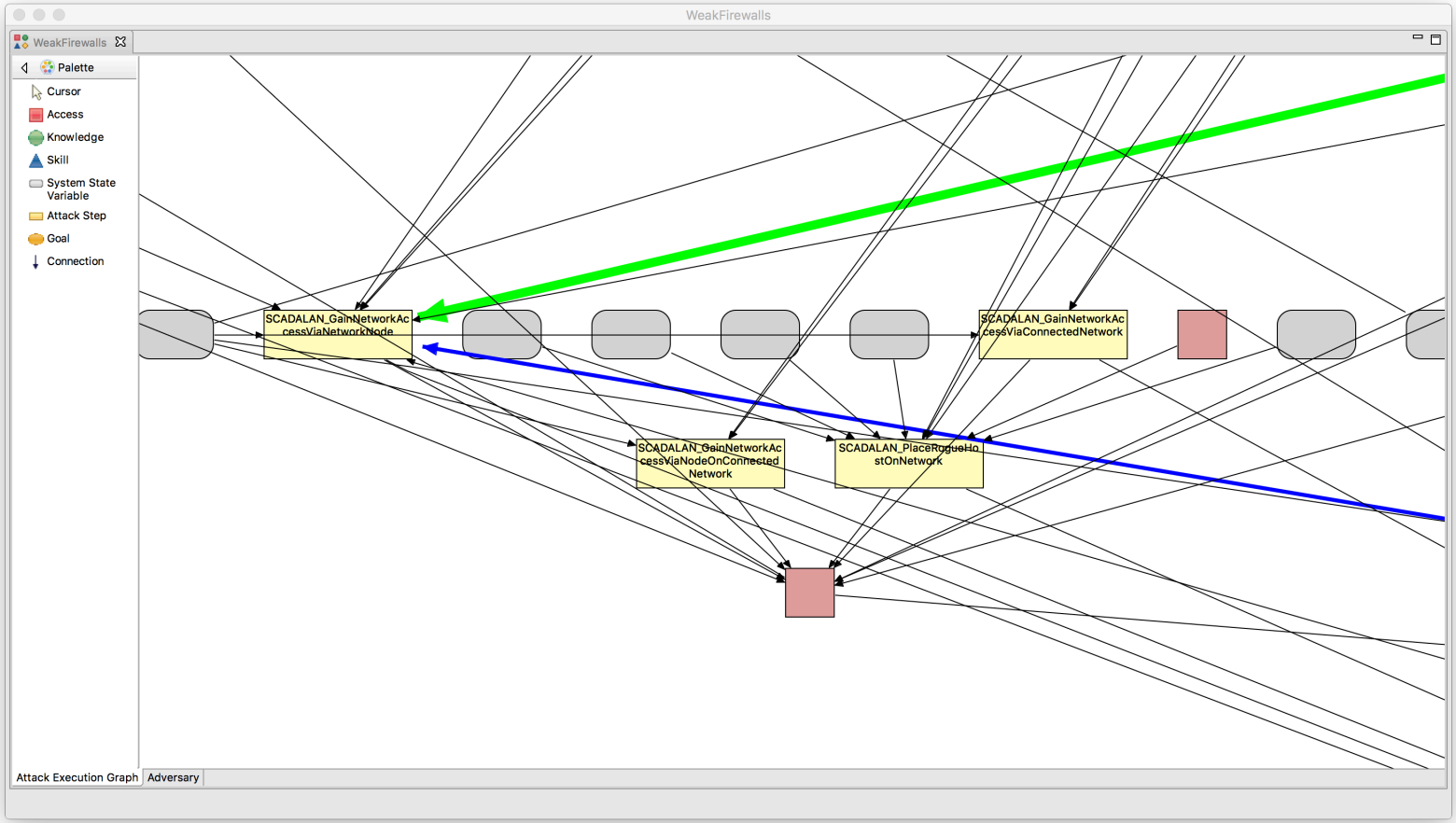
```
Experiment Name:                StrongFirewalls
Global Variable Settings:
        Short                   userAuthStrength        8
        Character               userAuthType            'T'


_____________________________________Mean Results_____________________________________
Name                    Time                Mean                        Confidence Interval
SCADANetworkCompromised  0.0                  0.0000000000E00   +/-   0.0000000000E00
SCADANetworkCompromised  2.0                  5.1500000000E-01  +/-   3.0991872098E-02
SCADANetworkCompromised  4.0                  9.7000000000E-01  +/-   1.0578396025E-02
SCADANetworkCompromised  6.0                  1.0000000000E00   +/-   0.0000000000E00
SCADANetworkCompromised  8.0                  1.0000000000E00   +/-   0.0000000000E00
SCADANetworkCompromised  10.0                 1.0000000000E00   +/-   0.0000000000E00
SCADANetworkCompromised  12.0                 1.0000000000E00   +/-   0.0000000000E00
SCADANetworkCompromised  14.0                 1.0000000000E00   +/-   0.0000000000E00
SCADANetworkCompromised  16.0                 1.0000000000E00   +/-   0.0000000000E00
SCADANetworkCompromised  18.0                 1.0000000000E00   +/-   0.0000000000E00
SCADANetworkCompromised  20.0                 1.0000000000E00   +/-   0.0000000000E00
SCADANetworkCompromised  22.0                 1.0000000000E00   +/-   0.0000000000E00
SCADANetworkCompromised  24.0                 1.0000000000E00   +/-   0.0000000000E00
```

Small SCADA Networks – Step 5

Visual Results

- Adversary chose to directly compromise the HMI, rather than go through the firewalls when the firewalls were hardened.



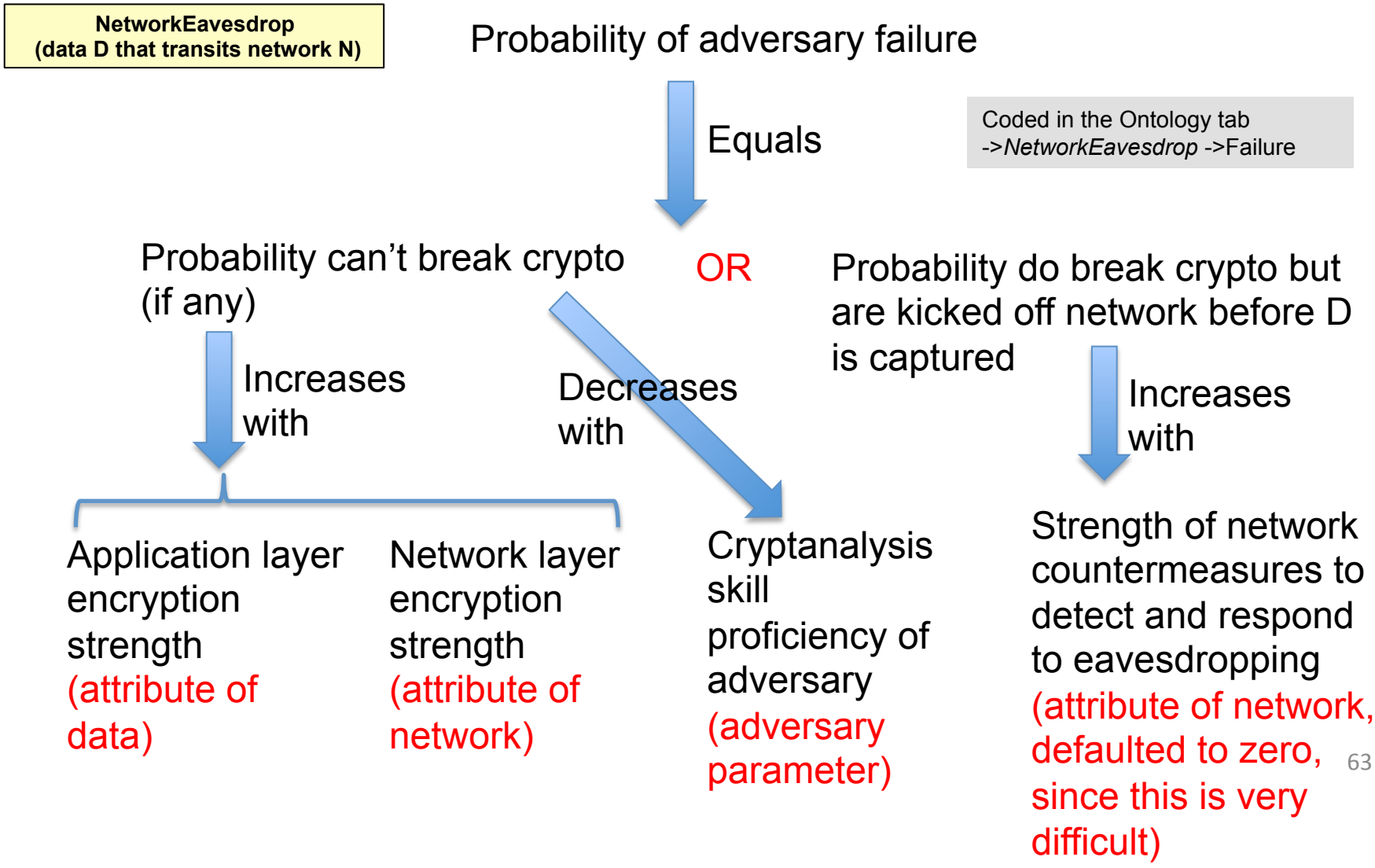
Step 5 – Interpret Results – Feedback

- Were you surprised by the results?
- Do you believe unexpected results could be useful?
- What more would you like to know about the model to make design decisions based on what you've learned?
- How could the results presentation be improved?

Agenda

- Registration and Continental Breakfast
- Welcome
- Goals
  - Tool
  - Workshop
- Steps to Use ADVISE Meta
- Hands on Sessions
- Case Studies and Custom Ontologies
- Wrap Up

Attack Step Details: Example Probability Calculation



Skill Details: What does skill proficiency mean?

Basic cyber offense	This is a set of skills not further distinguished, some level of which are available via relatively inexpensive tools to any adversary. These include the following elements from the Ethical Hacking Certification Syllabus at https://www.eccouncil.org/Certification/professional-series/ceh-course-outline : scanning, enumeration, phishing attack, password cracking based on external information (guessing, replay), privilege escalation, hijacking web servers, hacking web applications, SQL injection, buffer overflow, straightforward DoS attacks, network sniffing, social engineering without human contact (for which phishing is an example).	1000	Lead individual employed by a nation state to conduct cyber attacks
		800	Individual with broad skills including stealth, which would earn admirers in the hacking community
		600	Individual with solid skills that could be employed to perform ethical hacking engagements
		400	Individual with solid skills in many areas listed, but weak in a few
		50	Individual can perform simple script-based attacks

In the base ontology, probability of success/failure of an attack step often has a linear relationship with one or two skills

- e.g. a generic skill OR a specialized skill impacts outcome

Custom Ontologies

- The base ontology is data, it is not baked into the tool
- "Library designer" (tool distributor or user) may on the ontology tab:
  - Add to or modify base ontology
  - Define a new custom ontology
- This includes all categories of ontology elements:
  - Types of components 
  - Attributes of components by type 
  - Relationships between components 
  - Types of access,  skills,  and knowledge  an adversary may have
  - Types and characteristics of adversaries 
  - Attack steps 
  - State variables: other system, component, or adversary properties 

Features for Future Base Ontology

- Component ontology
  - Types of networks (LAN, WAN, VLAN)
  - VPN connections
  - Routers
  - Gateways
  - Device authentication
  - User roles

Features for Future Base Ontology (cont.)

- Attack steps
  - Disable or Damage
    - PhysicalDisconnect
    - NetworkFlood
    - Botnet
  - Malware
    - CreateRemovableMediaCauseMalwareInstall
    - Stage PackageCauseMalwareInstall
    - InstallMalwareFromRemovableMedia
    - InstallMalwareFromFixedMedia
    - Impact of installed malware
  - Data Confidentiality
    - Exfiltrate data
  - Network Infrastructure
    - Router and switch attacks
  - 0 - days

Examples for Custom Ontologies

- Add component types with unique defaults, attributes, and/or attack steps
  - Virtual OS – build model of data center
  - ATM machine – build model of banking organization
  - Smartmeter – build model of planned smart grid architecture
- Add customized adversary(e.g. contractor with specific types of access)
- Modify formulas used to calculate attack step characteristics
  - Probability of success/failure of attack step
  - Detectability of an attack step outcome
  - Cost of attack step
  - Time to execute attack step
- Build ontology to model internal architecture of a modern electric vehicle together with associated charging stations
- See tutorial to try out creating an ontology https://www.mobius.illinois.edu/wiki/index.php/ADVISE_Meta_Two_Nets_Tutorial

River Zonal Dispatcher Case Study

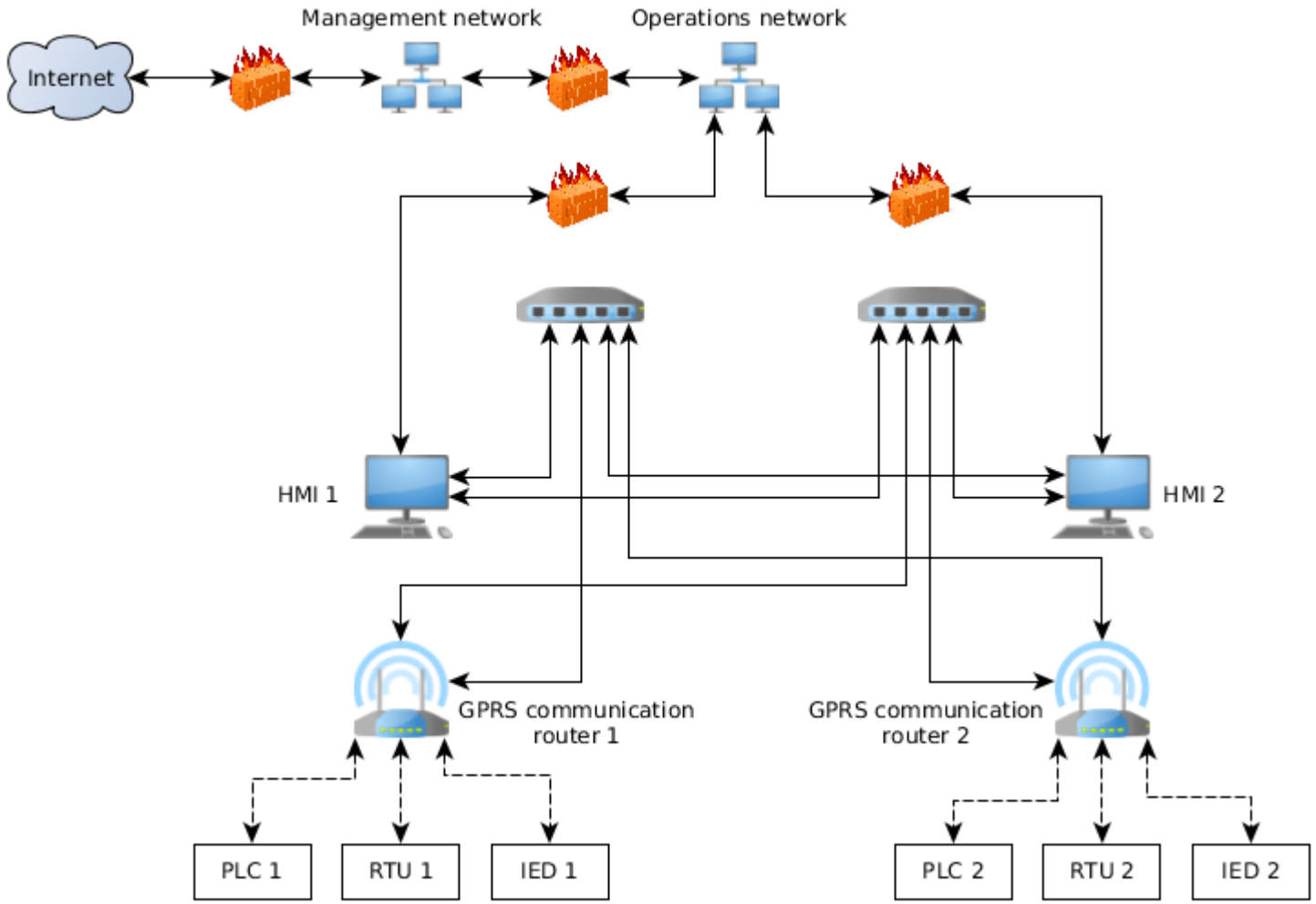
Purpose of analysis

- Investigate the effects of architectural changes on system security
- Analyze the security impact of intrusion detection systems (IDSes) and isolation
- Analyze the security impact of multiple subsystems

River Zonal Dispatcher Case Study

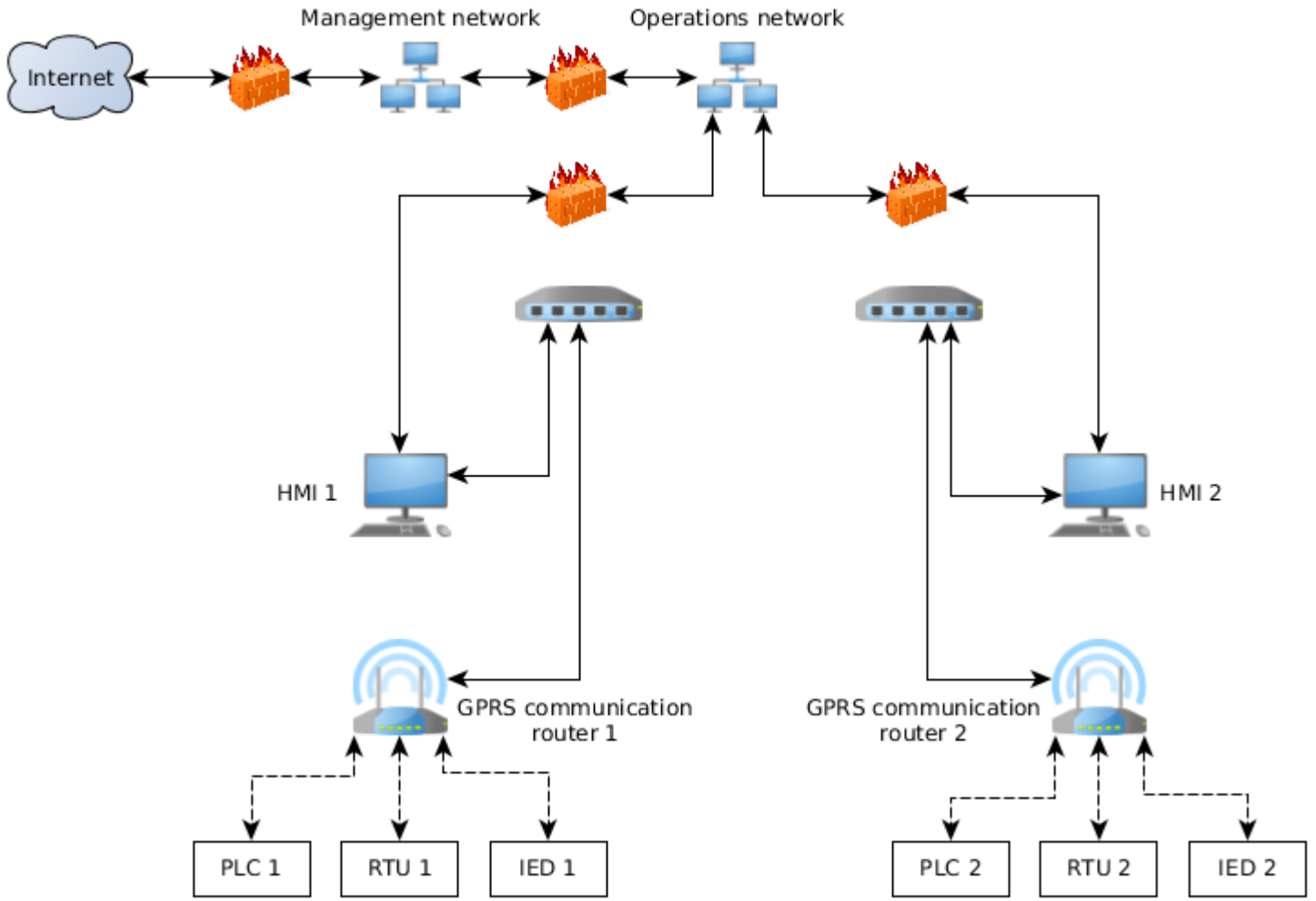
River Zonal Dispatcher Case Study

Without isolation

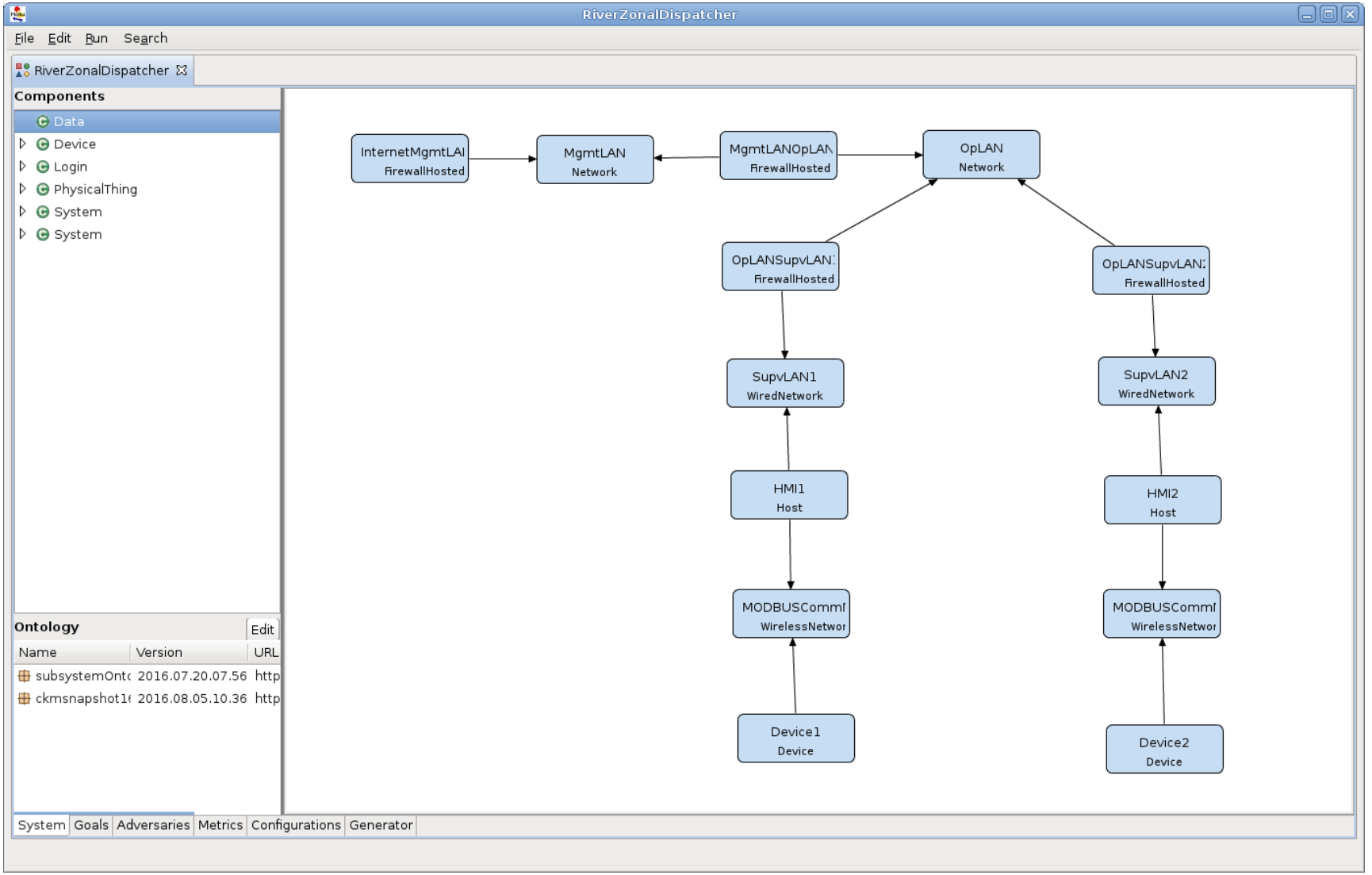


River Zonal Dispatcher Case Study

With isolation



River Zonal Dispatcher Case Study



River Zonal Dispatcher Case Study

Model attack goals

- Install malware on HMI
- Compromise system via router
- Compromise system via devices

Five adversaries are

- Foreign government
- Hacker
- Hostile Organization
- Insider Engineer
- Insider Operator

River Zonal Dispatcher Case Study

Select metrics

- Average Number of Successful Attacks
- Probability of Attack Goals Achieved at End Time
- Average Time-To-Achieve-Goal

River Zonal Dispatcher Case Study

Generate and execute models

- Set up 20 configurations for execution
  - Each of 5 adversaries X 4 system models
  - Calculate all metrics
- Simulation models adversary behavior over 1 year
- Ran 1,000 to 10,000 iterations

River Zonal Dispatcher Case Study

Results from hand-built model

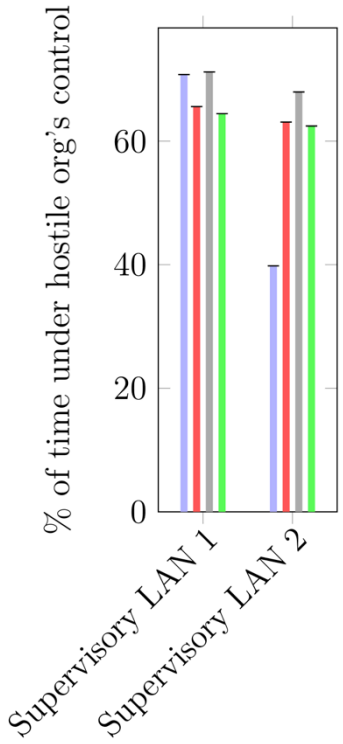


Figure 1: Average percentages of time in which the hostile organization has control of an on-site device on a particular supervisory network.

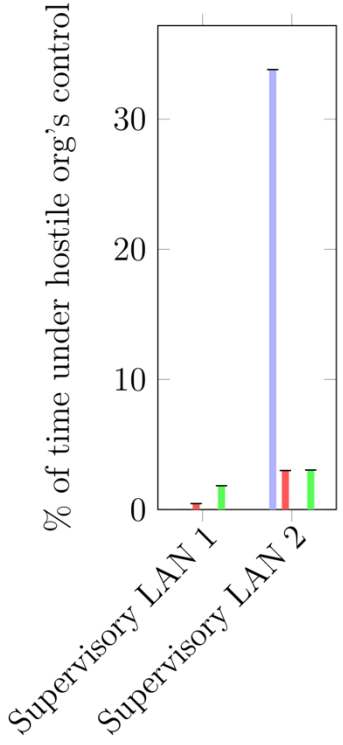


Figure 2: Average percentages of time in which the hostile organization has control of a GPRS communication router on a particular supervisory network.

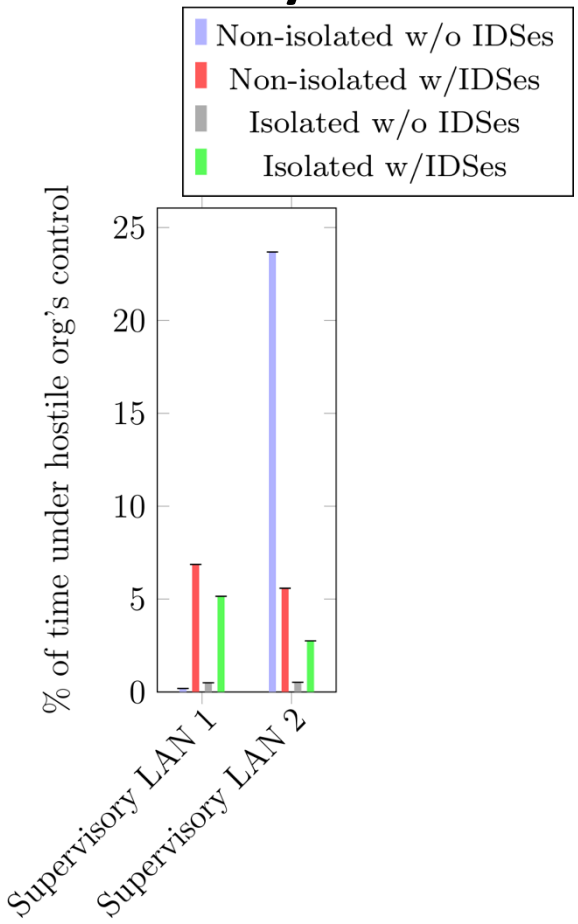


Figure 3: Average percentages of time that an HMI on a particular network has backdoor software installed by a hostile organization.

River Zonal Dispatcher Case Study

Results from hand-built model

- Greatest value seen in device attacks
- Neither IDSes nor isolation effective in minimizing device attacks
- IDSes very effective in minimizing router attacks and backdoor software installation on LAN 2 with non-isolated HMIs
- Isolation effective in minimizing router attacks and backdoor software installation overall
- LAN 2 preferred for router attacks and backdoor software installation, despite higher payoffs for attacks on LAN 1

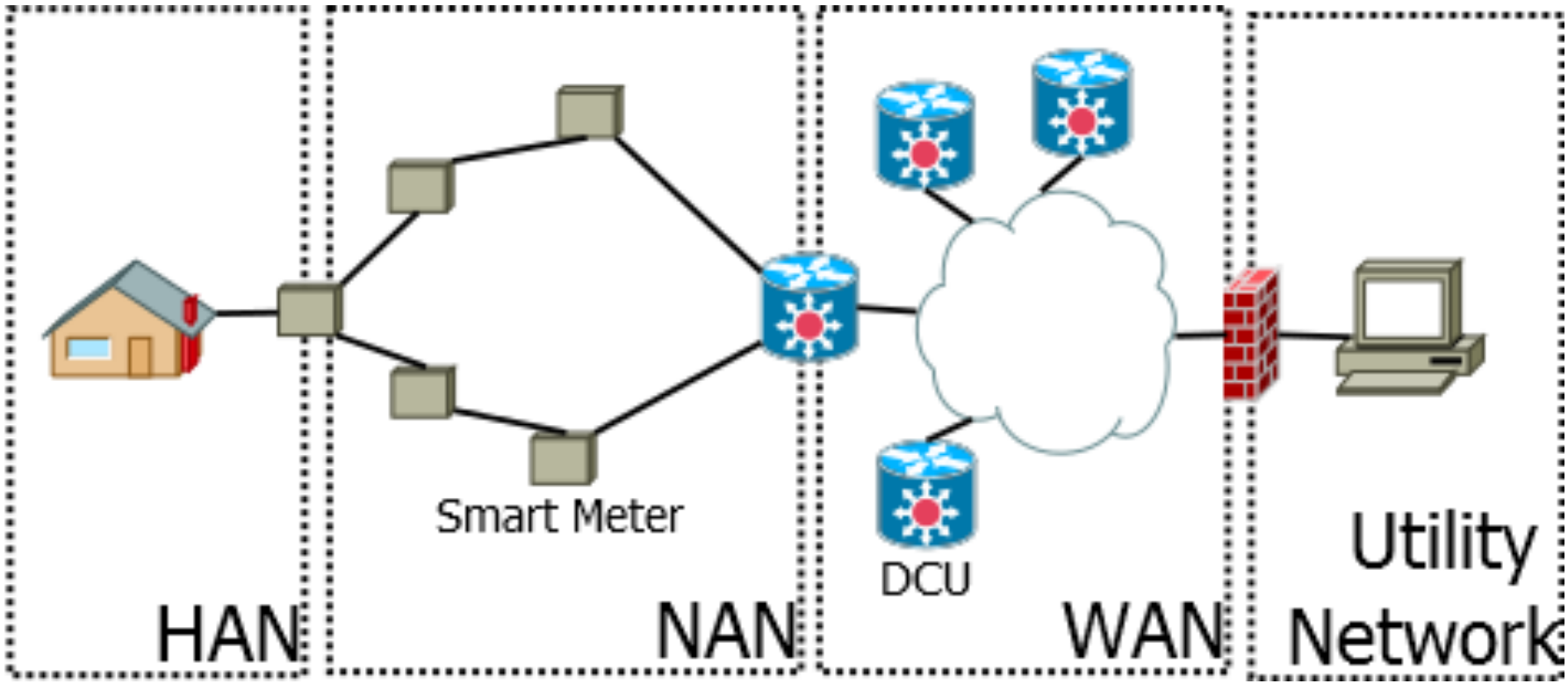
Advanced Metering Infrastructure Case Study

Define purpose of analysis

- Determine the cost-effectiveness of different intrusion detection systems (IDSes) in an Advanced Metering Infrastructure (AMI) network.
- In particular, compare
  - Centralized IDS,
  - Distributed IDS, and
  - Embedded IDS.

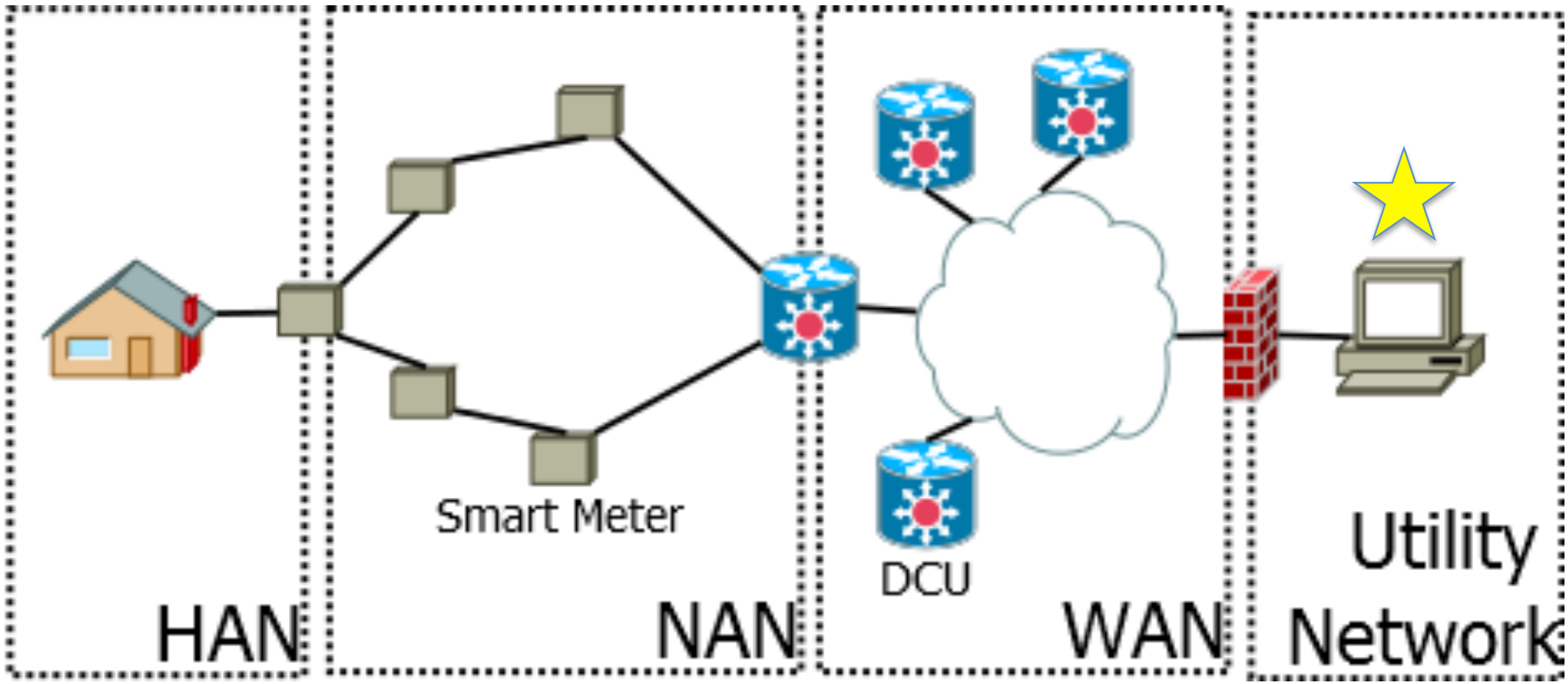
Advanced Metering Infrastructure Case Study

Define system components, relationship and attributes



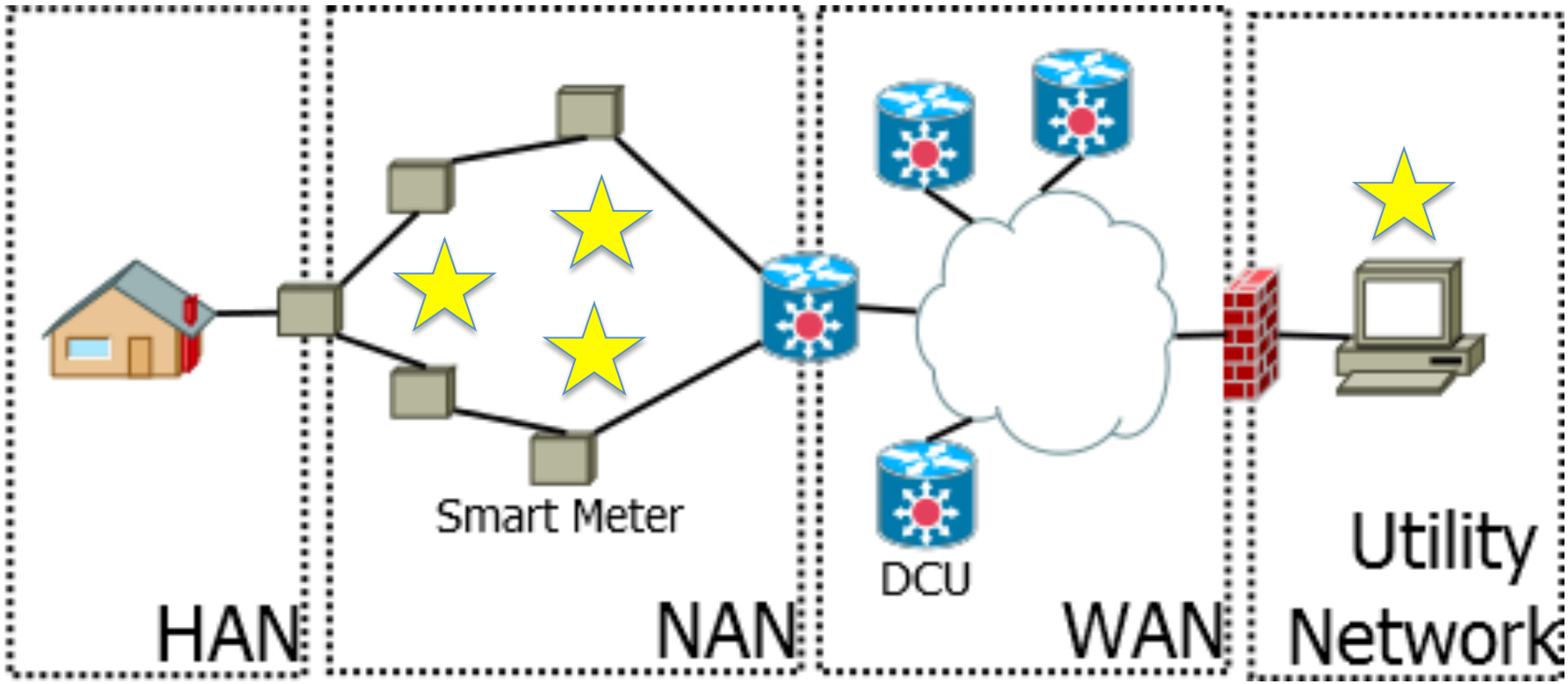
Advanced Metering Infrastructure Case Study

Define system components, relationship and attributes



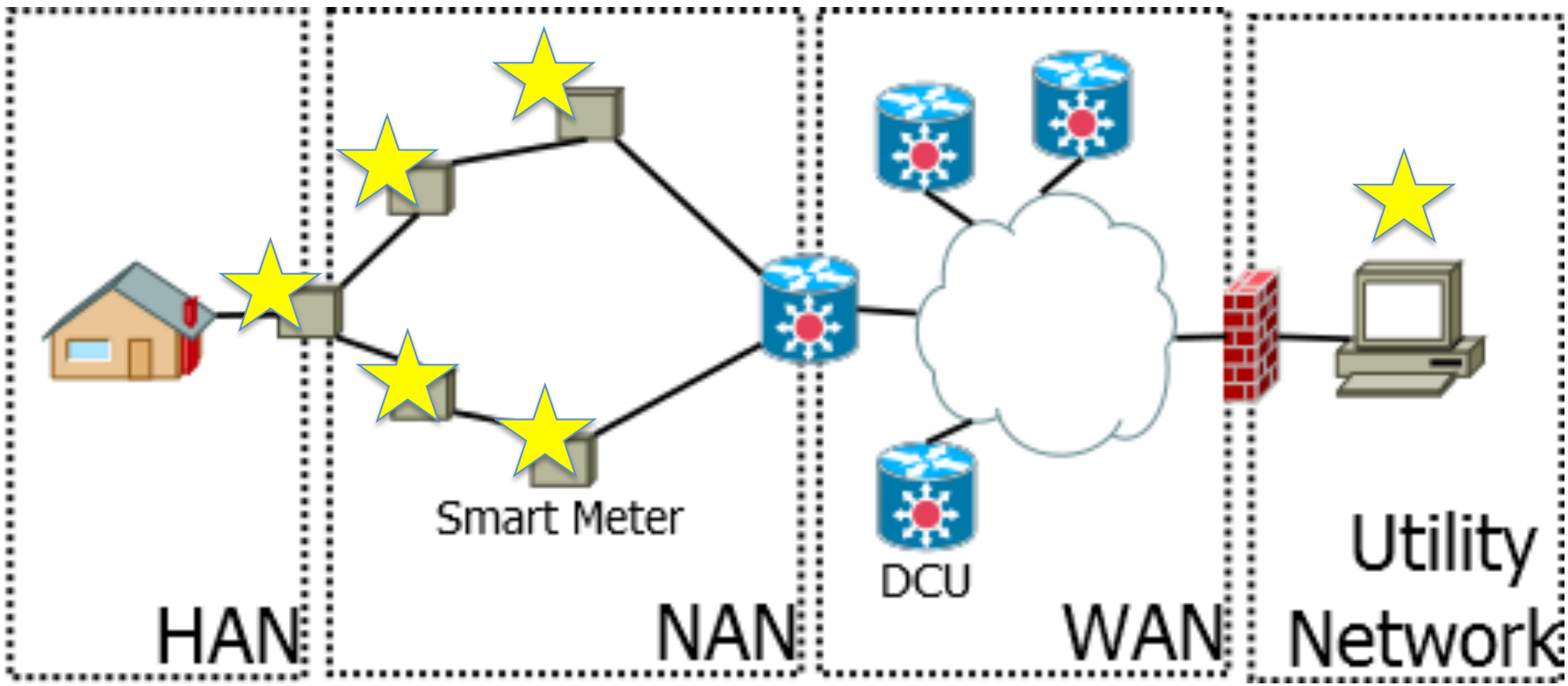
Advanced Metering Infrastructure Case Study

Define system components, relationship and attributes

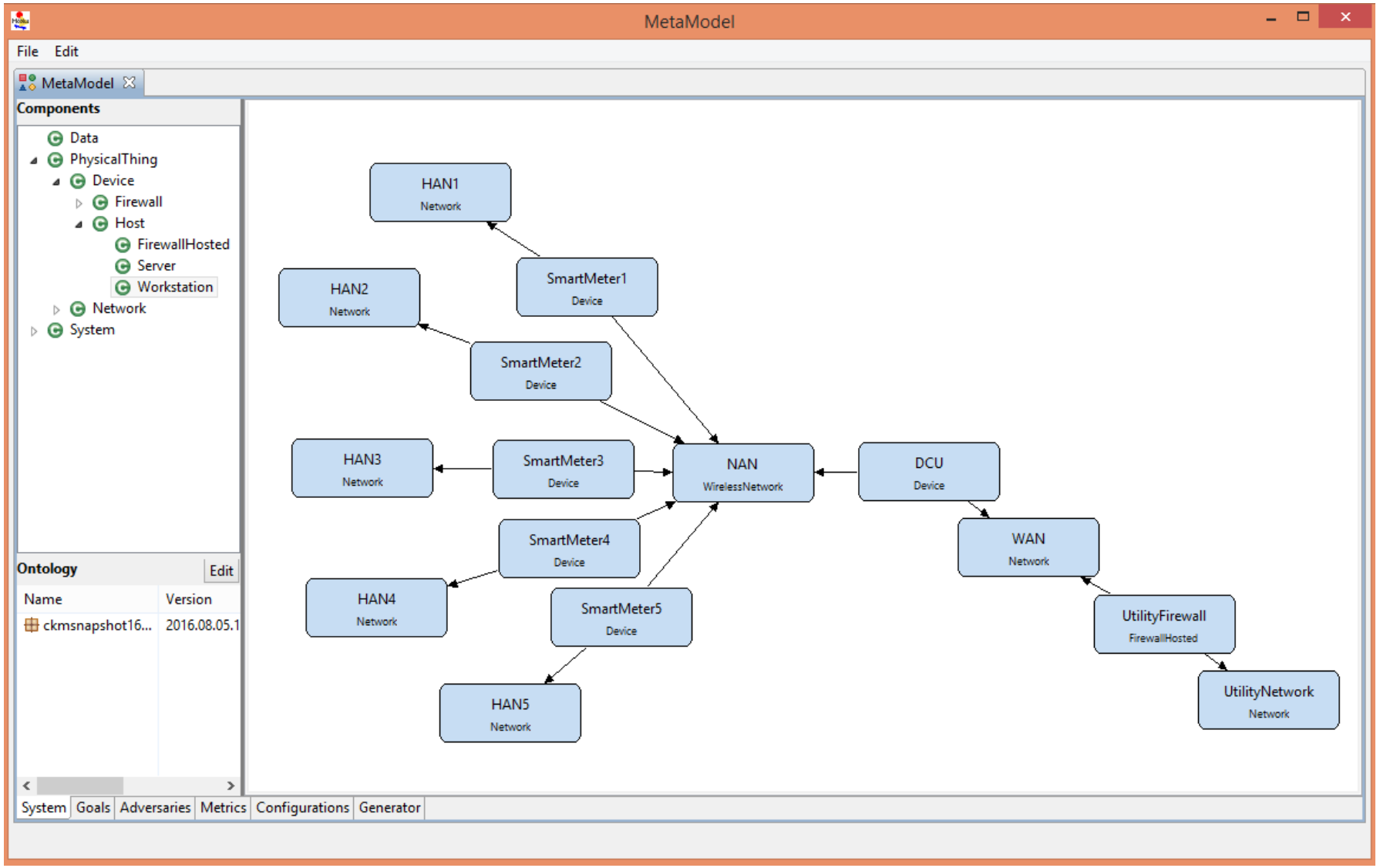


Advanced Metering Infrastructure Case Study

Define system components, relationship and attributes

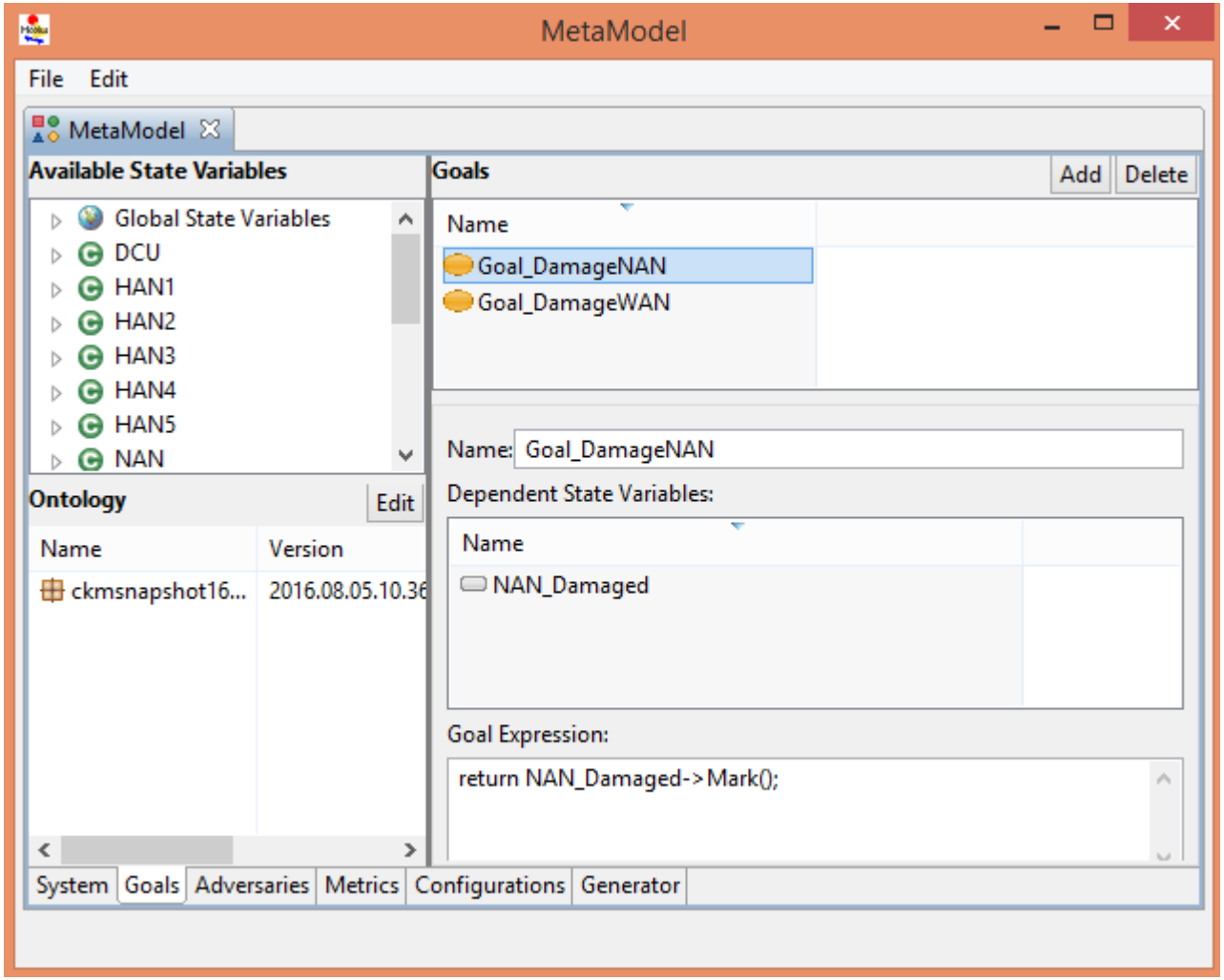


Advanced Metering Infrastructure Case Study



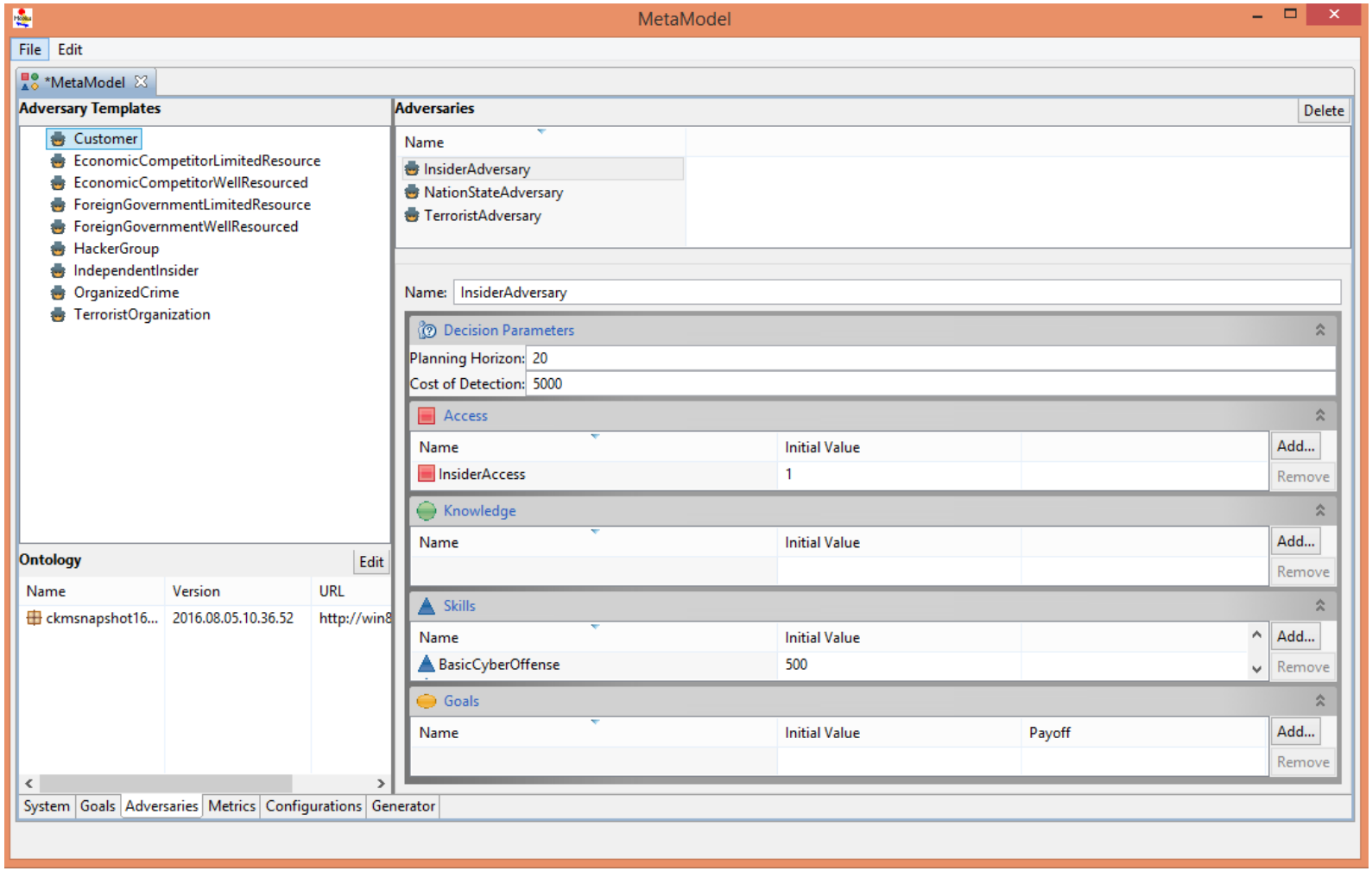
Advanced Metering Infrastructure Case Study

Model Attacker Goals



Advanced Metering Infrastructure Case Study

Model Adversaries



Advanced Metering Infrastructure Case Study

Select Metrics

- Damage to System
- Probability of Detecting Adversary
- Attack Path

Advanced Metering Infrastructure Case Study

Create Configurations

- Create one configuration for every pair of adversary/IDS, for a total of 3 adversaries X 4 IDS options = 12 configurations.

Advanced Metering Infrastructure Case Study

Results

IDS	Adversary	Attack	Monetary Damage
None	Insider Terrorist Nation-State	Routing Physical Routing	$1.07M $4.98M $876K
Centralized	Insider Terrorist Nation-State	Routing Physical Routing	$435K $4.98M $357K
Dedicated	Insider Terrorist Nation-State	None Physical None	$0 $4.98M $0
Embedded	Insider Terrorist Nation-State	None Physical None	$0 $5.02M $0

Agenda

- Registration and Continental Breakfast
- Welcome
- Goals
  - Tool
  - Workshop
- Steps to Use ADVISE Meta
- Hands on Sessions
- Case Studies and Custom Ontologies
- Wrap Up

Wrap Up

- General feedback
  - Was this tool useful?
  - How could you and your organization use it?
  - What areas need work?
- The Near Future
  - Improvements to ADVISE/Actor Model
  - Expanded Ontology
  - System to Easily Share Ontology Packages
  - Ontology Editor Improvements / Validation

Thank You!

- Contact Info
  - staff@mobius.illinois.edu
  - http://www.mobius.illinois.edu