Model Based Systems Engineering (MBSE) Process Using SysML for Architecture Design, Simulation and Visualization

March 1, 2011

Senior Principal Enterprise Architect
gundars.osvalds@ngc.com
Northrop Grumman
Objectives

- Motivation and description of an Model-Based Systems Engineering (MBSE) approach
- Present a sample Architecture, Simulation and Visualization
- Application of processes and tools for MBSE
  - OMG Systems Modeling Language (SysML)
  - IBM Rational Harmony Process for Systems Engineers
  - IBM Rational Rhapsody modeling tool for SysML and Harmony
Agenda

- Applying Modeling and Simulation for Systems Engineering
- Conceptual Model – Black Box
- Logical Model – White Box
- Visualization – Executable Model
Outline

• Applying Modeling and Simulation to System Engineering
  – Architectural Modeling Purpose
  – Advantages Model Based Systems Engineering (MBSE)
  – SysML and Model Based Systems Engineering
  – SysML Model Functional Grouping
  – MBSE Process Using SysML Rhapsody and Harmony
  – Application of Modeling
  – Demo Problem Description
Architectural Modeling Purpose

- **Why**
  - To provide a solution that satisfies the Stakeholders

- **When**
  - Before implementation is started

- **What**
  - Documents the design of the solution

- **How**
  - Use the Systems Modeling Language (SysML) specification for models

- **Where**
  - Executable Architecture provides system Simulation and Visualization

- **Who**
  - Systems Engineer and Architect
Advantages of Model Based Systems Engineering

• Provides a mechanism to capture and verify requirements

• Requirements can be allocated and traced to its source

• Diagrams are integrated with each other to provide a cohesive view of the architecture

• Models are used to define message definition and port interfaces that define the systems interface specification

• System integration and testing risks are reduced with the use of model diagrams that are the basis for system specifications and test plans

• Objects can be defined with interfaces (messages, message formats, and ports) and functions be defined with models that can be simulated
SysML and Model Based Systems Engineering (MBSE)

- SysML was developed as an extension to UML to provide a modeling capability for the Systems Engineers to create static and dynamic models of the systems architecture.

- Uses SysML to:
  - Support the concepts of describing a model with all activities performed by one or more system scenarios.
  - Provide allocation of scenario activates to objects that can then be defined as system hardware components.
  - Implement the architectural model using state diagram that when executed provide a simulation of the scenario execution on the architectural model.
  - Provides a verification of model execution state diagram functionality against the designed scenario activities and interactions between actors and the system.
SysML Model Functional Grouping

- SysML can be grouped into four functional areas
  - Each group is implemented using the shown SysML diagrams
  - The groups also interact with each other to provide a cohesive architectural model
Model Based Systems Engineering Framework

Requirements Repository
(Requisite Pro, Doors, Excel)

System Architecture Models
(SysML, Rhapsody, Gateway)

System Performance Simulations
(InterCAX, OpNet)

System Verification Models
(Rational Test Conductor)

System Visualizations
(GUI Software)

Site Infrastructure Models
(Puppet)

Copyright © 2010 NORTHROP GRUMMAN CORPORATION
Application of Modeling

Modeling artifacts can support the development of:

- Concept of Operations specification (CONOP)
- System Capabilities Validation
- Architecture Design
- System Data use and flow
- Component Specifications
  - Software
  - Hardware
- Inputs to OpNet performance modeler
  - Architecture
  - Scenarios
- Software
  - Activities
  - Messages
  - Data
- Hardware
  - Parts list
  - Interconnect diagram
- System Interface Verification
- Test Plans
Demo Problem Description

• Data Exfiltration Using Botnet Demo
  – Hacker wants to gain access to User data on his system and have it sent back
  – Hacker created a Botnet consisting of multiple Drones (use of un-secure computers) that are used to attack the User
  – On each Drone the hacker uses a Command and Control Computer to remotely install Malware
  – User protection consists of a Firewall and Analyst to evaluate questionable messages
  – If Firewall or Analyst determine message sent is an attack then the message is blocked from accessing the Users system
  – If Malware command gets through (unrecognized signature) the Firewall and Analyst then the Malware downloads data from the Users system to the Hacker
Conceptual Model - Black Box

System Requirements- Black Box Diagrams

- Use Case
- Activity – Scenario
- Sequence
- Internal Block
- State
- Sub-State

- Sequence – Executable
- State – Executable
- Sequence – Verified vs. Executable
System Requirements

Requirements in the model supports automated traceability and allocation
Define system context, interfaces and capabilities.
This activity will be highlighted throughout this presentation.

**REQ04 - Initialize Botnet**

- **ID = REQ04**
- The hacker will send the command to the Command Computer to create a Botnet of Drones.

**REQ06 - Traceability Avoidance**

- **ID = REQ06**
- The hacker will attempt to avoid detection by using a Botnet.

Engineer define actions required to perform scenario operations.
BB Sequence

ID = REQ08 - Malware

The hacker will create Malware to be hosted by a Drone.

ID = REQ04 - Initialize Botnet

The hacker will send the command to the Command Computer to create a Botnet of Drones.

Auto generate sequences from Activity diagram
The hacker will send the command to the Command Computer to create a Botnet of Drones.
BB State

Cyber Enterprise State

REQ02 - Create Botnet
ID = REQ02
The hacker will create a Botnet to perform the attack against the target.

REQ04 - Initialize Botnet
ID = REQ04
The hacker will send the command to the Command Computer to create a Botnet of Drones.

REQ09 - Analyst
ID = REQ09
The analyst will be alerted to suspicious traffic.

REQ16 - Data Exfiltration
ID = REQ16
The hacker will be able to remove sensitive data from the target machine and copy it to his own.

This is the state model of the activities defined to satisfy the requirements.
The hacker will send the command to the Command Computer to create a Botnet of Drones.

ID = REQ04

The hacker will be able to attack multiple targets simultaneously via the Drones.

ID = REQ07

Develop the behavior of systems via the executable model that is driven by the states.
BB Sequence - Executable

ID = REQ04
The hacker will send the command to the Command Computer to create a Botnet of Drones.

ID = REQ06
The hacker will attempt to avoid detection by using a Botnet.

Validate the executable sequence against the scenario requirements.
The Rhapsody modeling tool provides a built-in visualization of each state as the model is executed.
Verify that the executable sequence diagrams accurately implements the designed scenario.
Logical Model – White Box

- **White Box Diagrams**
  - Activity – Swim Lanes
  - Sequence – Logical
  - Internal Block – Physical
  - Block Definition – Physical
  - State – Allocated
  - Sub-State – Allocated
  - Sequence – Executable
  - State – Executable
  - Sequence – Verified vs. Executable
Add swim lanes to original Black Box Diagram and allocate Activities to the objects.
WB Sequence

 Presents the five objects that execute the use case functionality

REQ04 - Initialize Botnet
ID = REQ04
The hacker will send the command to the Command Computer to create a Botnet.

REQ06 - Traceability Avoidance
ID = REQ06
The hacker will attempt to avoid detection by using a Botnet.

REQ08 - Malware
ID = REQ08
The hacker will create Malware to be hosted by a Drone.
Objects are shown with Operations and Messages automatically allocated from the White Box Activity/Sequence diagrams.
System Objects are Logical but can be allocated to Physical devices
The hacker will send the command to the Command Computer to create a Botnet of Drones.
ID = REQ04

The hacker will send the command to the Command Computer to create a Botnet Command Computer to create a Botnet of Drones.

ID = REQ07

The hacker will be able to attack multiple targets simultaneously via the Drones.

Re-used state operations integrated into Hostile Enterprise Object
WB Sequence - Executable

ID = REQ04

The hacker will send the command to the Command Computer to create a Botnet of Drones.

Check for proper execution of reapportioned state diagram
The Rhapsody modeling tool provides a built-in visualization of each state as the model is executed.

ID = REQ04
The hacker will send the command to the Command Computer to create a Botnet of Drones.

ID = REQ07
The hacker will be able to attack multiple targets simultaneously via the Drones.
Verify that the reallocate activities correctly implement the scenarios in each object.
Visualization

• Purpose
  – Verification of Requirements
    • Models provides a mechanism to verify that Requirements are implemented in the design
  – Validation of Design
    • The model visualization allows the Stakeholder to Validate that the systems performs that capabilities that were intended

• Demonstration
  – Visualization of Executable Demo on World Map
    • A high level animation is shown on the world map to present visually how attacks are directed and detected
1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. Firewall routes attack packets to either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker
Command and Control Uploads Malware to Drones

1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. Firewall routes attack packets to either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker
Drones Use Malware to Attack Firewall

1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. Firewall routes attack packets to either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker
Firewall Blocks Packet

1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. Firewall routes attack packets to either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker
1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. **Firewall routes attack packets to** either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker
Analyst Blocks Packet

1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. Firewall routes attack packets to either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker

Copyright © 2010 NORTHROP GRUMMAN CORPORATION
1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. **Firewall routes attack packets to** either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker
Successful Data Exfiltration to Hacker

1. Hacker creates Malware
2. Uploads Malware to Command and Control computer
3. CC uploads Malware to Drones
4. Hacker instructs CC to command the Drones to attack User
5. Drones use Malware to attack the Firewall
6. Attack is blocked by Firewall or
7. Firewall routes attack packets to either Analyst or User
   - Attack is blocked by Analyst
   - or
   - Attack of User is successful and sends Exfiltrated data to Hacker via the Drones to the CC computer and then back to Hacker
Conclusions

• The Model Based System Engineering capability:
  – Reduce design and specification errors that have to be corrected at greater cost during the system development
  – Reduced manually induced design errors since the tool has the capability to automatically create diagrams from data entered into the previous diagram
  – Provides for modeling of the requirements in the architecture of the system for an integrated view of the system
  – The simulation of the architecture and its visualization provided a more accurate view for the Stakeholders to determine that the design meets the needs their needs
Data Exfiltration Using a Botnet Model Simulation
Questions

Gundars Osvalds
Senior Principal Enterprise Architect
Northrop Grumman
gundars.osvalds@ngc.com