A Model Based Systems Engineering Approach to Resiliency Analysis of a Cyberphysical System

Myron Hecht
The Aerospace Corporation

Presented to
EnergyTech 2016
Cleveland, OH

November, 2016
Outline

• Motivation
• Example System Description
• Resiliency Model
• SysML Model
• Comments
• Conclusions
Motivation

- Cyberphysical systems (aka “Internet of Things” in general and “Smart Grid” for the case of power distribution) are becoming increasingly common
  - *IEC 61850 standard establishes architecture and data types*
- Resiliency is an important property to reducing vulnerability and impact of cyberattacks on such systems
- Model Based Systems Engineering (MBSE) is being increasingly considered as an approach for developing new systems
- This work investigates the feasibility of incorporating resiliency assessments into MBSE
IEC 61850 System with Cybersecurity Devices


IED: Intelligent Electronic Device (IEC 61850 term)
Substation Network (process level)

CBTn: Transformer Circuit Breakers IEDs (33 KV to 11 KV)
CBFn: Distribution Line Circuit Breakers IEDs (11 KV)
CBB: Bus Circuit Breaker IED
Tn: Transformer

Resiliency Model

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>v</td>
<td>Rate of cyberattacks</td>
</tr>
<tr>
<td>a</td>
<td>Rate of in depth scanning</td>
</tr>
<tr>
<td>m</td>
<td>Rate of Recovery from system image replacement</td>
</tr>
<tr>
<td>w</td>
<td>Rate of initial scanning</td>
</tr>
<tr>
<td>k</td>
<td>Rate of infection from adjacent nodes</td>
</tr>
<tr>
<td>r</td>
<td>Scanning completion and malware removal rate</td>
</tr>
<tr>
<td>f</td>
<td>Probability of false positive</td>
</tr>
<tr>
<td>d</td>
<td>Probability of true positive</td>
</tr>
<tr>
<td>j</td>
<td>Probability of successful rejuvenation</td>
</tr>
<tr>
<td>S</td>
<td>Rate of spurious rejuvenation</td>
</tr>
</tbody>
</table>

State Descriptions

0 – initial state
A – security software gives false positive indication
P – system infected
Q – Replacement of system image (extended process)
R – Malware removed and system reinitialization

Relationship to Previous Work

SysML Model: Block Definition Diagram
SysML Model: Parametric Diagram

```
PR : Real
PQ : Real
PP : Real
PA : Real
P0 : Real

<k q d r j m w f a v>

resilstead3
{{P0,PA,PP,PQ,PR} = resilstead3(v,a,m,w,k,r,f,d,j,q)}

Rollback-restoration device

- successful_rollback_prob : Real = 0.3
- rollback_rate : Real = 0.5
- spurious_rollback_prob : Real
- true_positive_prob : Real = 0.7
- no_detection_rollback_prob : Real = 0.0

adj_node_infection_rate : Real = 10.0

Firewall

- attack_rate : Real = 0.1

Intensive malware scan SW

- intensive_scan_rate : Real = 16
- false_pos_prob : Real = 0.3

Initial Malware Scan SW

- initial_scanning_rate : Real = 30.0
```
## Analytical Model

<table>
<thead>
<tr>
<th>State</th>
<th>Rate Equations</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>( \frac{dP_0}{dt} = -(\lambda_1 + \lambda_2)P_0 + \lambda_3P_A + \lambda_5P_Q + \lambda_8P_R )</td>
</tr>
<tr>
<td>A</td>
<td>( \frac{dP_A}{dt} = -\lambda_3P_A + \lambda_2P_0 )</td>
</tr>
<tr>
<td>P</td>
<td>( \frac{dP_P}{dt} = -(\lambda_4 + \lambda_6)P_P + \lambda_1P_0 + \lambda_7P_R )</td>
</tr>
<tr>
<td>Q</td>
<td>( \frac{dP_Q}{dt} = -\lambda_5P_Q + \lambda_4P_P )</td>
</tr>
<tr>
<td>R</td>
<td>( \frac{dP_R}{dt} = -(\lambda_8 + \lambda_7)P_R + \lambda_6P_P )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transition</th>
<th>Meaning</th>
<th>expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \lambda_1 )</td>
<td>Under attack</td>
<td>( v + k )</td>
</tr>
<tr>
<td>( \lambda_2 )</td>
<td>False alarm</td>
<td>( w*f )</td>
</tr>
<tr>
<td>( \lambda_3 )</td>
<td>Recovery from false alarm</td>
<td>( S )</td>
</tr>
<tr>
<td>( \lambda_4 )</td>
<td>Replacement of system image</td>
<td>( a )</td>
</tr>
<tr>
<td>( \lambda_5 )</td>
<td>Recovery from system image replacement</td>
<td>( m )</td>
</tr>
<tr>
<td>( \lambda_6 )</td>
<td>To initialization</td>
<td>( w*d )</td>
</tr>
<tr>
<td>( \lambda_7 )</td>
<td>Unsuccessful initialization</td>
<td>( r (1 - j) )</td>
</tr>
<tr>
<td>( \lambda_8 )</td>
<td>Recovery from true re-initialization</td>
<td>( r^*j )</td>
</tr>
</tbody>
</table>
Steady State Solution

\[ b = \text{inv}(T) * P \]

Where \( b \) is the Solution vector

\[
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-(\lambda_1 + \lambda_2) & \lambda_3 & 0 & \lambda_5 & \lambda_8 \\
-\lambda_2 & \lambda_2 & 0 & 0 & 0 \\
\lambda_1 & 0 & -(\lambda_4 + \lambda_6) & 0 & \lambda_7 \\
0 & 0 & \lambda_4 & -\lambda_5 & 0 \\
0 & 0 & 0 & 0 & 0
\end{bmatrix}
\]

\[
\begin{bmatrix}
P \quad \text{is the “LHS” vector}
\end{bmatrix}
\]

\[
\begin{bmatrix}
1 \\
0 \\
0 \\
0 \\
0 \\
0
\end{bmatrix}
\]

\[ T \quad \text{is the Transition Matrix} \]
Transient Results

Greatest Benefit

Intermediate Benefit

Solved numerically using the Matlab ode45 solver
Steady State Results

Steady State Probability is more affected by Malware Propagation Propensity than by Attack Rate (in the absence of intervention)

Solved using Matlab matrix functions
function \([P_0, PA, PP, PQ, PR] = resilstead3( v,a,m,w,k,r,f,d,j,s)\)
%Transitions from Grottke et. al. (Phase II)
\(l_1 = v + k; \quad \% 0 \) to \(P\) (initial state) to (infected state)
\(l_2 = w*f; \quad \% 0 \) to \(A\) (initial state) to (spurious recovery state)
\(l_3 = s; \quad \% A \) to \(0\) (spurious recovery state) to (initial state)
\(l_4 = a; \quad \% P \) to \(Q\) (infected state) to (image replacement state)
\(l_5 = m; \quad \% Q \) to \(0\) (image replacement state) to (initial state)
\(l_6 = w * d; \quad \% P \) to \(R\) (infected state) to (true recovery state)
\(l_7 = r *(1 - j); \quad \% R \) to \(P\) (true recovery state) to (infected state)
\(l_8 = r*j; \quad \% R \) to \(0\) (true recovery state) to (initial state)
\(T = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 \\
-(l_1+l_2) & l_3 & 0 & l_5 & l_8 \\
-l_3 & l_2 & 0 & 0 & 0 \\
l_1 & 0 & -(l_4+l_6) & 0 & l_7 \\
0 & 0 & l_4 & -l_5 & 0
\end{bmatrix};
\)
\(P = [1 0 0 0 0]';\)
b = inv(T) * P;
P0 = b(1);
PA = b(2);
PP = b(3);
PQ = b(4);
PR = b(5);
end

SysML Constraint properties reference the Matlab Functions
Parametric diagrams enable mapping of input parameters to the Functions
Conclusions

• MBSE can incorporate resiliency analyses into critical infrastructure systems.
  – Such Models can enable design decisions
  – The specific analytical model and results are shown for the purposes of illustration of this point
  – Not intended to be generalized to other systems

• Motivations for using MBSE
  – A single repository for qualitative and quantitative data
  – Consistent propagation of changes as updates are made to the model, they are propagated to all of the related and associated elements,
  – Rapid recalculation of analytical results to explore design alternatives and the impacts of changes in the course of the development