THE GEORGE
WASHINGTON
UNIVERSITY

WASHINGTON, DC

Leveraging Systems Modeling to Assess and Mitigate Cyber-Based Mission Risk: A Cybersecurity Architecture Framework

Everett Oliver
Dr. Shahram Sarkani
Dr. Thomas Mazzuchi

October 2018

The Problem

Modern organizations depend on IT systems that face a steady stream of cyber threats.[9] In response, cybersecurity vendors produce a wide range of cyber defense products and tools. The challenge lies in developing cybersecurity strategies tailored to specific organizations and systems.[5,22]

Current Cybersecurity Solutions

Many solutions are available for different parts of the cybersecurity problem.

- NSA IAD's Top-10 list guides many of the solutions[13]
- DISA's Security Technical Implementation Guides (STIGs) provide IT configuration guidance[26]
- Software patches provide updates for identified vulnerabilities
- A wide range of tools address different threats: access control, whitelisting, IDS/IPS, anti-virus/anti-malware, etc.

Cybersecurity Research Directions

A short list would include these and many more:

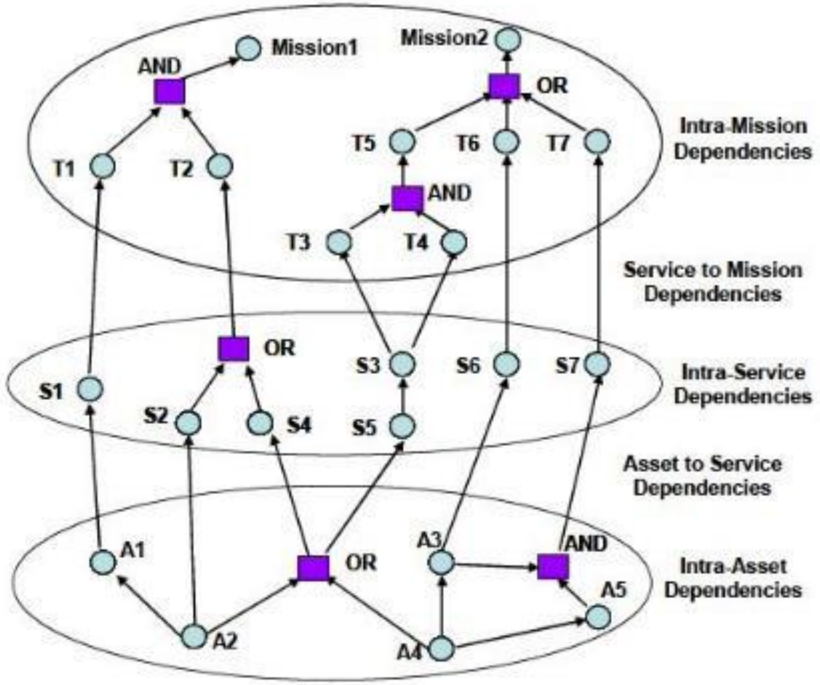
- New Vulnerabilities[15]
- Integrated/Automated tools[16]
- Risk scoring approaches[3,5,16]
- Heuristics[19]
- Modeling and Simulation[1,7,12,17,18,20,27,29]
- Security extensions to SysML[2]

What’s Missing?

With all the work that has been done and is being done in cybersecurity, what is missing?

A systems approach that treats cyber threats as mission-impacting problems that need solutions tailored to each organization.[3,5,22]

Multi-Level Cybersecurity Challenge


Mission1
Mission2
AND
OR
T1
T2
T5
T6
T7
AND
T3
T4
Intra-Mission Dependencies
Service to Mission Dependencies
OR
S1
S2
S4
S3
S5
S6
S7
Intra-Service Dependencies
Asset to Service Dependencies
A1
A2
OR
A3
AND
A4
A5
Intra-Asset Dependencies

Impact Dependency Graph (Jakobson, 2011)[14]

- An organization derives its capabilities from different levels in its hierarchy.
- However, cybersecurity challenges also arise at different levels within the organization.

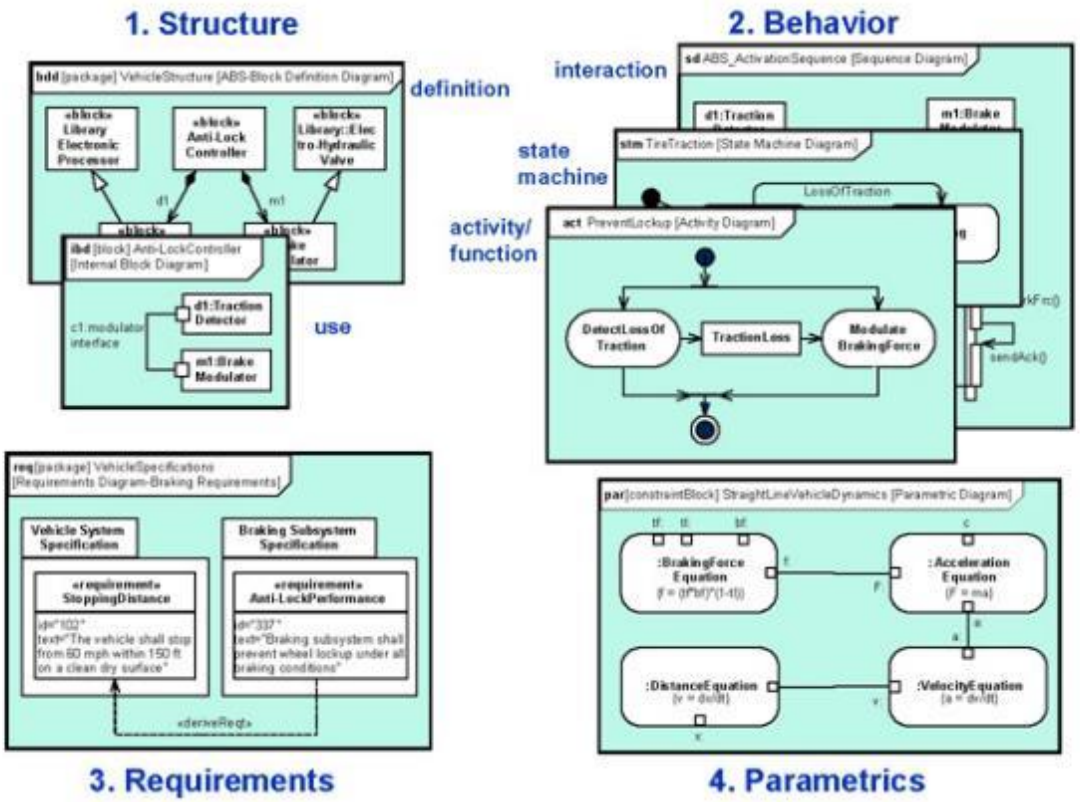
Leveraging Systems Engineering

What can Systems Engineers bring to the multi-level cybersecurity challenge?

- A systems engineering/architecture perspective – understanding how and why all the pieces fit together (the holistic view).[4,22,23,25]

- Tools for connecting systems architecture with analysis techniques such as modeling and simulation.[8]

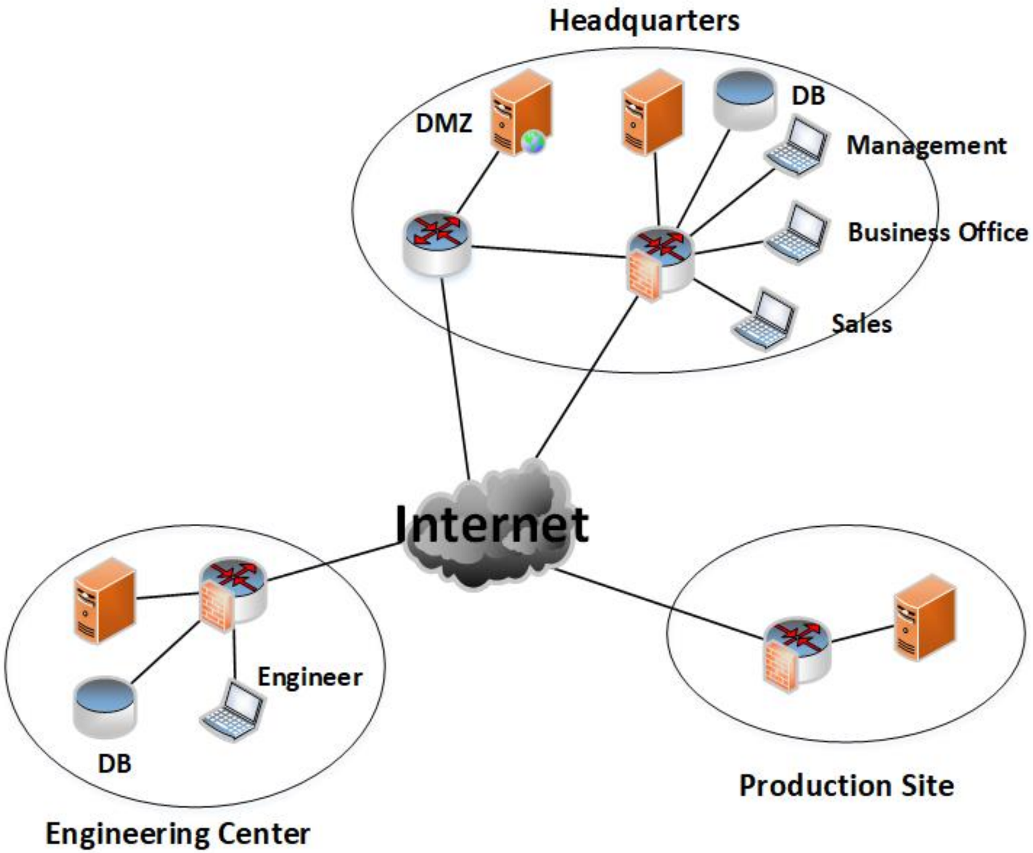
Systems Modeling Overview


1. Structure
bdd [package] VehicleStructure [ABS-Block Definition Diagram]
definition
«block» Library Electronic Processor
«block» Anti-Lock Controller
«block» Library::Electro-Hydraulic Valve
d1
m1
ibd [block] Anti-LockController [Internal Block Diagram]
d1:Traction Detector
m1:Brake Modulator
c1:modulator interface
use
2. Behavior
interaction
sd ABS_ActivationSequence [Sequence Diagram]
d1:Traction Detector
m1:Brake Modulator
state machine
stm TireTraction [State Machine Diagram]
LossOfTraction
activity/ function
act PreventLockup [Activity Diagram]
DetectLossOf Traction
TractionLoss
Modulate BrakingForce
sendAck()
3. Requirements
req [package] VehicleSpecifications [Requirements Diagram-Braking Requirements]
Vehicle System Specification
«requirement» StoppingDistance
id="102"
text="The vehicle shall stop from 60 mph within 150 ft on a clean dry surface"
Braking Subsystem Specification
«requirement» Anti-LockPerformance
id="337"
text="Braking subsystem shall prevent wheel lockup under all braking conditions"
«deriveReqt»
4. Parametrics
par [constraintBlock] StraightLineVehicleDynamics [Parametric Diagram]
:BrakingForce Equation
:Acceleration Equation
(F = ma)
:DistanceEquation
:VelocityEquation
(v = dx/dt)
(a = dv/dt)

Note that the Package and Use Case diagrams are not shown in this example, but are respectively part of the structure and behavior pillars

The Four Pillars of SysML (OMG website, 2018)[28]

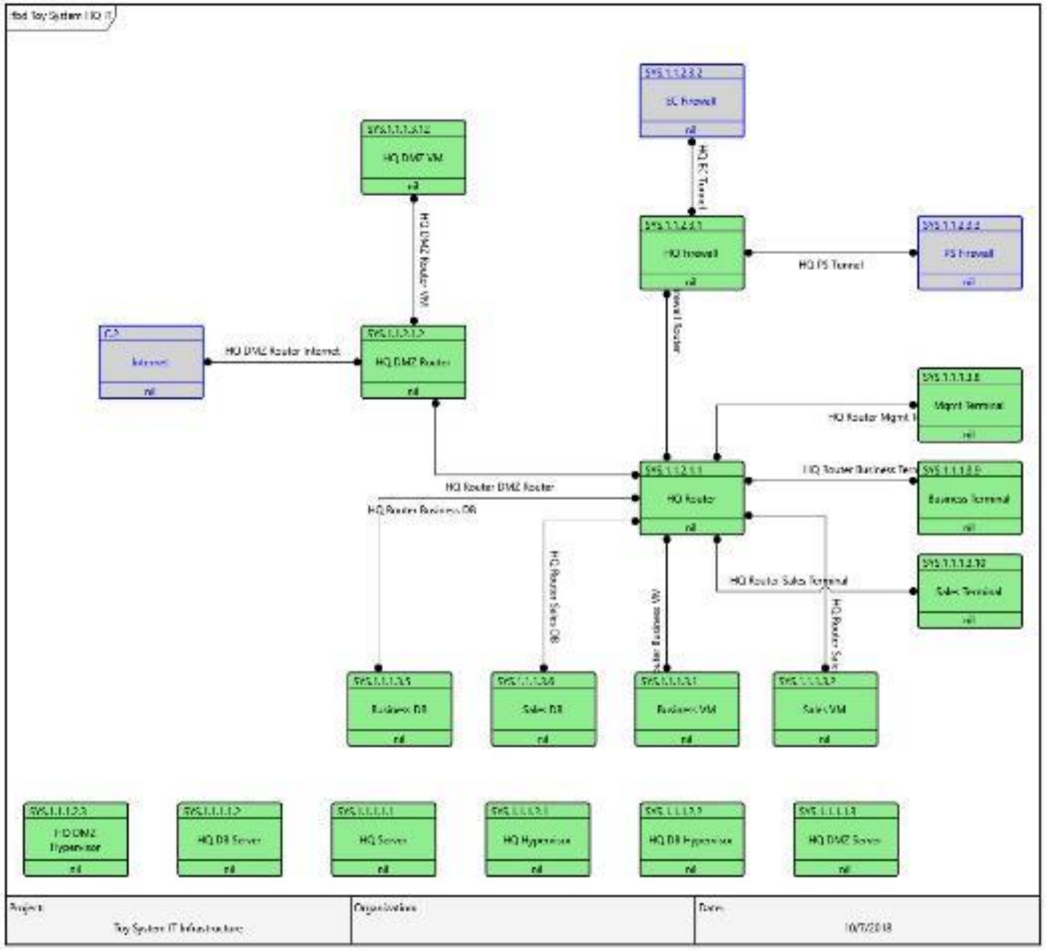
Test System Example



Missions

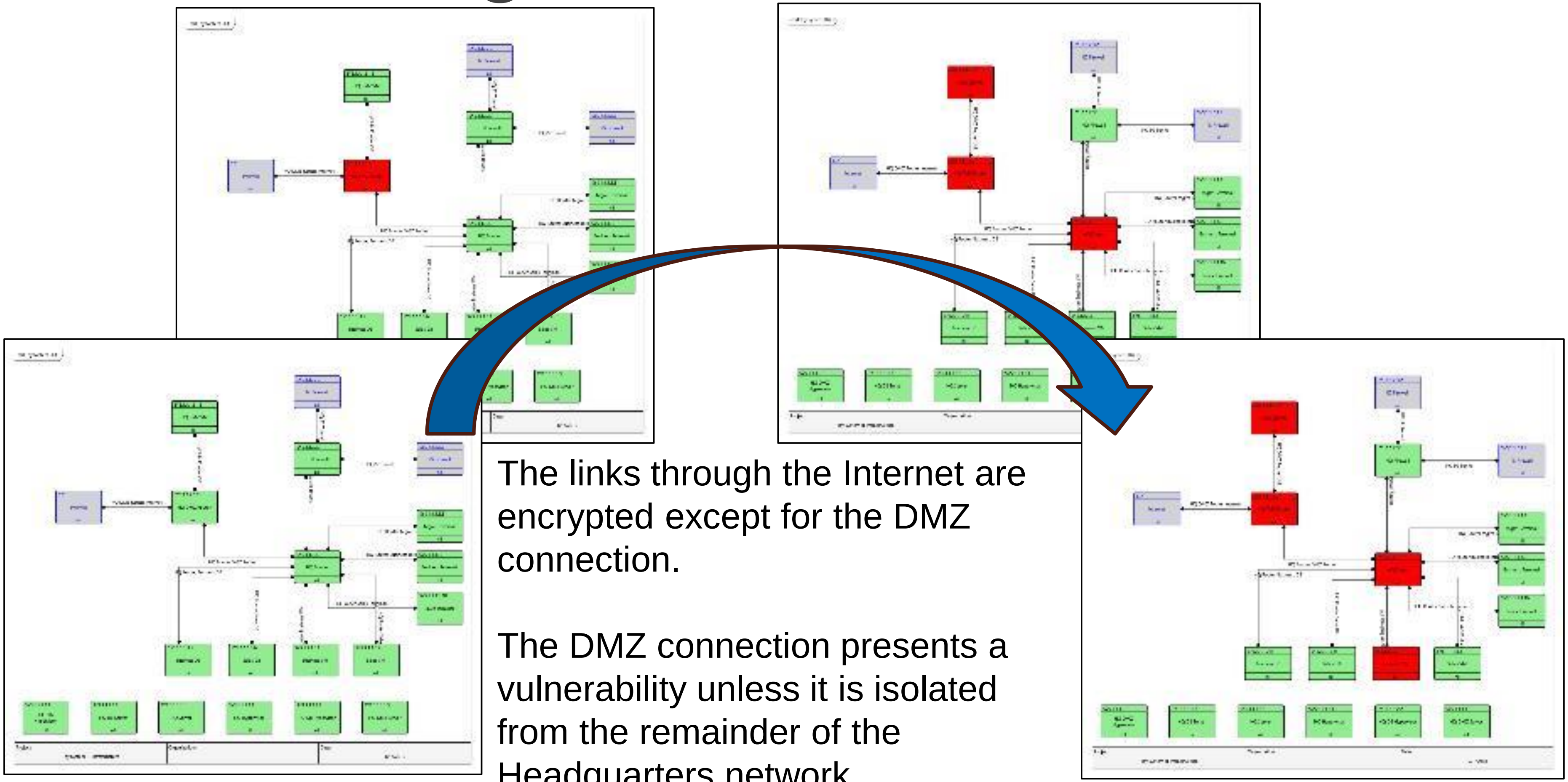
#	Mission	Owner
1	Make money by producing and selling products	Company
1.1	Develop and distribute rules and priorities	Management
1.2	Sell products	Sales
1.3	Specify production to satisfy sales	Business Office
1.3.1	Configure production systems	Engineering
1.3.1.1	Troubleshoot and repair production systems	Engineering
1.3.2	Make products	Production
1.3.3	Report production status	Engineering
1.3.3.1	Generate production alarms	Production
1.4	Protect company assets	Company
1.4.1	**Protect business financial records**	**Business Office**
1.4.2	Protect proprietary product information	Engineering

SysML for Headquarters Interfaces



Diagrams from GENESYS 6.0, Vitech Corporation[8]

Protecting Business Records



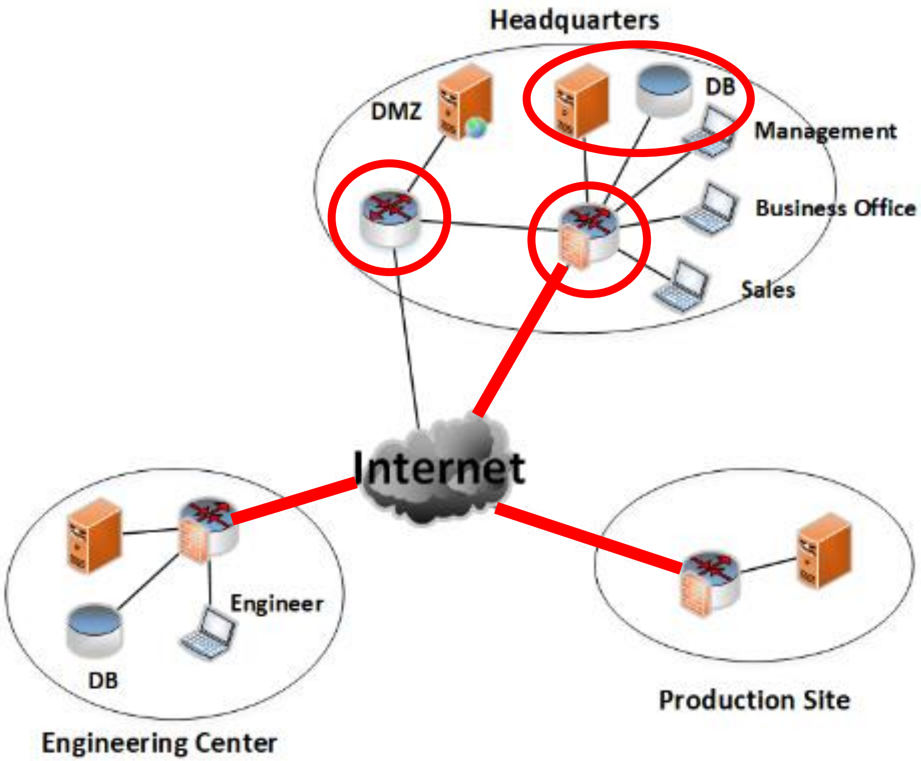
The links through the Internet are encrypted except for the DMZ connection.

The DMZ connection presents a vulnerability unless it is isolated from the remainder of the Headquarters network.

Diagrams from GENESYS 6.0, Vitech Corporation[8]

Are the business records protected?

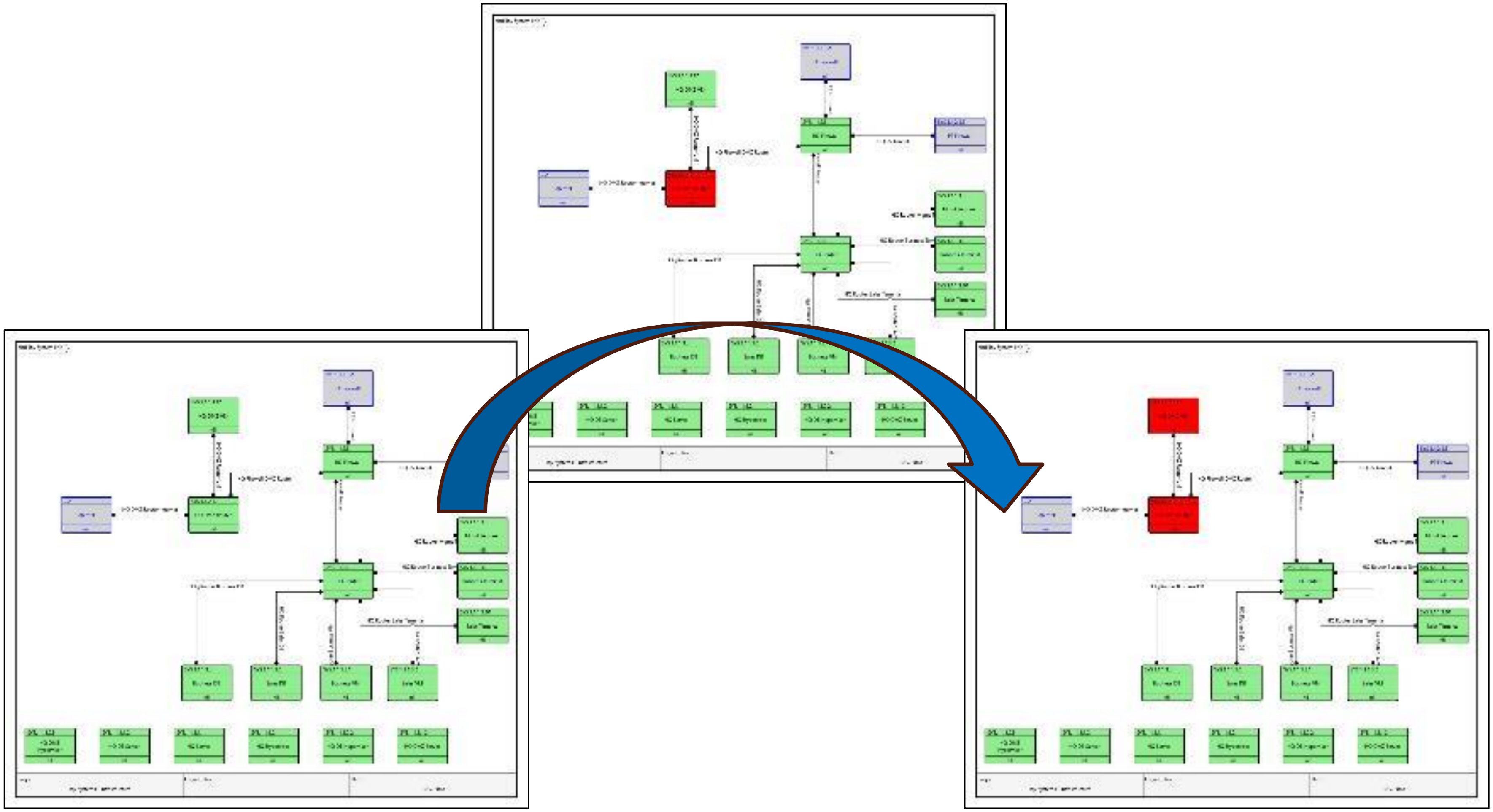
Protecting the business records



Even through the primary links from each site through the Internet are encrypted, the company’s business records are at risk.

The DMZ presents a potential path through the Headquarters Site to attack the business systems despite the secure tunnels.

Network Change to Mitigate Risk



Diagrams from GENESYS 6.0, Vitech Corporation[8]

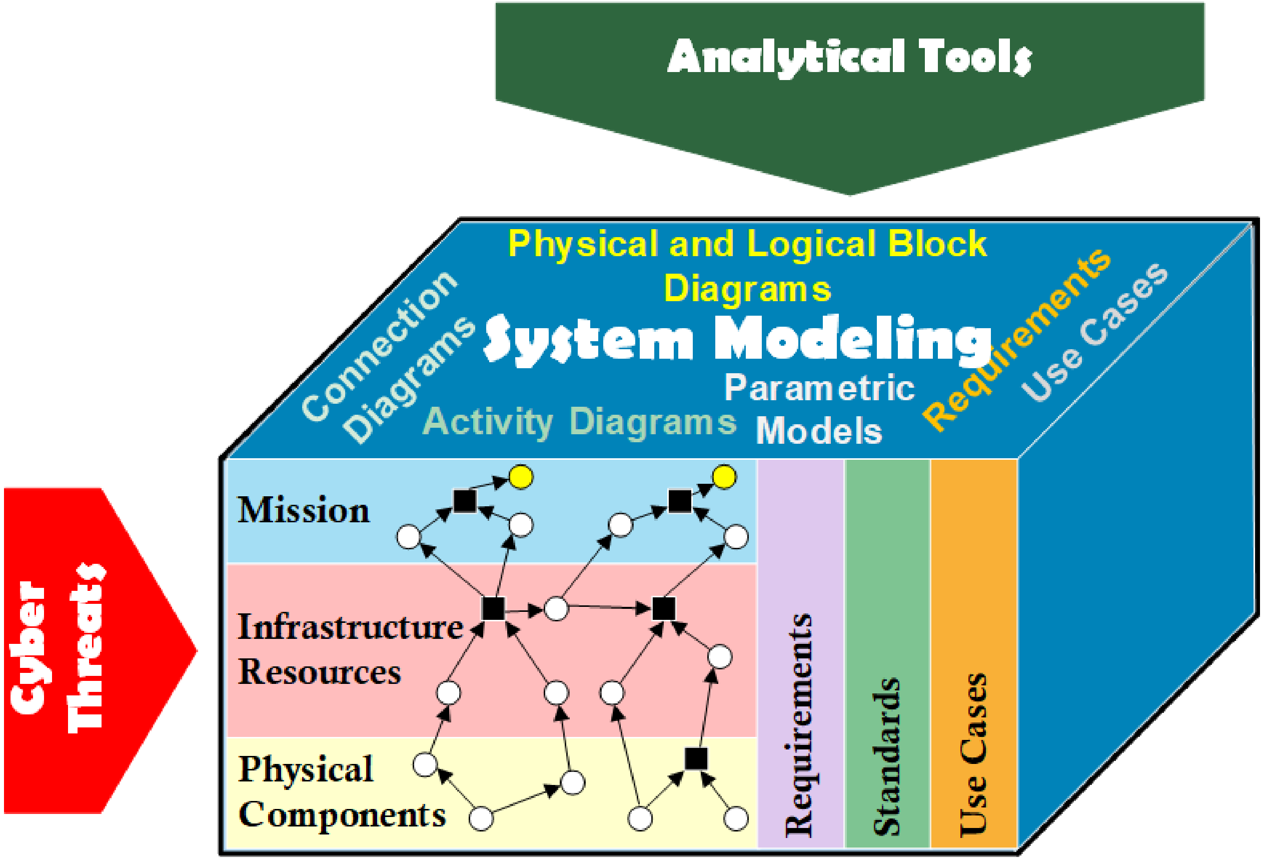
Extending the Use of Systems Modeling

- This example relied on the simple application of systems modeling and analysis displayed through the modeling diagrams.[8]
- For more sophisticated analyses, systems models can provide the framework for automating data analysis and modeling and simulation.
- SysML and model based systems engineering tools on the market provide application programming interfaces (APIs) to support multi-level cybersecurity research and assessments of specific system implementations.[6,8,21]

A Cybersecurity Architecture Framework for Leveraging Systems Modeling

- To leverage the capabilities of systems modeling and apply a holistic approach to cybersecurity, we propose a cybersecurity architecture framework.
- This architecture framework would combine the structures, behaviors, and parametric capabilities of the system models with analytical tools to support an enhanced systems engineering approach to cybersecurity.

The Cybersecurity Architecture Framework



Cybersecurity Architecture Framework Application to Current Practices

- Reusing Systems Engineering efforts that produce the systems models.[8]
- Capturing known cybersecurity considerations in modeling constructs:
  - Attack trees and attack propagation[13,24]
  - Vulnerabilities in homogeneous systems[13]
  - Attack surfaces[13]

Cybersecurity Architecture Framework Advancing Systems Engineering Research

- Identifying extensions to SysML and model based systems engineering tools to support cybersecurity
- Applying systems engineering to future cybersecurity research :
  - Speculative execution vulnerabilities[15]
  - Methods to jump air gaps[10]
  - Applications of game theory, stochastic modeling, and other analytical techniques[11,12,17,18,20,27,29]
  - Supply chain impacts[9]
  - Cyber physical systems[1,2]

Summary

- Cybersecurity Architecture Framework provides a structure for applying systems modeling techniques and analytical tools to cybersecurity
- Leverages capabilities of systems modeling to address the multi-level challenges of cybersecurity in a holistic manner
- Supports system development lifecycle applications and cybersecurity research

Questions?

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Contact Information

Everett Oliver, George Washington University (Ph.D. Candidate)
everettoliver@gwu.edu
(814) 414-5210

Dr. Shahram Sarkani, Ph.D., P.E., George Washington University
sarkani@gwu.edu
(888) 694-9627

Dr. Thomas Mazzuchi, D.Sc., George Washington University
mazzu@gwu.edu
(888) 694-9627

References

1. Abdo, H., M. Kaouk, J. -M Flaus, and F. Masse. 2018. "A Safety/Security Risk Analysis Approach of Industrial Control Systems: A Cyber Bowtie – Combining New Version of Attack Tree with Bowtie Analysis." *Computers & Security* 72: 175-195.
2. Apvrille, L. and Y. Roudier. 2013. "SysML-Sec: A Model-Driven Environment for Developing Secure Embedded Systems." Sep. 16-18, 2013.
3. Dedeke, A. 2017. "Cybersecurity Framework Adoption: Using Capability Levels for Implementation Tiers and Profiles." *IEEE Security & Privacy* 15 (5): 47-54.
4. Forsberg, K., editor, R. D. Hamelin editor, G. J. Roedler editor, T. M. Shortell editor, D. D. Walden editor, and et al. 2015. *Systems Engineering Handbook : A Guide for System Life Cycle Processes and Activities*. Hoboken, New Jersey: John Wiley & Sons Inc.
5. *Framework for Improving Critical Infrastructure Cybersecurity,* 2018. Version 1.1. ed. Gaithersburg, Md.: National Institute of Standards and Technology.
6. Friedenthal, S., A. Moore, R. Steiner, and Ebooks Corporation. 2012. *Practical Guide to SysML*: *The Systems Modeling Language*. Waltham, MA: Morgan Kaufmann.
7. Garg, U., G. Sikka, and L. K. Awasthi. 2018. "Empirical Analysis of Attack Graphs for Mitigating Critical Paths and Vulnerabilities." *Computers & Security* 77: 349-359.
8. GENESYS 6.0. Vitech Corporation. http://www.vitechcorp.com.
9. Gosler, J. and L. Von Thaer. 2013. *Resilient Military Systems and the Advanced Cyber Threat*. Washington, DC: Defense Science Board.

References (cont.)

10. Guri, M., M. Monitz, and Y. Elovici. 2017. "Bridging the Air Gap between Isolated Networks and Mobile Phones in a Practical Cyber-Attack." *ACM Transactions on Intelligent Systems and Technology (TIST)* 8 (4): 1-25.
11. Harang, R. and A. Kott. 2017. "Burstiness of Intrusion Detection Process: Empirical Evidence and a Modeling Approach." *IEEE Transactions on Information Forensics and Security* 12 (10): 2348-2359.
12. Huff, J., H. Medal, and K. Griendling. 2018. "A Model-Based Systems Engineering Approach to Critical Infrastructure Vulnerability Assessment and Decision Analysis." *Systems Engineering*.
13. “IAD’s Top 10 Information Assurance Mitigation Strategies,” NSA, https://www.sans.org/security-resources/IAD_top_10_info_assurance_mitigations.pdf, July 2013.
14. Jakobson, G. 2011, “Mission Cyber Security Situation Assessment Using Impact Dependency Graphs,” *Fusion 2011 - 14th International Conference on Information Fusion*.
15. Kocher, P., D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom. 2019. "Spectre Attacks: Exploiting Speculative Execution.“*40th IEEE Symposium on Security and Privacy (S&P'19)*.
16. Kott, A. and C. Arnold. 2013. "The Promises and Challenges of Continuous Monitoring and Risk Scoring." *IEEE Security & Privacy* 11 (1): 90-93.
17. Kott, A., J. Ludwig, and M. Lange. 2017. "Assessing Mission Impact of Cyberattacks: Toward a Model-Driven Paradigm." *IEEE Security & Privacy* 15 (5): 65-74.
18. Leslie, N. O., R. E. Harang, L. P. Knachel, and A. Kott. 2018. "Statistical Models for the Number of Successful Cyber Intrusions." *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* 15 (1): 49-63.

References (cont.)

19. Libicki, M. C., L. Ablon, and T. Webb. 2015. *The Defenders Dilemma: Charting a Course Toward Cybersecurity*. RAND Corporation.
20. Musman, S. and A. Turner. 2018. "A Game Theoretic Approach to Cyber Security Risk Management." *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* 15 (2): 127-146.
21. "OMG Systems Modeling Language, Version 1.5," Object Management Group, May 2017, http://www.omg.org/spec/SysML/1.5/ (accessed Apr. 23, 2018).
22. Ross, R., M. McEvilley, and J. C. Oren. 2018. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. SP 800-160*. Gaithersburg, Maryland: NIST.
23. Sage, A.P, W. B. Rouse. "An Introduction to Systems Engineering and Systems Management," *Handbook of Systems Engineering and Management*. 2 ed. John Wiley & Sons, Hoboken, NJ. 2009.
24. Schneier, B. 1999. "Attack Trees [Computer Security]." *Dr.Dobb's Journal* (1989) 24 (12): 21-9.
25. SEBoK contributors, "Download SEBoK PDF," SEBoK, https://www.sebokwiki.org/w/index.php?title=Download_SEBoK_PDF&oldid=52787 (accessed Sept. 14, 2018).
26. "Security Technical Implementation Guides (STIGs)," DISA, https://iase.disa.mil/stigs.
27. Wagner, N., C. Ş Şahin, M. Winterrose, J. Riordan, D. Hanson, J. Peña, and W. W. Streilein. 2017. "Quantifying the Mission Impact of Network-Level Cyber Defensive Mitigations." *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* 14 (3): 201-216.
28. "What is SysML®?" Object Management Group, http://www.omgsysml.org/what-is-sysml.htm.
29. Yu, S., G. Gu, A. Barnawi, S. Guo, and I. Stojmenovic. 2015. "Malware Propagation in Large-Scale Networks." *IEEE Transactions on Knowledge and Data Engineering 27* (1): 170-179.