Uncovering Cascading Vulnerabilities in Model-Centric Acquisition Programs

16TH ANNUAL ACQUISITION RESEARCH SYMPOSIUM
May 8, 2019

Donna H. Rhodes

Massachusetts Institute Of Technology

rhodes@mit.edu

617.324.0473

SEAri Systems Engineering Advancement Research Initiative

How can we enable identifying and mitigating vulnerabilities within a model-centric enterprise?

Digital engineering tranformation changes how systems are acquired and developed using model-based engineering practices and toolsets, leading to potential new programmatic vulnerabilities.

Desired Research Result:

Provide model-centric (digital engineering) enterprises with a means to uncover cascading vulnerabilities (technical related, social-related, human-related) and determine where interventions can most effectively be taken

Research Relevance

DoD Digital Engineering Strategy

… mitigate cyber risks and secure digital engineering environments against attacks from internal and external threats

…mitigate known vulnerabilities that present high risk to DoD networks and data

…mitigate risk posed by collaboration and access to vast amount of information in models

https://www.acq.osd.mil/se/docs/2018-DES.pdf

Research Approach

Cause-Effect Mapping (CEM)

(Mekdeci, 2012)

Analytic technique for identifying cascading failures and intervention points

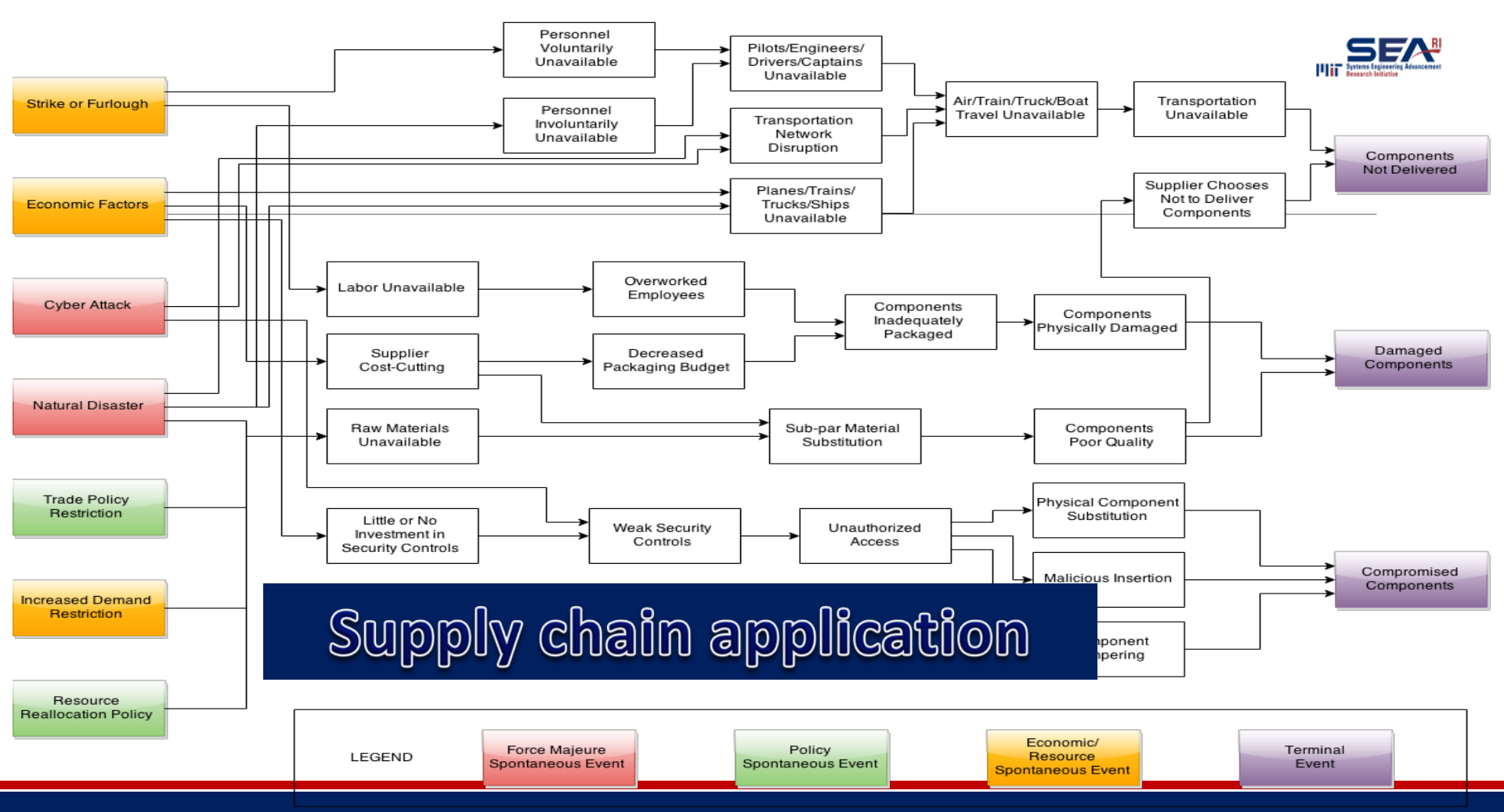
Models a system/enterprise using disruptions, disturbances, causal chains, and terminal conditions

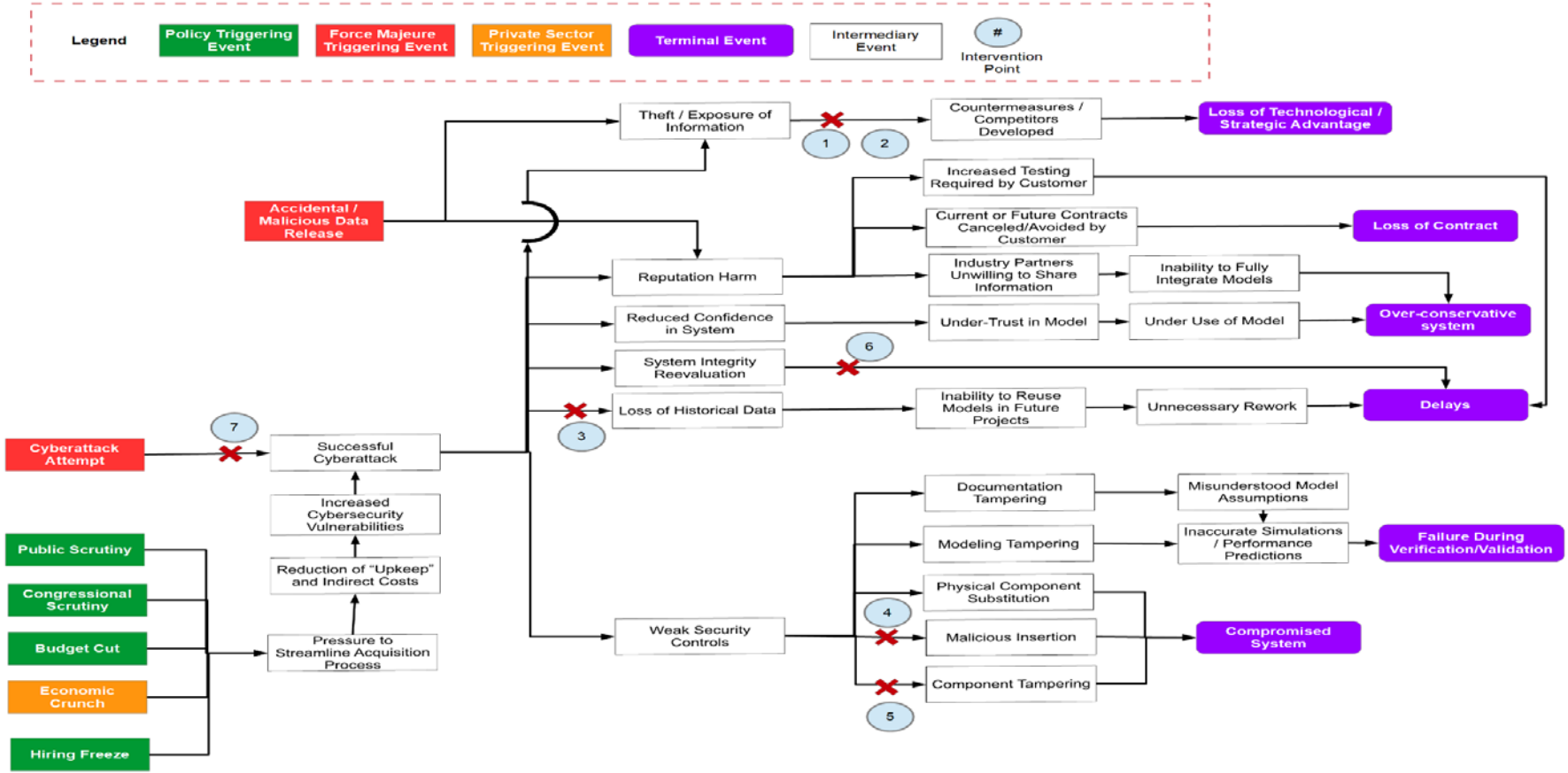
Highlights relationships between causes and effects of perturbations (disturbances and disruptions)

Hazard ("spontaneous event")
A system or environmental state that has the potential to disrupt the system

Vulnerability
Causal means by which one or more hazards results in the system disruption / value loss

Mekdeci, B., Ross, A.M., Rhodes, D.H., Hastings, D.E., "A Taxonomy of Perturbations: Determining the Ways that Systems Lose Value," 6th Annual IEEE SysCon, Vancouver, Canada, Mar2012

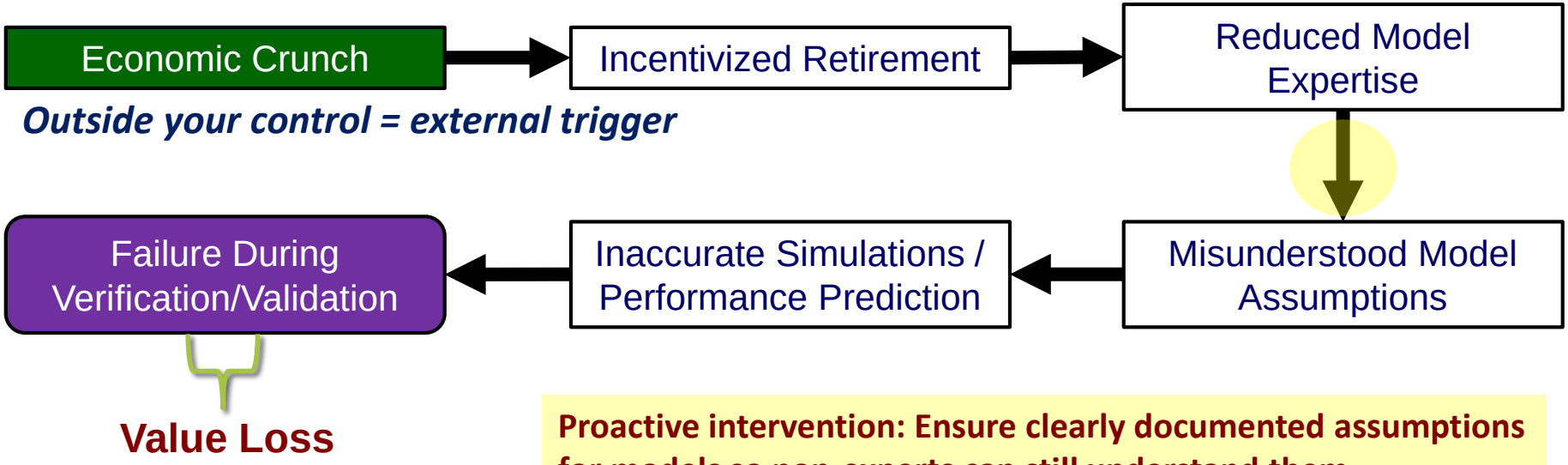

Strike or Furlough
Economic Factors
Cyber Attack
Natural Disaster
Trade Policy Restriction
Increased Demand Restriction
Resource Reallocation Policy
Personnel Voluntarily Unavailable
Personnel Involuntarily Unavailable
Pilots/Engineers/ Drivers/Captains Unavailable
Transportation Network Disruption
Planes/Trains/ Trucks/Ships Unavailable
Air/Train/Truck/Boat Travel Unavailable
Transportation Unavailable
Components Not Delivered
Supplier Chooses Not to Deliver Components
Labor Unavailable
Overworked Employees
Components Inadequately Packaged
Components Physically Damaged
Damaged Components
Supplier Cost-Cutting
Decreased Packaging Budget
Raw Materials Unavailable
Sub-par Material Substitution
Components Poor Quality
Little or No Investment in Security Controls
Weak Security Controls
Unauthorized Access
Physical Component Substitution
Malicious Insertion
Compromised Components
Supply chain application
LEGEND
Force Majeure Spontaneous Event
Policy Spontaneous Event
Economic/ Resource Spontaneous Event
Terminal Event



Reid, J. and Rhodes, D.H., Applying Cause-Effect Mapping to Assess Cybersecurity Vulnerabilities in Model-Centric Acquisition Program Environments, 15th Annual Acquisition Research Symposium, Monterey, CA, May 2018

Simplified example

Intervention in the Vulnerability Causal Chain



Proactive intervention: Ensure clearly documented assumptions for models so non-experts can still understand them

Reference Map for Model-Centric Vulnerabilities

potential uses

Assess potential future vulnerabilities and plan possible interventions

Determine specific vulnerabilities to address in response to specific hazard

Change program processes and technology to mitigate/eliminate vulnerabilities

Organize and classify vulnerabilities into various categories or types

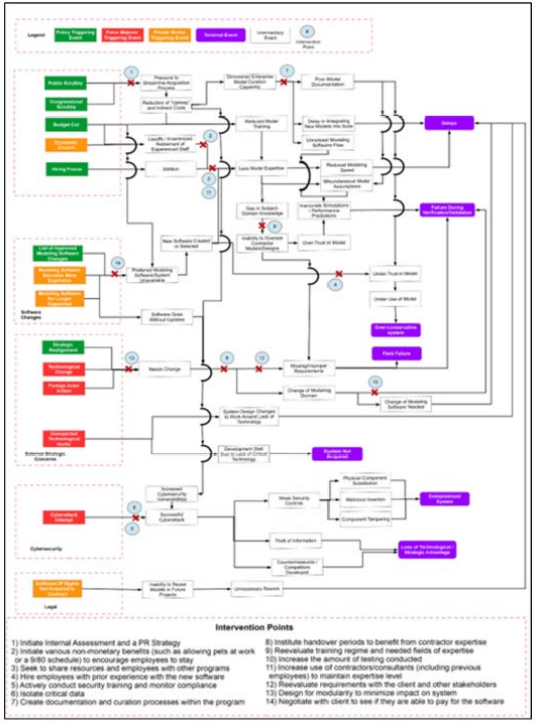
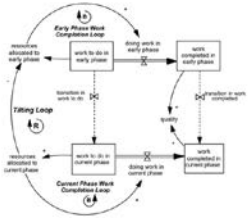


Figure 5. Reference CEM for Model-Centric Vulnerabilities (Preliminary)

Desired future research directions

1. Empirical studies to validate and enrich reference map
2. Leading indicators of vulnerability and mitigation strategies
3. Quantification of value of interventions (cost, benefit)
4. Dynamic simulation using system dynamics with CEM for accessing potential strategies



*With more experience and knowledge of vulnerabilities inherent in digital engineering practice and infrastructure, the systems community may find it valuable to establish a **generalized Reference CEM** to guide future programs and enterprises to assess and manage vulnerabilities, leading to more successful program outcomes*

Questions?

rhodes@mit.edu

This material is based upon work supported by the Acquisition Research Program under Grant No. HQ00341810013. The views expressed in written materials or publications, and/or made by speakers, moderators, and presenters, do not necessarily reflect the official policies of the Department of Defense nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.

Key Contributions by MIT Graduate Student Researchers:
Jack Reid, Sarah Rovito, Brian Mekdeci