Uncovering Cascading Vulnerabilities in Model-Centric Acquisition Programs

Donna H. Rhodes

Massachusetts Institute Of Technology

rhodes@mit.edu

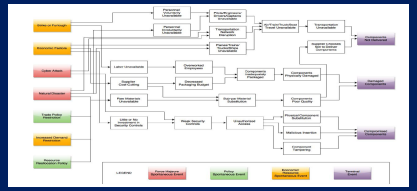
617.324.0473

SEA RI Systems Engineering Advancement Research Initiative

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

How can we enable identifying and mitigating vulnerabilities within the enterprise itself?

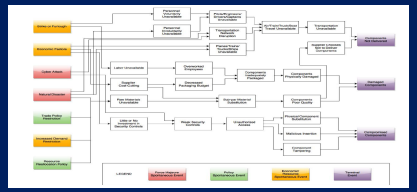
Research on Three Intertwined Aspects

humans in the loop	vulnerability analysis methods	digital engineering environment
Human-Model Interaction preferences and behaviors	Cause-Effect Mapping for Vulnerability Analysis	Model Curator and Model Curation Capabilities
		

Technical and Non-technical Influences

TECHNICAL FACTORS	SOCIAL FACTORS	COGNITIVE/PERCEPTUAL
Model Complexity	Talent/Skills of People	Automation Bias
Data Availability	Inertia/Resistance to Change	Complacency
Data Quality	Changing Preferences	Mode Errors
Fidelity and Uncertainty	Lack of Trust	Anchoring Bias
Inadequate Methods	Generational Differences	Information Overload
Lack of Transparency	Willingness to Share Models	Preference-Performance Dissociation
Verified Algorithms	Ability to Socialize Models	

Research on Three Intertwined Aspects

humans in the loop	vulnerability analysis methods	digital engineering environment
Human-Model Interaction preferences and behaviors	Cause-Effect Mapping for Vulnerability Analysis	Model Curator and Model Curation Capabilities
		

Cause-Effect Mapping
(Mekdeci, 2012)

Analytic technique for identifying cascading failures and system intervention points

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

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

Mekdeci, B., Ross, A.M., Rhodes, D.H., and Hastings, D.E., "A Taxonomy of Perturbations: Determining the Ways that Systems Lose Value," 6th Annual IEEE Systems Conference, Vancouver, Canada, March 2012

Definitions

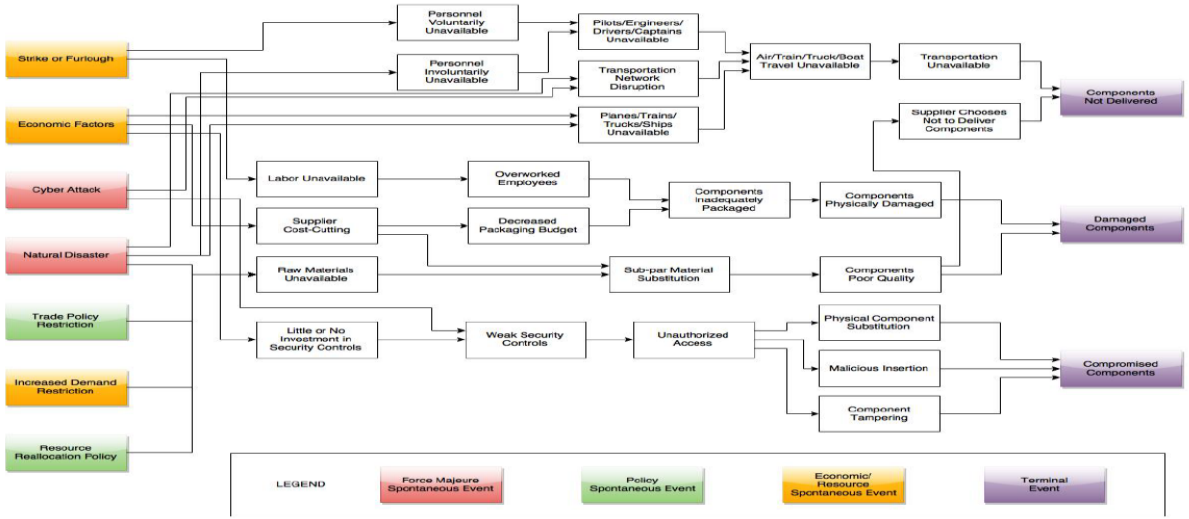
Hazard ("spontaneous event")

A system or environmental state that has the potential to disrupt the system

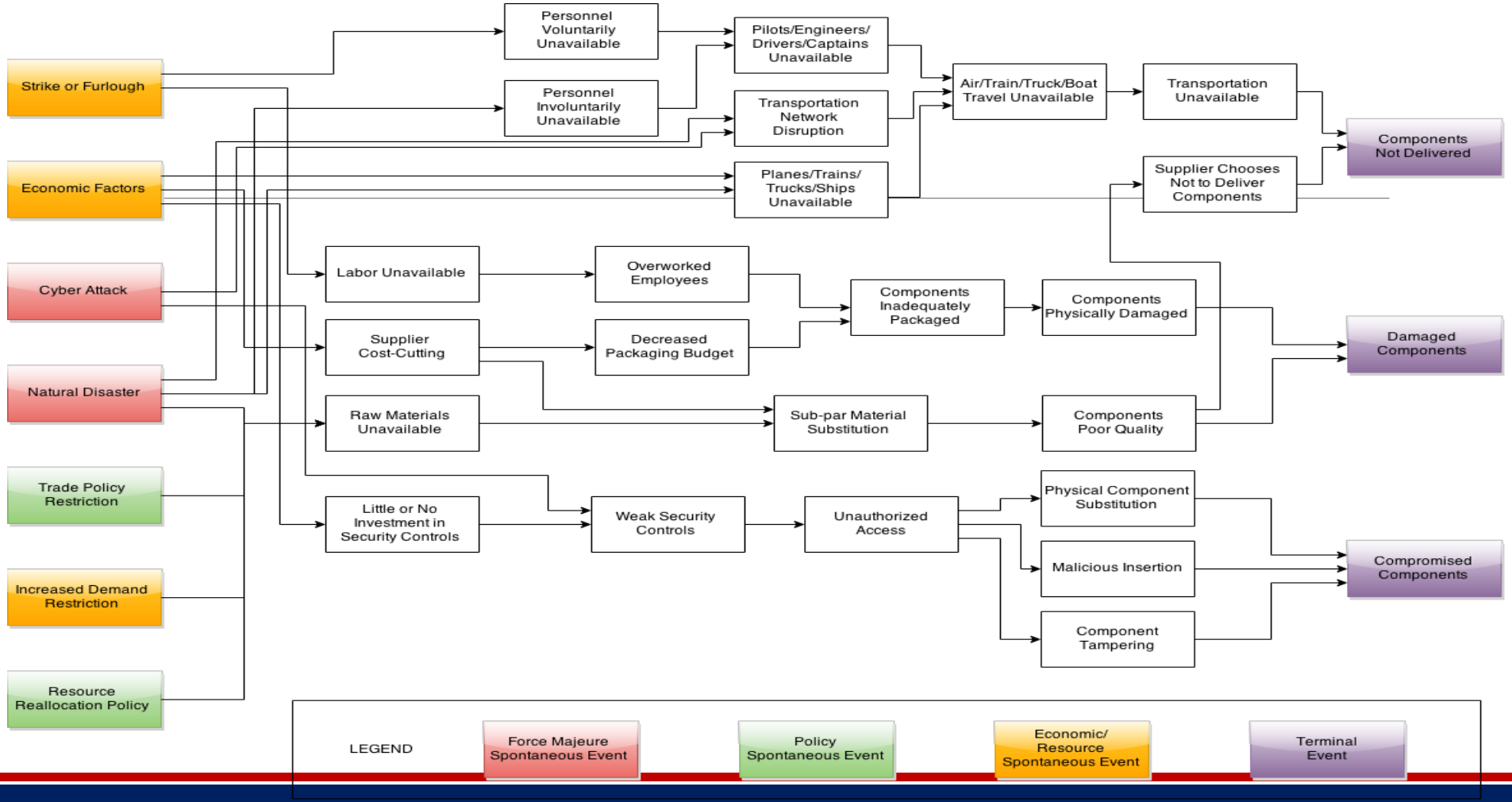
Vulnerability

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

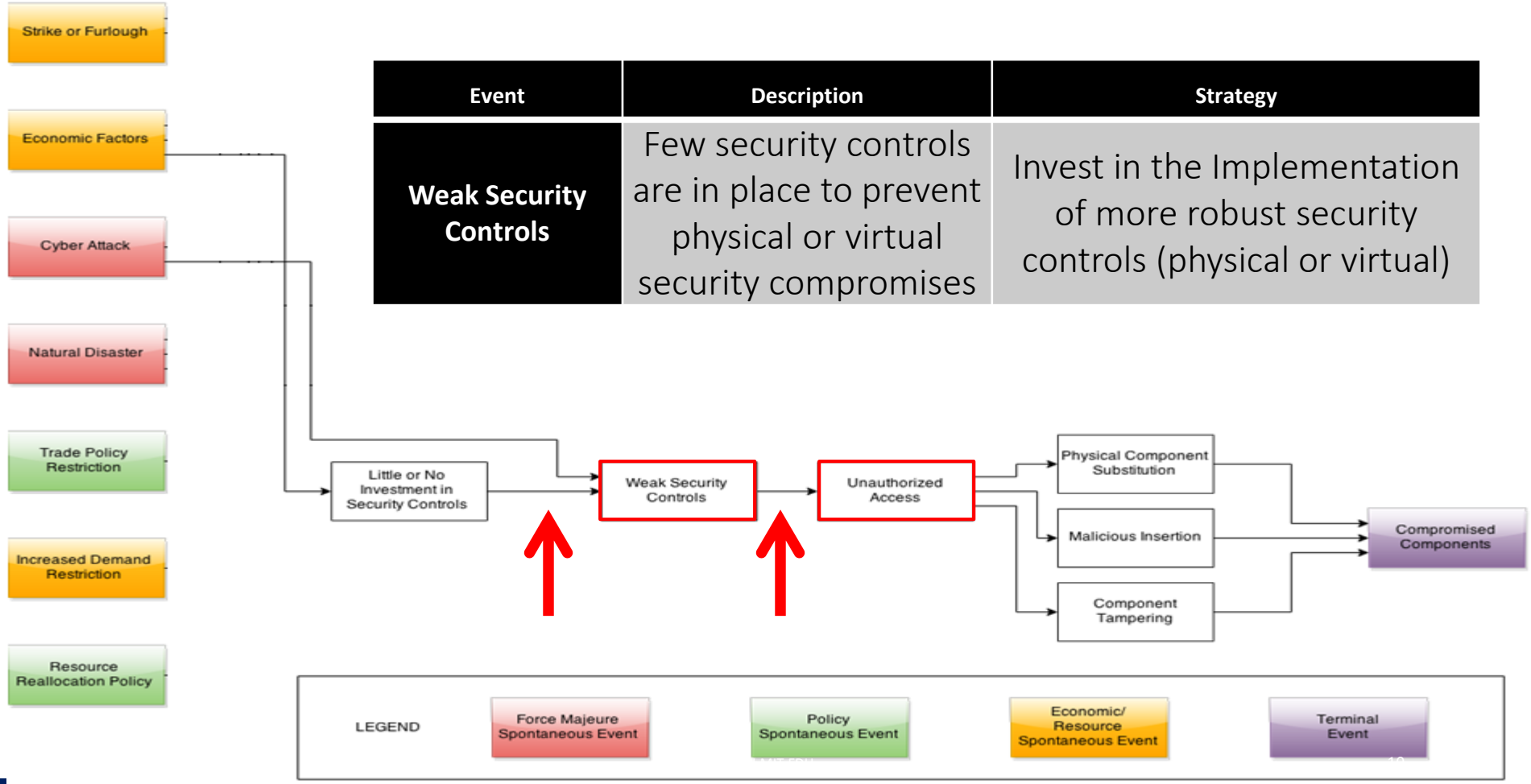
Cause-Effect Mapping Applied to Supply Chains



Rovito, S.M., and Rhodes, D.H., "Enabling Better Supply Chain Decisions Through a Generic Model Utilizing Cause-Effect Mapping," 10th Annual IEEE Systems Conference, Orlando, FL, April 2016


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
Supplier Cost-Cutting
Decreased Packaging Budget
Components Inadequately Packaged
Components Physically Damaged
Damaged Components
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
Component Tampering
Compromised Components
LEGEND
Force Majeure Spontaneous Event
Policy Spontaneous Event
Economic/ Resource Spontaneous Event
Terminal Event

Event	Description	Strategy
Weak Security Controls	Few security controls are in place to prevent physical or virtual security compromises	Invest in the Implementation of more robust security controls (physical or virtual)



Can Cause-Effect Mapping be Useful in Digital Engineering Enterprises?

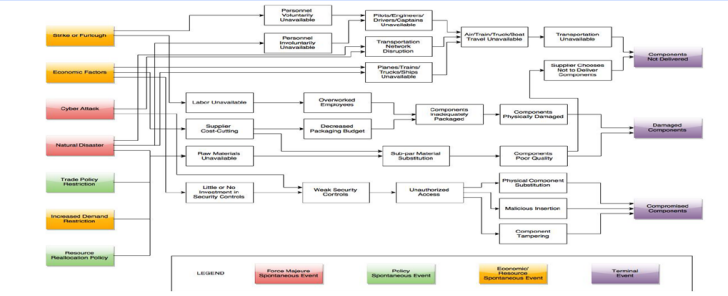
Emergent uncertainties (e.g., **policy change, budget cuts, disruptive technologies, threats, changing demographics**) and related programmatic decisions (e.g., **staff cuts, reduced training hours, process shortcuts**) may lead to cascading vulnerabilities in programs that may jeopardize success

Goal: assist program leaders to readily identify digital engineering related vulnerabilities (technical related, social-related, human-related) and determine where interventions can most effectively be taken

Cause-Effect Mapping for Vulnerability Analysis (CEM-VA)

Ongoing research has evolved CEM-VA method for better enabling program leaders to anticipate and respond to vulnerabilities related to digital engineering practice and model-centric environments

CEM-VA reference map resulting from research shows promise for considering cascading vulnerabilities and potential intervention options



Reference Map for Model-Centric Vulnerabilities

four potential uses

Assess potential future vulnerabilities and planning possible interventions

Determine specific vulnerabilities to address in response to specific hazard

Change program processes to mitigate or eliminate vulnerabilities

Organize and classify vulnerabilities into various categories or types

Reid & Rhodes, 2018

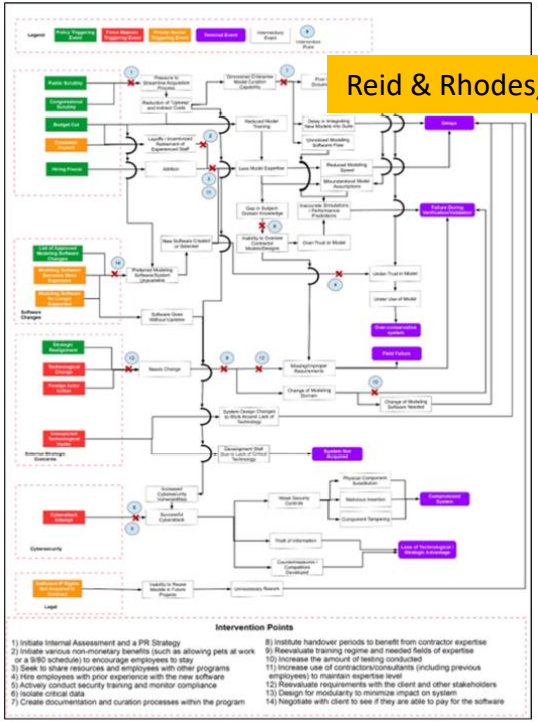
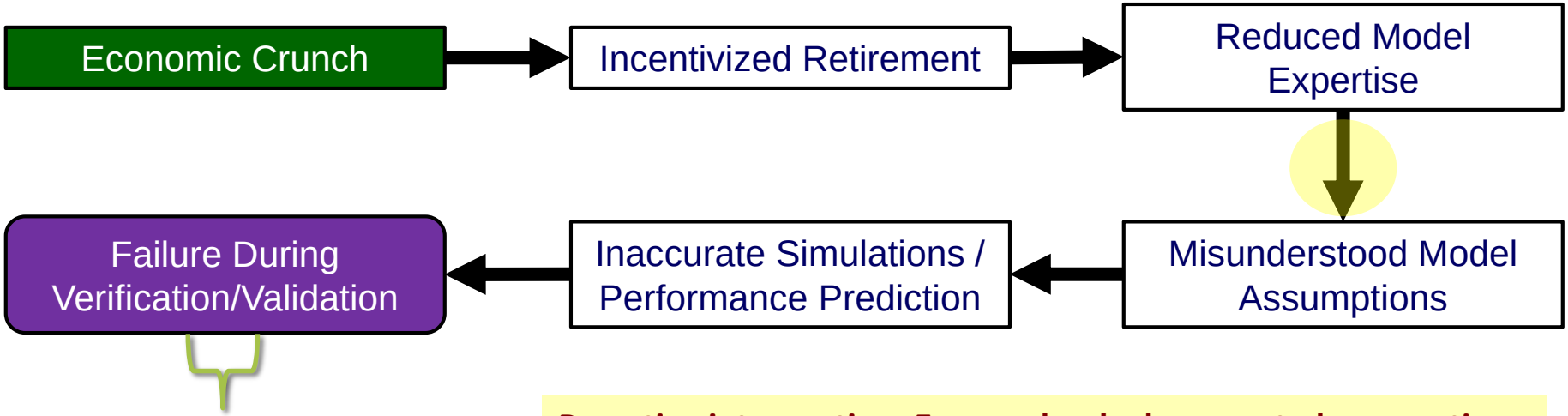


Figure 5. Reference CEM for Model-Centric Vulnerabilities (Preliminary)

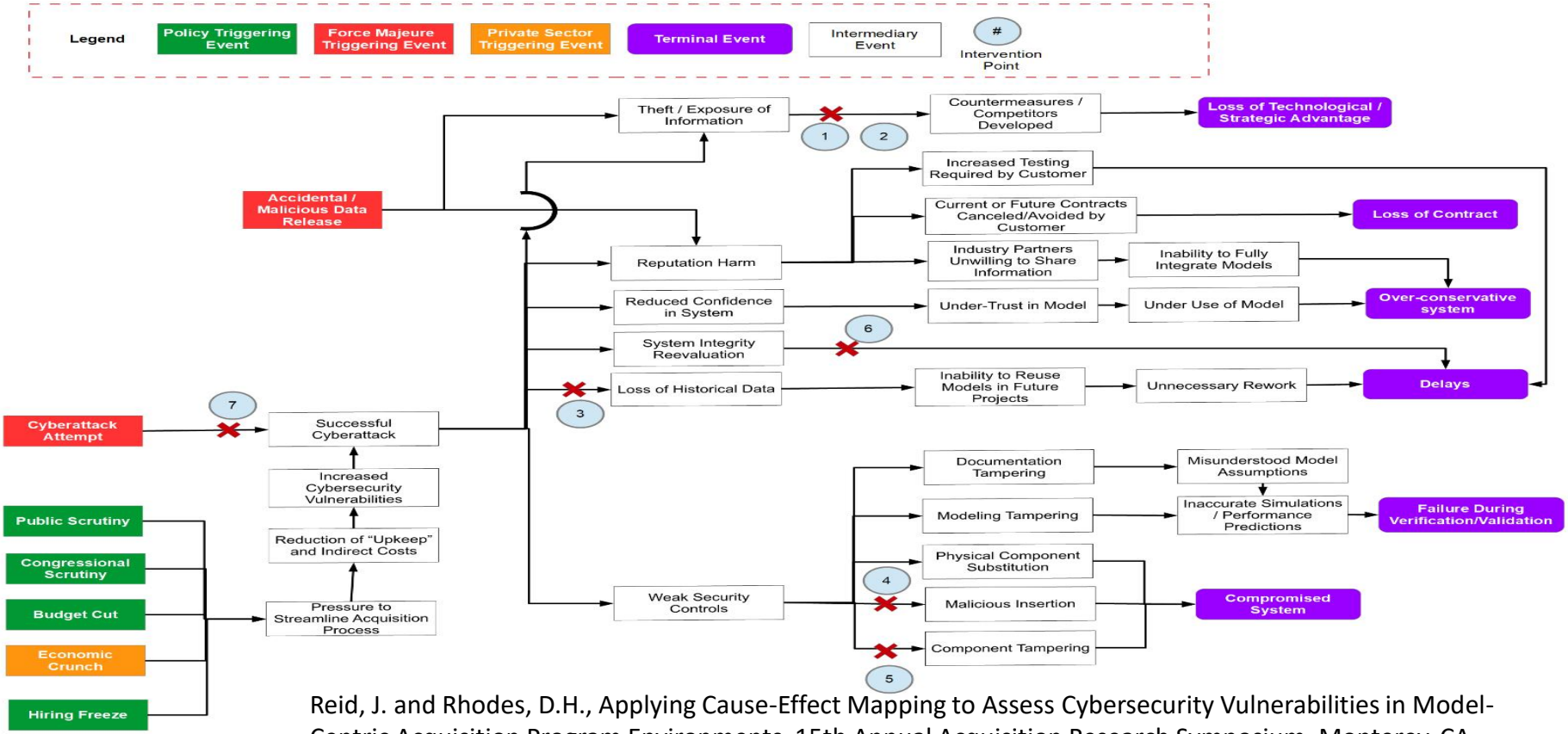
Causal Chain

Outside your control = external trigger



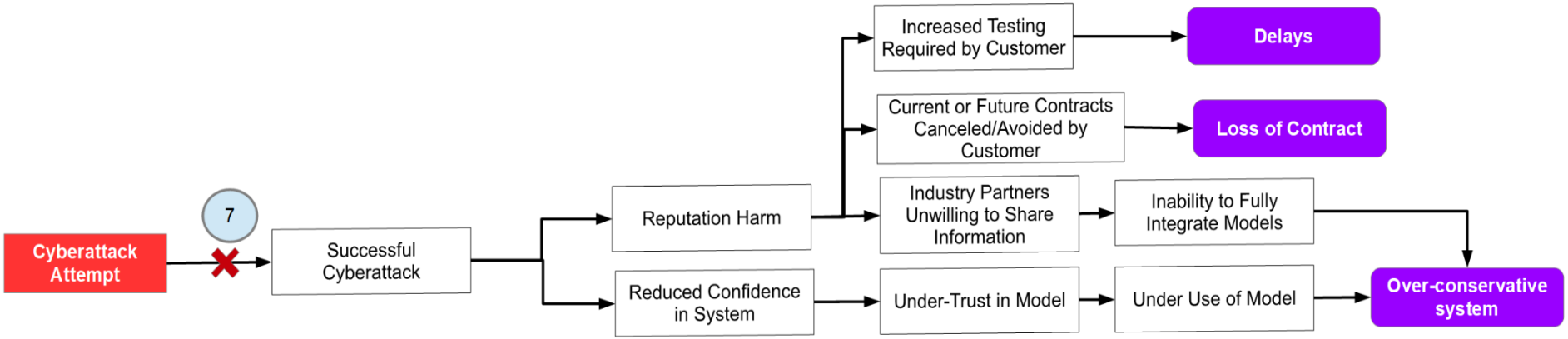
Proactive intervention: Ensure clearly documented assumptions for models so non-experts can still understand them

Work in Progress: CEM-VA - Cybersecurity



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

Preventing Non-technical Impacts



Reference model also addresses potential issues like harm to the reputation of the organization and reduced confidence in the modeling environment integrity

Preliminary CEM-VA Usability Testing

Graduate student assessment

1. Identifying high priority intervention points: (70%)
2. Identifying new vulnerabilities: (55%)
3. Understanding causal path / Reframing concept of vulnerabilities: (45%)
4. Understanding interrelationships between vulnerabilities: (40%)

Industry expert evaluation

1. Positive response to viewing vulnerabilities as causal chains
2. Positive feedback on usefulness of approach

CEM-VA Reference Maps

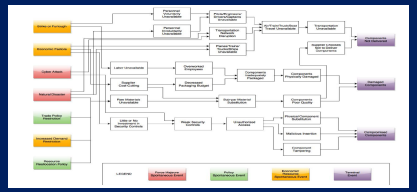
Generated/customized to a specific class of decision-maker

Hazards (referred to as “spontaneous events”) are exogenous from the point of view of the decision-maker

In this way, CEM avoids “blaming someone else” problem by making all hazards exogenous

- Decision-maker only has control over the intermediary events
- Decision-maker, while not necessarily at fault for any of the vulnerabilities, has responsibility to address them

Research on Three Intertwined Aspects

humans in the loop	vulnerability analysis methods	digital engineering environment
Human-Model Interaction preferences and behaviors	Cause-Effect Mapping for Vulnerability Analysis	Model Curator and Model Curation Capabilities
		

model curator

- enterprise model accessions
- valuation of model and digital artifacts
- strategic loan/acq of models
- oversight of model collection activities
- set model collection policy/practices
- strategies for model-centric future
- leadership for model demonstrators

CEM-VA has potential to be a valuable tool for model curator

Research Application 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

Current research focus

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

Mature CEM-VA Reference model with focus on cybersecurity

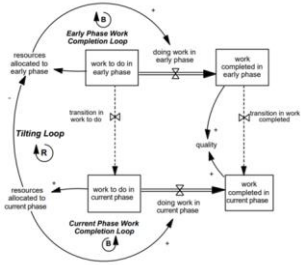
Explore network analysis and dynamic modeling of CEM

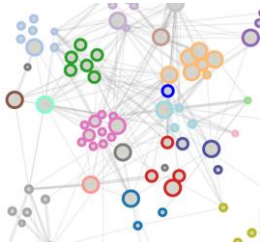
SYSTEMS ENGINEERING
Research Center

Leverage findings for model curation/model curator research (DoD SERC Sponsorship)

Desired future research directions

1. Collaborative research with industry/government to transition research to practice
2. Additional study of leading indicators of vulnerability and mitigation strategies
3. Quantification of value of interventions (cost, benefit)
4. Model-based implementation of CEM-VA to enable interaction and anticipator analysis
5. Dynamic simulation using system dynamics with CEM for accessing potential strategies





Questions?

rhodes@mit.edu

SEA RI Systems Engineering Advancement Research Initiative

DRAPER

SYSTEMS ENGINEERING Research Center

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

CEM research publications

Mekdeci, B., Ross, A.M., Rhodes, D.H., and Hastings, D.E., "A Taxonomy of Perturbations: Determining the Ways that Systems Lose Value," 6th Annual IEEE Systems Conference, Vancouver, Canada, March 2012

Rovito, S.M., and Rhodes, D.H., "Enabling Better Supply Chain Decisions Through a Generic Model Utilizing Cause-Effect Mapping," 10th Annual IEEE Systems Conference, Orlando, FL, April 2016 (BEST PAPER AWARD)

Reid, J. and Rhodes, D.H., Accessing Vulnerabilities in Model-Centric Acquisition Programs Using Cause-Effect Mapping, 15th Annual Acquisition Research Symposium, Monterey, CA, May 2018

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

http://seari.mit.edu/publications.php