SEAri

MIT Systems Engineering Advancement Research Initiative

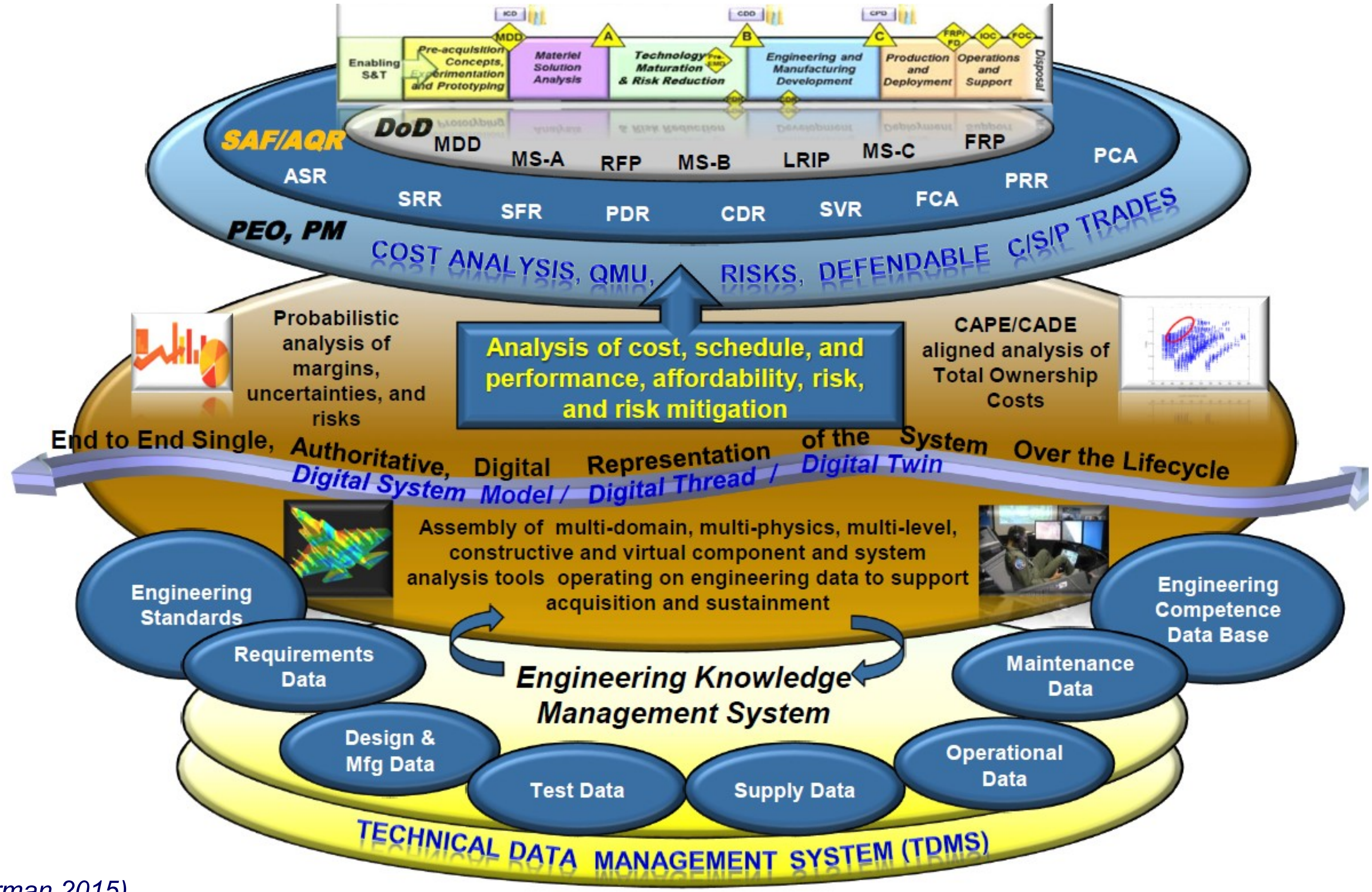
Applying Cause-Effect Mapping to Assess Cybersecurity Vulnerabilities in Model-Centric Acquisition Program Environment

Jack Reid, Donna Rhodes
Massachusetts Institute of Technology

Acquisition Research Symposium
May 9-10, 2018
Embassy Suites Monterey Bay Seaside
Monterey, California

Acquisition Research Program
Naval Postgraduate School

Model-Centric Engineering (MCE)



ICD
CDD
CPD
MDD
A
B
C
FRP/FD
IOC
FOC
Enabling S&T
Pre-acquisition Concepts, Experimentation and Prototyping
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Pre-EMD
Engineering and Manufacturing Development
Production and Deployment
Operations and Support
Disposal
PDR
CDR
DoD
MDD
MS-A
RFP
MS-B
LRIP
MS-C
FRP
SAF/AQR
ASR
SRR
SFR
PDR
CDR
SVR
FCA
PRR
PCA
PEO, PM

COST ANALYSIS, QMU, RISKS, DEFENDABLE C/S/P TRADES

Probabilistic analysis of margins, uncertainties, and risks

Analysis of cost, schedule, and performance, affordability, risk, and risk mitigation

CAPE/CADE aligned analysis of Total Ownership Costs

End to End Single, Authoritative, Digital Representation of the System Over the Lifecycle

Digital System Model / Digital Thread / Digital Twin

Assembly of multi-domain, multi-physics, multi-level, constructive and virtual component and system analysis tools operating on engineering data to support acquisition and sustainment

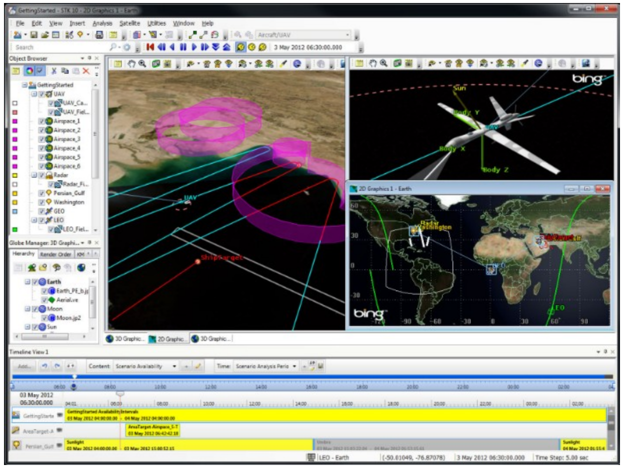
Engineering Knowledge Management System

TECHNICAL DATA MANAGEMENT SYSTEM (TDMS)

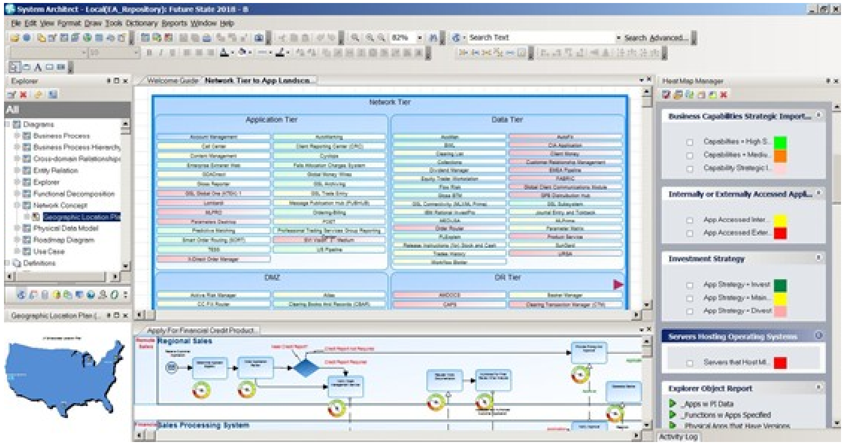
(Zimmerman 2015)

Current State of MCE

STK



UNICOM System Architect



JPL Team-X

NAVAIR

MCE and Cybersecurity

(Some) Benefits		Cybersecurity Concerns
System-level optimization and “authoritative source of truth”	→	“All eggs in one basket”
Increased collaboration across teams	→	More points of entry
Removal of barriers between stages Design ▼ Manufacturing ▼ Testing ▼ Operation	→	Tampering in design can make its way into the field

Systems Engineering Advancement Research Initiative

MCE and Cybersecurity

MCE make **e *program* even more important**

Cyber- : A
case st

Logan D.
Robert P

The Telegraph

Kremlin returns to typewriters to avoid computer leaks

The Kremlin is returning to typewriters in an attempt to avoid damaging leaks from computer hardware, it has been claimed.

Boeing production p
ransomware attack

The widespread and devastating cyberat

By Nick Statt | @nickstatt | Mar 28, 2018, 7:23pm EDT

Convicted in
rade Secrets

M EST

Bloomberg

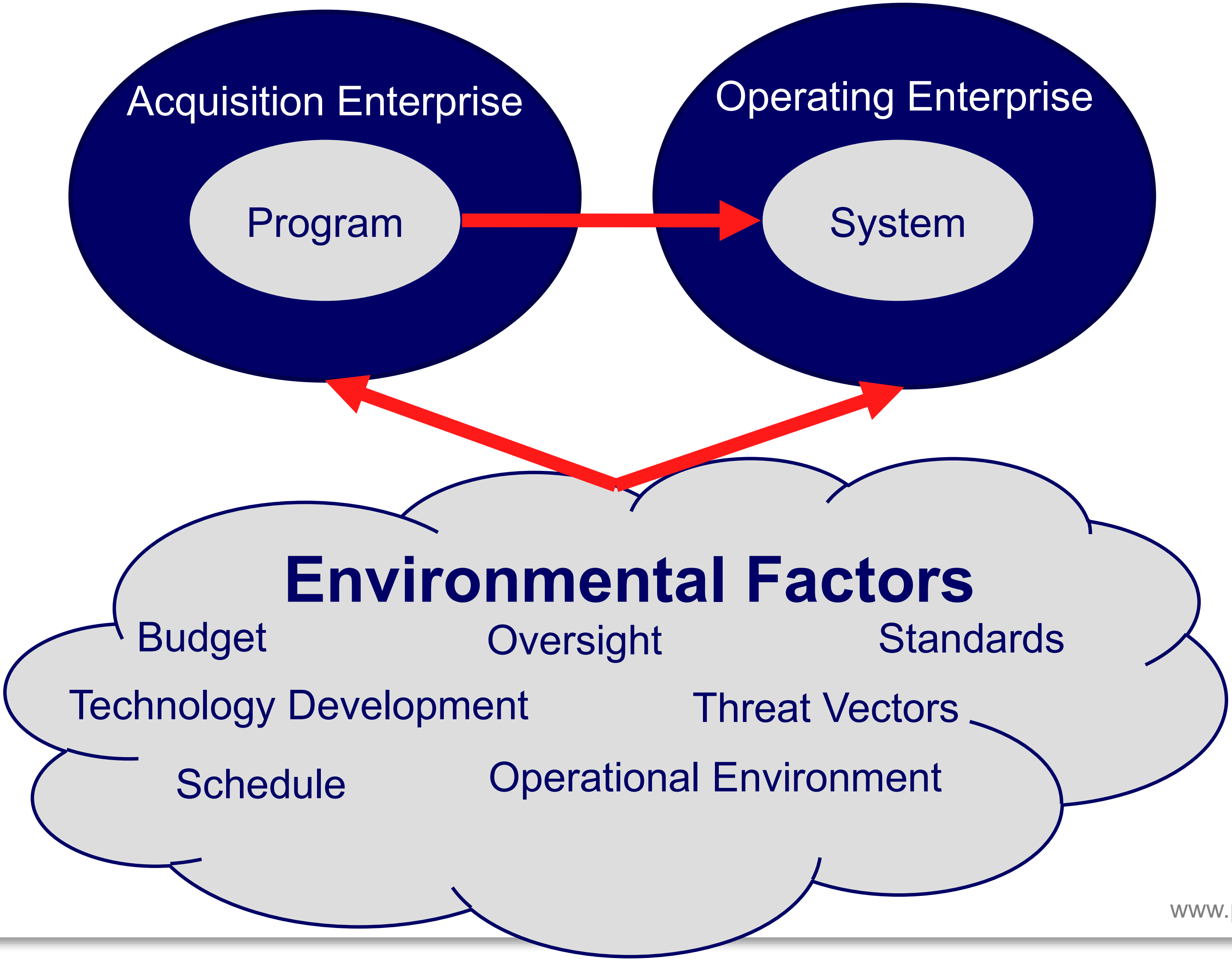
Motivating Questions

MCE introduces vulnerabilities beyond cybersecurity

1. What are program managers doing now in the face of external hazards and uncertainties?
2. How can they be prepared to tackle the new vulnerabilities that MCE introduces in the **program**?

These general questions led us to a focus on cybersecurity

Program vs System



www.public.navy.mil

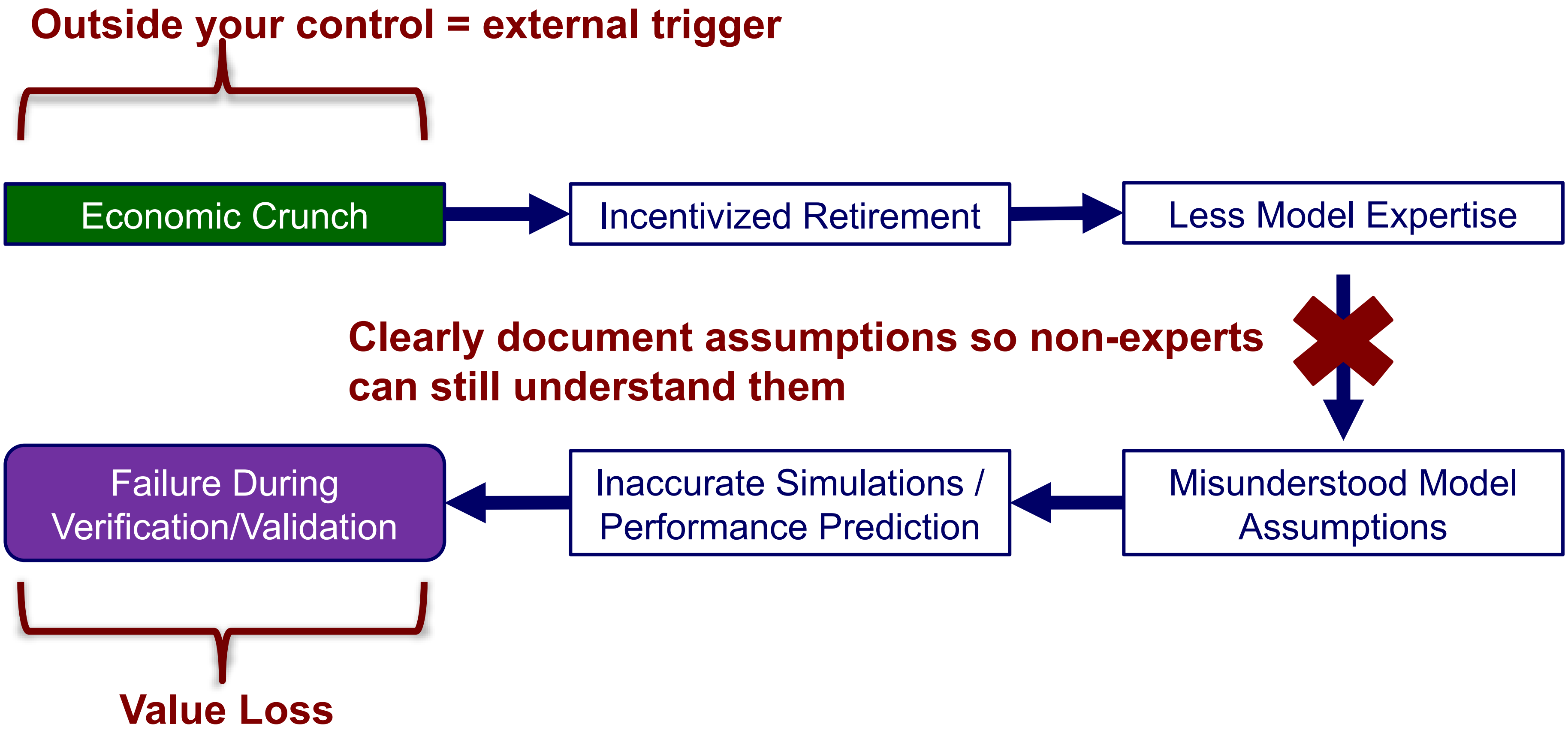
Definitions

- **Hazard:** A system or environmental state that has the potential to disrupt the system
- **Vulnerability:** The causal means by which the hazard results in the system disruption / value loss
  - "Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis" (CVE-2017-5753)
  - "We are vulnerable to man-in-the-middle attacks"
  - "A schedule delay would cost us $10M."

Vulnerability Chain

- **Causal Chain:** A series of events, with each event causing or being an integral part of the cause, or the next “link” in the chain
- Enables easy dissection of a vulnerability and identification of interventions

Causal Chain



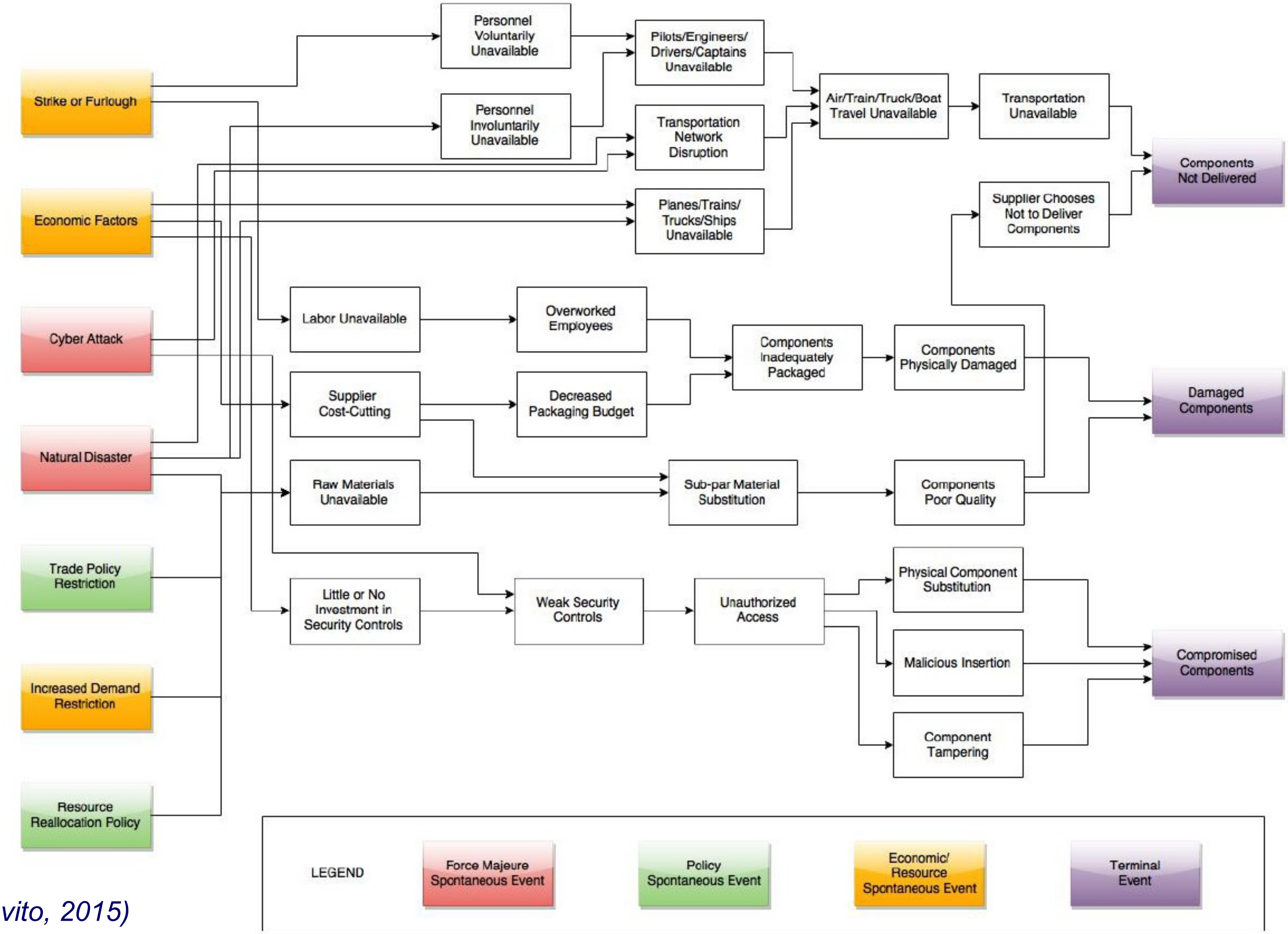
Outside your control = external trigger

Economic Crunch → Incentivized Retirement → Less Model Expertise → Misunderstood Model Assumptions → Inaccurate Simulations / Performance Prediction → Failure During Verification/Validation

Clearly document assumptions so non-experts can still understand them

Value Loss

Cause-Effect Mapping (CEM)

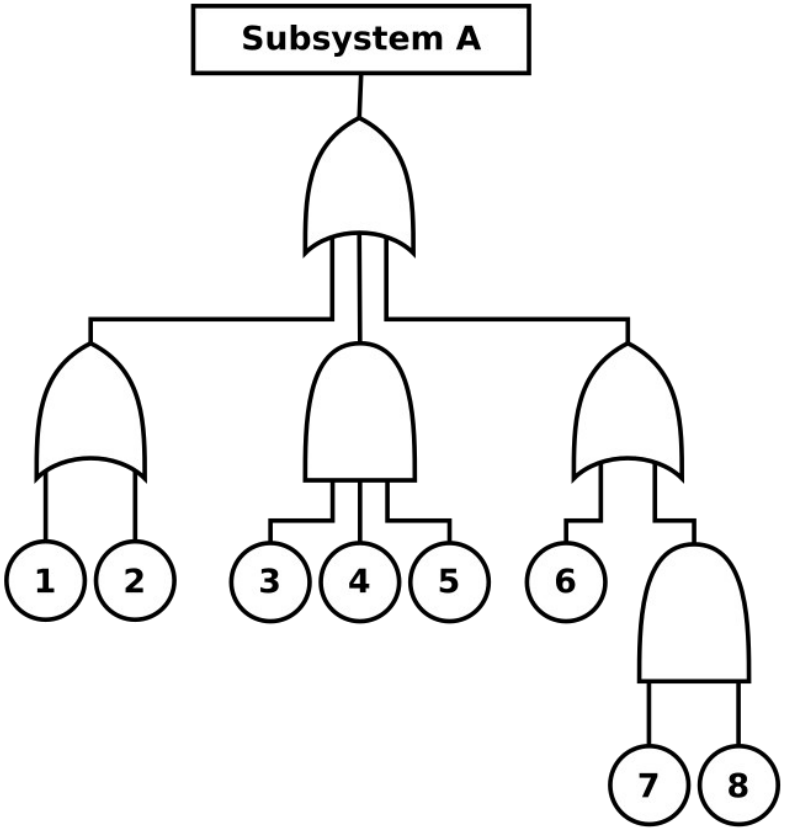

Strike or Furlough
Economic Factors
Cyber Attack
Natural Disaster
Trade Policy Restriction
Increased Demand Restriction
Resource Reallocation Policy
Personnel Voluntarily Unavailable
Personnel Involuntarily Unavailable
Pilots/Engineers/ Drivers/Captains Unavailable
Transportation Network Disruption
Planes/Trains/ Trucks/Ships Unavailable
Air/Train/Truck/Boat Travel Unavailable
Transportation Unavailable
Supplier Chooses Not to Deliver Components
Components Not Delivered
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

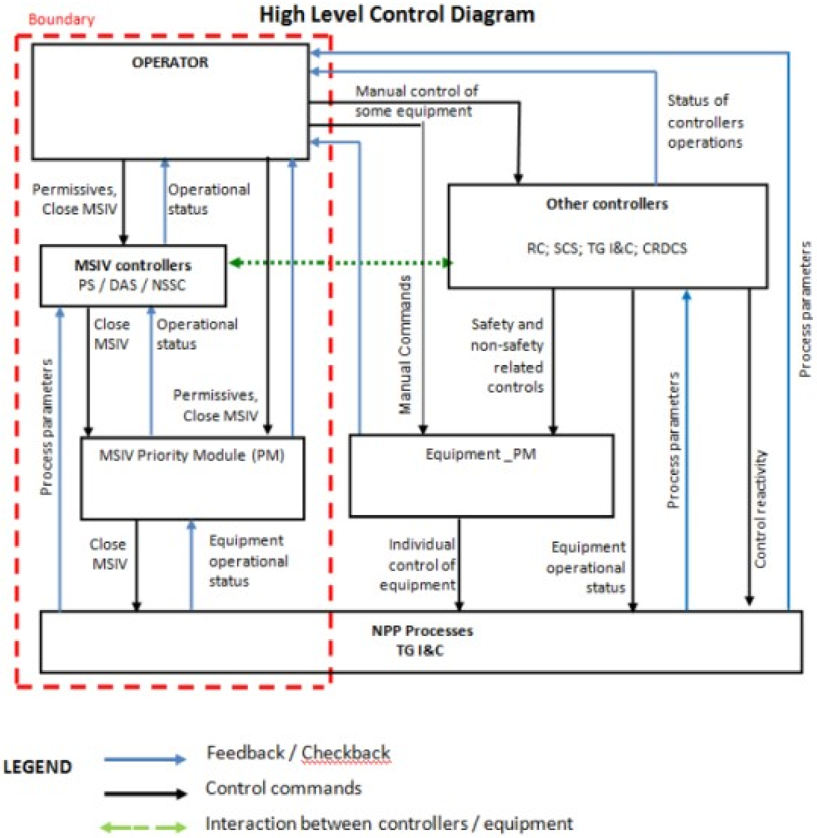
(Rovito, 2015)

Uses of CEM / Typology

- Enables identification and understanding of
  - Connections between vulnerabilities
  - Priority forms of intervention
- A CEM is made with a particular user in mind
- Does not assign “blame,” focuses on action

Comparisons



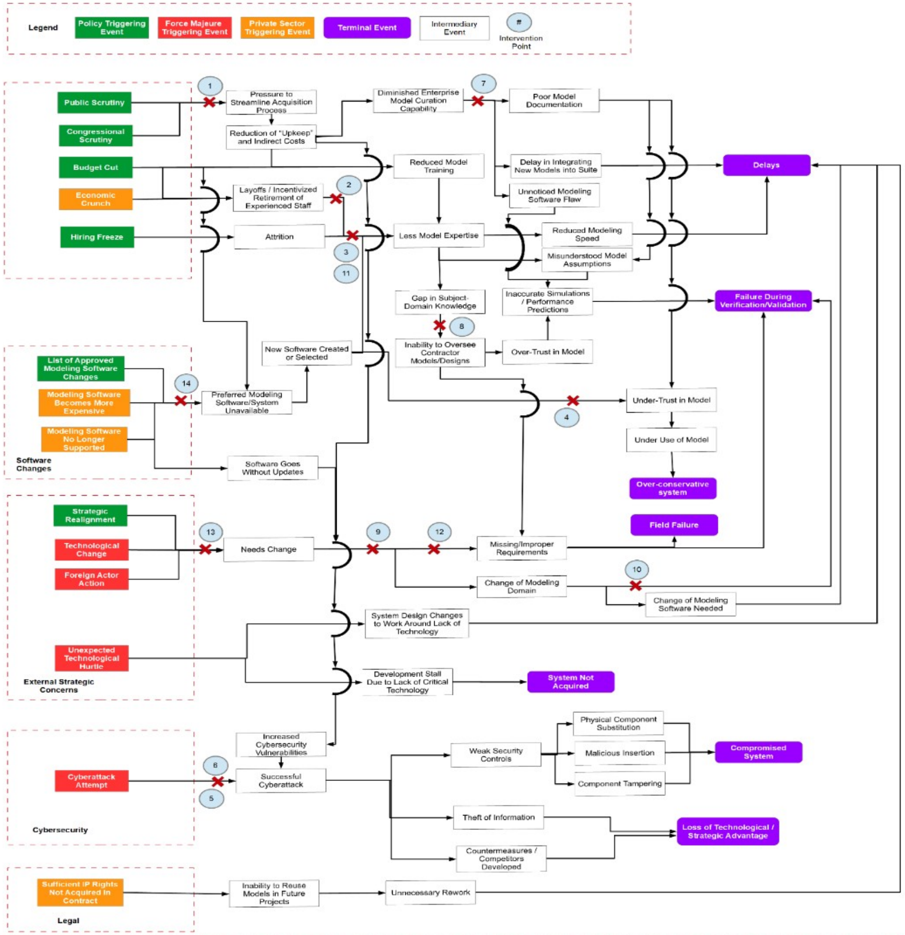


(Leveson 2013)

Interviews

- Disciplines
  - Aerospace
  - Nuclear Physics
  - Automotive
  - Oil & Gas
  - Medical
  - Defense
- “Networking and MCE is hard to do while staying secure. Particularly when dealing with large groups across departments.”
- “The environment keeps changing and it is always getting bigger. You have to protect yourself from old threats and vulnerabilities, while continuing to adapt and move forward.”

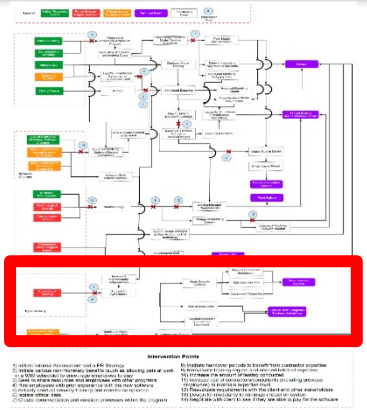
MCE Cause-Effect Mapping


Legend
Policy Triggering Event
Force Majeure Triggering Event
Private Sector Triggering Event
Terminal Event
Intermediary Event
#
Intervention Point
Public Scrutiny
Congressional Scrutiny
Budget Cut
Economic Crunch
Hiring Freeze
1
Pressure to Streamline Acquisition Process
Reduction of "Upkeep" and Indirect Costs
Diminished Enterprise Model Curation Capability
7
Poor Model Documentation
Reduced Model Training
Delay in Integrating New Models into Suite
Unnoticed Modeling Software Flaw
Delays
2
Layoffs / Incentivized Retirement of Experienced Staff
Attrition
3
11
Less Model Expertise
Reduced Modeling Speed
Misunderstood Model Assumptions
Gap in Subject-Domain Knowledge
Inaccurate Simulations / Performance Predictions
Failure During Verification/Validation
8
Inability to Oversee Contractor Models/Designs
Over-Trust in Model
New Software Created or Selected
List of Approved Modeling Software Changes
Modeling Software Becomes More Expensive
Modeling Software No Longer Supported
14
Preferred Modeling Software/System Unavailable
Software Changes
Software Goes Without Updates
4
Under-Trust in Model
Under Use of Model
Over-conservative system
Field Failure
Strategic Realignment
Technological Change
Foreign Actor Action
13
Needs Change
9
12
Missing/Improper Requirements
Change of Modeling Domain
10
Change of Modeling Software Needed
System Design Changes to Work Around Lack of Technology
Unexpected Technological Hurtle
External Strategic Concerns
Development Stall Due to Lack of Critical Technology
System Not Acquired
Increased Cybersecurity Vulnerabilities
6
Cyberattack Attempt
5
Successful Cyberattack
Cybersecurity
Weak Security Controls
Physical Component Substitution
Malicious Insertion
Component Tampering
Compromised System
Theft of Information
Countermeasures / Competitors Developed
Loss of Technological / Strategic Advantage
Sufficient IP Rights Not Acquired In Contract
Legal
Inability to Reuse Models in Future Projects
Unnecessary Rework

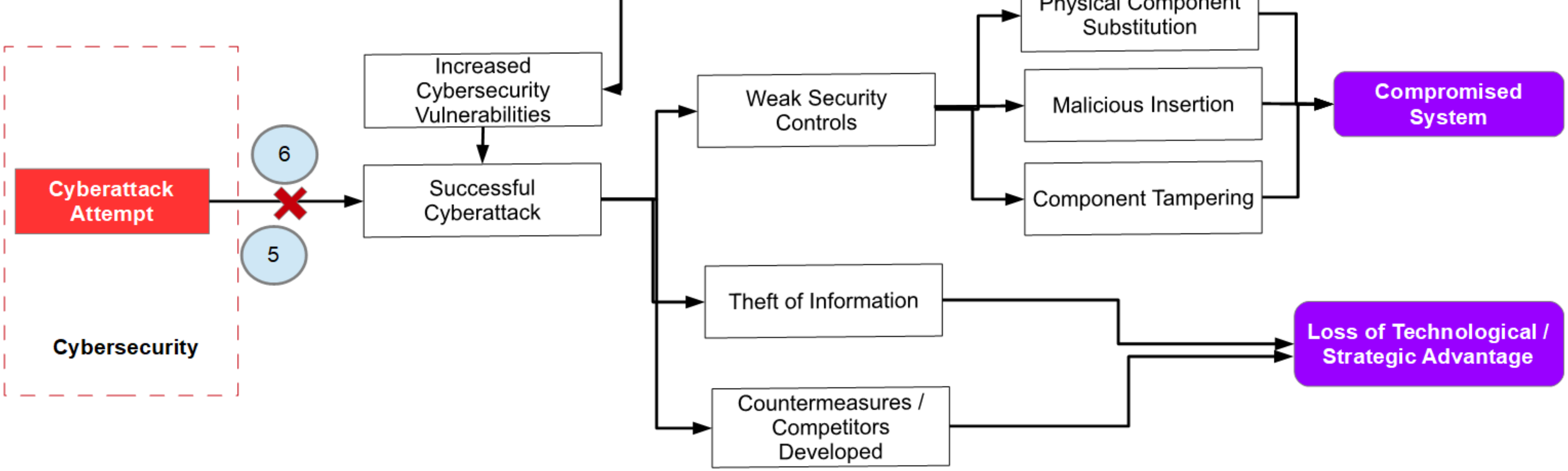
Intervention Points

1) Initiate Internal Assessment and a PR Strategy
2) Initiate various non-monetary benefits (such as allowing pets at work or a 9/80 schedule) to encourage employees to stay
3) Seek to share resources and employees with other programs
4) Hire employees with prior experience with the new software
5) Actively conduct security training and monitor compliance
6) Isolate critical data
7) Create documentation and curation processes within the program
8) Institute handover periods to benefit from contractor expertise
9) Reevaluate training regime and needed fields of expertise
10) Increase the amount of testing conducted
11) Increase use of contractors/consultants (including previous employees) to maintain expertise level
12) Reevaluate requirements with the client and other stakeholders
13) Design for modularity to minimize impact on system
14) Negotiate with client to see if they are able to pay for the software

Cause-Effect Mapping - Cybersecurity



Version 1.0



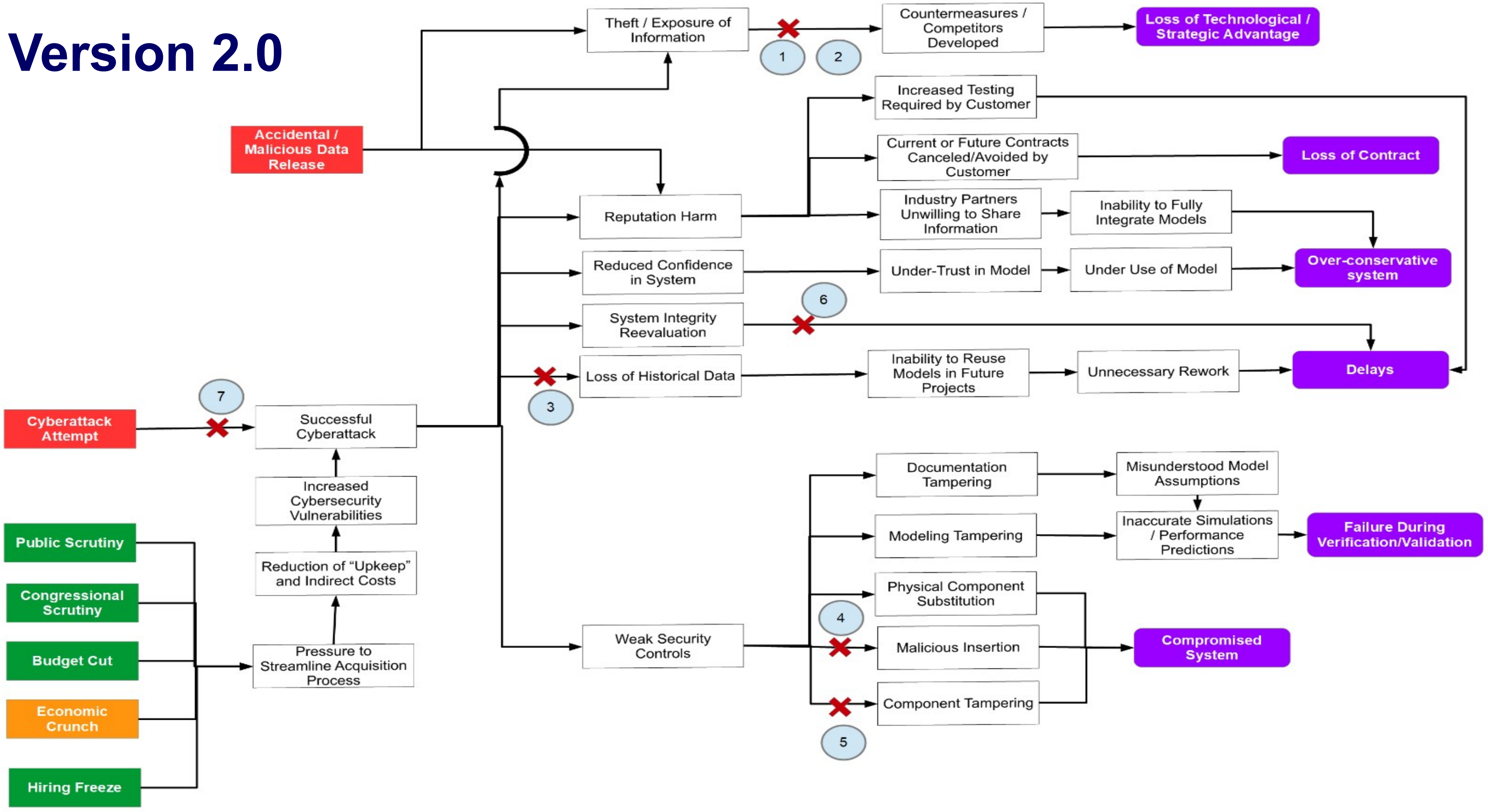
5) Actively conduct security training and monitor compliance
6) Isolate critical data

CEM - Cybersecurity

Legend

- 🟩 Policy Triggering Event
- 🟥 Force Majeure Triggering Event
- 🟧 Private Sector Triggering Event
- 🟪 Terminal Event
- □ Intermediary Event
- # Intervention Point

Version 2.0



Accidental / Malicious Data Release

Theft / Exposure of Information

1

2

Countermeasures / Competitors Developed

Loss of Technological / Strategic Advantage

Increased Testing Required by Customer

Current or Future Contracts Canceled/Avoided by Customer

Loss of Contract

Reputation Harm

Industry Partners Unwilling to Share Information

Inability to Fully Integrate Models

Reduced Confidence in System

Under-Trust in Model

Under Use of Model

Over-conservative system

System Integrity Reevaluation

6

Loss of Historical Data

3

Inability to Reuse Models in Future Projects

Unnecessary Rework

Delays

Cyberattack Attempt

7

Successful Cyberattack

Increased Cybersecurity Vulnerabilities

Reduction of "Upkeep" and Indirect Costs

Pressure to Streamline Acquisition Process

Public Scrutiny

Congressional Scrutiny

Budget Cut

Economic Crunch

Hiring Freeze

Weak Security Controls

Documentation Tampering

Misunderstood Model Assumptions

Modeling Tampering

Inaccurate Simulations / Performance Predictions

Failure During Verification/Validation

Physical Component Substitution

4

Malicious Insertion

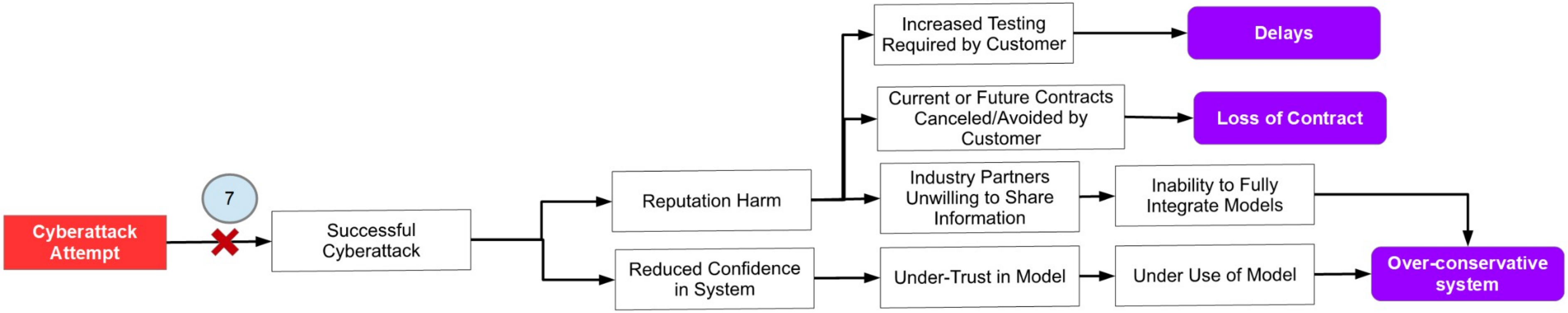
Compromised System

Component Tampering

5

Discussion

Program Managers are not solely interested in the technical impacts of cyberattacks…


Cyberattack Attempt
7
Successful Cyberattack
Reputation Harm
Reduced Confidence in System
Increased Testing Required by Customer
Current or Future Contracts Canceled/Avoided by Customer
Industry Partners Unwilling to Share Information
Under-Trust in Model
Inability to Fully Integrate Models
Under Use of Model
Delays
Loss of Contract
Over-conservative system

Issues like harm to the reputation of the organization and reduced confidence in the modeling environment’s integrity are also quite important

Next Steps and Recommendations

Take-Aways / Recommendations

- Causal Chains provide additional insight into vulnerabilities
- Program managers know that cybersecurity is important
- PMs need tools to understand the threat and take action
- PMs also need better knowledge on how to *respond* to attacks
  - Responsibility for this also lies at the organizational level

Next Steps

- Discussions with MCE tool developers and organizational leaders
- Develop a prototype interactive CEM to use as a training tool
- Generate analogy case studies from other industries

Questions?

This material is based upon work by the Naval Postgraduate School Acquisition Research Programs under Grant No. N00244-17-1-0011.

References

P. Zimmerman, “MBSE in the Department of Defense.” 2015.

B. Mekdeci, A. M. Ross, D. H. Rhodes, and D. E. Hastings, “A taxonomy of perturbations: Determining the ways that systems lose value,” in *2012 IEEE International Systems Conference, Proceedings*, 2012, pp. 507–512.

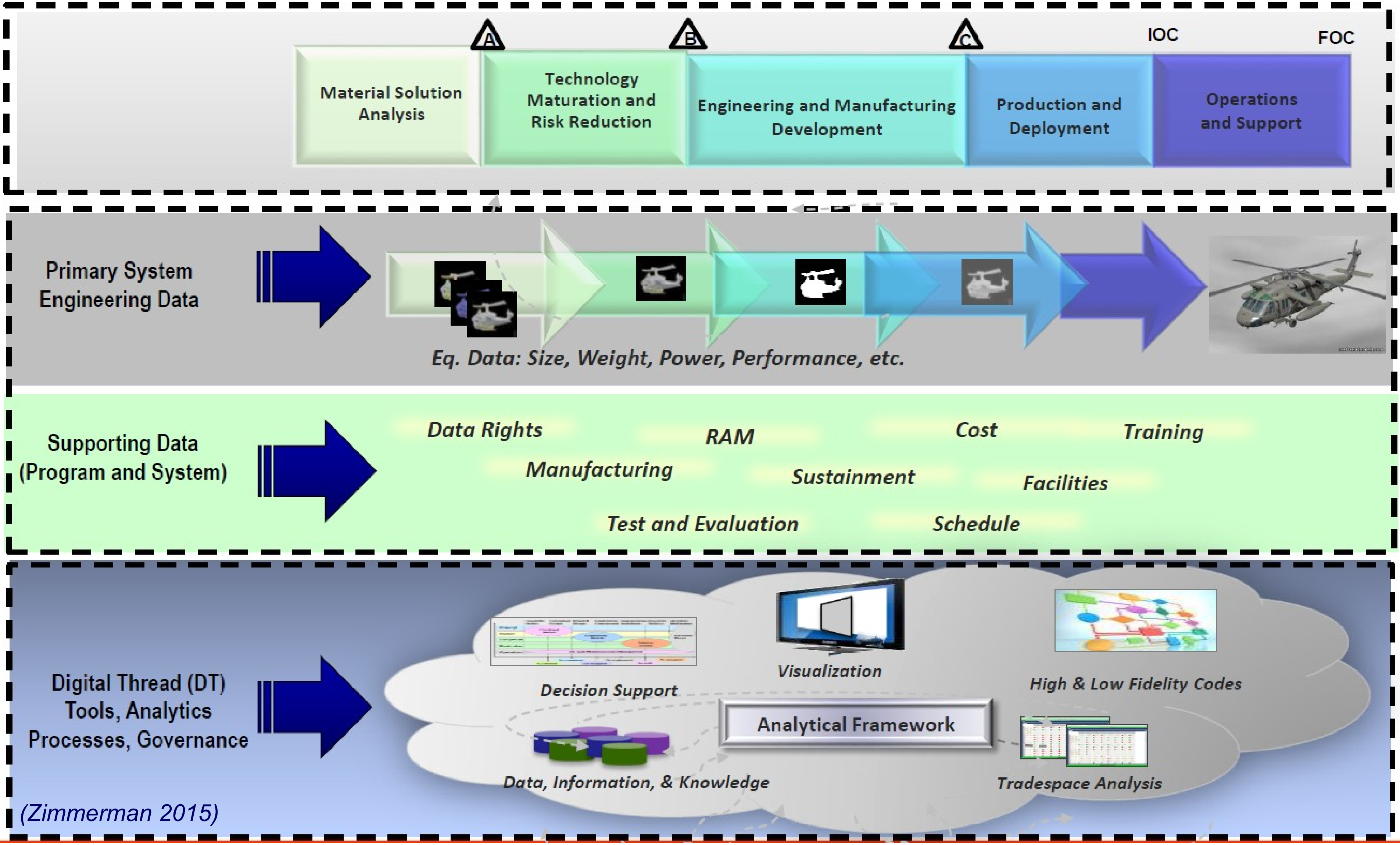
S. M. Rovito, “An Integrated Framework for the Vulnerability Assessment of Complex Supply Chain Systems,” Massachusetts Institute of Technology, 2016.

The MITRE Corporation, “CVE-2017-5753,” Common Vulnerabilities and Exposures, 2017. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5753. [Accessed: 20-Feb-2018].

N. Leveson, “An STPA Primer,” Cambridge, MA, 2013.

SUPPORT/BACKUP SLIDES

Model-Centric Acquistion



A B C IOC FOC

Material Solution Analysis

Technology Maturation and Risk Reduction

Engineering and Manufacturing Development

Production and Deployment

Operations and Support

Primary System Engineering Data

Eq. Data: Size, Weight, Power, Performance, etc.

Supporting Data (Program and System)

Data Rights

RAM

Cost

Training

Manufacturing

Sustainment

Facilities

Test and Evaluation

Schedule

Digital Thread (DT) Tools, Analytics Processes, Governance

Decision Support

Visualization

High & Low Fidelity Codes

Analytical Framework

Data, Information, & Knowledge

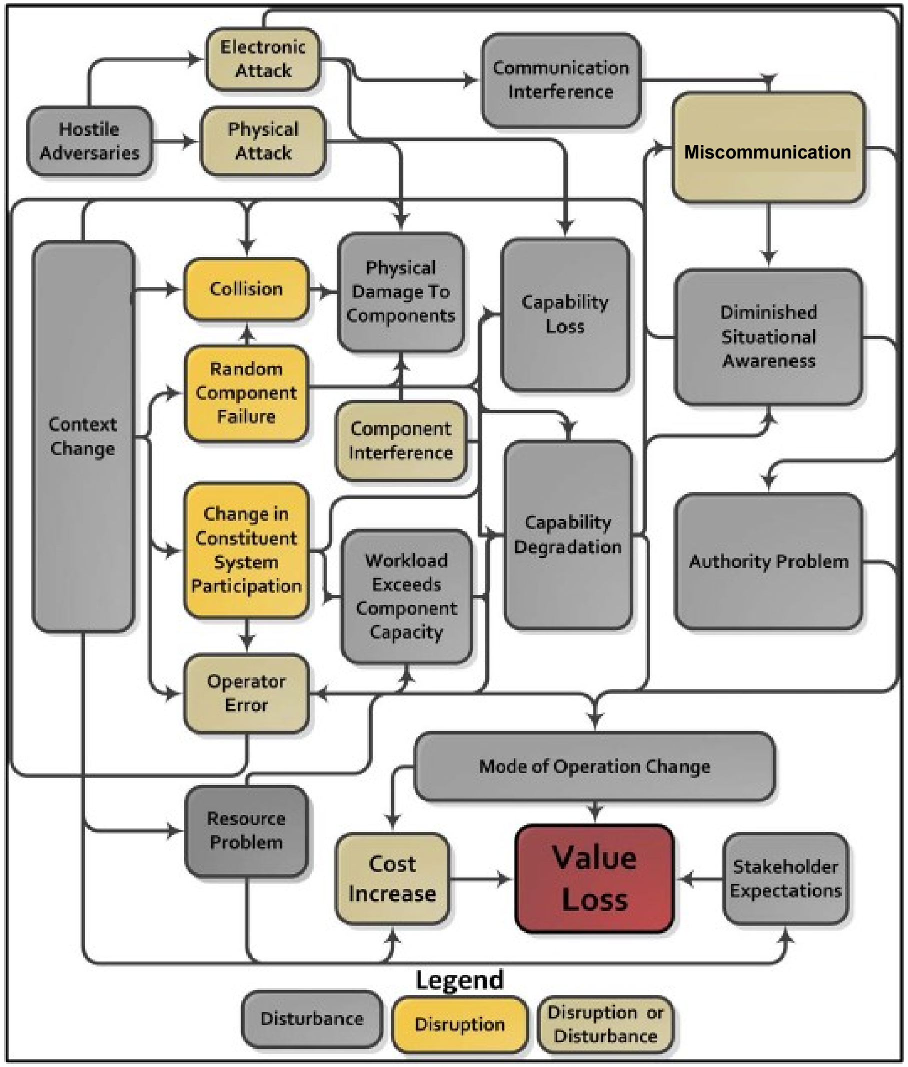
Tradespace Analysis

(Zimmerman 2015)

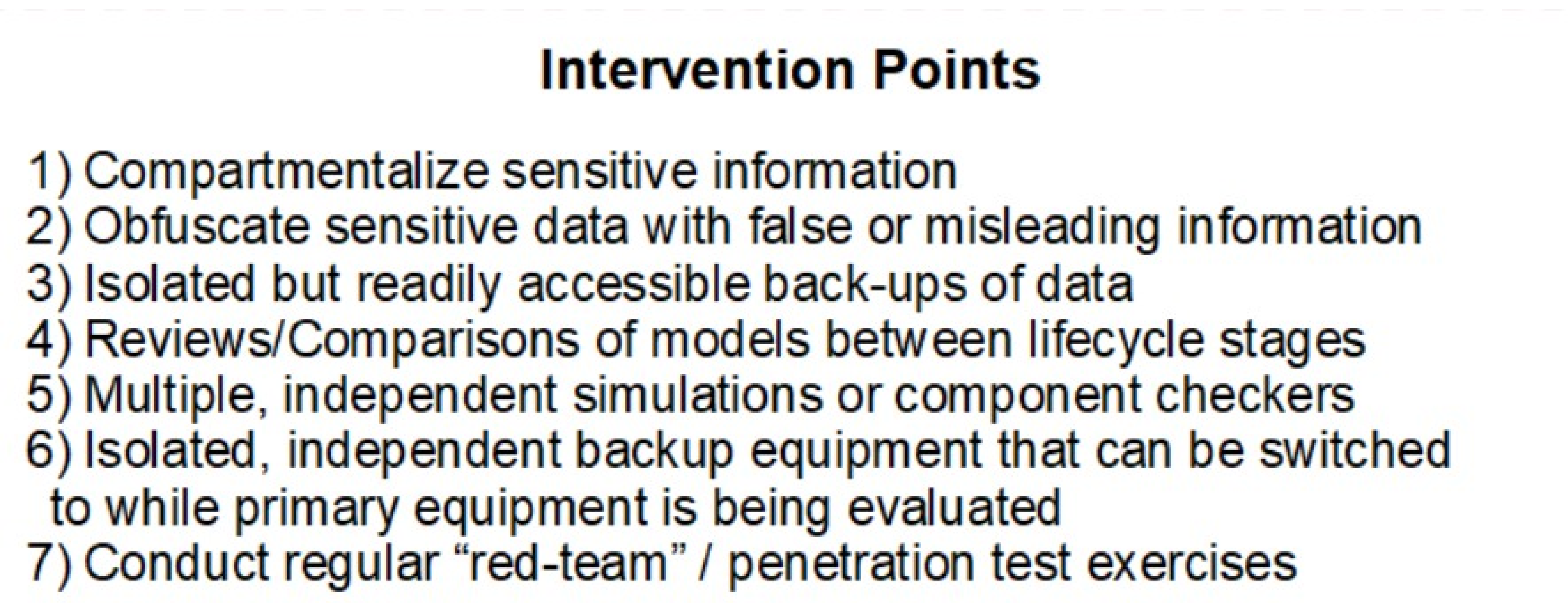
Cause-Effect Mapping (CEM)

- **Hazard:** A system or environmental state that has the potential to disrupt the system
- **Vulnerability:** The causal means by which the hazard results in the system disruption / value loss

(Mekdeci, 2012)



Cybersecurity Interventions

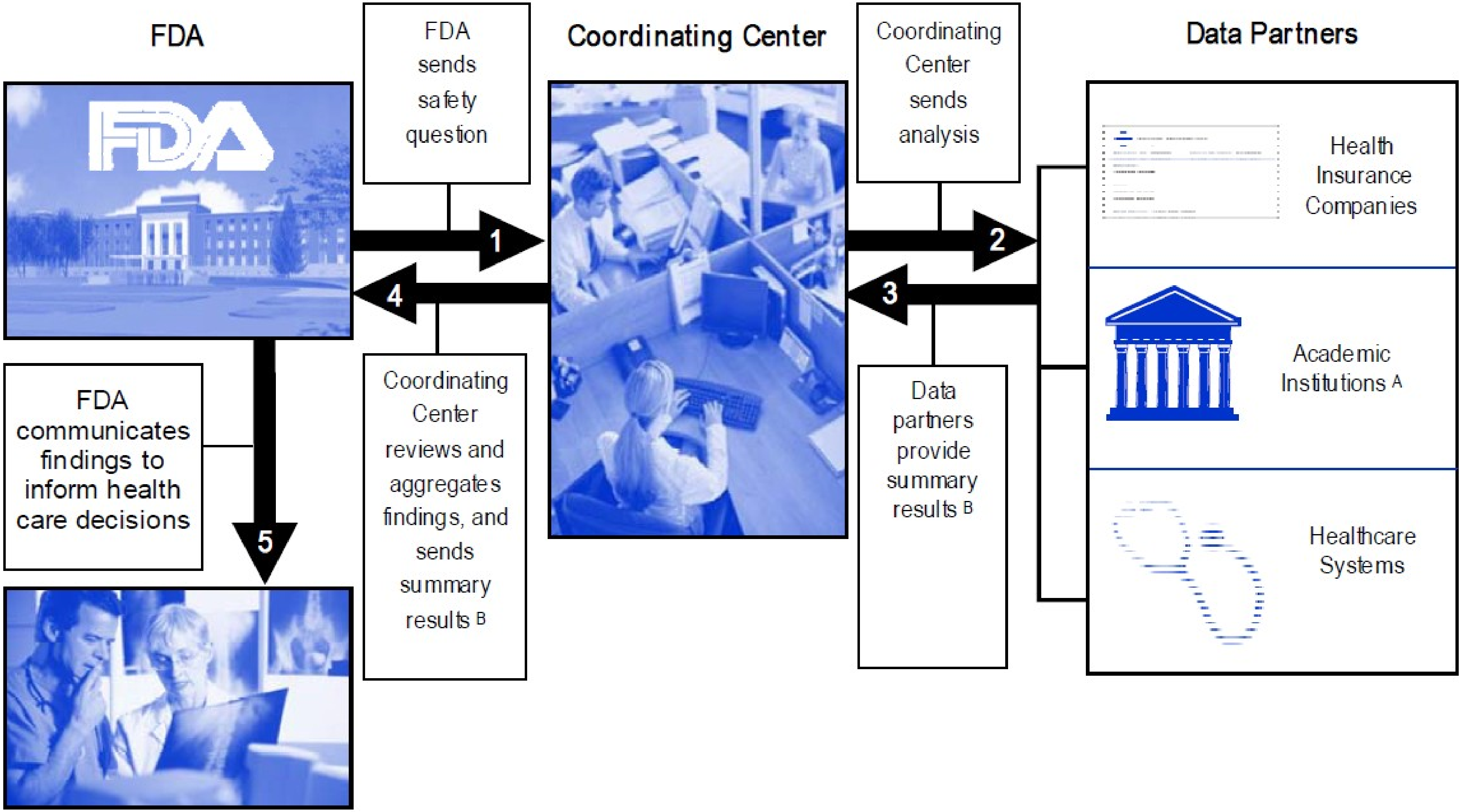


Intervention Points

1) Compartmentalize sensitive information
2) Obfuscate sensitive data with false or misleading information
3) Isolated but readily accessible back-ups of data
4) Reviews/Comparisons of models between lifecycle stages
5) Multiple, independent simulations or component checkers
6) Isolated, independent backup equipment that can be switched to while primary equipment is being evaluated
7) Conduct regular "red-team" / penetration test exercises

www.public.navy.mil

FDA Sentinel Intiative



FDA

Coordinating Center

Data Partners

FDA sends safety question

Coordinating Center sends analysis

Health Insurance Companies

Academic Institutions A

Healthcare Systems

Data partners provide summary results B

Coordinating Center reviews and aggregates findings, and sends summary results B

FDA communicates findings to inform health care decisions