Calhoun: The NPS Institutional Archive

DSpace Repository

Acquisition Research Program | Acquisition Research Symposium

2018-04-30

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

Reid, Jack; Rhodes, Donna

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/58709

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

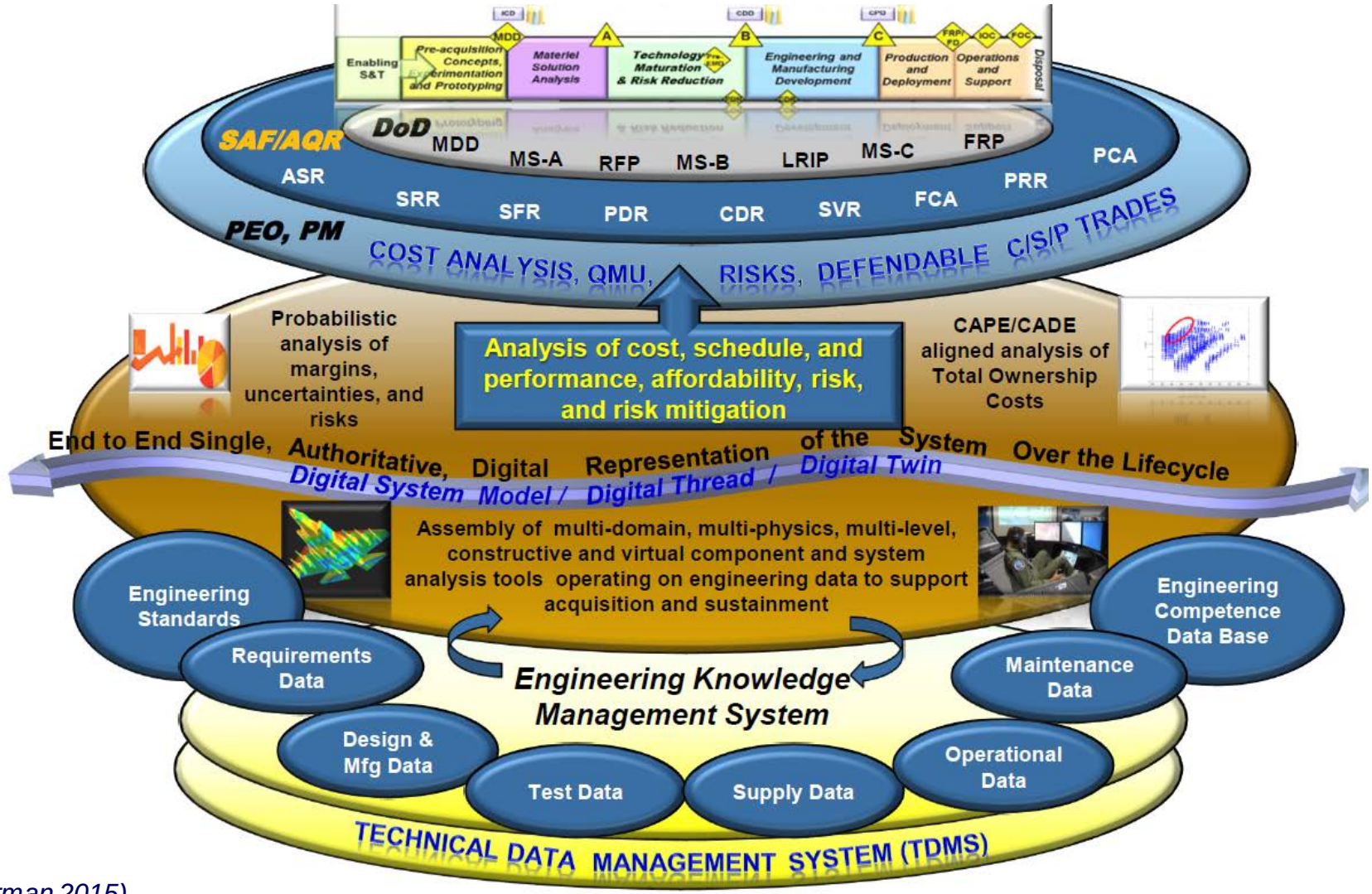
Applying Cause-Effect Mapping to Assess Cybersecurity Vulnerabilities in Model-Centric Acquisition Program Environment

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)

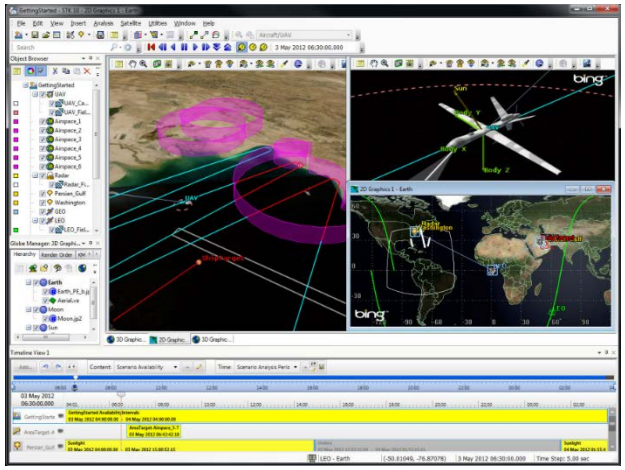


(Zimmerman 2015)

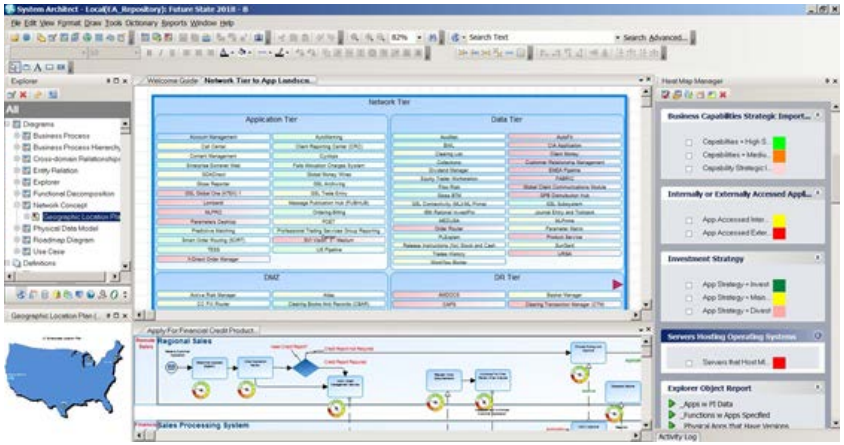
© 2018 Massachusetts Institute of Technology

Current State of MCE

STK



UNICOM System Architect



JPL Team-X

NAVAIR

© 2018 Massachusetts Institute of Technology

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

© 2018 Massachusetts Institute of Technology

MCE and Cybersecurity

MCE make[illegible] *program* even more important

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.

Cyber-[illegible]: A case st[illegible]

Logan D.
Robert P[illegible]

Boeing production [illegible] ransomware attack

The widespread and devastating cyberat[illegible]

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

Convicted in [illegible] Trade Secrets

[illegible]PM EST Bloomberg

© 2018 Massachusetts Institute of Technology

Motivating Questions

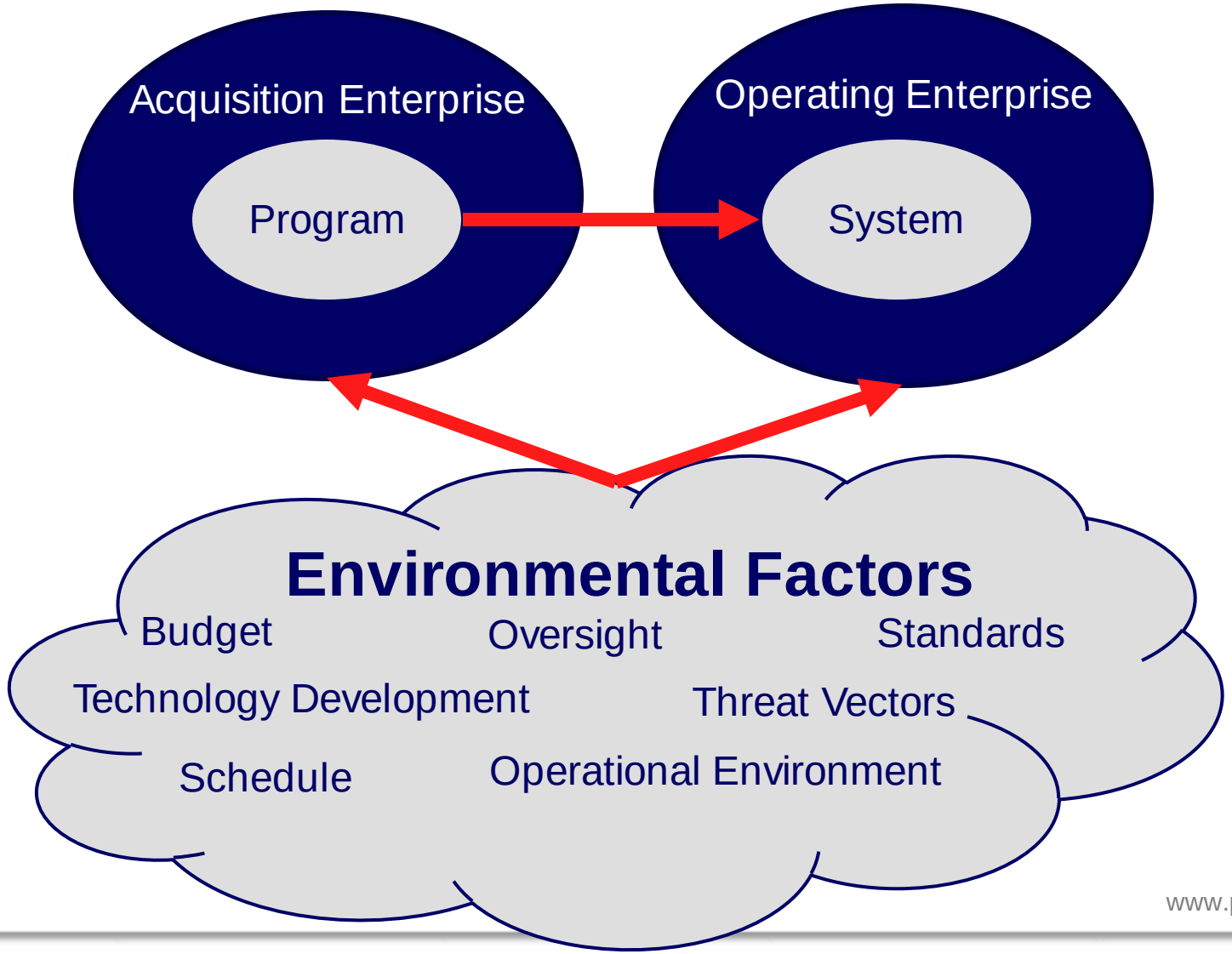
MCE introduces vulnerabilities beyond cybersecurity

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

© 2018 Massachusetts Institute of Technology

Program vs System



www.public.navy.mil

© 2018 Massachusetts Institute of Technology

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."

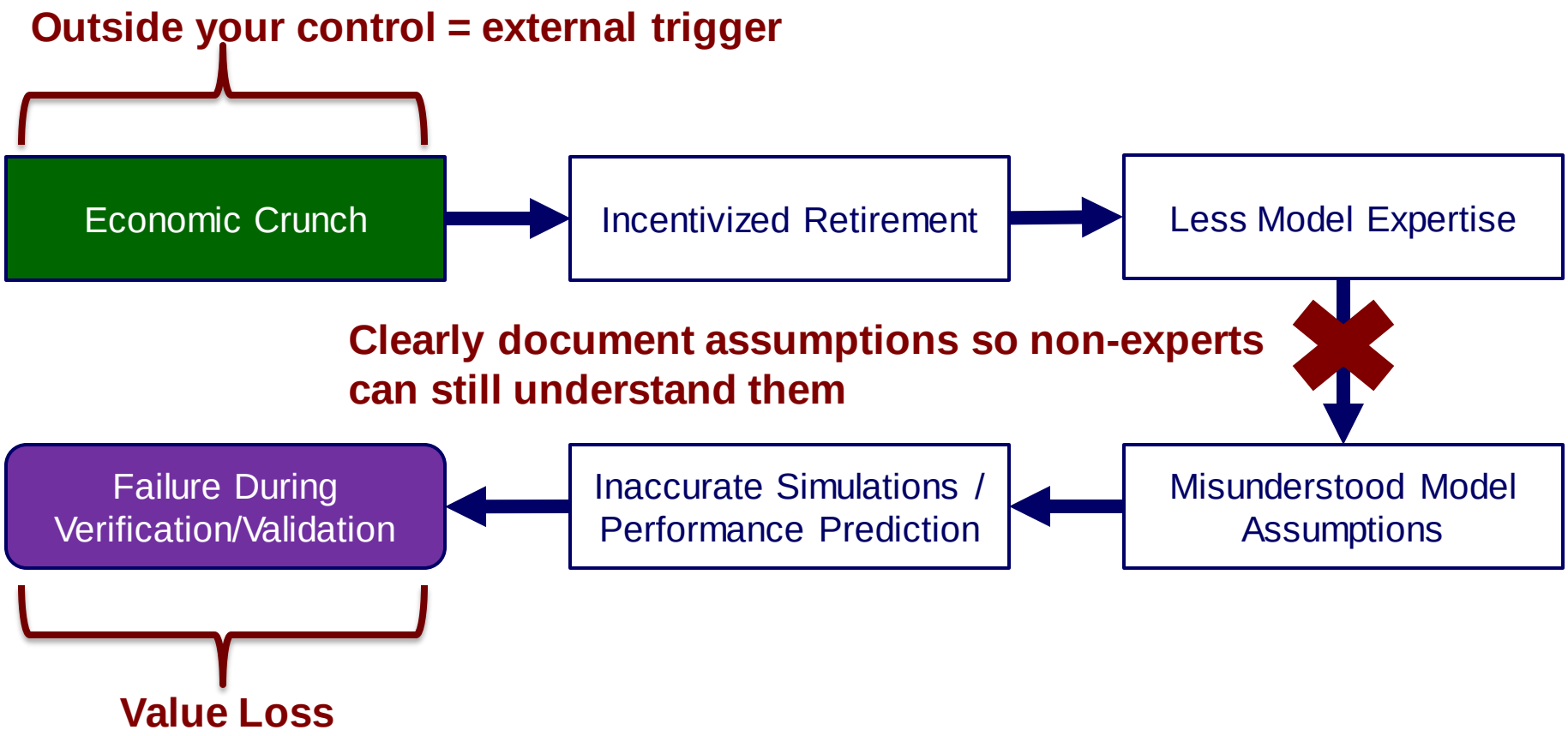
© 2018 Massachusetts Institute of Technology

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

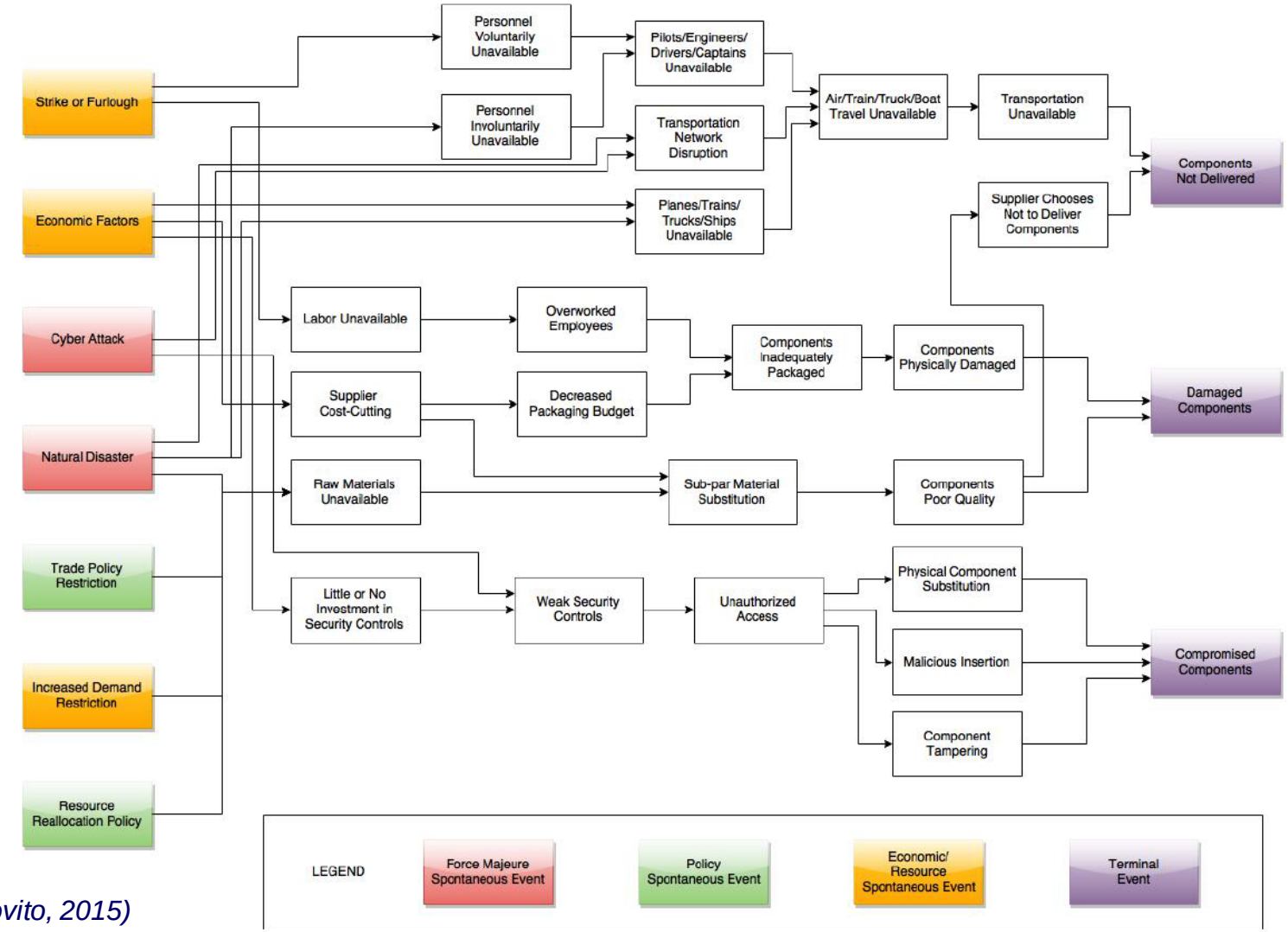
© 2018 Massachusetts Institute of Technology

Causal Chain



© 2017 Massachusetts Institute of Technology

Cause-Effect Mapping (CEM)



(Rovito, 2015)

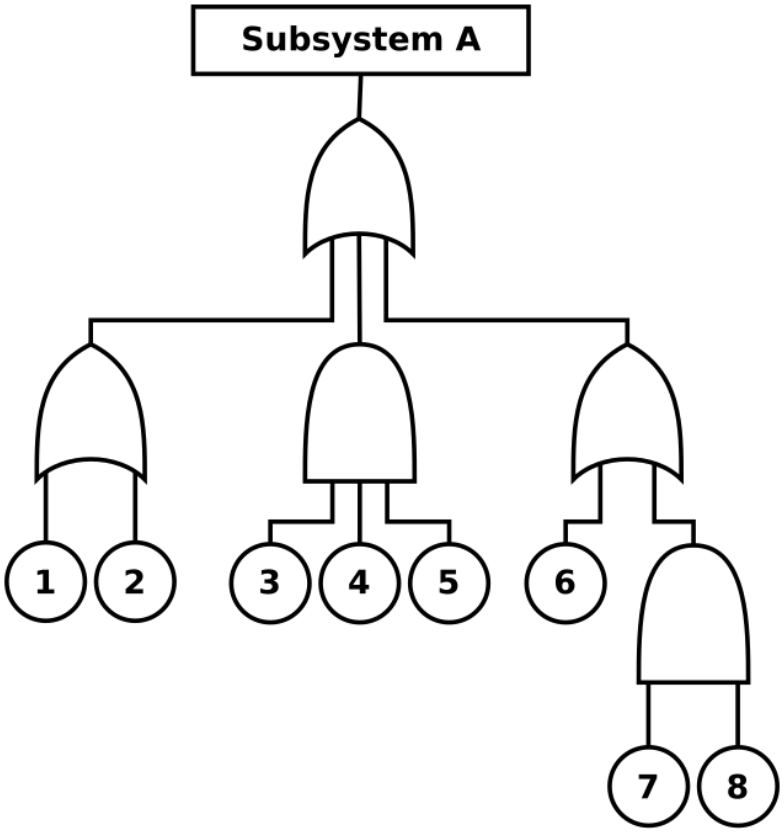
© 2018 Massachusetts Institute of Technology

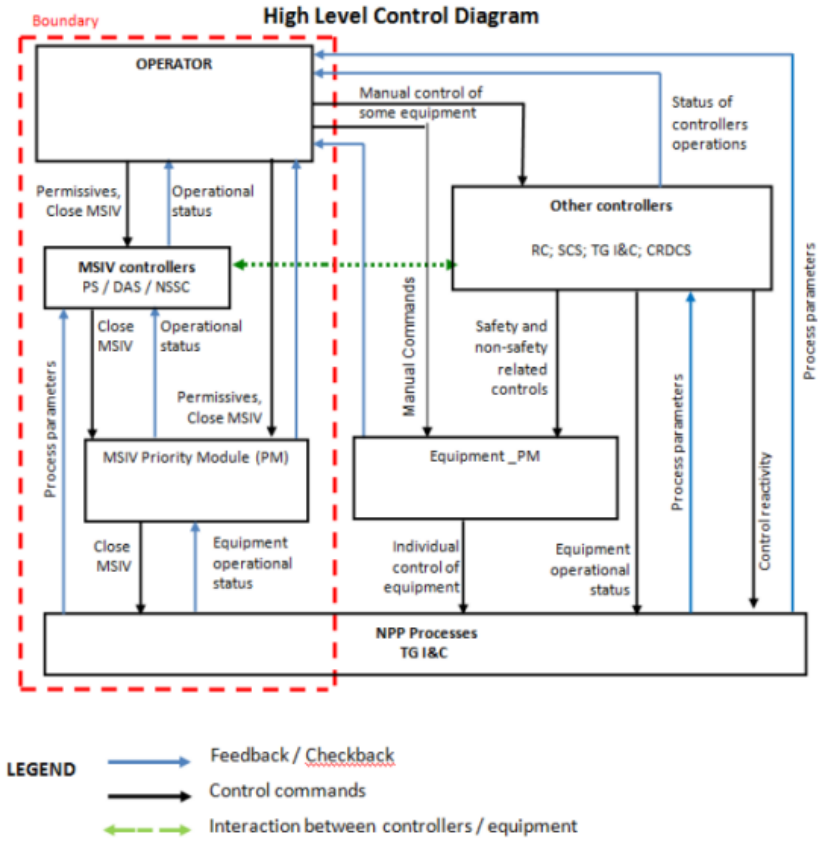
Uses of CEM / Typology

- 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

© 2018 Massachusetts Institute of Technology

Comparisons





(Leveson 2013)

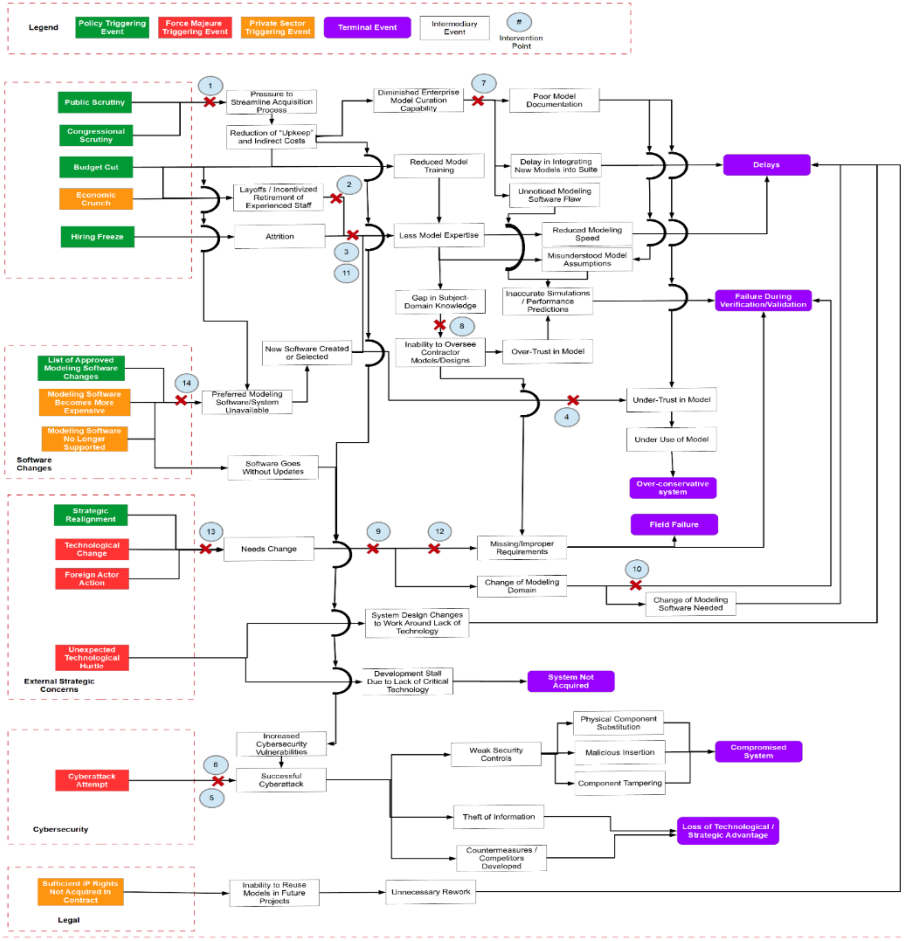
© 2018 Massachusetts Institute of Technology

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.”

© 2018 Massachusetts Institute of Technology

MCE Cause-Effect Mapping

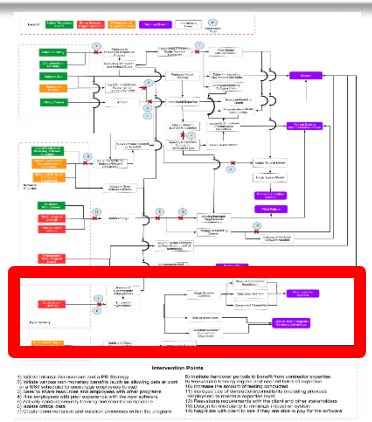


Intervention Points

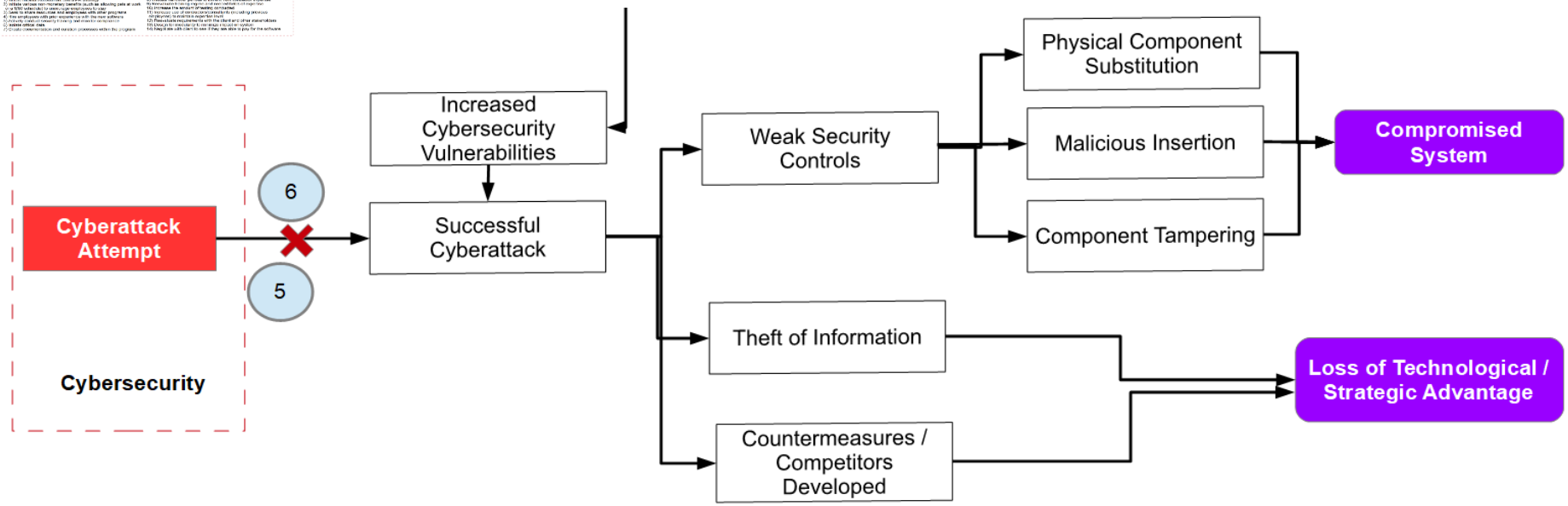
1) Initiate Internal Assessment and a PR Strategy
2) Initiate various non-monetary benefits (such as allowing pets at work or a 9/80 schedule) to encourage employees to stay
3) Seek to share resources and employees with other programs
4) Hire employees with prior experience with the new software
5) Actively 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

© 2018 Massachusetts Institute of Technology

Cause-Effect Mapping - Cybersecurity



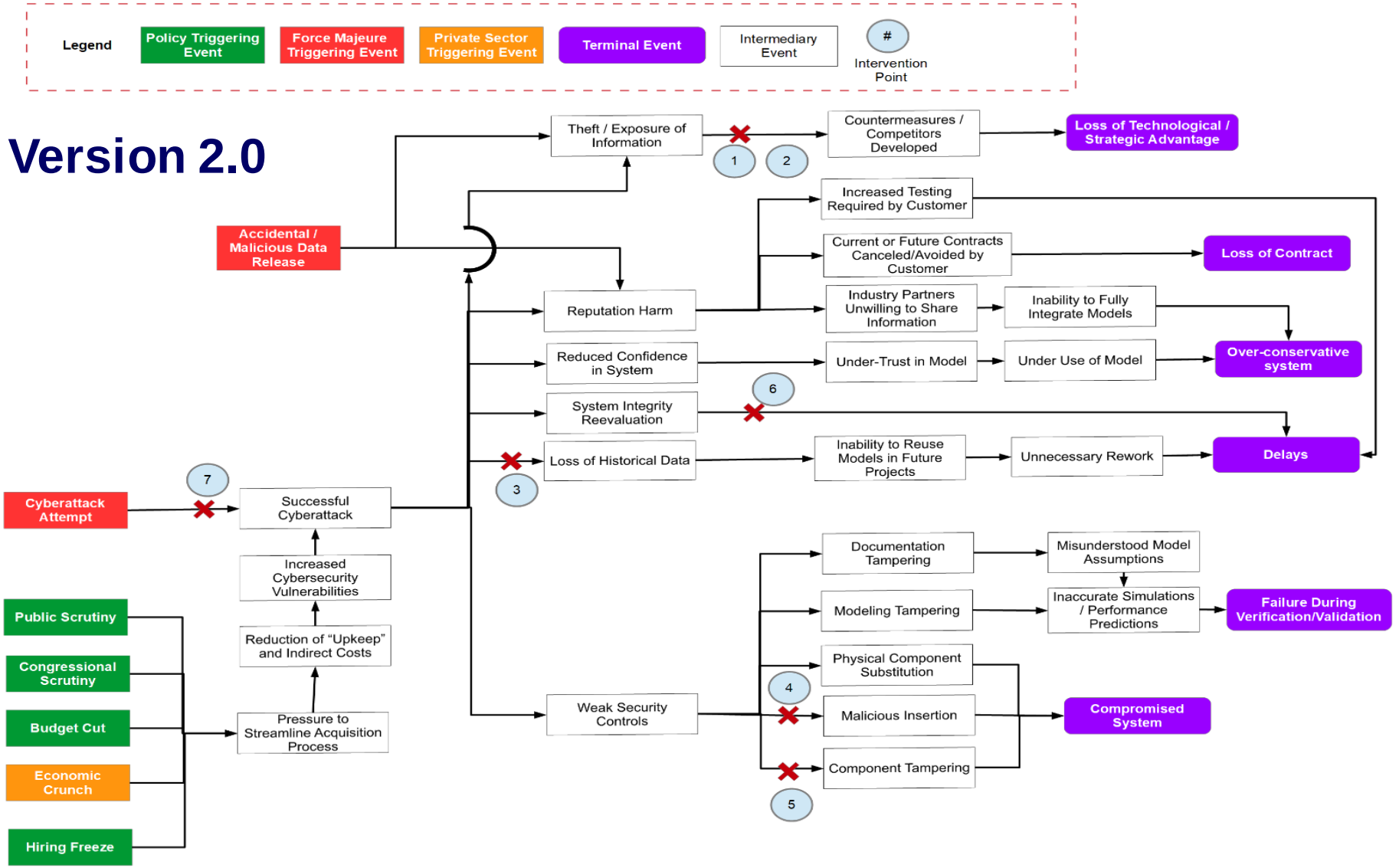
Version 1.0



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

© 2018 Massachusetts Institute of Technology

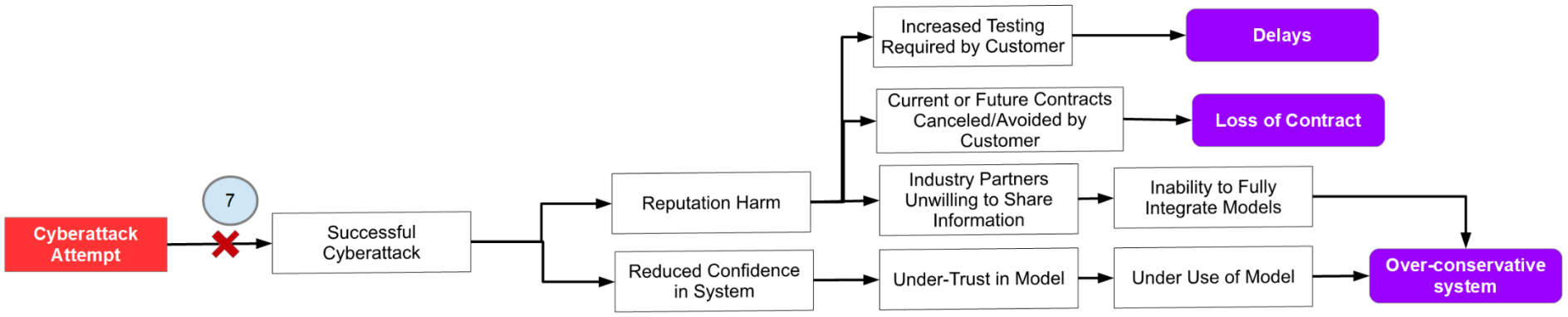
CEM - Cybersecurity



© 2018 Massachusetts Institute of Technology

Discussion

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



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

© 2018 Massachusetts Institute of Technology

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

© 2018 Massachusetts Institute of Technology

Questions?

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

© 2018 Massachusetts Institute of Technology

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].

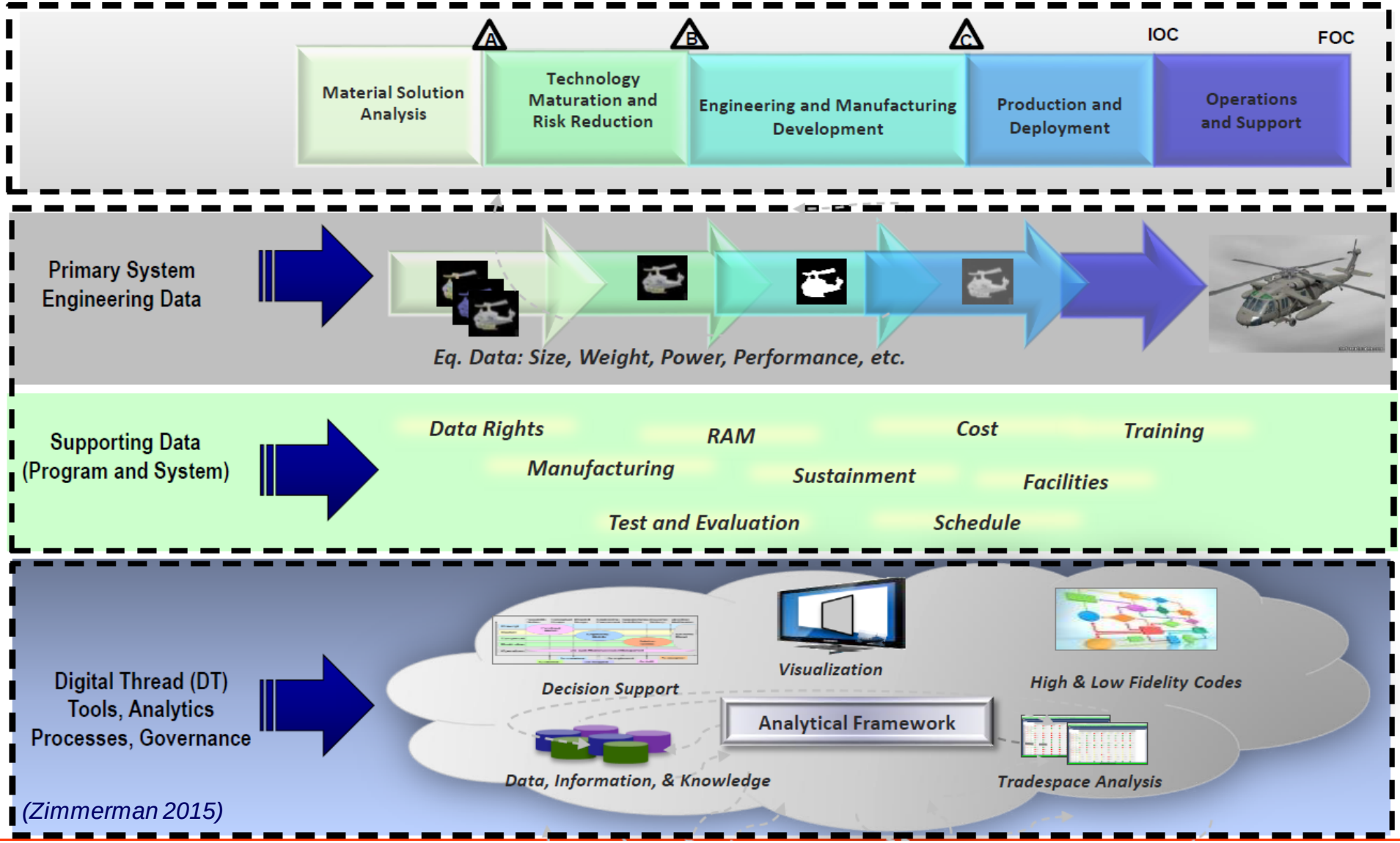
N. Leveson, “An STPA Primer,” Cambridge, MA, 2013.

© 2018 Massachusetts Institute of Technology

SUPPORT/BACKUP SLIDES

© 2018 Massachusetts Institute of Technology

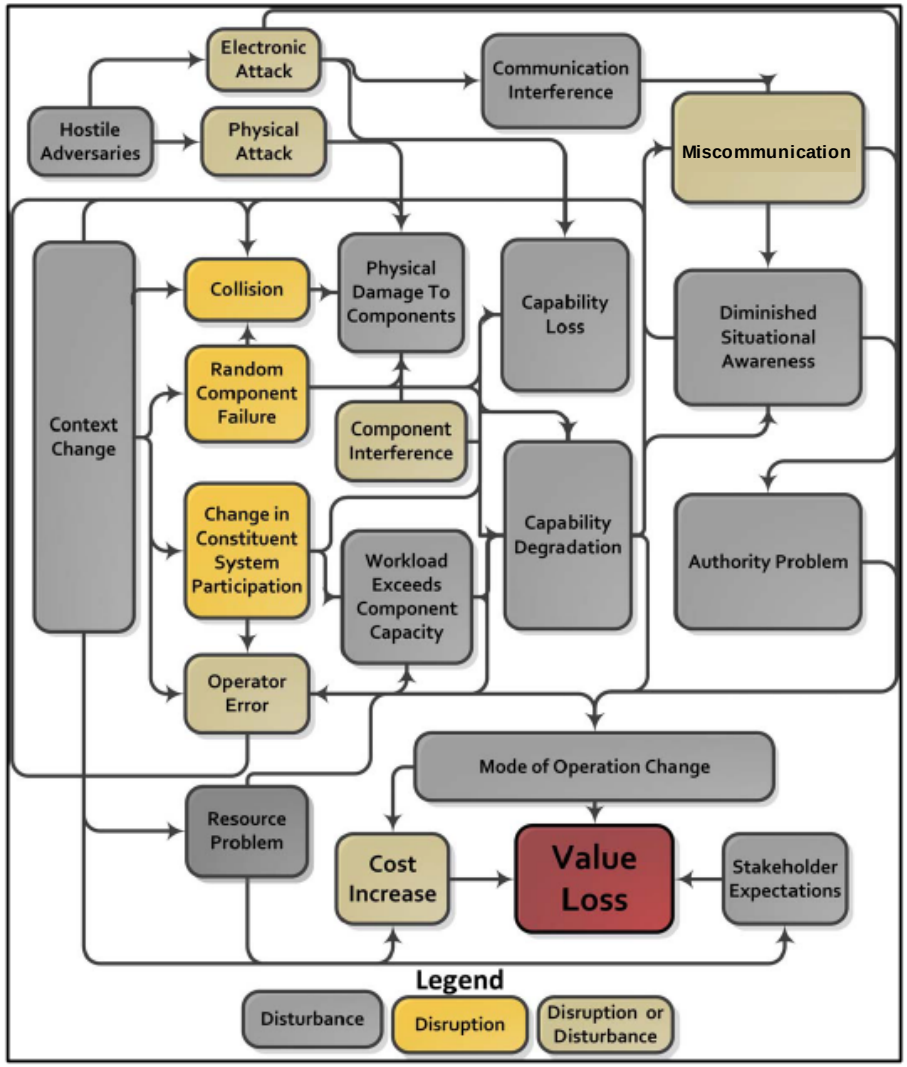
Model-Centric Acquistion



© 2018 Massachusetts Institute of Technology

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)

© 2018 Massachusetts Institute of Technology

Cybersecurity Interventions

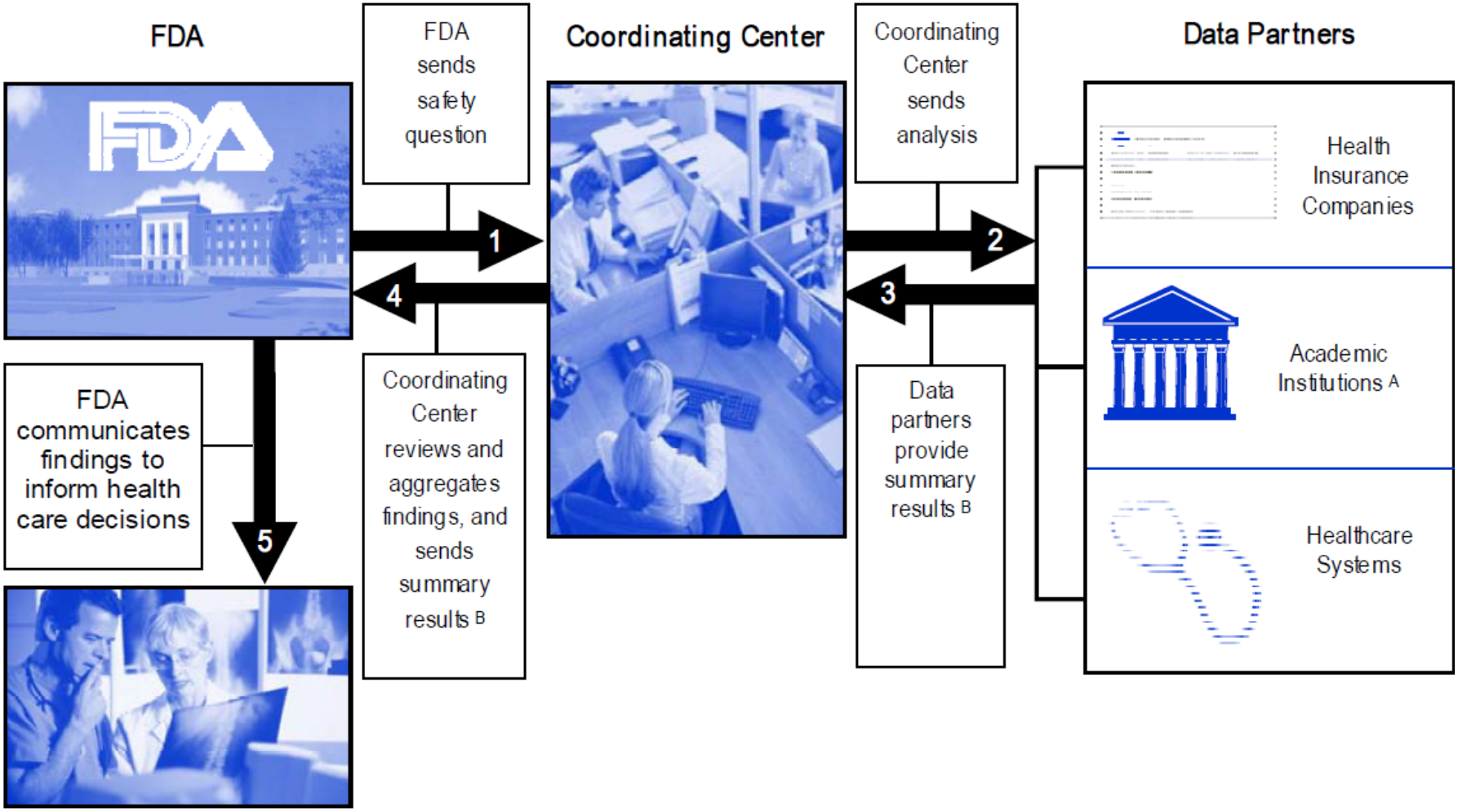
Intervention Points

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

© 2018 Massachusetts Institute of Technology

FDA Sentinel Intiative



© 2018 Massachusetts Institute of Technology