



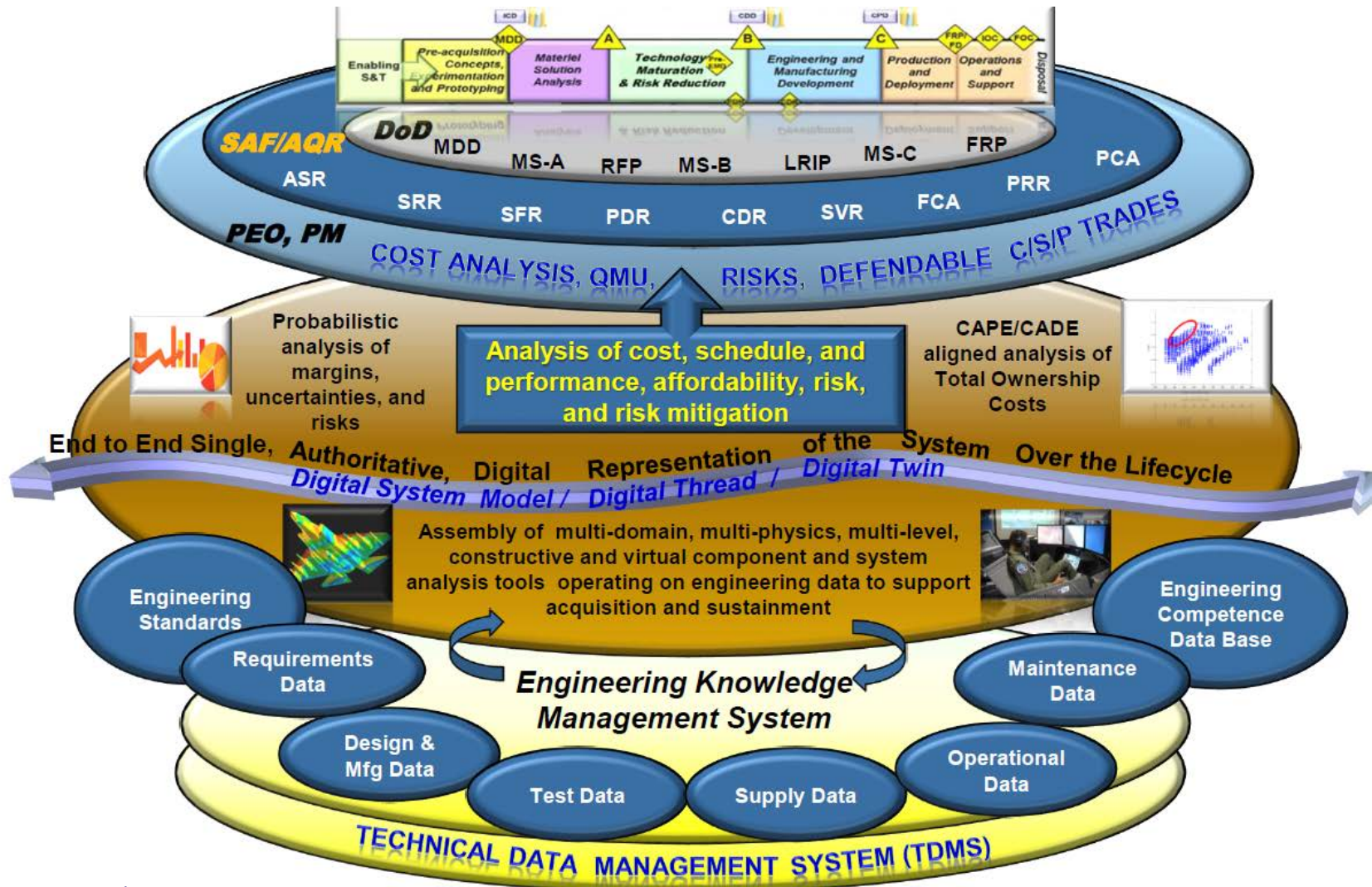
Applying Cause-Effect Mapping to Assess Cybersecurity Vulnerabilities in Model-Centric Acquisition Program Environment

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

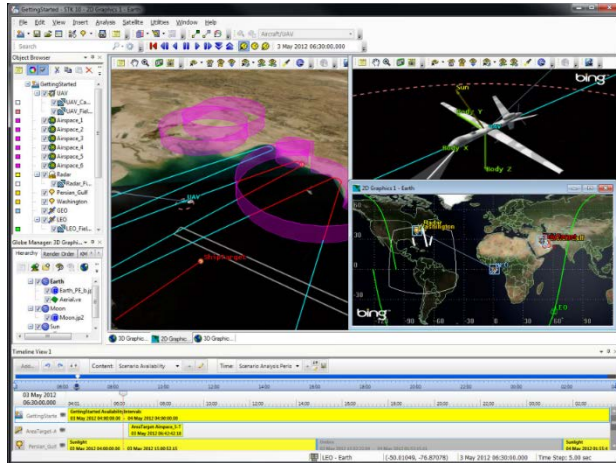
Model-Centric Engineering (MCE)



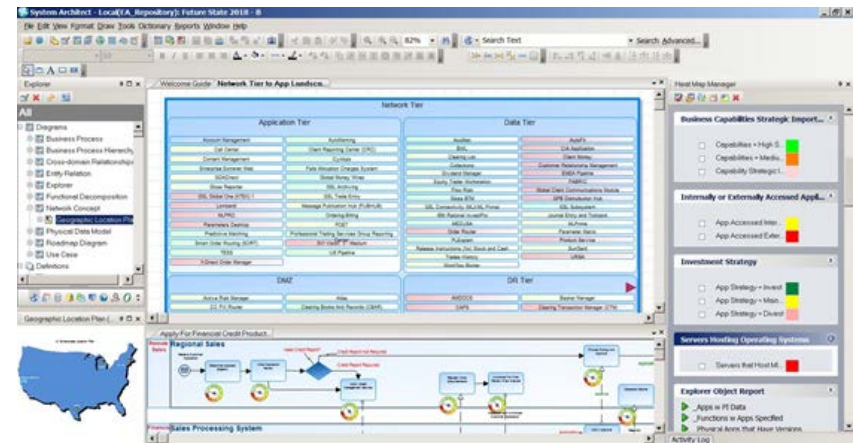
(Zimmerman 2015)

Current State of MCE

STK



UNICOM System Architect



JPL Team-X



NAVAIR

MCE and Cybersecurity

(Some) Benefits

System-level optimization
and “authoritative source
of truth”



Increased collaboration
across teams



Removal of barriers between stages



Cybersecurity Concerns

“All eggs in one basket”

More points of entry

Tampering in design can
make its way into the field

MCE makes the 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-
case st

Logan D.
Robert P



Boeing production p
ransomware attack

The widespread and devastating cyberat

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

Convicted in
 Trade Secrets
 Bloomberg

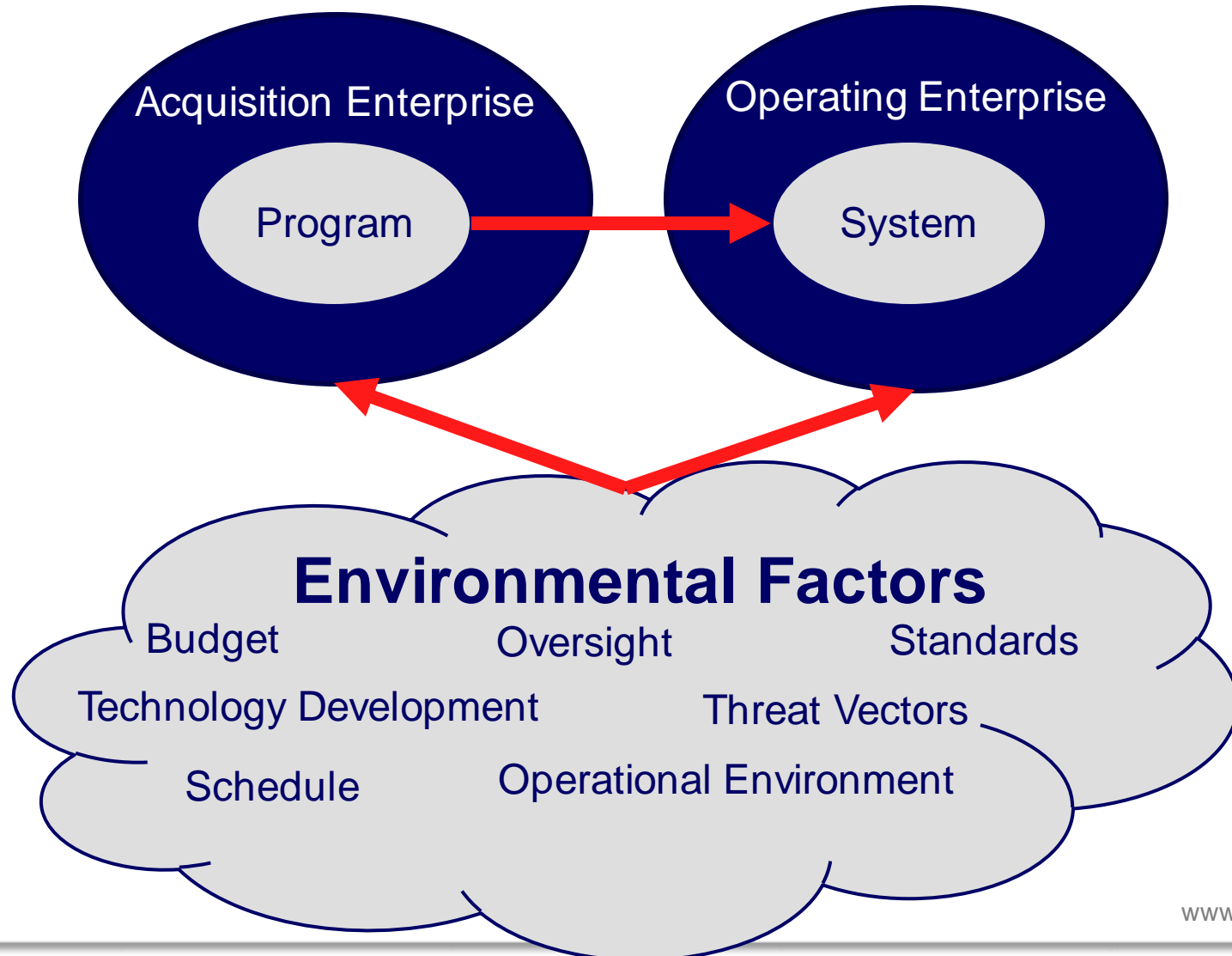
Motivating Questions

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



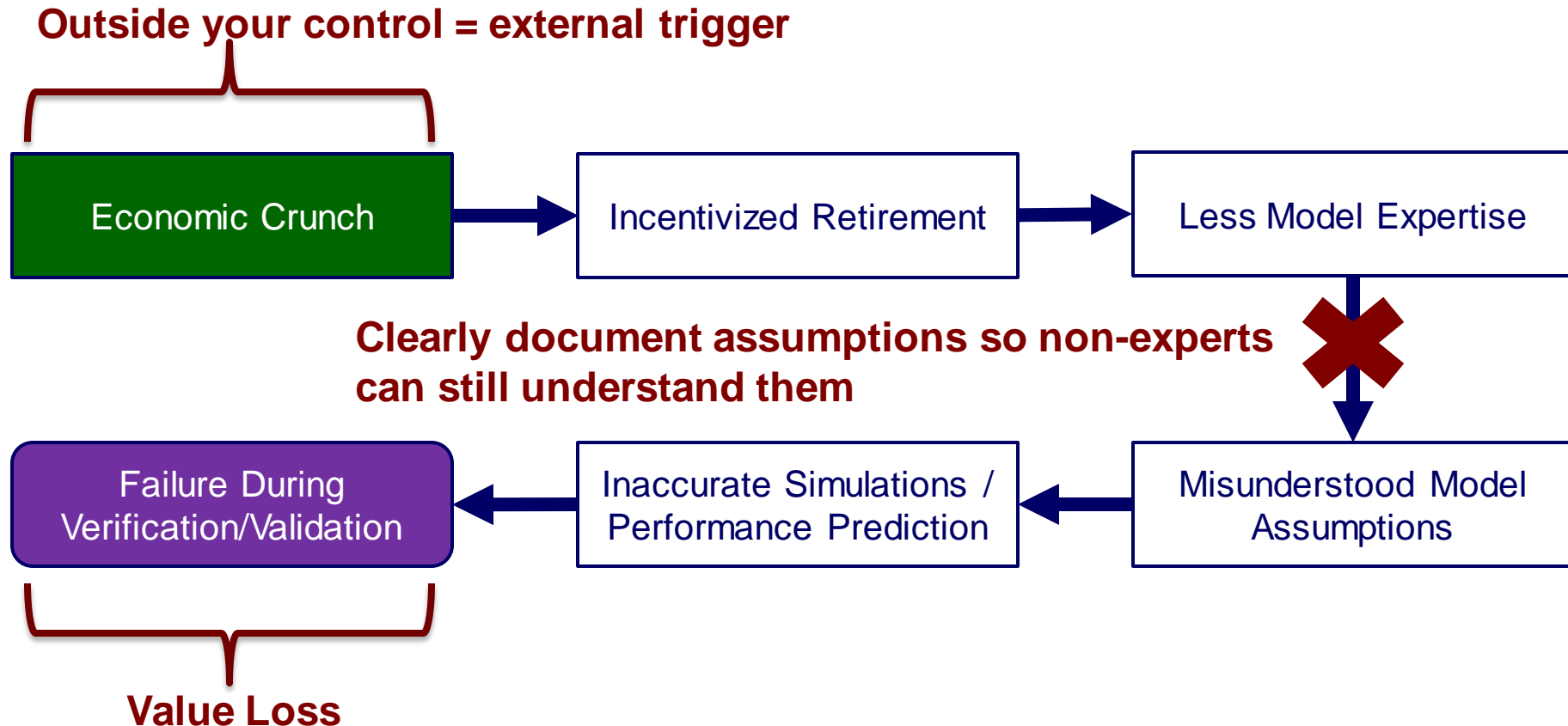
Definitions

- **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.”

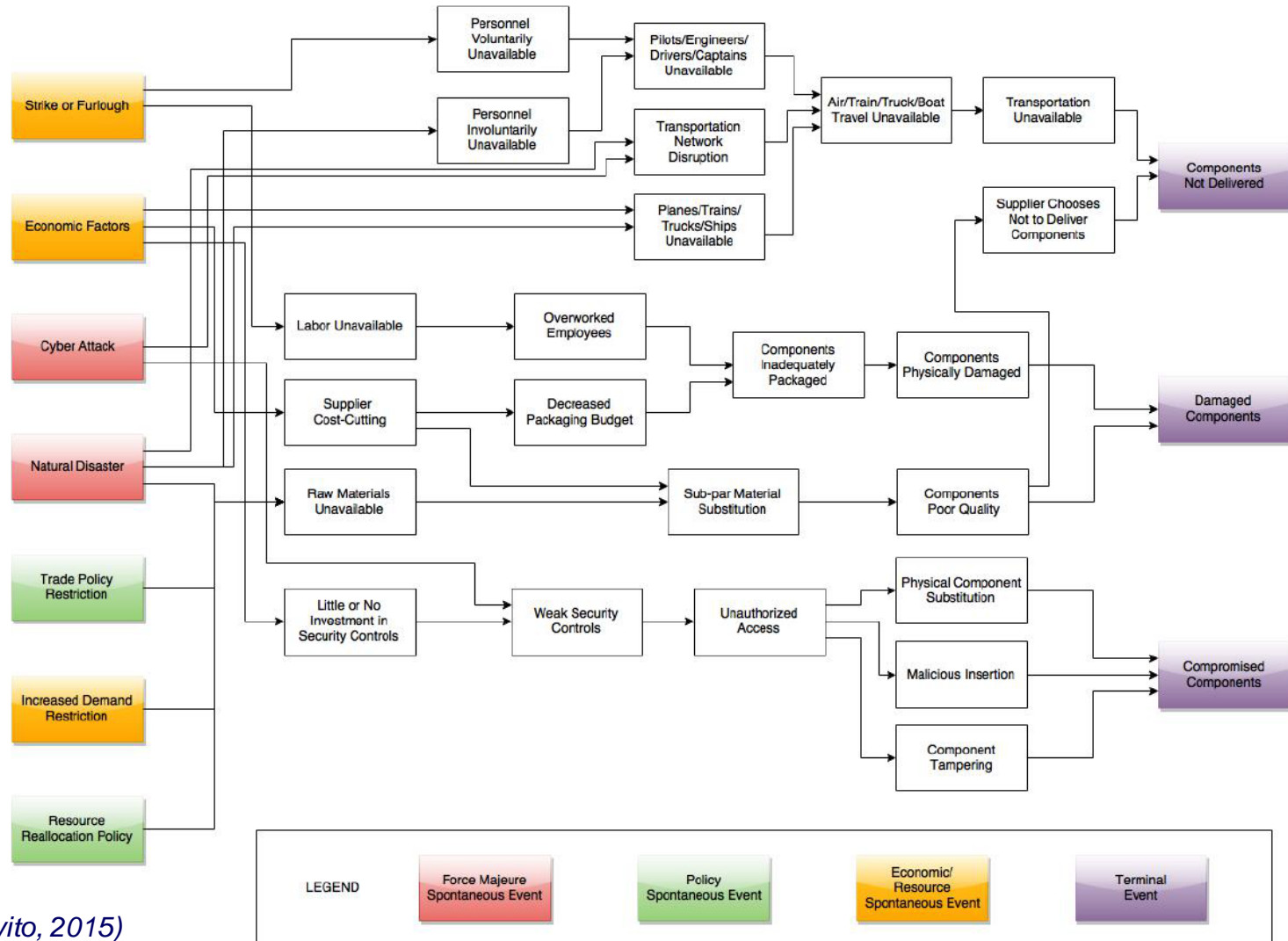
Vulnerability Chain

- **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



Cause-Effect Mapping (CEM)

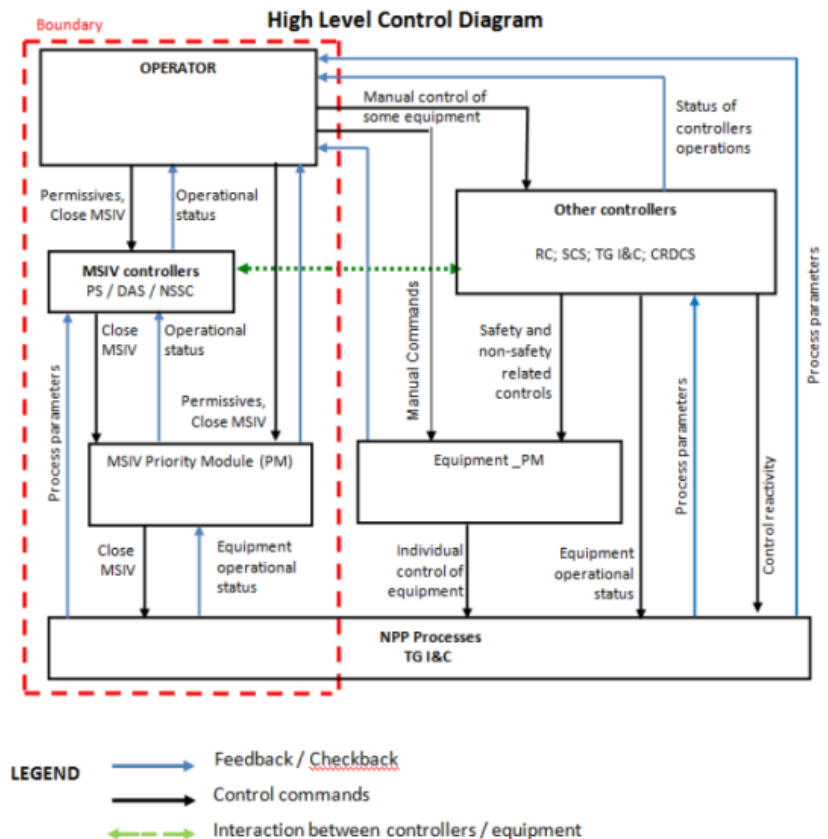
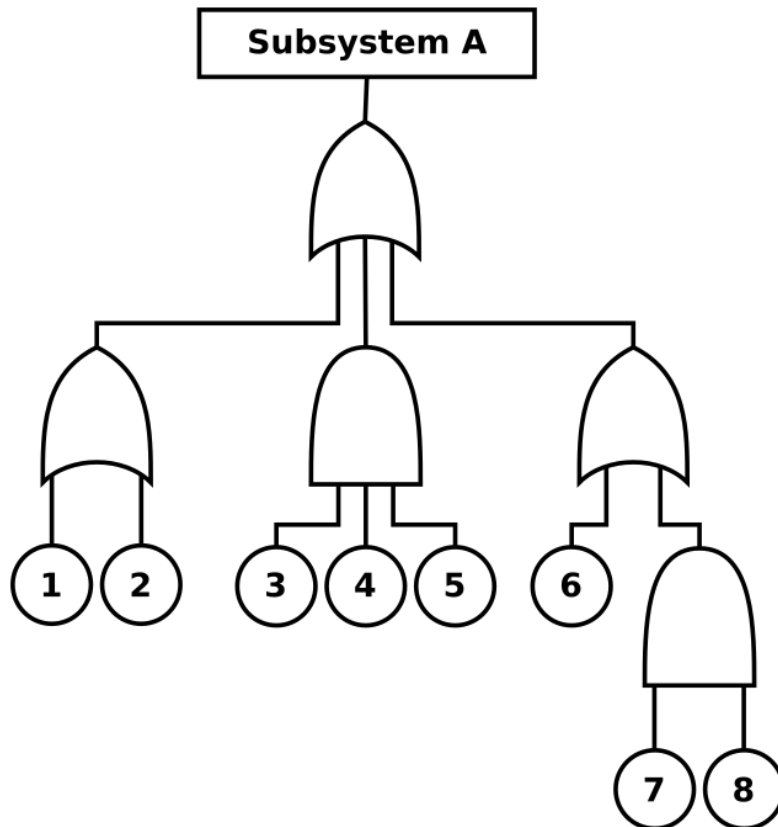


(Rovito, 2015)

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

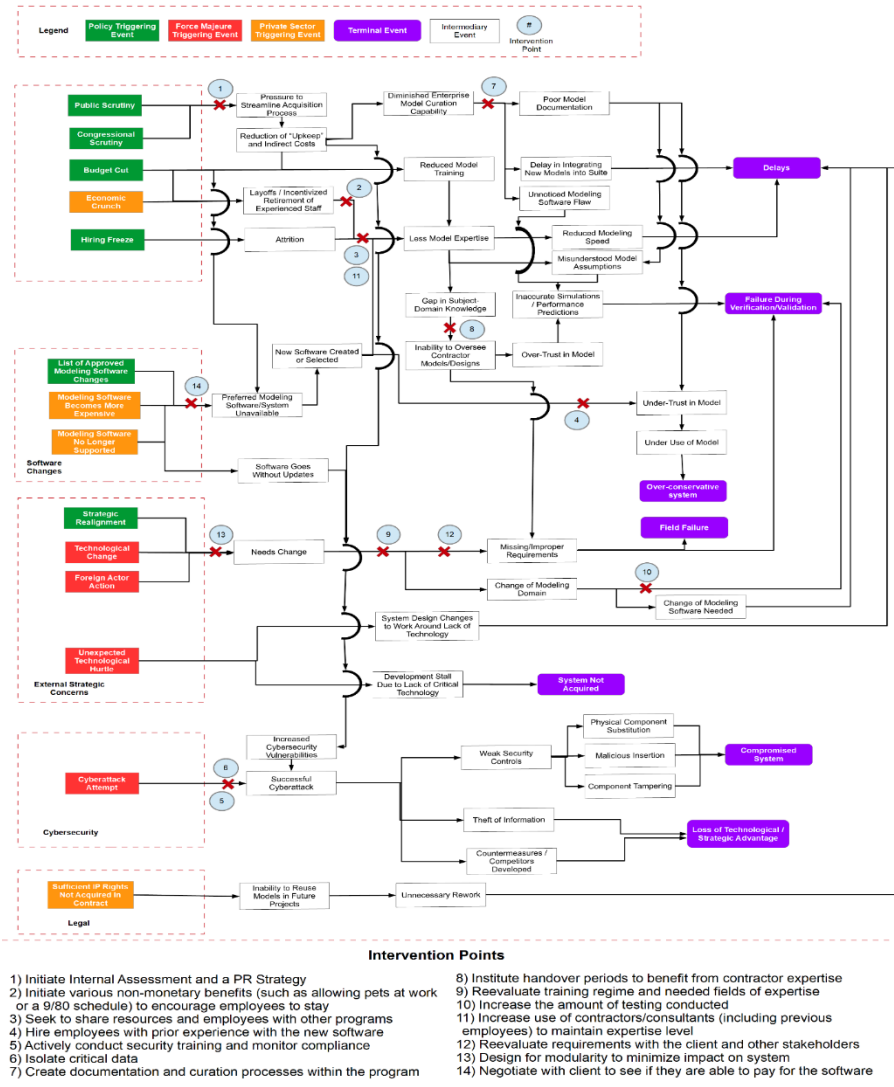
Comparisons



(Leveson 2013)

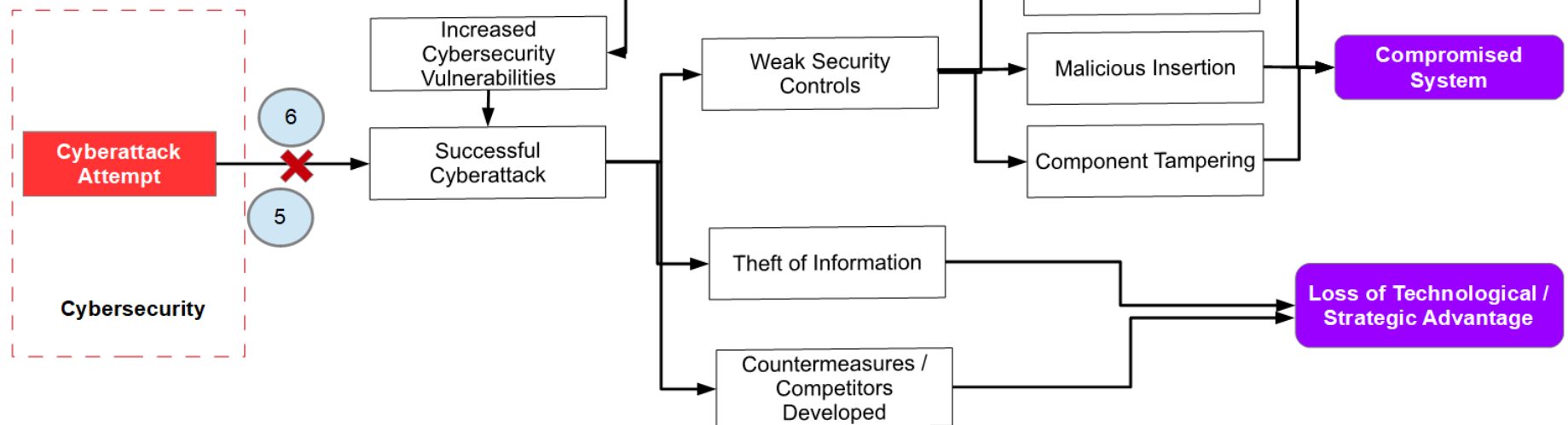
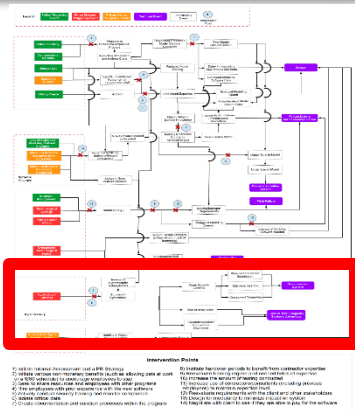
- Disciplines
 - Aerospace
 - Nuclear Physics
 - Automotive
 - Oil & Gas
 - Medical
 - Defense
- “Networking and MCE is hard to do while staying secure. Particularly when dealing with large groups across departments.”
- “The environment keeps changing and it is always getting bigger. You have to protect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

MCE Cause-Effect Mapping



Cause-Effect Mapping - Cybersecurity

Version 1.0

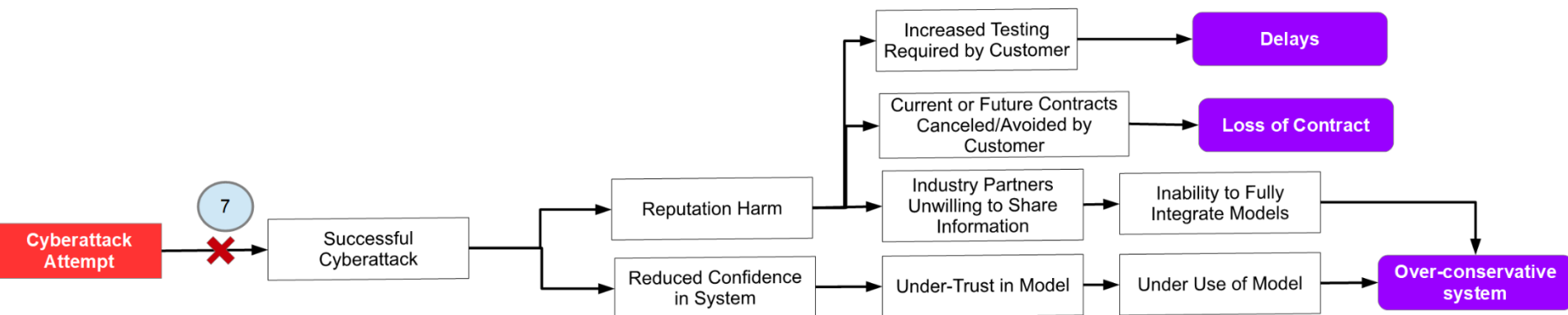


- 5) Actively conduct security training and monitor compliance
- 6) Isolate critical data



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

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].

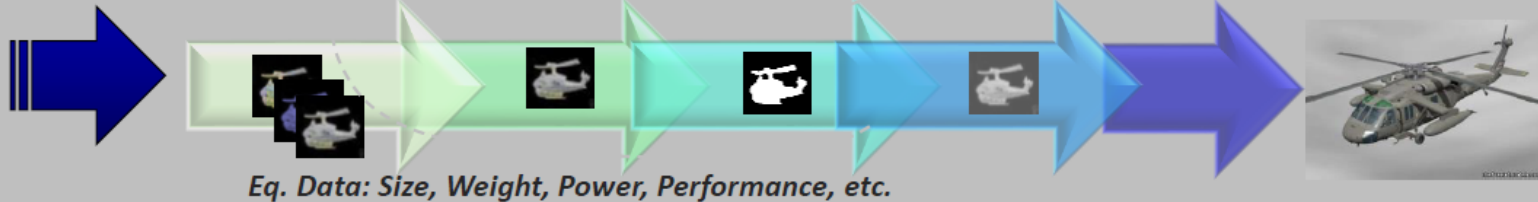
N. Leveson, “An STPA Primer,” Cambridge, MA, 2013.

SUPPORT/BACKUP SLIDES

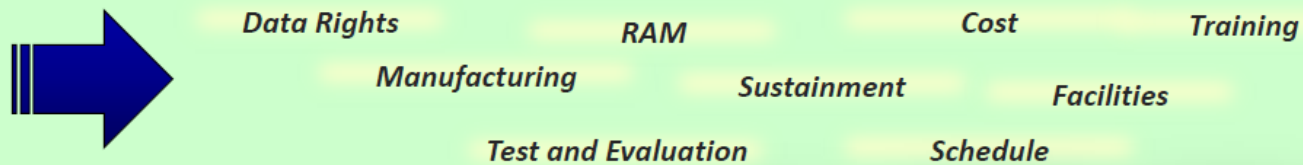
Model-Centric Acquisition



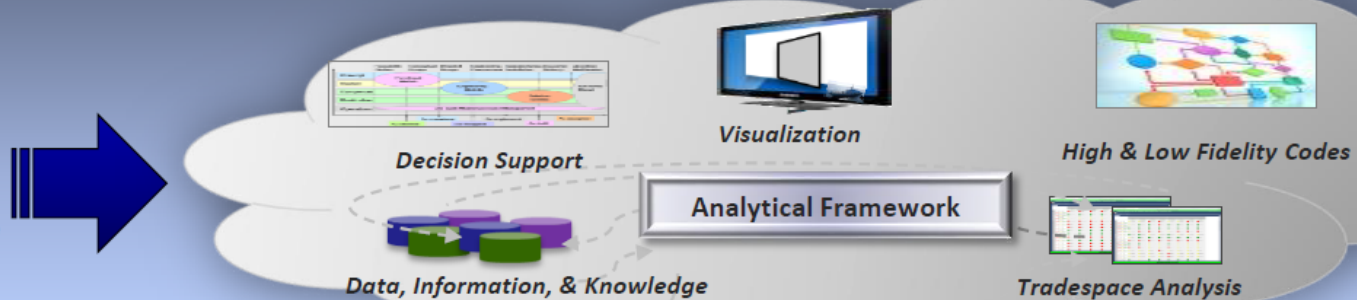
Primary System Engineering Data



Supporting Data (Program and System)



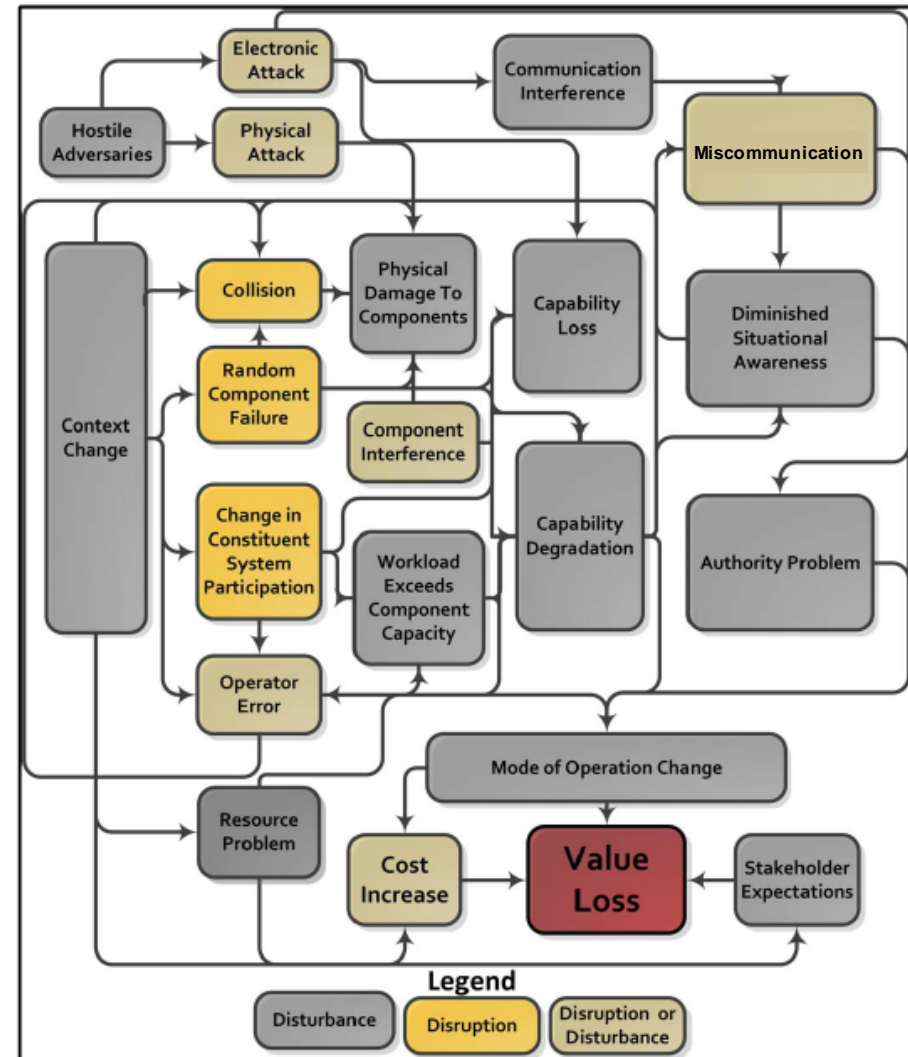
Digital Thread (DT) Tools, Analytics Processes, Governance



(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)

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

FDA Sentinel Initiative

