Enabling Better Supply Chain Decisions Through a Generic Model Utilizing Cause-Effect Mapping

Sarah M. Rovito

Donna H. Rhodes

Massachusetts Institute of Technology

April 19, 2016

Vulnerability and Supply Chains

- Vulnerability
  - Lack of a holistic understanding of how applies to complex systems
  - Paucity of support tools for identifying and accounting for vulnerability in supply chains [1]

- Supply Chains
  - Ensure safe, secure, and timely movement of goods and information
  - Potential for exploitation
  - Complexity of DoD supply chain

This research seeks to contribute to resilient systems, through both the prevention and mitigation of vulnerabilities

© 2016 Massachusetts Institute of Technology

Definitions

Vulnerability Assessment is the study of characteristics of a system in order to discern vulnerabilities and can be used to evaluate and record vulnerabilities that may impede or degrade the performance or capabilities of a system [3]

Supply Chain Vulnerability takes into consideration unplanned and unanticipated events that disrupt the normal flow of goods and materials

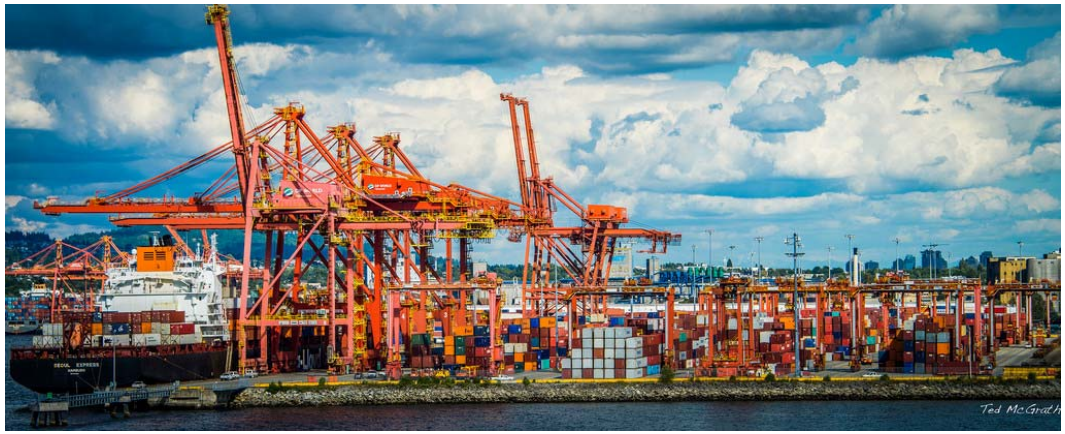
Vulnerability describes a flaw or weakness in a system that renders it susceptible to a hazard or threat [2]

© 2016 Massachusetts Institute of Technology

Research Motivation

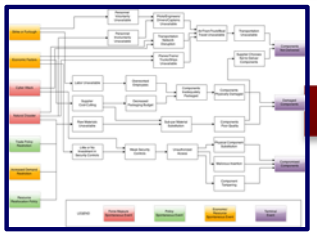
- Vulnerability Assessment Issues (Reed, 2014)
  - Lack of objective criteria and significant variability in results
  - Often not performed during each phase of acquisition life cycle
  - Not applied to legacy software and components [15]

- Seeking to create a guiding framework capable of:
  - Making use of existing vulnerability assessment tools
  - Providing decision-makers with a better grasp of the vulnerability space from a holistic systems perspective

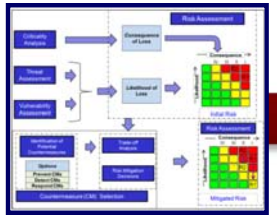


© 2016 Massachusetts Institute of Technology

Inputs to Generic Model



CEM



SSE/TSN [4]

Leading Indicators [5]

Findings from Expert Judgment

Generic Model

1st Step: Identification and Initial Analysis (CEM)

1.1 Development of adequate system understanding
1.2 Evaluation of historical data and previous empirical investigations
1.3 Identification of terminal events, perturbations, and spontaneous events
1.4 Identification of set of system vulnerabilities
1.5 Execution of CEM analytic technique

2nd Step: Application of SSE Principles (TSN Analysis)

2.1 Selection of applicable TSN analysis vulnerability identification technique(s)
2.2 Comparison of CEM and TSN analysis findings

3rd Step: Additional Insight (Leading Indicators)

3.1 Evaluation of set of system vulnerabilities identified through CEM and TSN analysis
3.2 Selection of relevant leading indicators
3.3 Application of relevant leading indicators to provide additional insight on set of system vulnerabilities

NO ← Results Credible? → YES

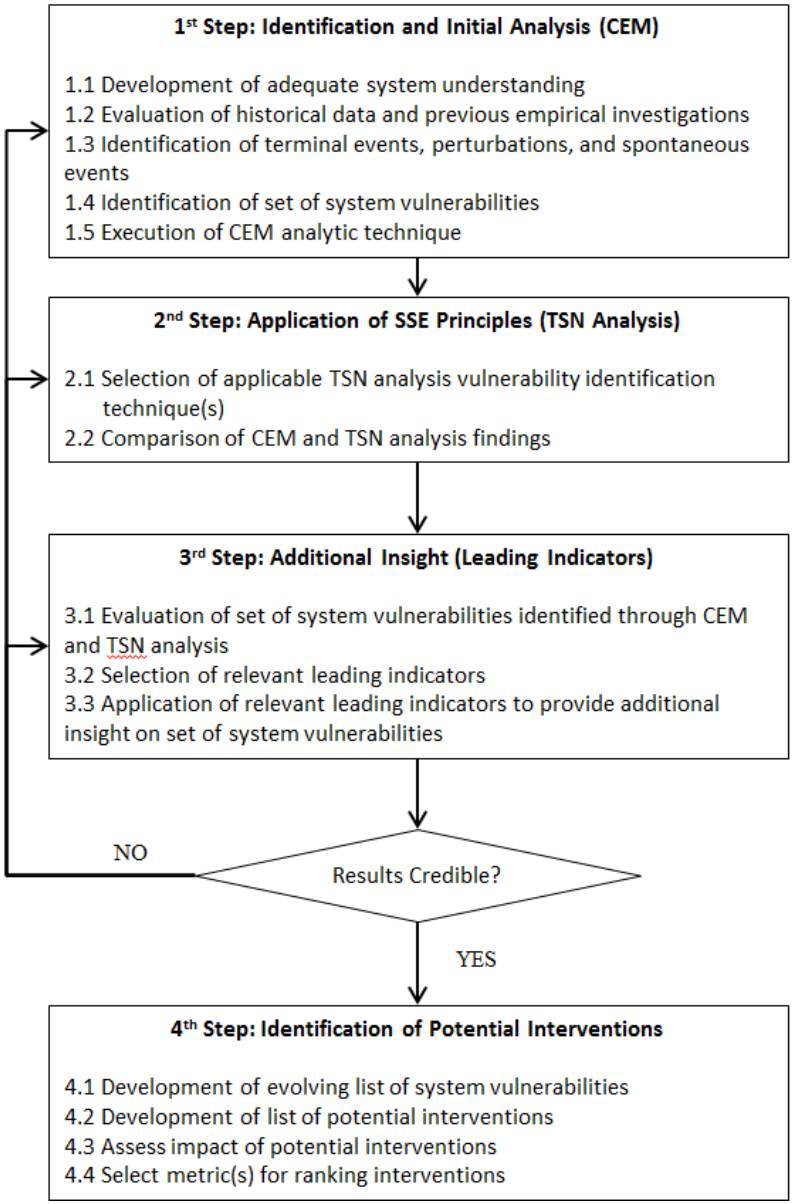
4th Step: Identification of Potential Interventions

4.1 Development of evolving list of system vulnerabilities
4.2 Development of list of potential interventions
4.3 Assess impact of potential interventions
4.4 Select metric(s) for ranking interventions

Goal: Allow an organization or individual to develop comprehensive understanding of a supply chain, to make informed decisions regarding potential mitigations, and to ensure more resilient systems

© 2016 Massachusetts Institute of Technology

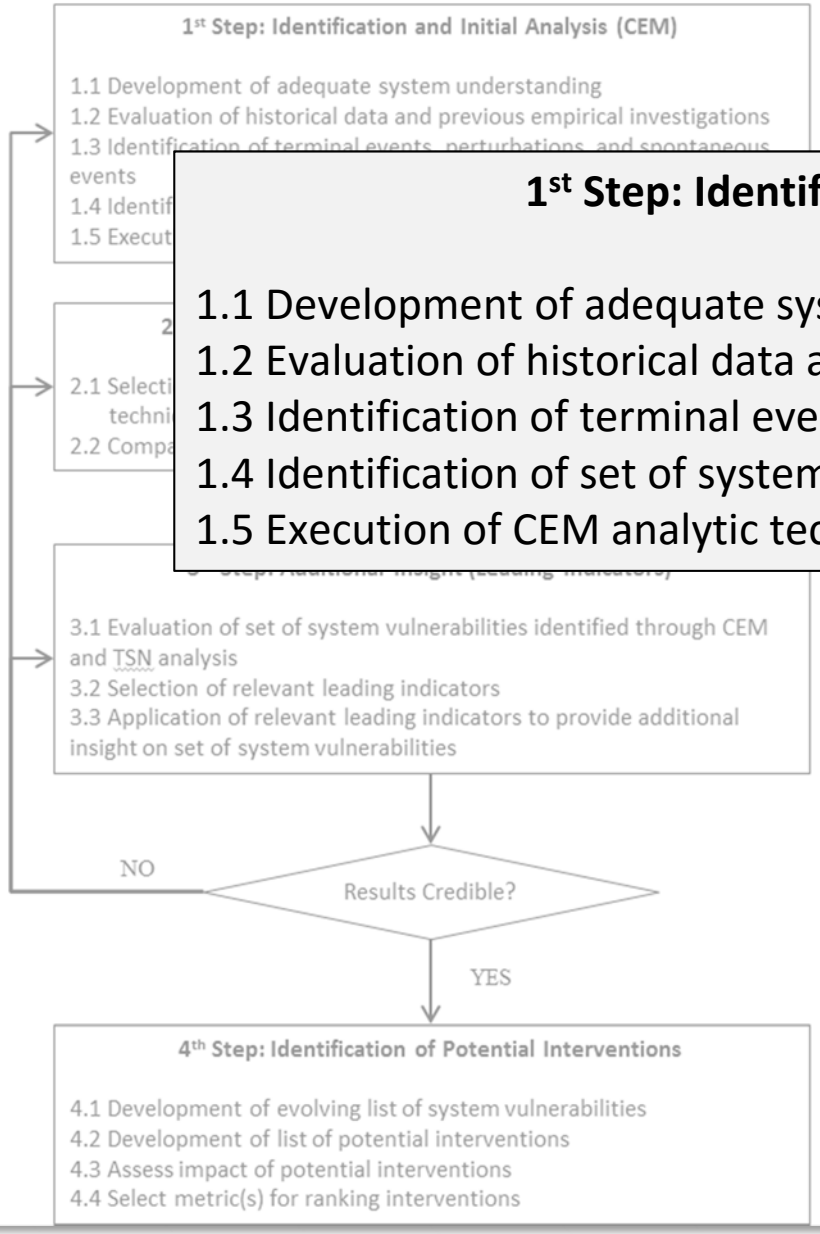
Generic Model



- Guides the user through sequential process to gain system understanding and to uncover potential sources of vulnerability
- Allows for exploration of system interdependencies

© 2016 Massachusetts Institute of Technology

1st Step: Identification and Initial Analysis (CEM)



1st Step: Identification and Initial Analysis (CEM)

1.1 Development of adequate system understanding
1.2 Evaluation of historical data and previous empirical investigations
1.3 Identification of terminal events, perturbations, and spontaneous events
1.4 Identification of set of system vulnerabilities
1.5 Execution of CEM analytic technique

© 2016 Massachusetts Institute of Technology

Cause-Effect Mapping
(Mekdeci, 2013)

- Analytic technique for identifying cascading failures and system intervention points [6]
- Models a system using disruptions, disturbances, causal chains, and terminal conditions
- Highlights relationships between causes and effects of perturbations
- Complements other analysis techniques

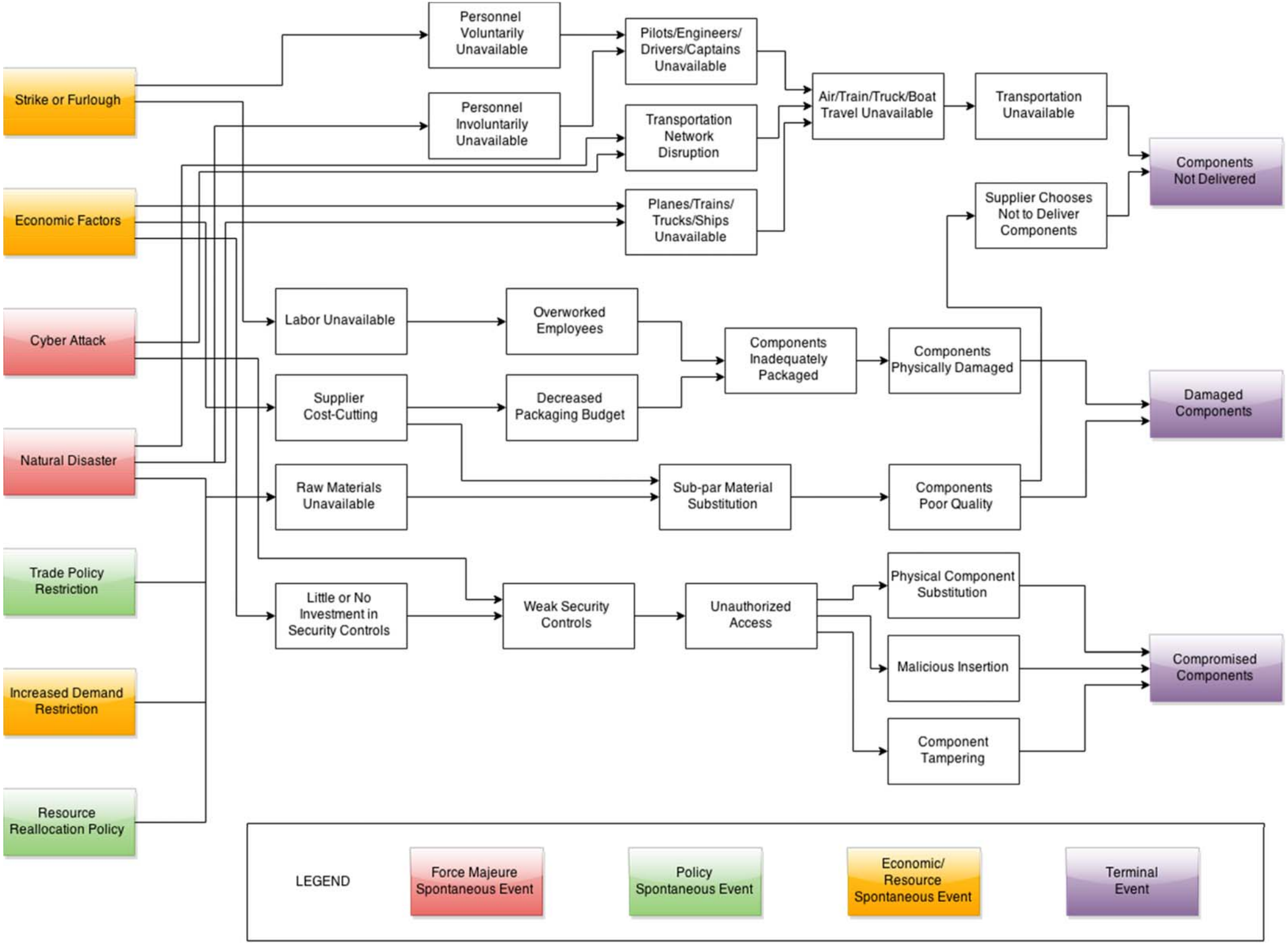
Enables decision-makers to pinpoint where strategies can be implemented to prevent the occurrence of terminal events through the avoidance and mitigation of and recovery from root-cause perturbations

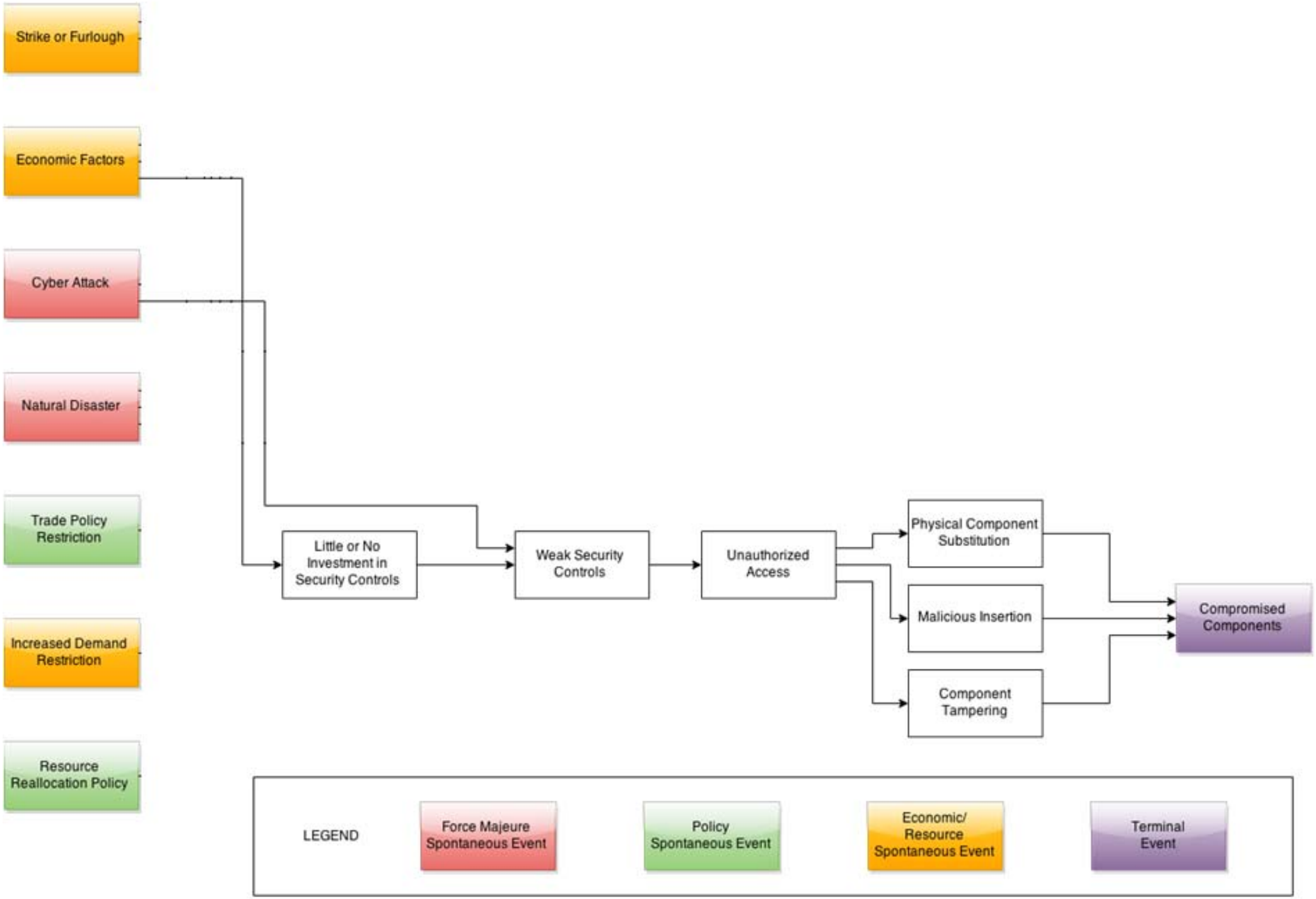
© 2016 Massachusetts Institute of Technology

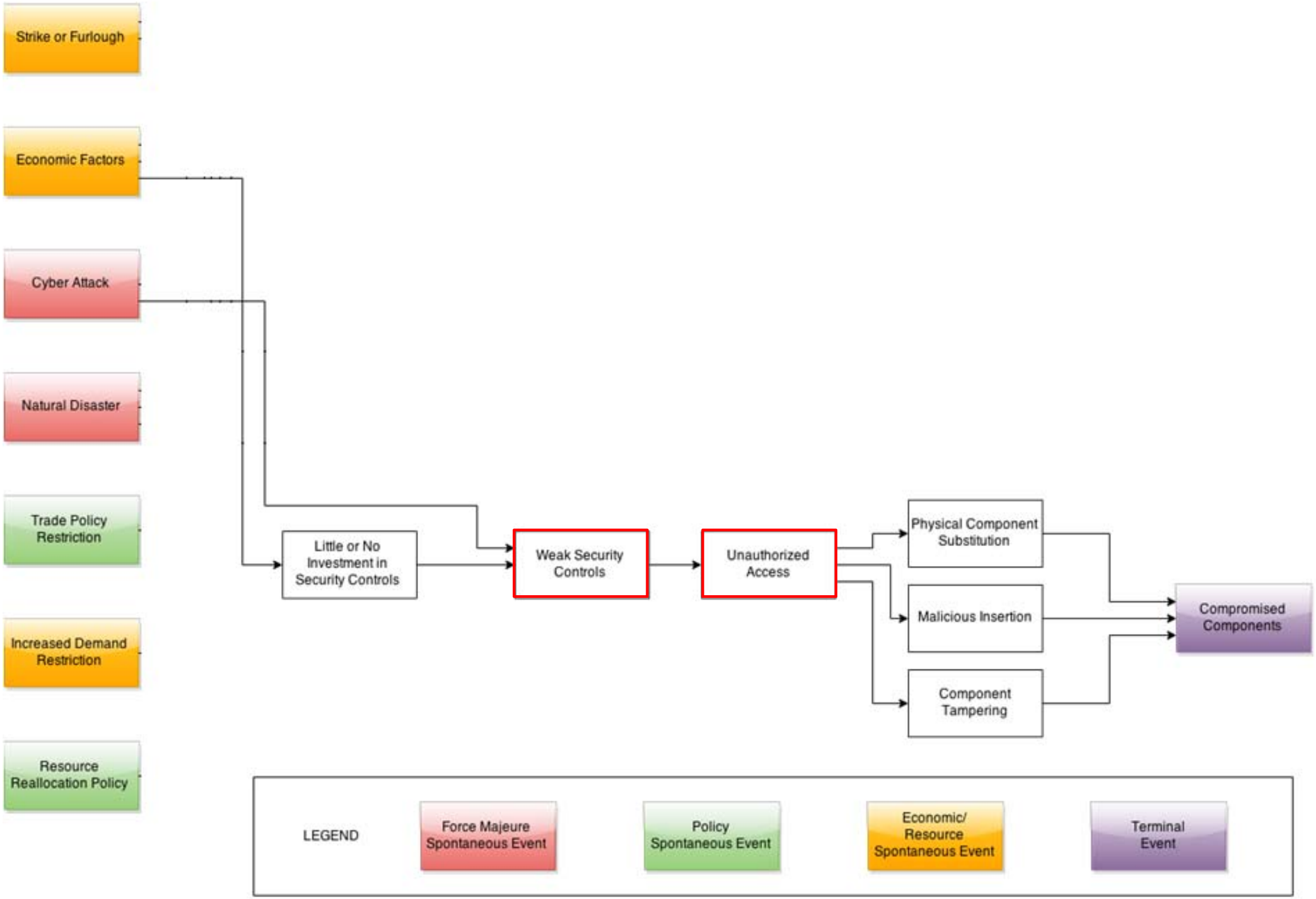
Technique Comparison [7] [8] [9]

	Cause-Effect Mapping	FTA	FMEA/FMECA
Focus	Entire system	Failure outcome	Each system component
Methodology	Linkage of causes to perturbations to effects	Deductive, top-down method	Inductive, bottom-up method
Specialty	Identification of cascading failures and intervention points	Analyzing effects of initiating faults	Analyzing effects of single component or function failure
Strengths	Exposing causal flows	Showing system resistance to initiating faults	Classifying initiating faults and identifying effects
Weaknesses	Methodology not yet mature	Finding all possible initiating faults	Examining multiple failures and effects at system level

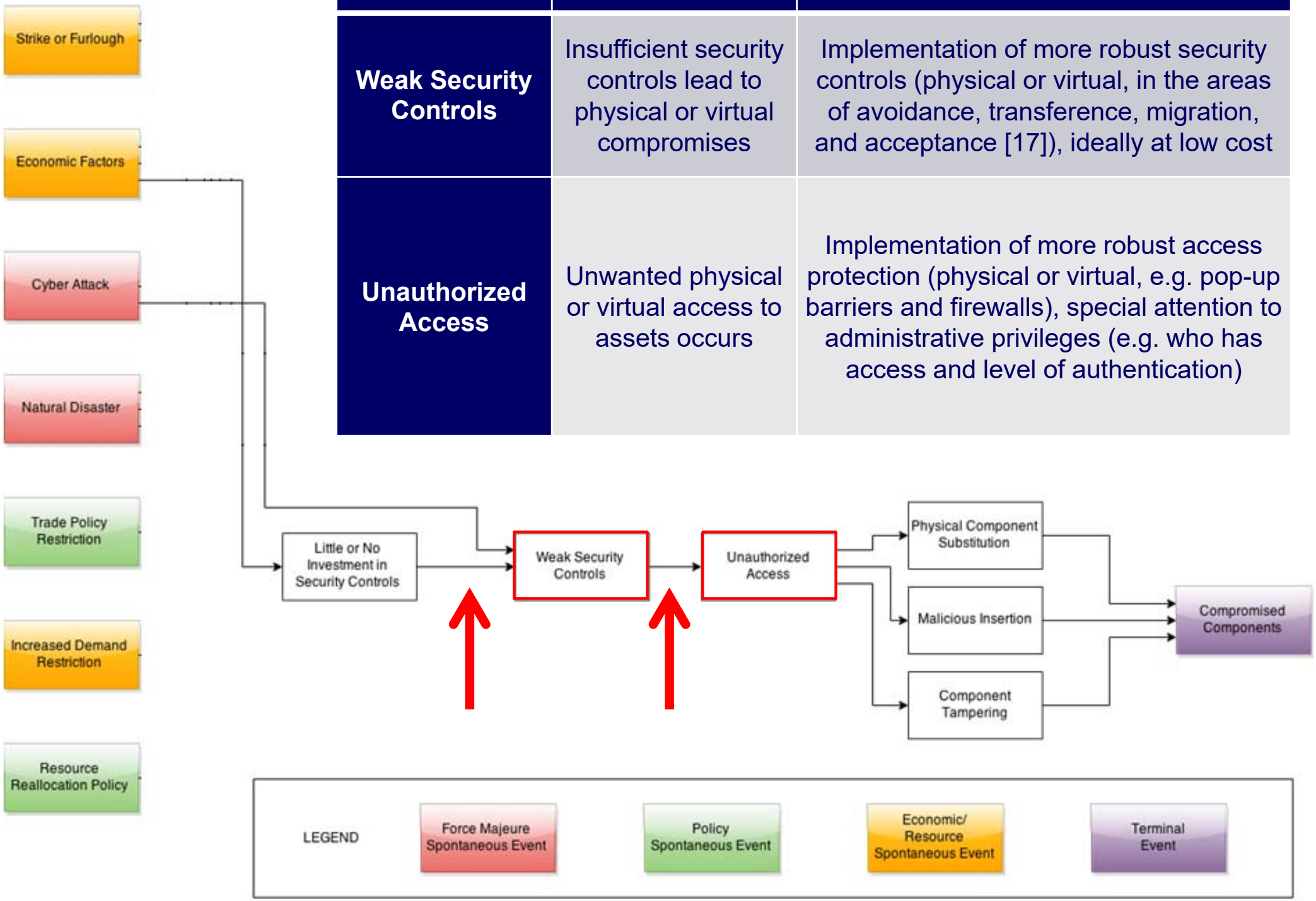
© 2016 Massachusetts Institute of Technology


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

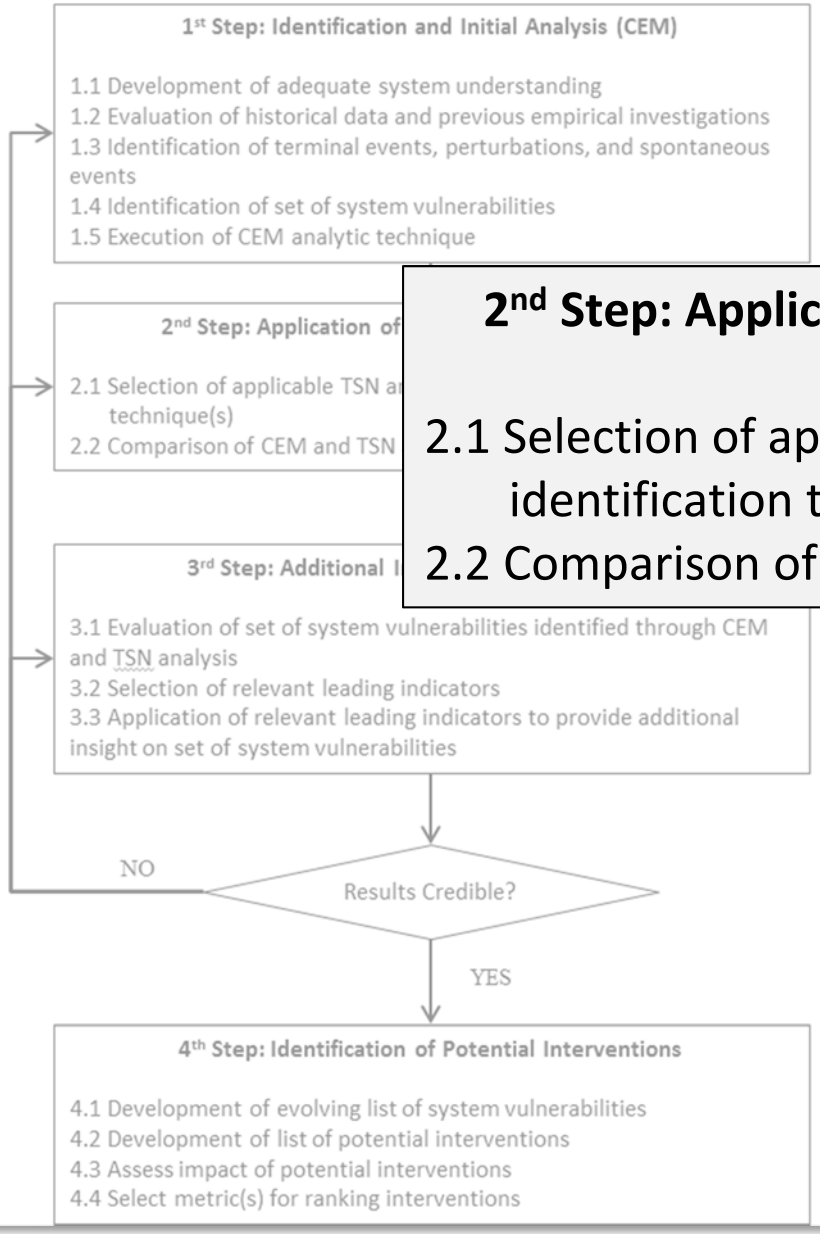

Strike or Furlough
Economic Factors
Cyber Attack
Natural Disaster
Trade Policy Restriction
Increased Demand Restriction
Resource Reallocation Policy
Little or No Investment in Security Controls
Weak Security Controls
Unauthorized Access
Physical Component Substitution
Malicious Insertion
Component Tampering
Compromised Components
LEGEND
Force Majeure Spontaneous Event
Policy Spontaneous Event
Economic/ Resource Spontaneous Event
Terminal Event


Strike or Furlough
Economic Factors
Cyber Attack
Natural Disaster
Trade Policy Restriction
Increased Demand Restriction
Resource Reallocation Policy
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

Perturbation	Description	Strategy
Weak Security Controls	Insufficient security controls lead to physical or virtual compromises	Implementation of more robust security controls (physical or virtual, in the areas of avoidance, transference, migration, and acceptance [17]), ideally at low cost
Unauthorized Access	Unwanted physical or virtual access to assets occurs	Implementation of more robust access protection (physical or virtual, e.g. pop-up barriers and firewalls), special attention to administrative privileges (e.g. who has access and level of authentication)



2nd Step: Application of SSE Principles (TSN Analysis)



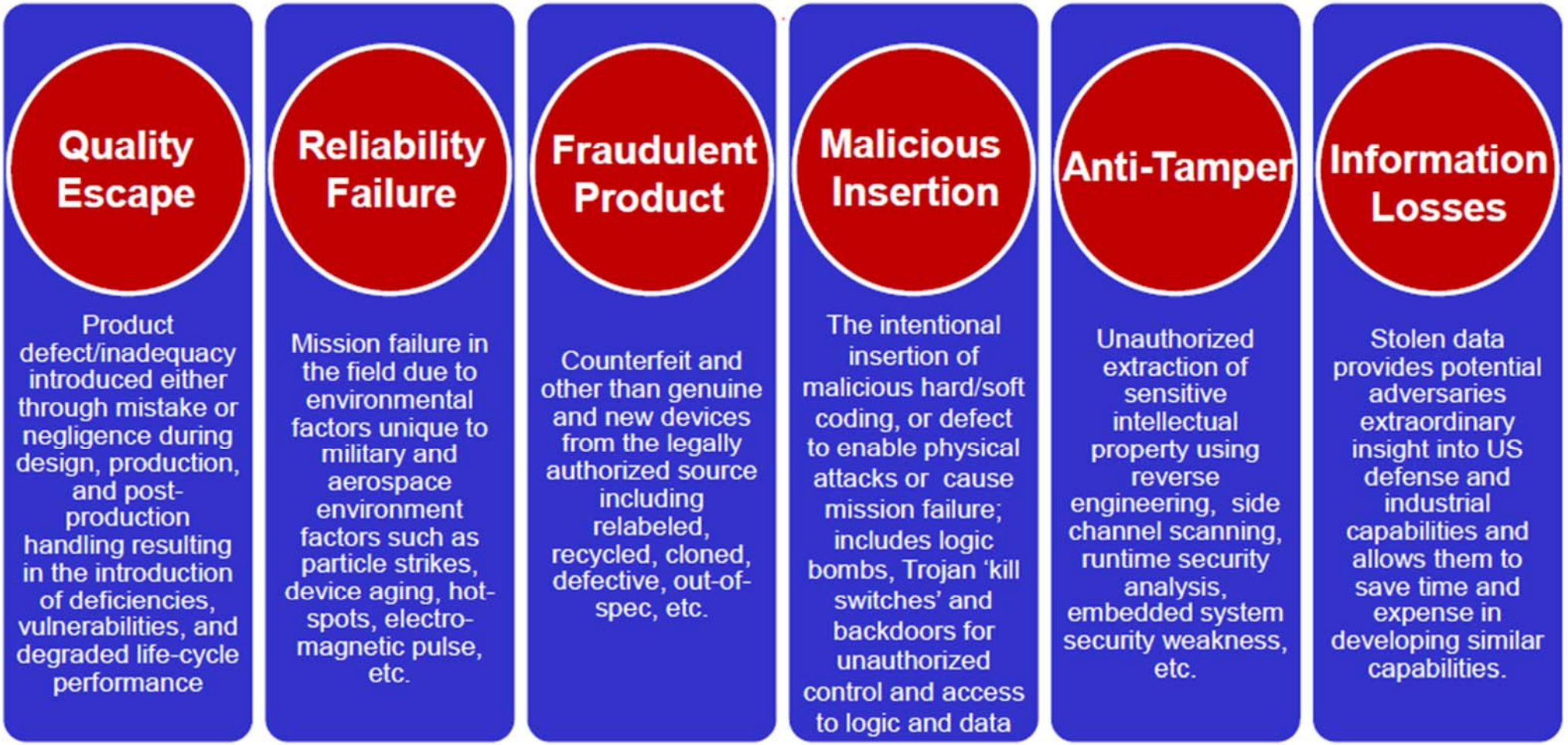
2nd Step: Application of SSE Principles (TSN Analysis)

2.1 Selection of applicable TSN analysis vulnerability identification technique(s)

2.2 Comparison of CEM and TSN analysis findings

© 2016 Massachusetts Institute of Technology

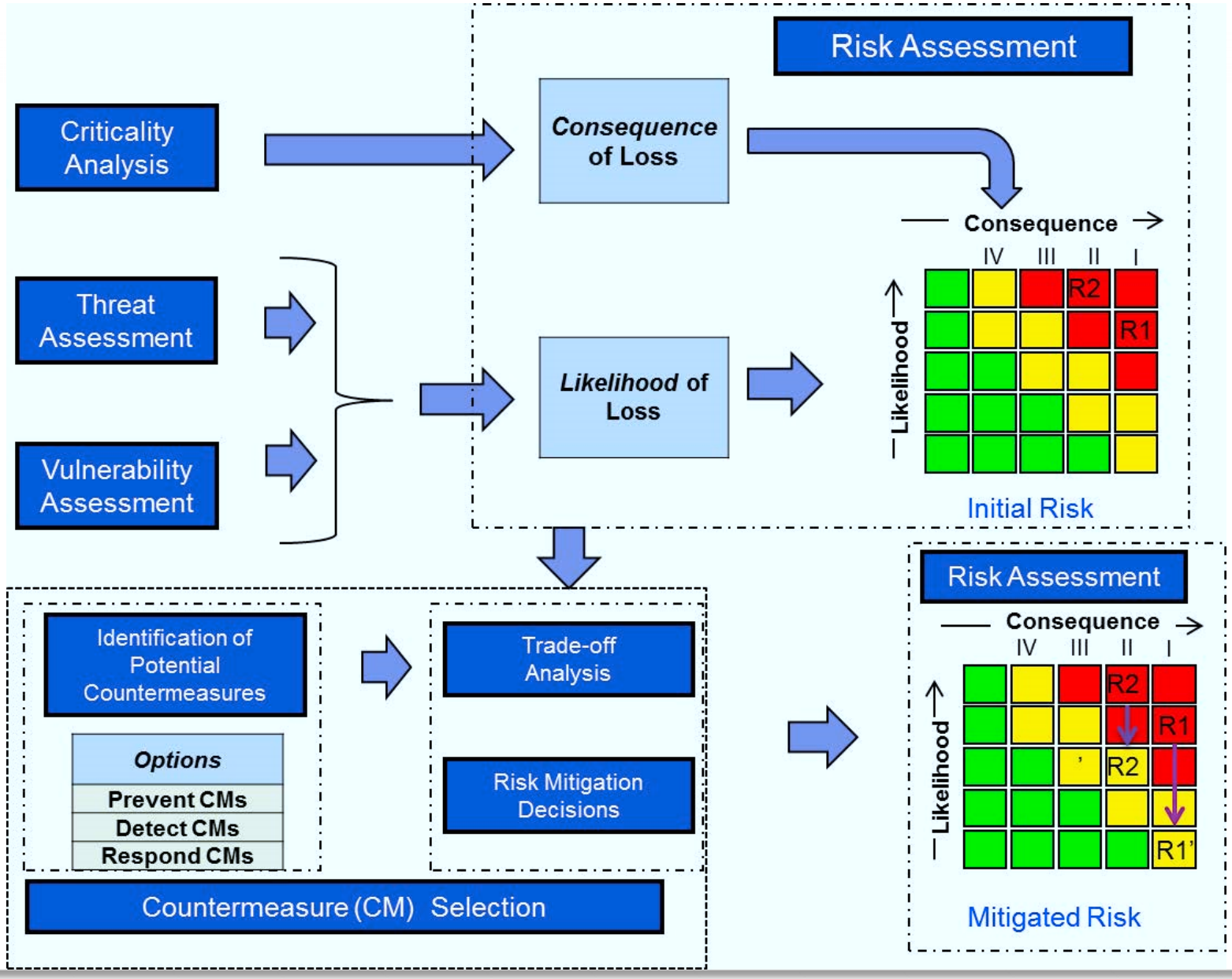
Supply Chain Risks to Consider



Systems Security Engineering (SSE) addresses a range of critical security risks [10] (source: Baldwin, 2014)

© 2016 Massachusetts Institute of Technology

DoD Trusted Systems and Networks (TSN) Analysis [4]



© 2015 Massachusetts Institute of Technology

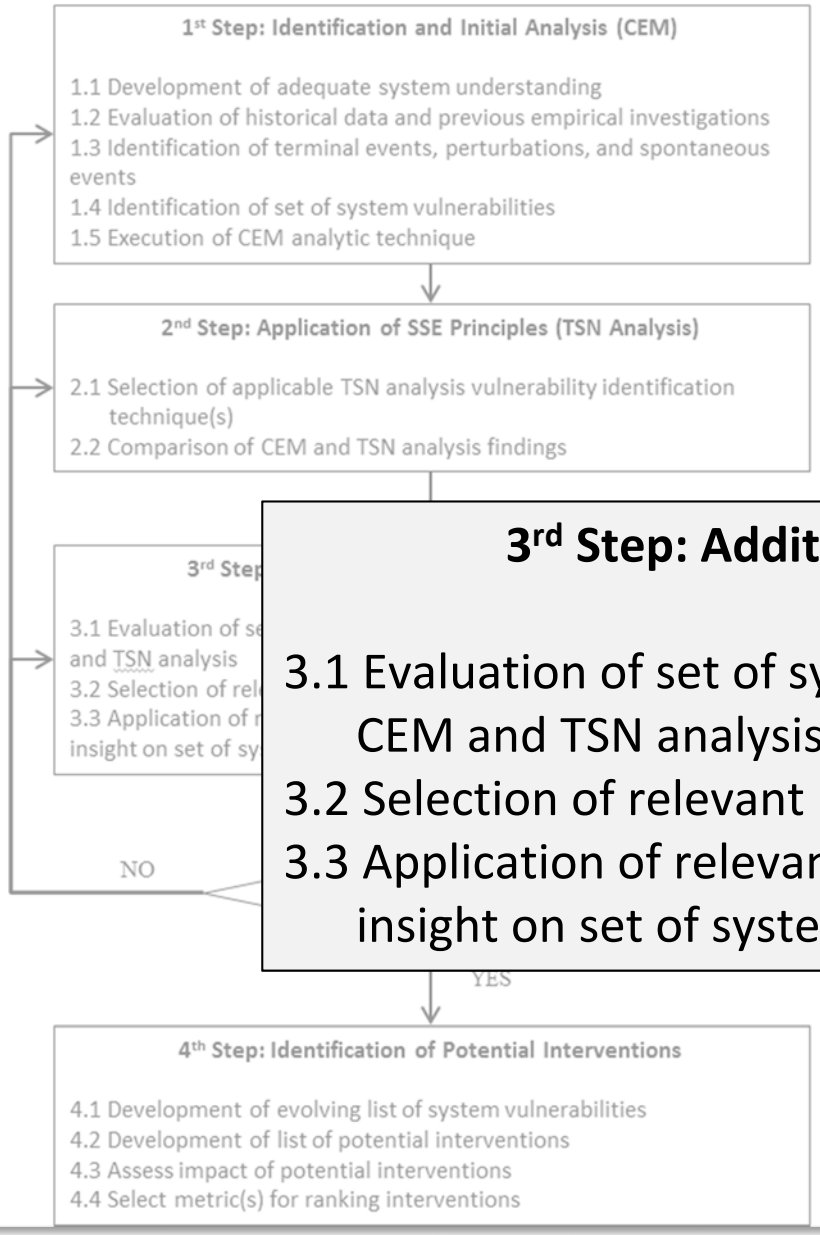
TSN Vulnerability Assessment Techniques [16]

Analysis Technique	High-Level Description
Vulnerability Assessment Questionnaire	A set of questions a program answers to identify vulnerabilities that can be mitigated by Statement of Work and system requirements additions to the Request For Proposal
Vulnerability Database Assessments	Assessment using three databases of publically-available information that define attack patterns, vulnerabilities, and weaknesses (CAPEC, CVE, CWE)
Static Analyzer Tools and Other Detection Techniques	Static analysis, dynamic analysis, and other testing, tools, and techniques to identify vulnerabilities in software during development, in legacy software, and in open source
Component Diversity Analysis	Assessment of the potential impact of malicious insertion in a component that is used multiple times in one or more critical functions or sub-functions
Fault Tree Analysis (FTA)/ Attack Tree Analysis (ATA)	Analysis commonly used in system safety and reliability, adjusted for use in system security to account for malicious actors introducing intentional system faults, as opposed to random sources of failure
Red Team and Penetration Testing	Subjecting a system, supply chain, and/or the development environment to a series of attacks, simulating the tactics of an actual threat through the use of misuse cases

Source: LeSaint et al., 2015

© 2016 Massachusetts Institute of Technology

3rd Step: Additional Insight (Leading Indicators)



3rd Step: Additional Insight (Leading Indicators)

3.1 Evaluation of set of system vulnerabilities identified through CEM and TSN analysis
3.2 Selection of relevant leading indicators
3.3 Application of relevant leading indicators to provide additional insight on set of system vulnerabilities

© 2016 Massachusetts Institute of Technology

Leading Indicators

- Predictive in nature
- Allow an organization or individual to adjust/adapt based on results [11]
- Can be thought of as information about how the vulnerability of the system will develop [5]
- Portray direction of vulnerabilities [12]

Table 2. Examples of different threats and possible corresponding indicators for monitoring vulnerability

	Indicator for threats	Indicator for susceptibility
Natural hazard: Storm	Wind prognosis Historical wind data	Localisation (exposure to wind) of critical power lines Technical condition of critical power lines Competence on condition evaluation of power lines Competence on system analyses and vulnerability evaluations
Human threat: Digging	Construction work near critical locations in the power system Historical data on cable joint failures	Number and localisation of junctions where infrastructures meet Technical condition of power cables including joints Competence on condition evaluation of power cables including joints Competence on system analyses and cross sector vulnerability evaluations
Operational conditions: Overload	Overload Stepwise increase in loading degree	Loading degree for critical systems and components Technical condition of critical systems and components Competence on condition evaluation of critical components Competence on system analyses and vulnerability evaluations

	Indicator for coping capacity	Indicator for criticality
All threats	System control centre competence (including cooperation and coordination between infrastructures) Competence on repair (of power lines, cables, other critical components) Available transport for repair (of power lines, cables, other critical components)	Localisation of critical loads including dependent infrastructures Interruption costs including dependent infrastructures Categories of end users affected Temperature

Source: Hofmann et al., 2012

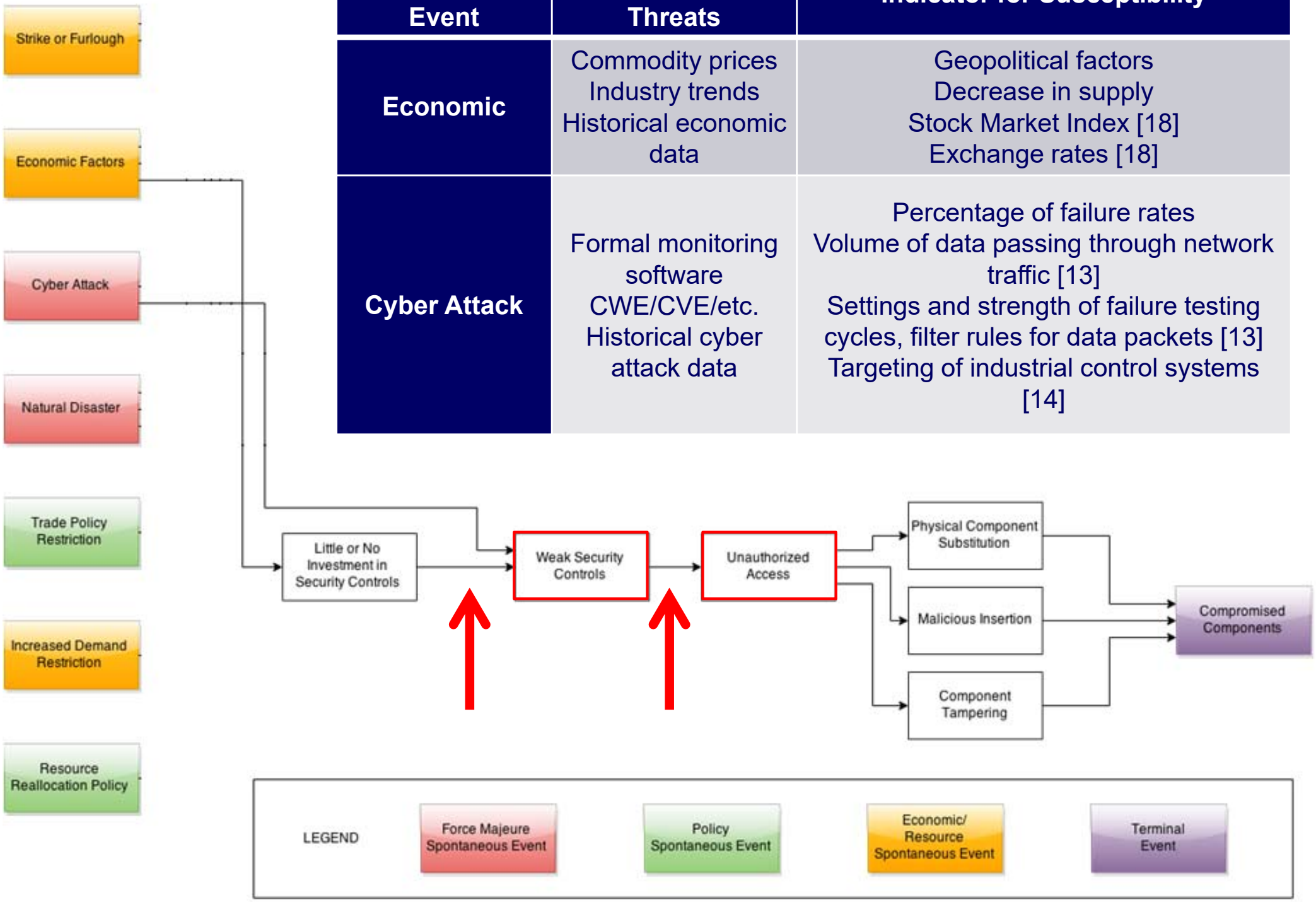
© 2016 Massachusetts Institute of Technology

Vulnerability Threats and Indicators

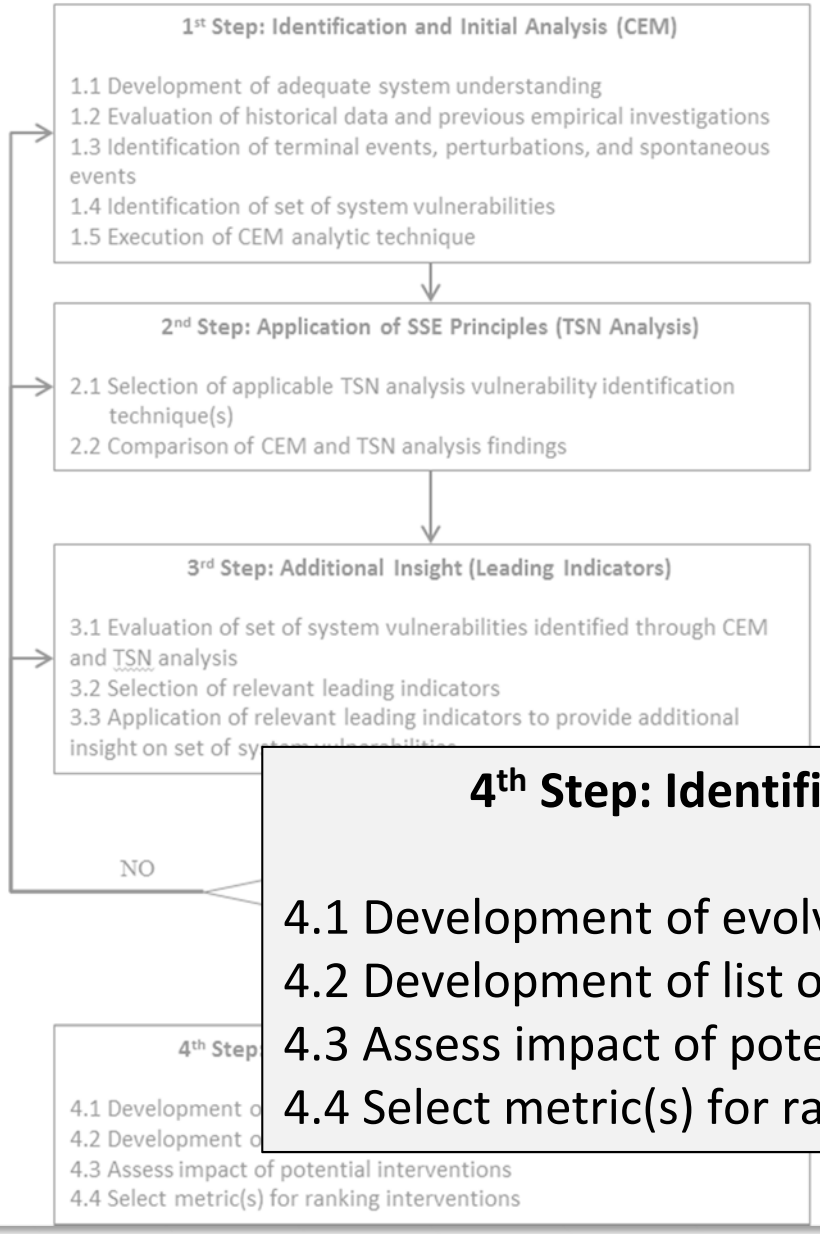
Spontaneous Event	Indicator for Threats	Indicator for Susceptibility
Strike/Furlough	Labor relations Contract status Historical strike/furlough data	Union issues/demands Upcoming contract expiration/renewal
Economic	Commodity prices Industry trends Historical economic data	Geopolitical factors Decrease in supply Stock Market Index [18] Exchange rates [18]
Cyber Attack	Formal monitoring software CWE/CVE/etc. Historical cyber attack data	Percentage of failure rates Volume of data passing through network traffic [13] Settings and strength of failure testing cycles, filter rules for data packets [13] Targeting of industrial control systems [14]
Natural Disaster	Weather prognosis Historical weather data	Localization (exposure to elements) of critical resource infrastructure (e.g. power lines) Technical condition of critical resource infrastructure Competence on condition evaluation of critical resource infrastructure Competence on system analyses and vulnerability evaluations
Trade Policy Restriction	Diplomatic relations Historical trade policy data	Geopolitical factors Pending legislation
Increased Demand	Industry trends Historical demand data	Geopolitical factors Shortage of substitute products Changes to manufacturing processes
Resource Reallocation	Industry trends Historical demand data	Adoption of new technologies Pending legislation

© 2016 Massachusetts Institute of Technology

Spontaneous Event	Indicator for Threats	Indicator for Susceptibility
Economic	Commodity prices Industry trends Historical economic data	Geopolitical factors Decrease in supply Stock Market Index [18] Exchange rates [18]
Cyber Attack	Formal monitoring software CWE/CVE/etc. Historical cyber attack data	Percentage of failure rates Volume of data passing through network traffic [13] Settings and strength of failure testing cycles, filter rules for data packets [13] Targeting of industrial control systems [14]



4th Step: Identification of Potential Interventions



4th Step: Identification of Potential Interventions

4.1 Development of evolving list of system vulnerabilities
4.2 Development of list of potential interventions
4.3 Assess impact of potential interventions
4.4 Select metric(s) for ranking interventions

© 2016 Massachusetts Institute of Technology

Set of Interventions

Perturbation	Description	Strategy
Air/Train/Truck/Boat Travel Unavailable	Travel is unavailable regardless of mode of transportation	Strategic reserves of components and potential for 3-D printing of temporary replacement parts
Overworked Employees	Employees are overworked due to labor shortages	Policies to prevent employees from becoming overworked, potential automation of tasks
Raw Materials Unavailable	Raw materials are unavailable due to various force majeure, policy, and economic/ resource reasons	Strategic reserves and studies on potential replacement materials
Components Poor Quality	Components are of inferior quality and prone to failure	Use of lean initiatives to catch quality problems earlier in the design and manufacturing process
Weak Security Controls	Insufficient security controls lead to physical or virtual compromises	Implementation of more robust security controls (physical or virtual, in the areas of avoidance, transference, migration, and acceptance [17]), ideally at low cost
Unauthorized Access	Unwanted physical or virtual access to assets occurs	Implementation of more robust access protection (physical or virtual, e.g. pop-up barriers and firewalls), special attention to administrative privileges (e.g. who has access and level of authentication)

- Allow the system to avoid, mitigate, or recover from perturbations
- Important to identify reinforcing loops (non-linear relationships) in order to prevent cascading failures
- Prevention and mitigation of perturbations with multiple effects is key
- Set of interventions can be prioritized based on benefit to system, ease of implementation, and cost among other factors

© 2016 Massachusetts Institute of Technology

Conclusions and Future Work

- Generic Model proposed as guiding framework for making use of existing tools and providing better, holistic grasp of vulnerability space
  - Imparts holistic system-level understanding
  - Formulates list of vulnerabilities and associated interventions allowing for informed decisions

- Future Work
  - Knowledge transfer – “Silver Tsunami”
  - Incorporation of quantitative metrics
  - Synergies with industry
  - Policy implications

© 2016 Massachusetts Institute of Technology

Questions?

The authors gratefully acknowledge funding for this research provided through the Charles Stark Draper Fellowship Program

© 2016 Massachusetts Institute of Technology

References

[1] Centre for Logistics and Supply Chain Management at the Cranfield School of Management. (2003). *Understanding Supply Chain Risk: A Self-Assessment Workbook* (pp. 1–54). Cranfield, Bedford, UK: Cranfield University.

[2] Kröger, W., & Zio, E. (2011). *Vulnerable Systems*. London: Springer London.

[3] Svensson, G. (2002). A conceptual framework of vulnerability in firms' inbound and outbound logistics flows. *International Journal of Physical Distribution & Logistics Management*, *32*(2), 110–134.

[4] Deputy Assistant Secretary of Defense for Systems Engineering, & Department of Defense Chief Information Officer. (2014). Trusted Systems and Networks (TSN) Analysis.

[5] Hofmann, M., Kjølle, G. H., & Gjerde, O. (2012). Development of Indicators to Monitor Vulnerabilities in Power Systems. Presented at the PSAM 11 and ESREL 2012 Conference on Probabilistic Safey Assessment.

[6] Mekdeci, B. (2013). *Managing the Impact of Change Through Survivability and Pliability to Achieve Viable Systems of Systems*. Massachusetts Institute of Technology.

[7] Federal Aviation Administration. (2000). *FAA System Safety Handbook, Chapter 9: Analysis Techniques*.

[8] Hampl, V. (2010). *FMEA and FTA*.

[9] Yu, S. (2011). A Comparison of FMEA , AFMEA and FTA, 954–960.

[10] Baldwin, K. J. (2014). Complexity: Driver of Systems Engineering Reflecting on Defense Strategic Guidance, 1–17.

[11] International Customer Management Institute. (n.d.). Leading & Lagging Indicators.

[12] Zimmerman, R. (2004). Decision-making and the vulnerability of interdependent critical infrastructure. *IEEE International Conference on Systems, Man and Cybernetics, 2004*, *5*, 4059–4063.

[13] Koh, A. (2015). *Defending Against Cyber Security Threats to the Payment and Banking Systems*. Presented at the NYU Leonard N. Stern School of Business Master of Science Risk Management Risk Management Symposium.

[14] Assante, M. (2014, November 11). America's Critical Infrastructure Is Vulnerable To Cyber Attacks. Retrieved April 8, 2016.

[15] Reed, M. (2014). Vulnerability Analysis Techniques to Support Trusted Systems and Networks (TSN) Analysis Office of the Deputy Assistant Secretary of Defense, 1–37.

[16] LeSaint, J., Popick, P., & Reed, M. (2015). System Security Engineering Vulnerability Assessments for Mission-Critical Systems and Functions (pp. 608–613). Presented at the Systems Conference (SysCon), 2015 9th Annual IEEE International, Vancouver, BC.

[17] Carbone, T. A., & Tippett, D. D. (2004). Project Risk Management Using the Project Risk FMEA. *Engineering Management Journal*, *16*(4), 28–35.

[18] Inter-American Development Bank. (n.d.). The Prevalent Vulnerability Index (PVI). Retrieved April 15, 2016, from http://www.iadb.org/exr/disaster/idea_pvi.pdf

© 2016 Massachusetts Institute of Technology