

REPORT DOCUMENTATION PAGE					Form Approved OMB No. 0704-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.						
1. REPORT DATE (DD-MM-YYYY)		2. REPORT TYPE			3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE				5a. CONTRACT NUMBER		
				5b. GRANT NUMBER		
				5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)				5d. PROJECT NUMBER		
				5e. TASK NUMBER		
				5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)					8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)					10. SPONSOR/MONITOR'S ACRONYM(S)	
					11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT						
15. SUBJECT TERMS						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON	
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include area code)	

Operating in a Degraded, Denied or Disconnected Environment Winning in the Face of Adversity

Mr. David Michalowicz

Mobile Deployable Communications Conference

Warsaw, Poland

30 - 31 January 2020

Overview

- **MITRE at a glance**
- **MITRE has been assessing “resiliency” and what it means in the national defense context**
- **A systems thinking methodology to holistically assess “resilience” against adverse events**
- **Determine “resiliency” requirements**

MITRE at a Glance

Our History

MITRE is a private, independent, not-for-profit organization, chartered to work in the public interest

Founded in 1958 to provide engineering and technical services to the U.S. Air Force

Supports a broad and diverse set of sponsors within the U.S. government, as well as internationally

Currently manages Federally Funded Research and Development Centers for the:

- Department of Defense
- Federal Aviation Administration
- Department of Health and Human Services
- Department of Homeland Security
- Department of Commerce/National Institute of Standards and Technology
- Department of Veterans Affairs
- Administrative Office of the U.S. Courts
- Department of the Treasury
- Internal Revenue Service



1958

2020

Understanding FFRDCs

Operate as strategic partners with their sponsoring government agencies

Organized as independent entities with limitations and restrictions on their activities

Assist the U.S. government with scientific research and analysis, development and acquisition, and systems engineering/integration

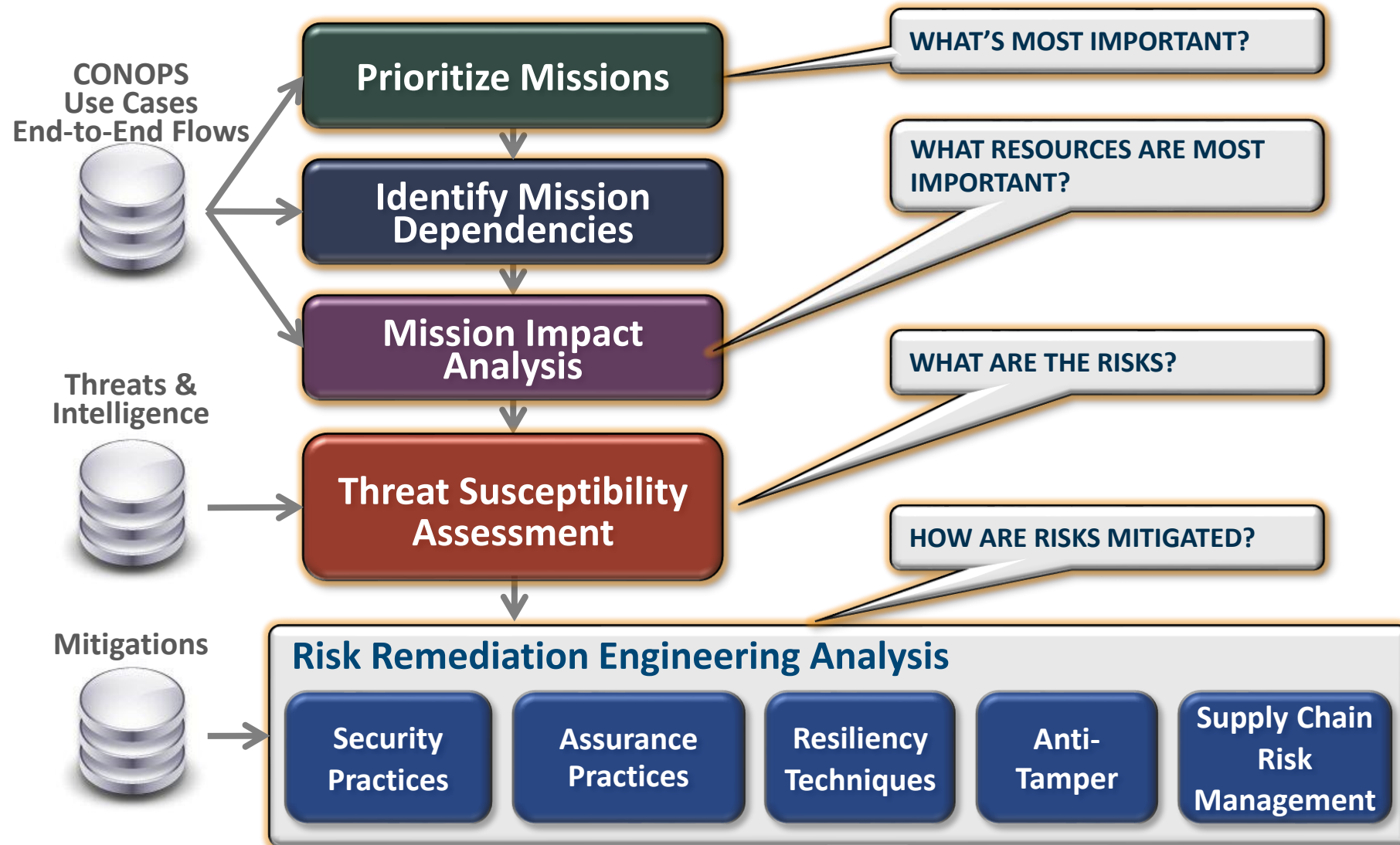
Bring together the expertise and outlook of government, industry, public-private partnerships and academia to solve complex technical problems

Assessing resiliency in the national defense context

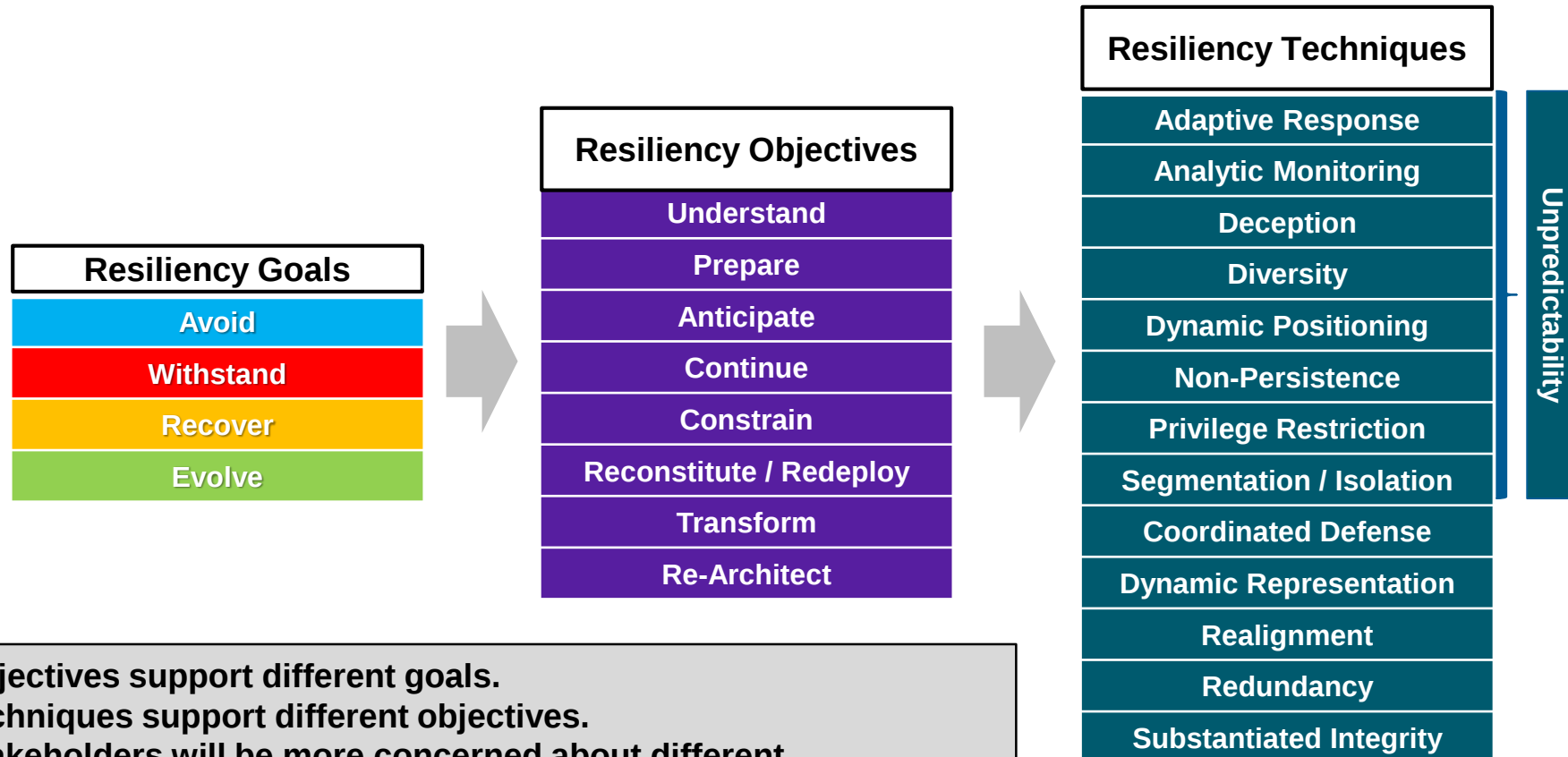
Problem Statement

- **When confronting a peer adversary, operating in a degraded, denied or disconnected environment is a certainty.**
- **All echelons of command require resilient networks and communications infrastructures that, in the face of adversity, provide commanders with reliable options to accomplish their missions.**

Transformation of Thought



A Resiliency Engineering Framework



- Different objectives support different goals.
- Different techniques support different objectives.
- Different stakeholders will be more concerned about different goals & objectives.
- Techniques vary in maturity, applicability to architectural layers, and suitability to operational environments
- No system can (or should) apply them all.

Resiliency Engineering Framework Goals

Avoid

Eliminate or reduce exposure to adversity

Withstand

Resist capability degradation when faced by adverse conditions - continue essential functions

Recover

Replenish lost or diminished capability subsequent to adverse conditions - restore essential functions

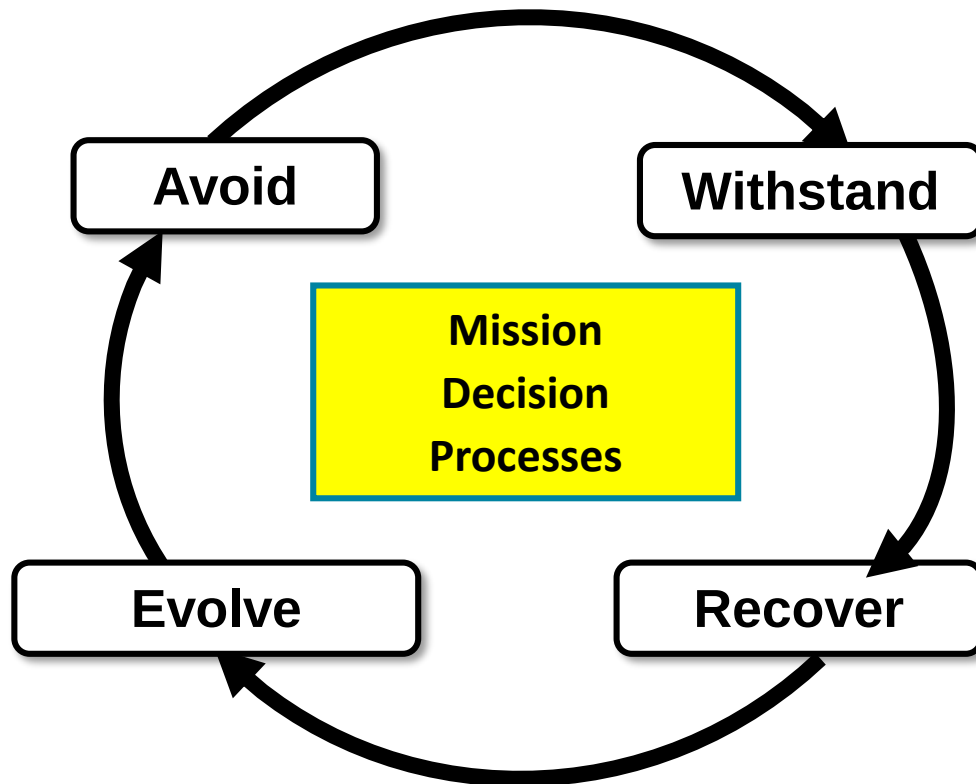
Evolve

Adapt essential mission/business functions and/or supporting capabilities to predicted changes in the technical, operational, or threat environments

A Systems Thinking methodology and resiliency

A Systems Thinking Model – An Iterative Process

Cyber Resiliency Engineering Framework Goals



Anticipate - Eliminate or reduce exposure to adversity

Withstand - Resist capability degradation when faced by adverse conditions - continue essential functions

Recover - Replenish lost or diminished capability subsequent to adverse conditions

Evolve - Adapt essential mission/business functions and/or supporting capabilities to predicted changes in the technical, operational, or threat environments

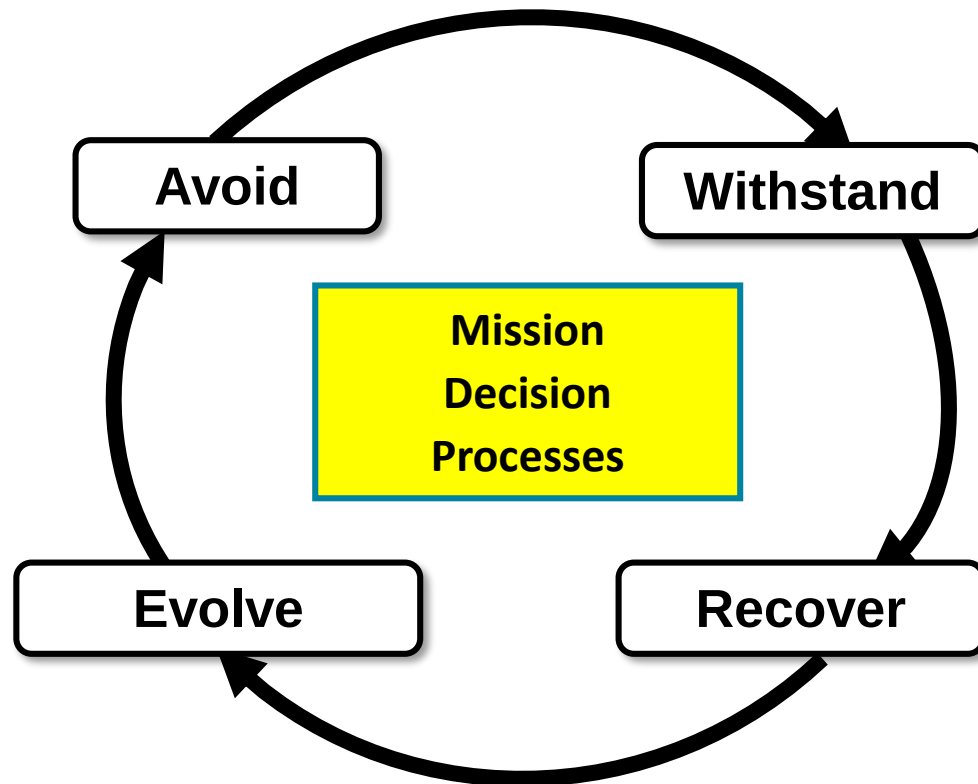
Conditions of Adversity

Infinite number of Events and Combinations

- **Natural Disasters**
 - Floods, Storms, Fires, Earthquake, Lightning Strikes, landslides
- **Kinetic Effects**
 - Bombs, Explosions, Impacts, Maneuvers
- **Non-Kinetic Effects**
 - Cyber-Attacks, Economic Warfare, Electronic Warfare, Psychological Operations
- **Human Error**
 - System misconfiguration, Lost Devices, Poor patch management, Cut cables from an excavation gone wrong

A Systems Thinking Model – An Iterative Process

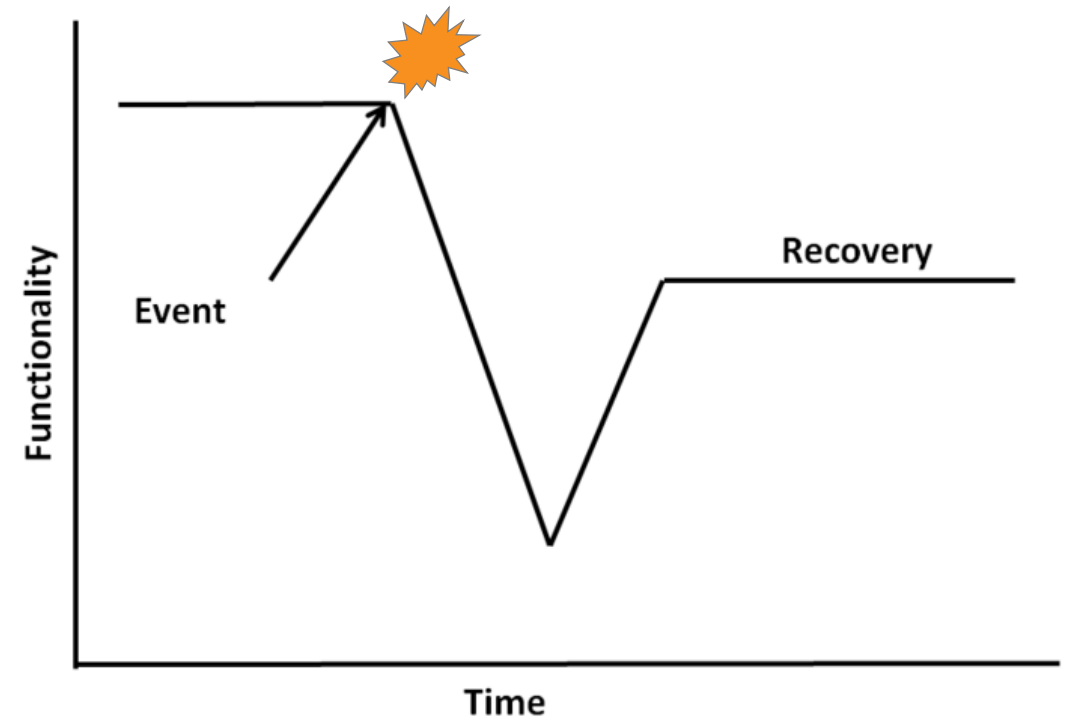
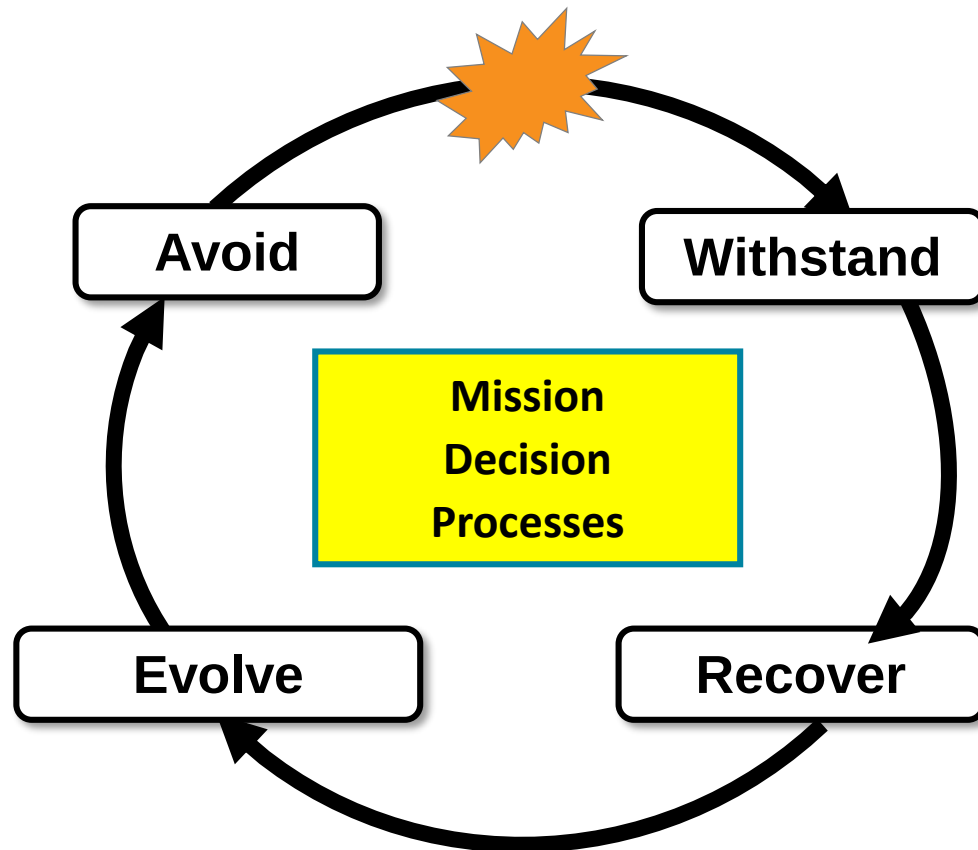
Primary Communications and Networks to Conduct Mission



Primary Communications and Networks

A Systems Thinking Model – An Iterative Process

Introduce Adverse Event(s)



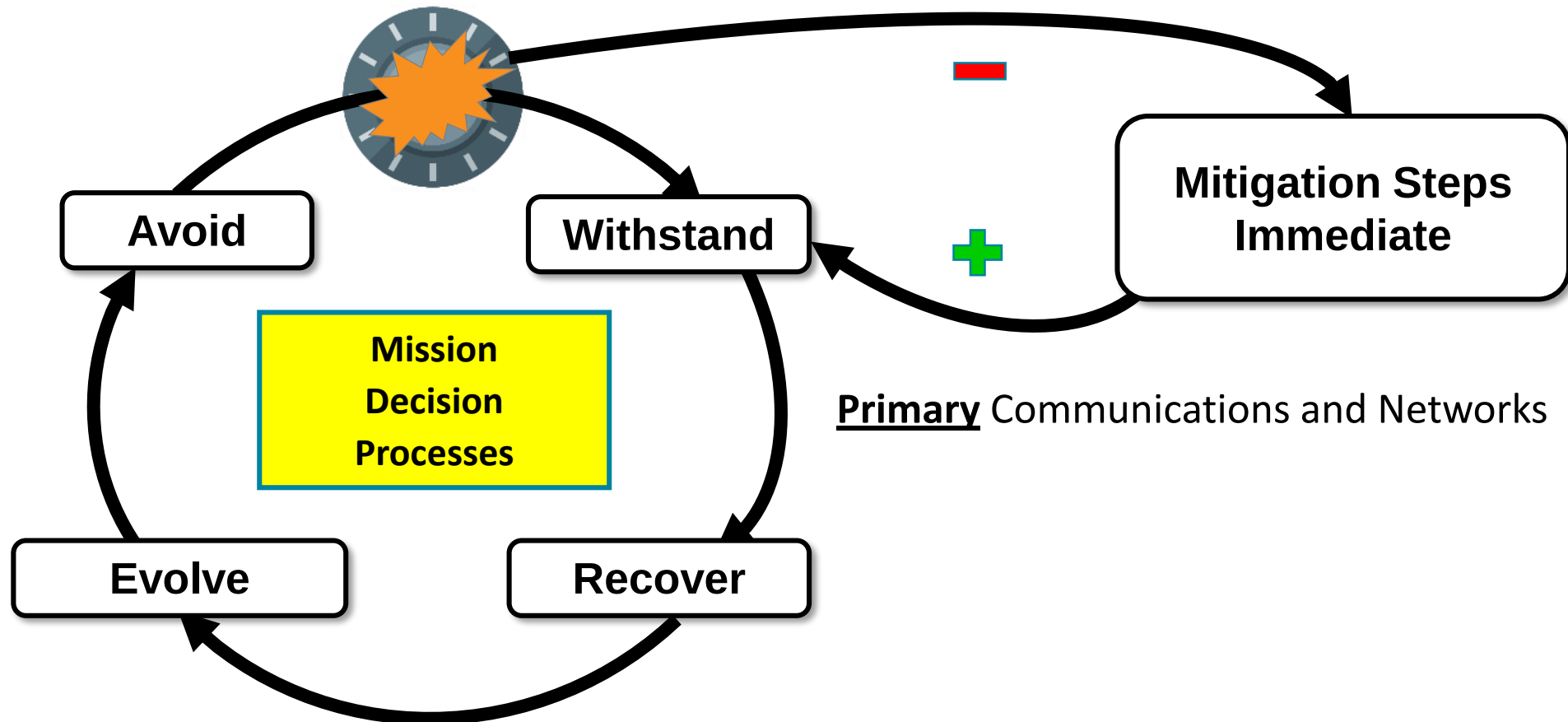
Disruption Model for Resilience and Survivability

Source: Systems Engineering Body of Knowledge (SEBoK) – Resilience Engineering

http://sebokwiki.org/wiki/File:Disruption_Diagram.PNG

A Systems Thinking Model – An Iterative Process

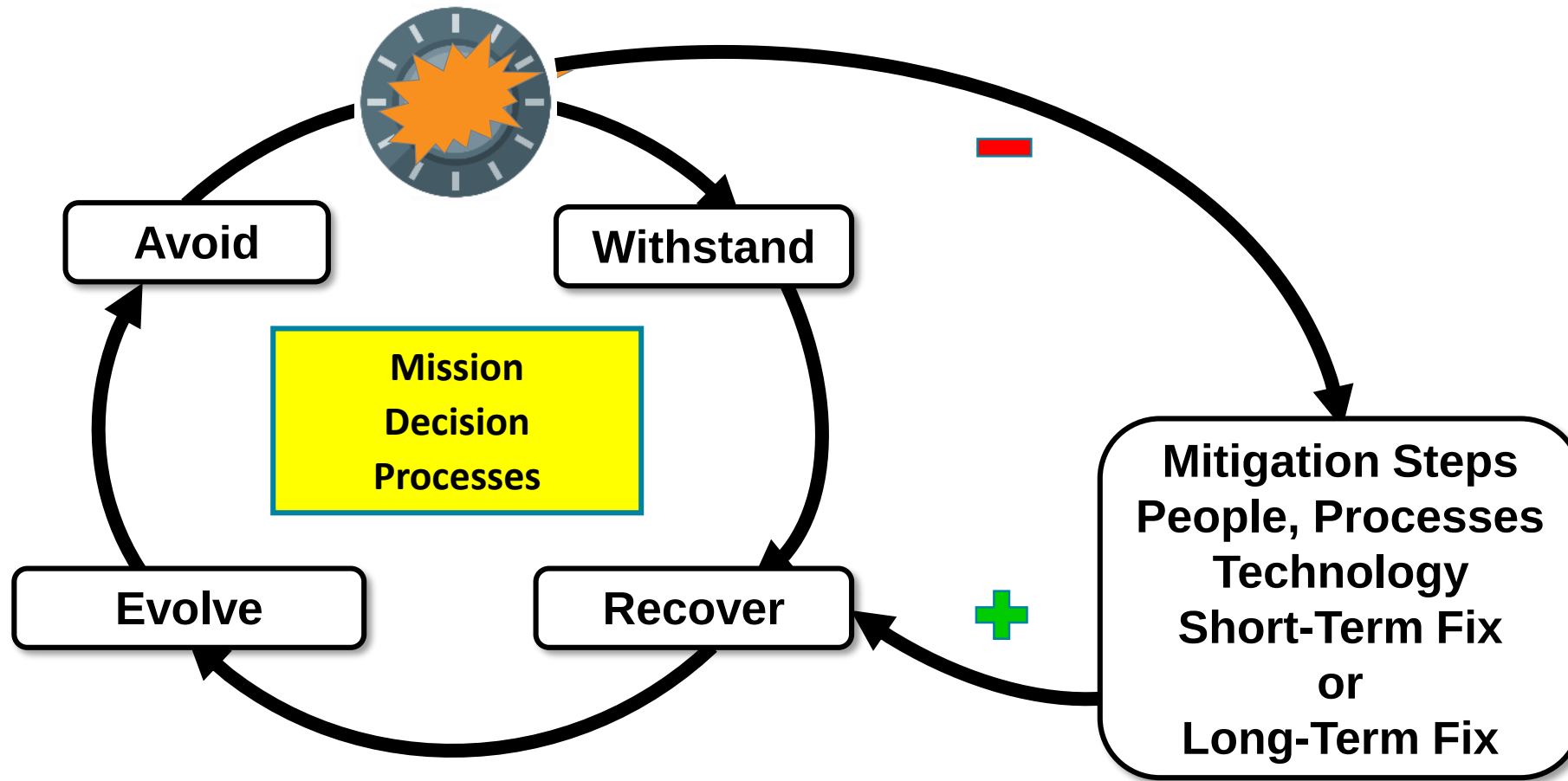
Mitigation Steps - Immediate



- If a mitigation is in place to immediately fix the problem: Withstand the Event

A Systems Thinking Model – An Iterative Process

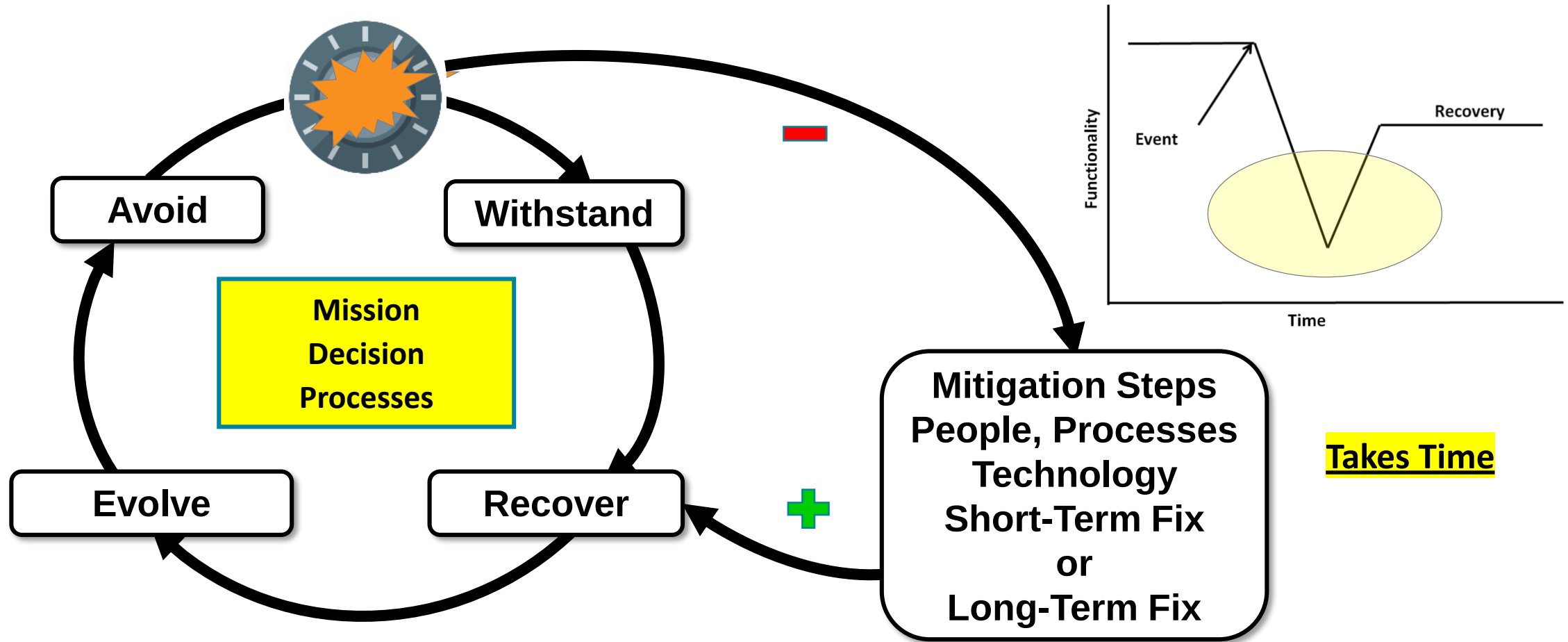
Mitigation Steps – Short-Term or Long-Term Fix



- Other mitigation steps need to be considered: People, Processes and Technology

A Systems Thinking Model – An Iterative Process

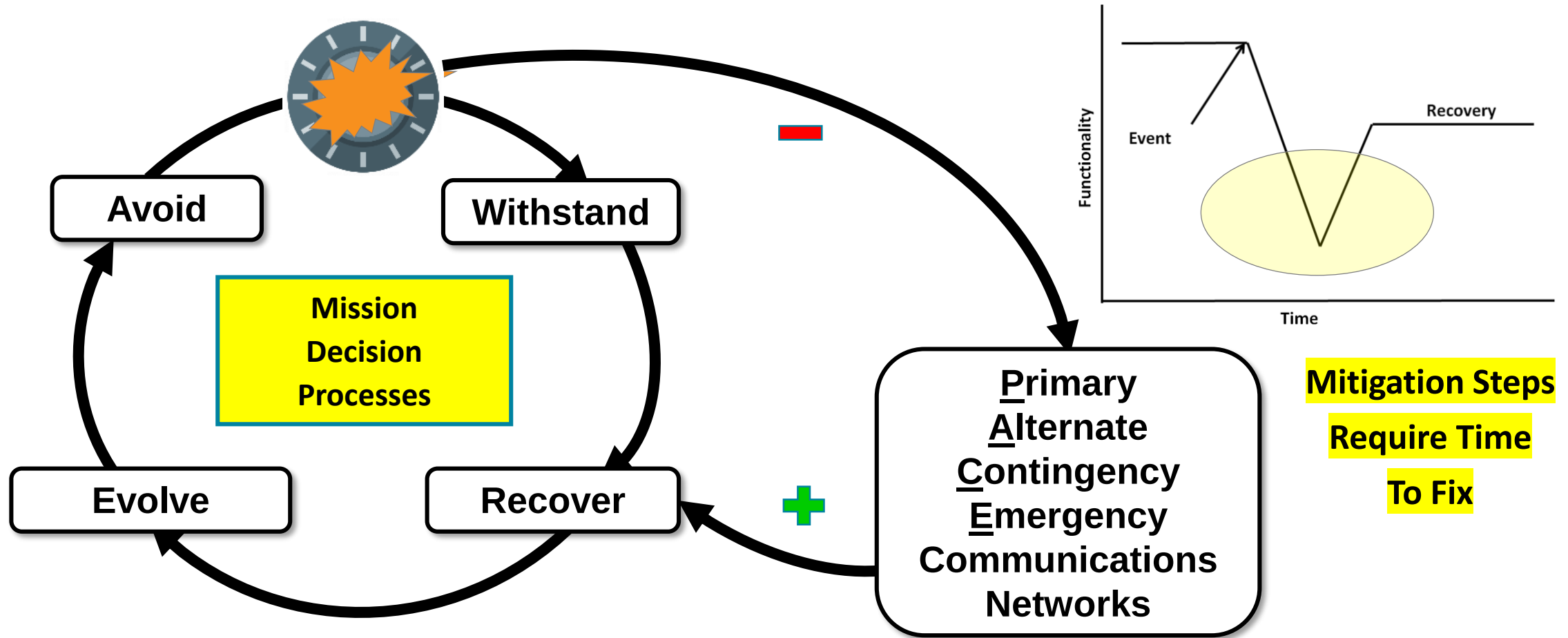
Mitigation Steps – Short-Term or Long-Term Fix



- Other mitigation steps need to be considered: People, Processes and Technology

A Systems Thinking Model – An Iterative Process

Execute PACE Plan



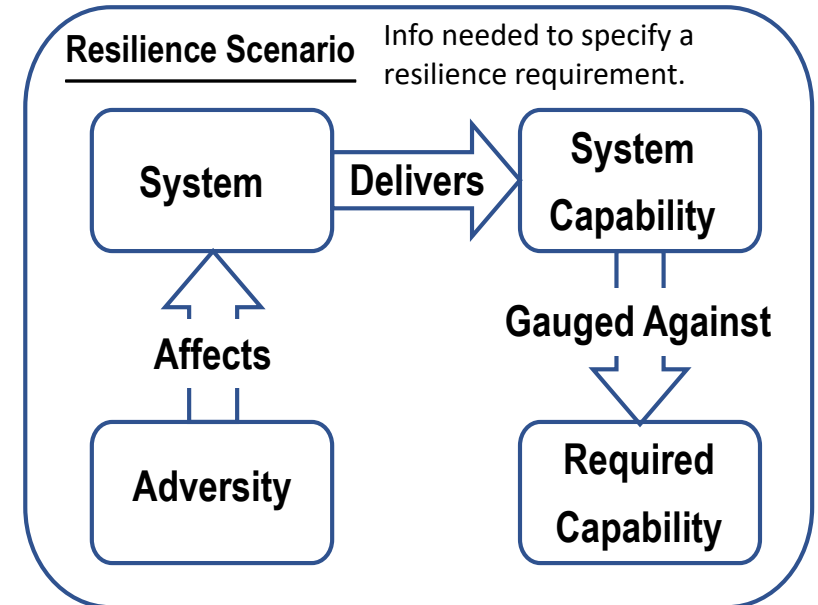
- When mitigation steps take time, execute PACE Plan to Recover

Determine Resiliency Requirements

Determine Resilience Requirements

- **Resilience requirements are crafted from the parameters in the resilience scenario**

- Adversity event considered
- System capability of interest
 - A system can deliver several capabilities
- Required capability (performance target)
 - Performance measure of the required capability
- Timeframe of interest
- Required resilience of the capability
 - Example: availability, maximum allowed degradation



Some Example Resilience Requirements

- In the event that electric power to a Hospital is lost: Backup power to all critical circuits shall be available within 300ms and available for up to 72 hours without any external sources of fuel. This shall be achieved with a 99.9% confidence.
- In the event that an end-user device (e.g. radio) is broken or lost: Spare parts or a complete replacement capability shall be made available within 24 hours. Mean time to repair shall take on average no more than 30 minutes to accomplish.
- In the event that communications connectivity for end user device is lost: Alternative communications capabilities or transport paths shall be provided at multiple geographical locations with inter-supporting systems to ensure that communications continue (i.e. no single points of failure).
- In the event that enterprise services provided from a data center fail: Enterprise services shall be locally hosted or forward deployed to ensure mission essential services are provided to support mission essential functions.

Summary

- **Operational decision processes and the ability to execute the mission dictates what resources are important.**
- **Systems Thinking can be used to holistically investigate adverse events and the resilience of your architecture to mitigate the risks.**
- **Adverse events will drive mitigation strategies and alternative communication and network capabilities.**
- **Having an informed understanding of resilience requirements can guide future investment decisions.**



MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Learn more www.mitre.org

