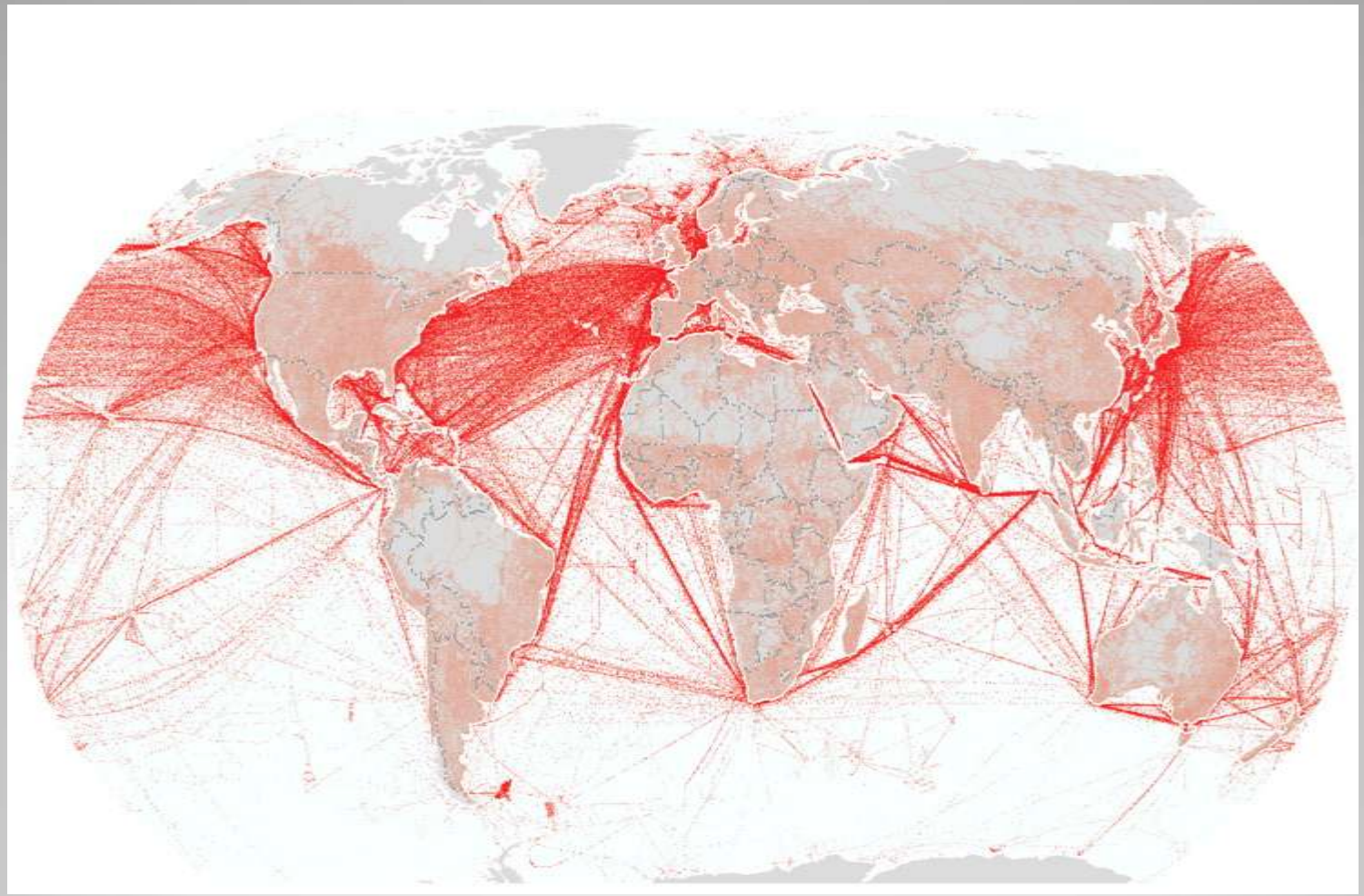
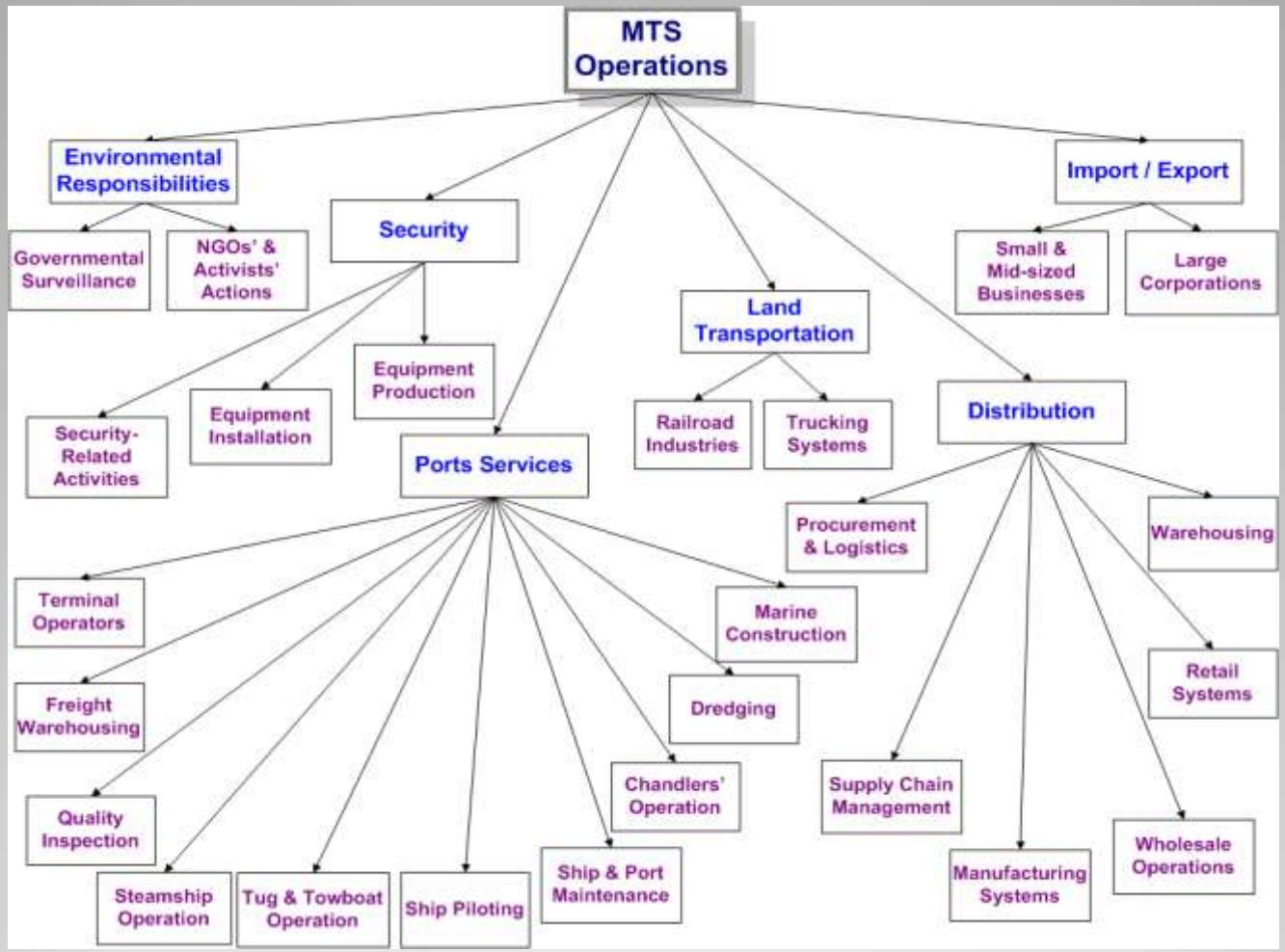
System Resilience

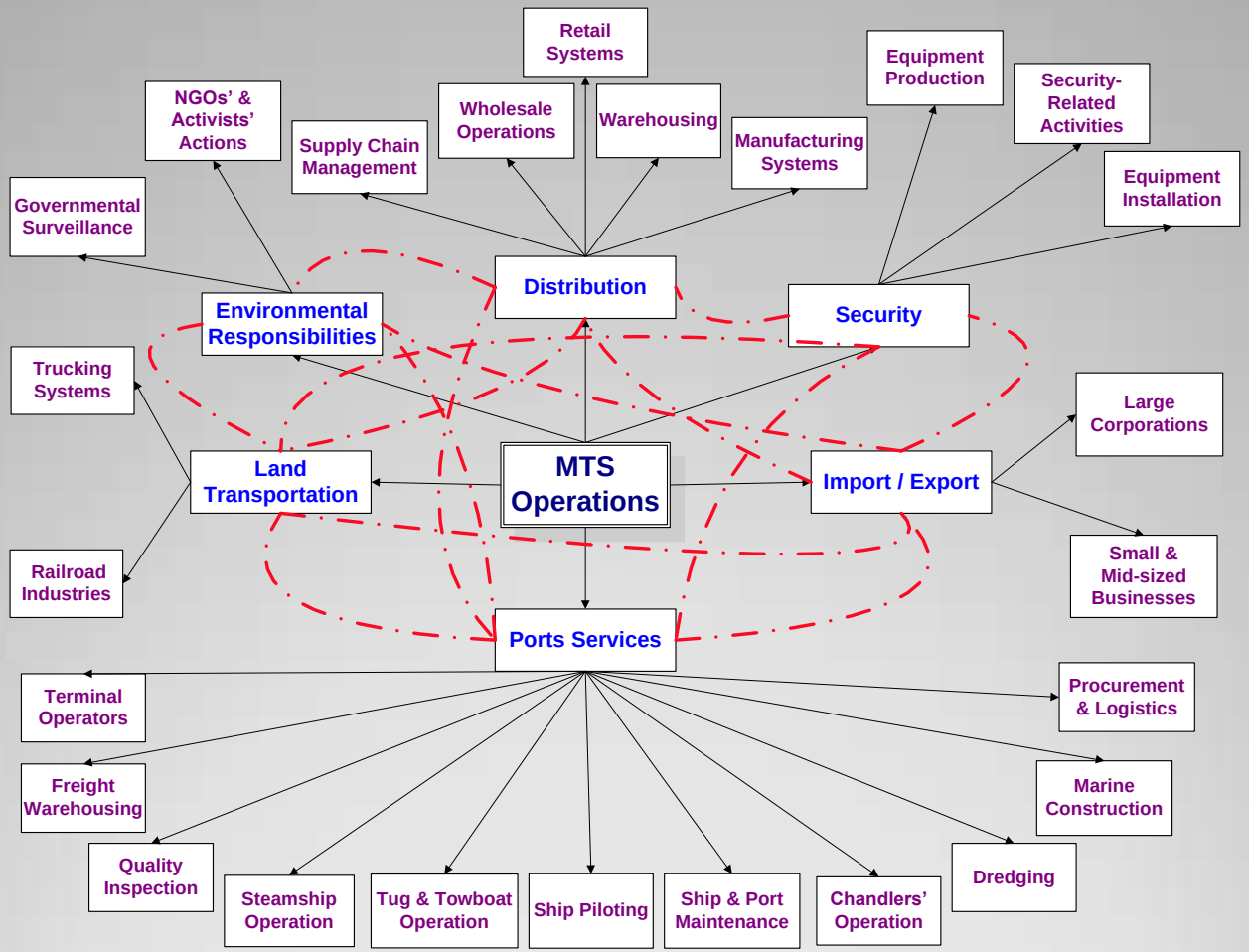
Brian Sauser, Ph.D.
Stevens Institute of Technology
Center for Secure and Resilient Maritime Commerce
Hoboken, NJ, USA



Global Shipping Network



Hierarchy of Operational Roles



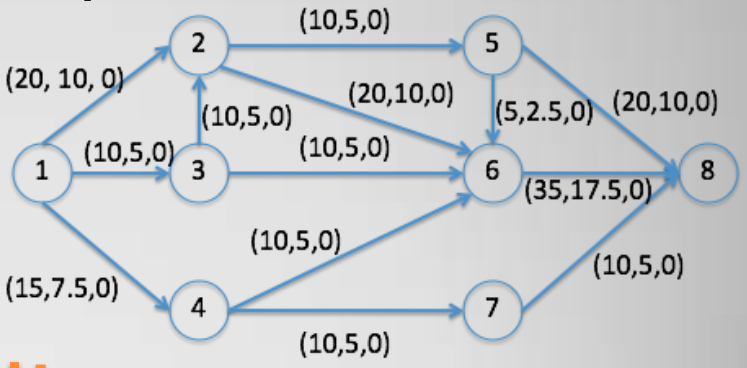
Holarchy of Operational Roles

Key Research Questions

- **What is System Resilience?** The word resilience has its origins in the Latin word "resiliere", which can be described as to "bounce back".
- **What does System Vulnerability describe?** From the latin vulnerare, which is defined as open to attack or damage
- **What is the relationship of System Resilience & Vulnerability to System Protection Approaches?**

Vulnerability & Resilience

- **System Vulnerability**: Describes how the delivery function of a network is affected by external failure events
- **System Resilience**: Describes how the delivery function of a network returns to "normalcy" after a vulnerable event
- *Protection Policies are developed to Increase reliability, reduce vulnerability and increase resilience*



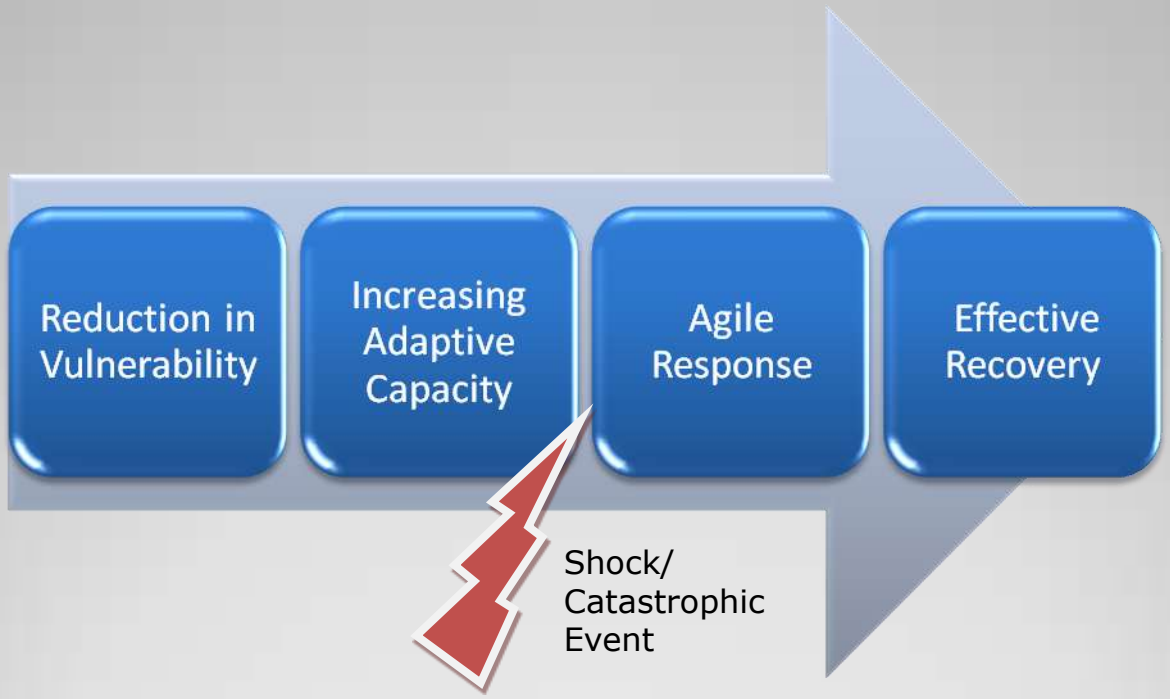
Characteristics of Resilience

- The capability of a system to provide and maintain an **acceptable level of service** in the face of major changes or **disruption**
- The ability of a system to be **less susceptible to disruption**, and be able to **recover** from major sudden changes by returning back to a near **original service** delivery level
- The main characteristics of resilience are:
  - Less vulnerability to disruption
  - Ability to absorb external shocks and return back to an acceptable service level timely

- Resilience can be defined as a function of vulnerability and adaptive capacity.
- In order to make a system more resilient, we want to:
  - Reduce the likelihood of disruption (minimize system's vulnerability)
  - Manage the consequences (maximize the adaptive capacity)

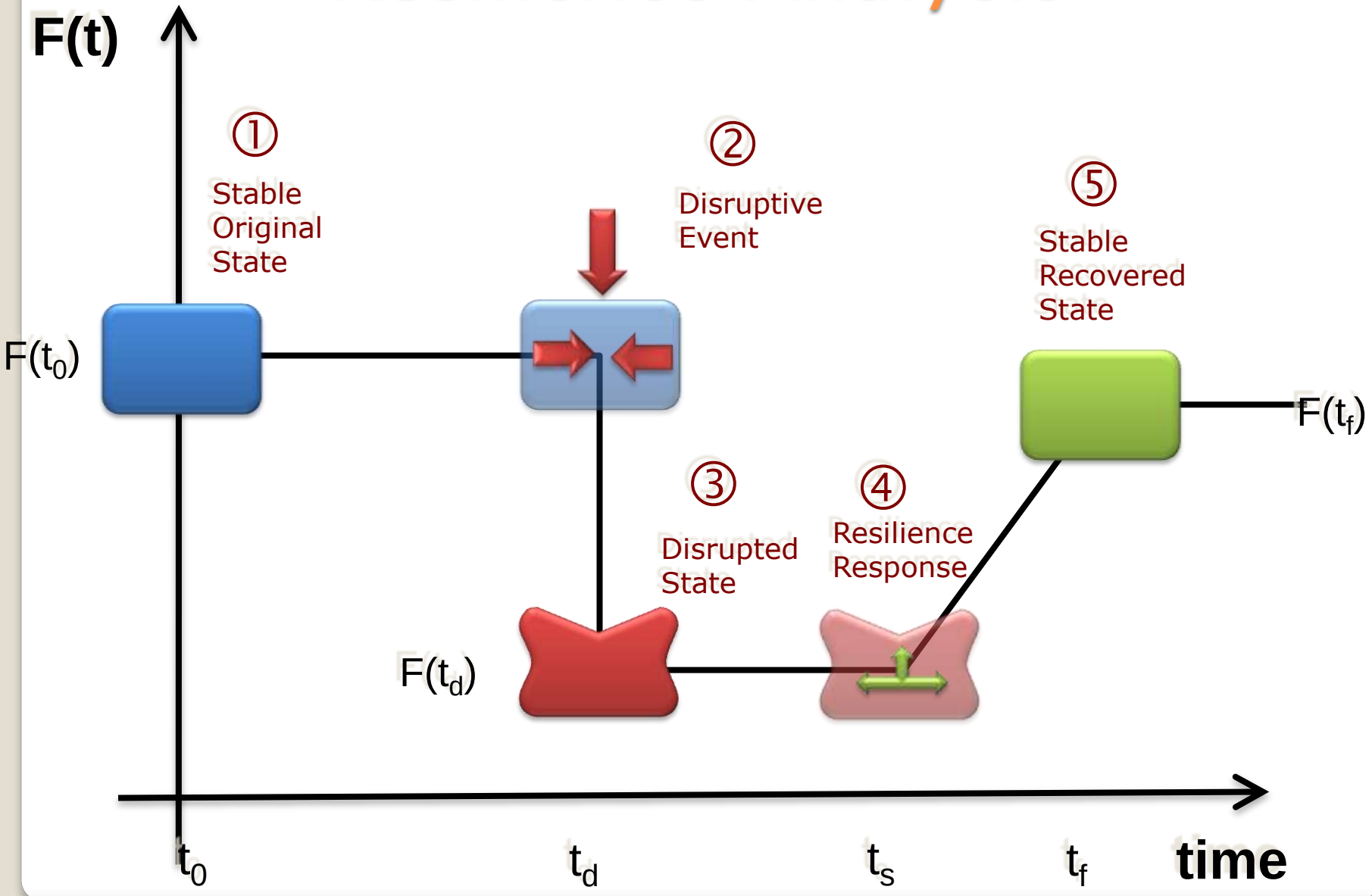
Resilience in a System

To withstand damage or disruption, and if affected, by major non-catastrophic failures can be readily and cost-effectively restored.

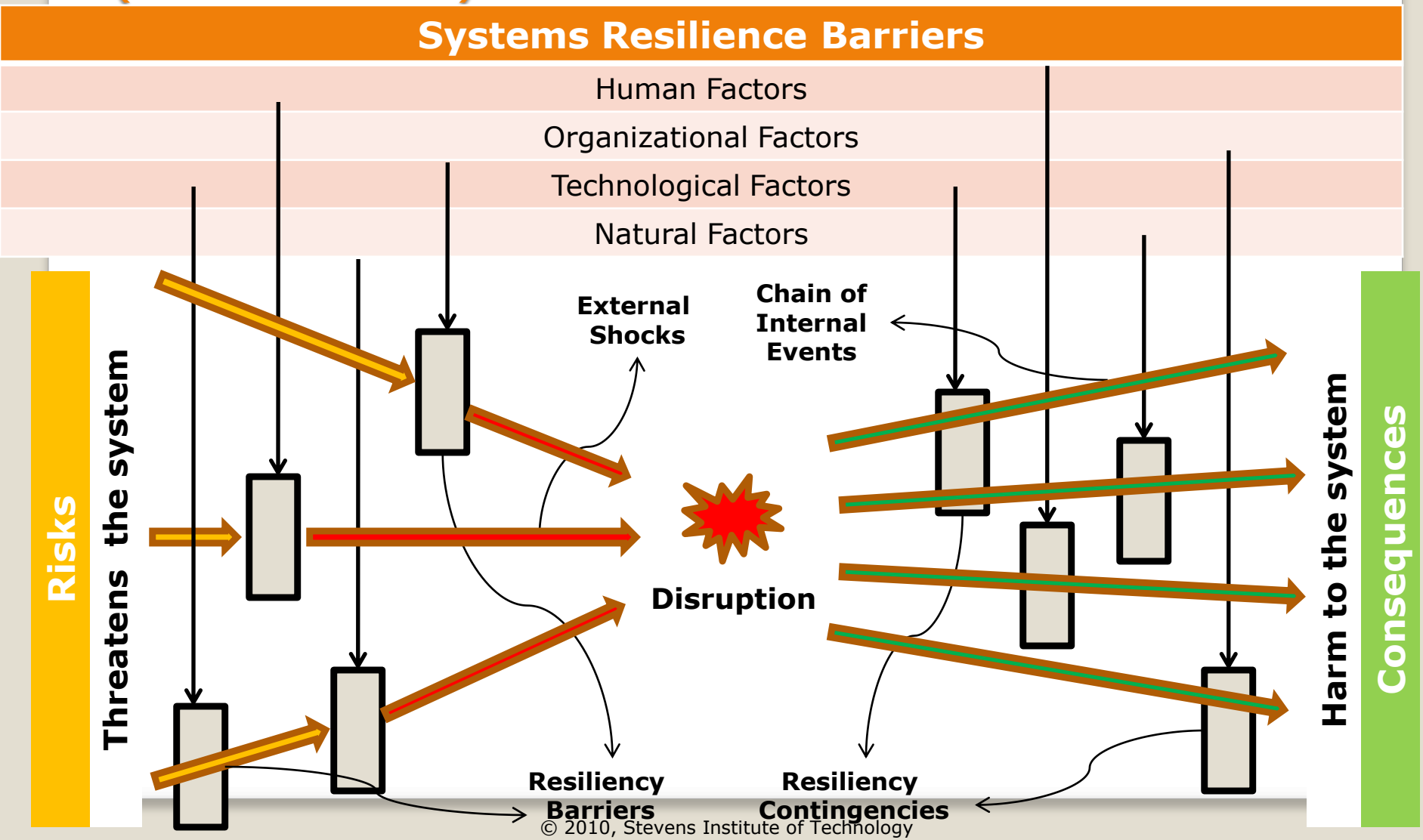


Resilience therefore depends both on the *vulnerability* of a system to major disruptions, and its *adaptive capacity* to recover.

Resilience Analysis

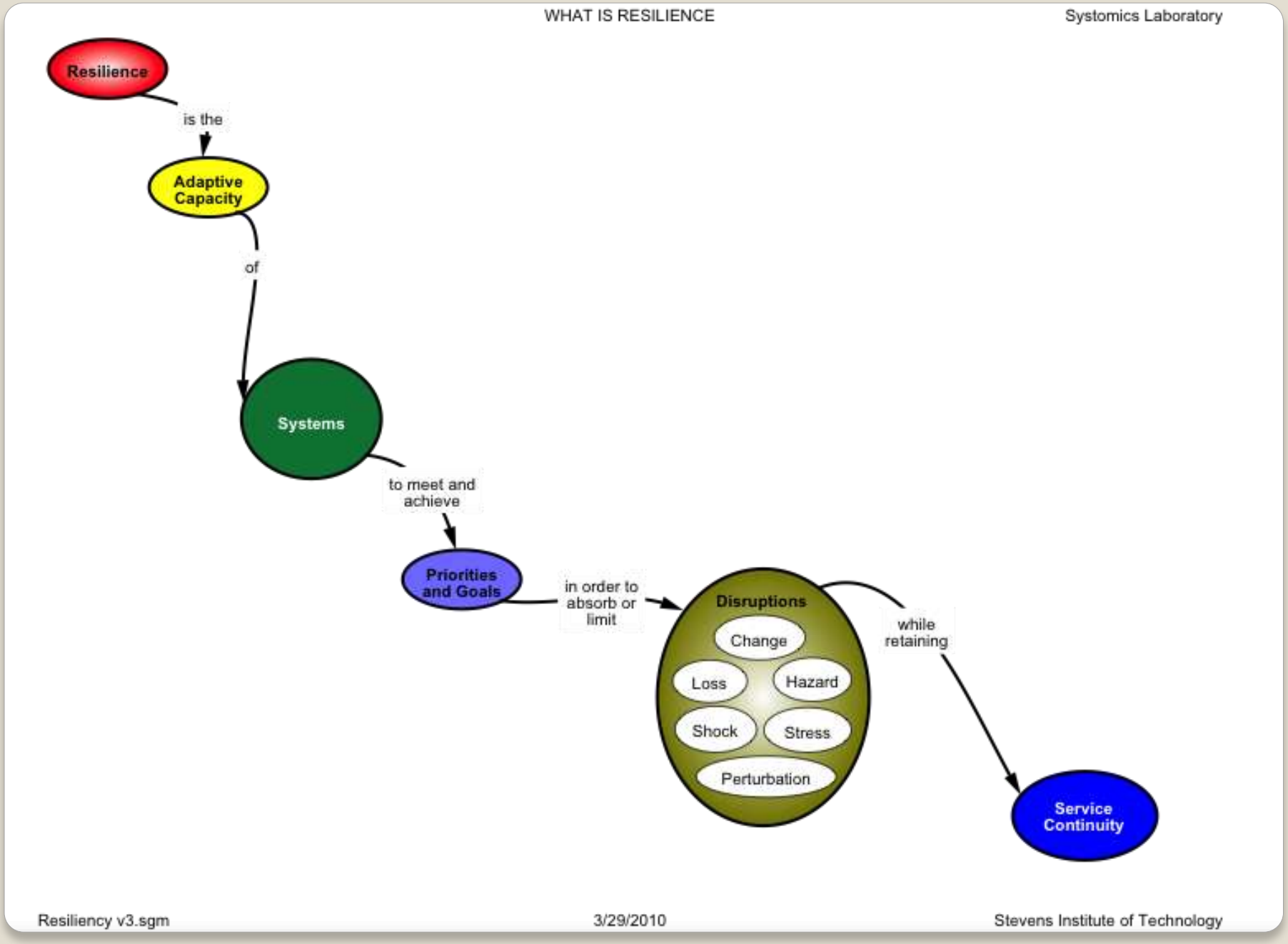


Disruption Scenario and Resilience (Bowtie Model)

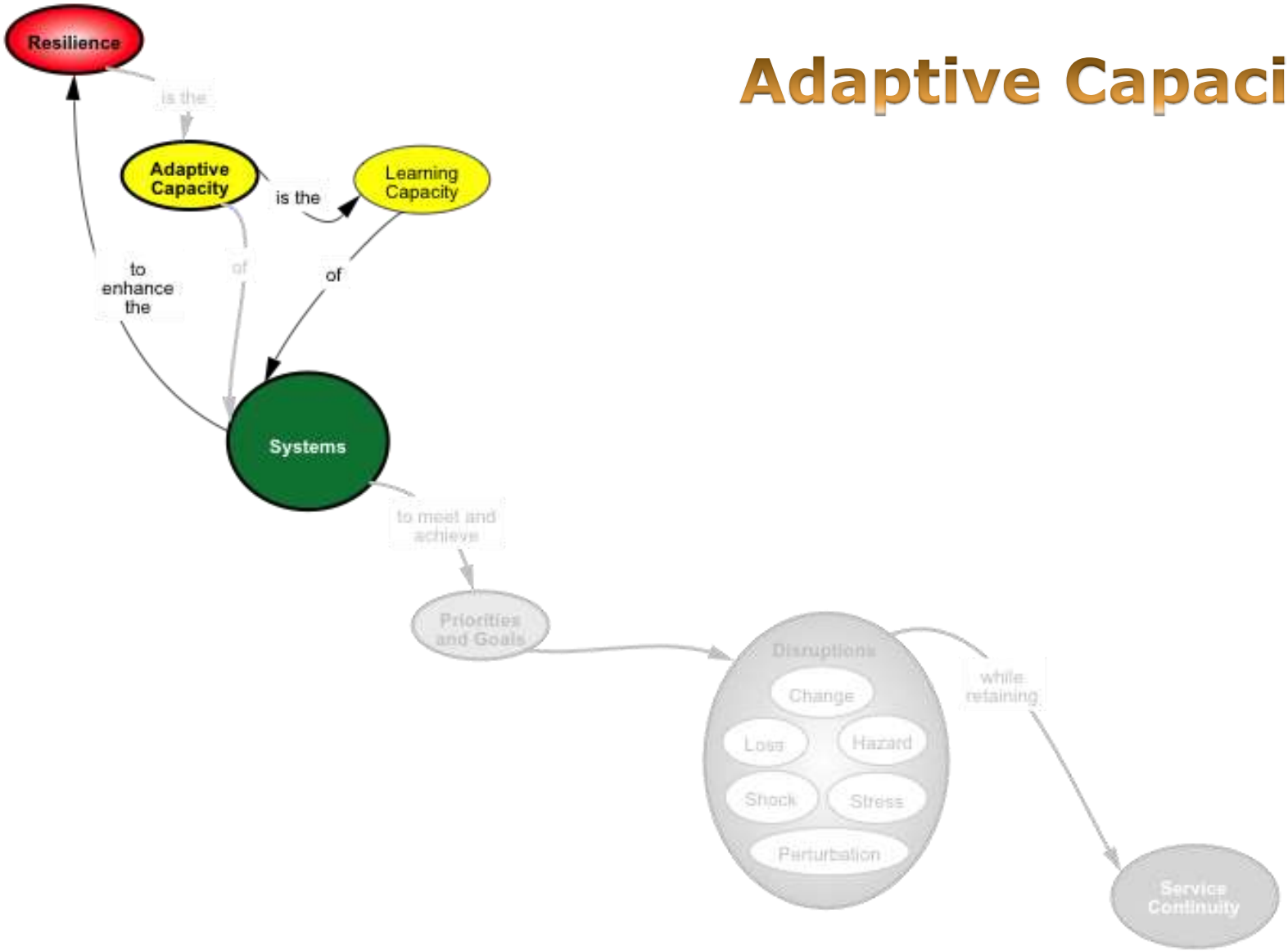


Raising Resilience Factors

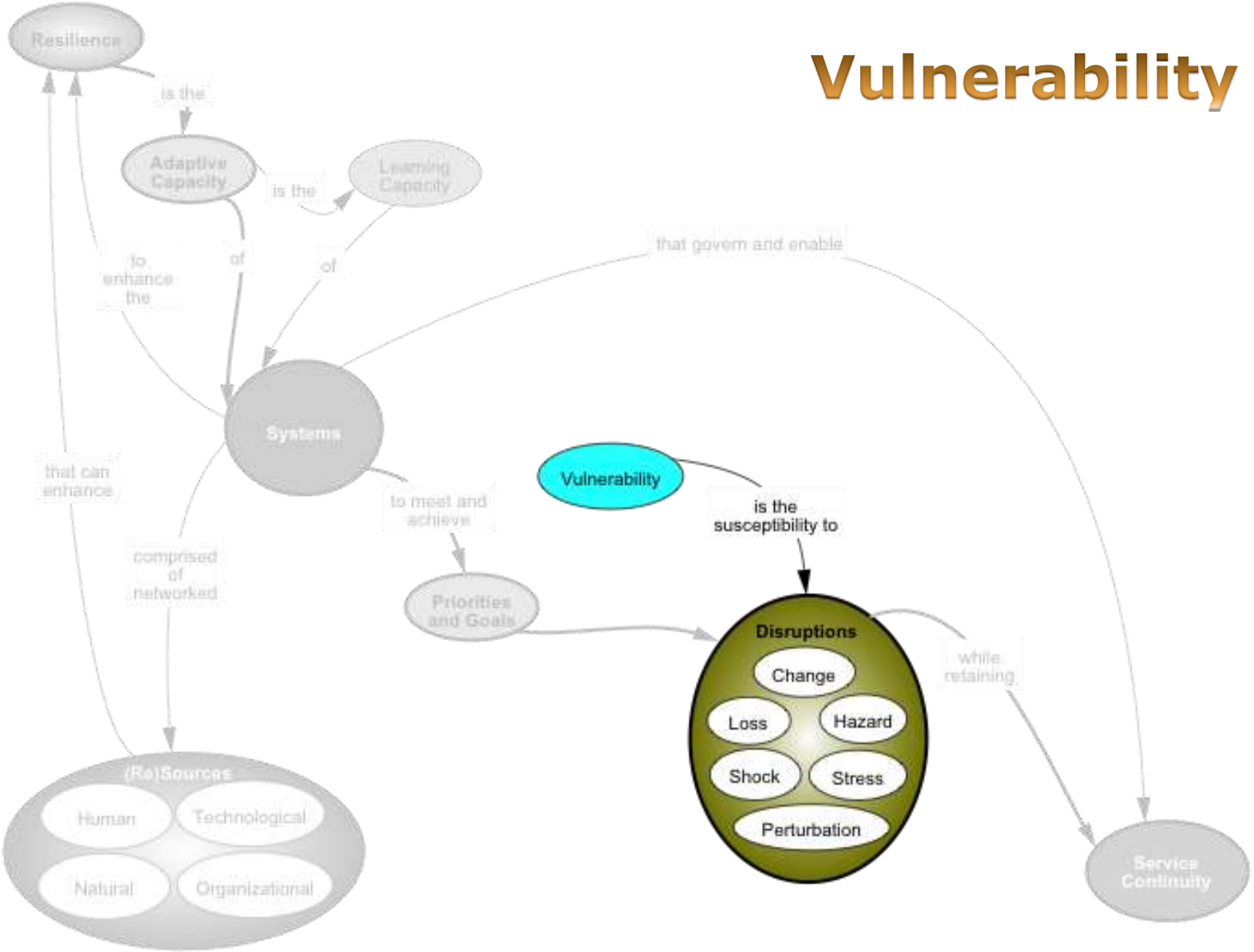
	Human Factors	Organizational Factors	Technological Factors	Natural Factors
Systems Resilience Barriers and Contingencies	Human error analysis	Effective communication	MIS & DSS	Meteorology
	Decision-making models development	Systematic documentation	Security instruments & system	Prediction of natural incidents
	Educational systems and training	Instructions & manuals	Surveillance technology	Analysis of existing data and occurrence likelihood
	Flow of Information	Clarity of responsibilities	Integrated intelligent security systems	Crisis management,
	Ergonomic design	Integration among stakeholders	Security maritime domain from Sky or under water	Recovery and Mitigation
		Clarity of rules, regulations & laws	Geographical information system	Markovian plots



Adaptive Capacity



Vulnerability



Disruptions