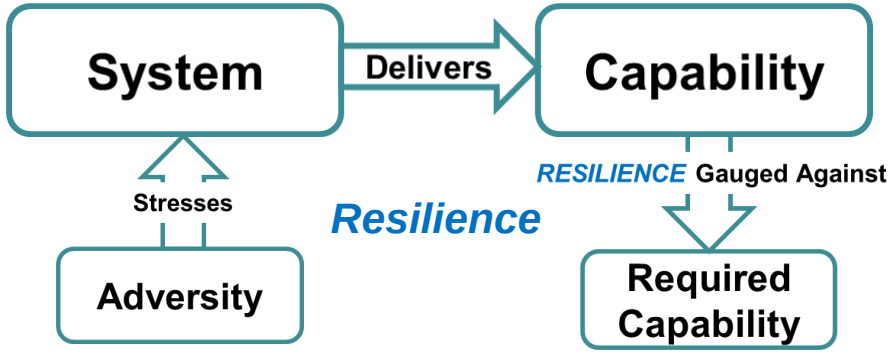
Resilience in Today's and Tomorrow's Systems

Mr. Kenneth L. Cureton (Ken)

- Professional Societies (Senior Member): AIAA, INCOSE, IEEE
  - **INCOSE Resilient Systems Working Group (RSWG) chair**
  - AIAA Space Settlement Technical Committee (SSTC) member
  - IEEE SMC former co-chair MBSE Working Group
  - Network-Centric Operations Industry Consortium (NCOIC) Technical Council Chair Emeritus
- Senior Systems Engineer (Retired) for The Boeing Company
  Huntington Beach CA— Boeing Defense, Space, & Security: Phantom Works
  - 29 years in Manned Space, Launch Systems, Satellite Systems, Networked Systems, Cyber Security, and Defense Conversion
- Previously employed as a Computer Hardware/Software Engineer and Manager for 17 years: Government and Small Business Sectors
- Part-Time Adjunct Lecturer at the University of Southern California (USC) Viterbi School of Engineering, Systems Architecting & Engineering (SAE) Program
- Formal Education:
  - BS in High-Energy & Nuclear Physics
  - MS in Systems Architecting & Engineering

What is System Resilience?

System Resilience is the ability of an Engineered System to provide required capability when facing adversity



- **As defined by International Council on Systems Engineering (INCOSE) Resilient Systems Working Group (RSWG)**
  - **Definition is limited to human-made systems containing software, hardware, humans (e.g., socio-technical), infrastructures, concepts, and processes**

Source: INCOSE RSWG https://www.incose.org/communities/working-groups-initiatives/resilient-systems

What Adversities?

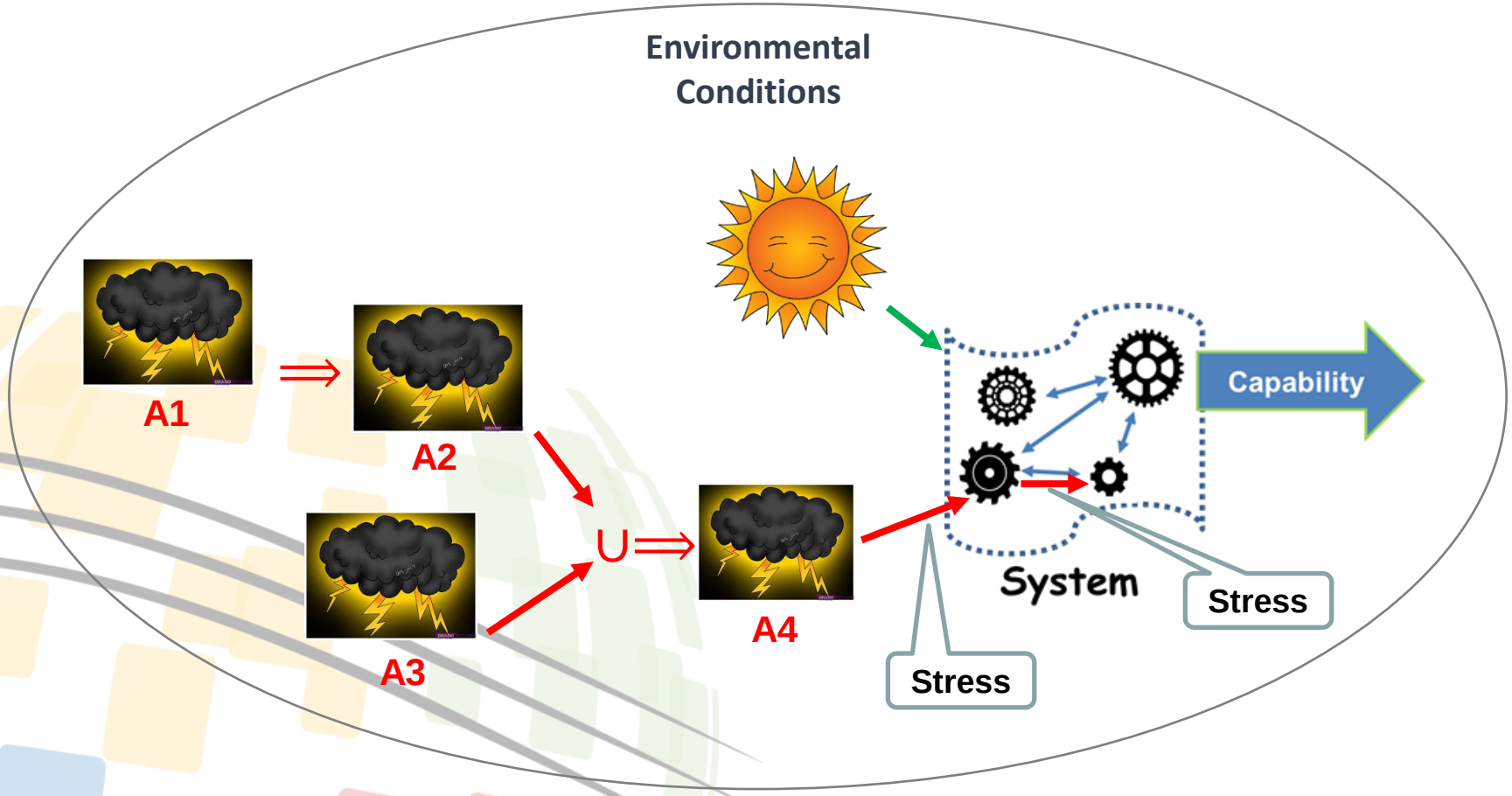
Adversity is ANY condition that may degrade the desired capability of a system

- **Should consider all sources and types of adversity:**
  - **Environmental sources**
  - **Normal failure(s), as well as failures caused by opponents, friendlies and neutral parties**
  - **Adversity from human sources (may be malicious or accidental)**
  - **Adversities may be expected or not**
  - **Adversity may include "unknown unknowns"**
  - **A single incident may be the result of multiple adversities, such as a human error committed in the attempt to recover from another adversity**

Source: INCOSE Systems Engineering Body of Knowledge (SEBoK) https://sebokwiki.org/wiki/System_Resilience (see SEBoK System Resilience section references for more details)

System Resilience to Adversity (or Adversities)

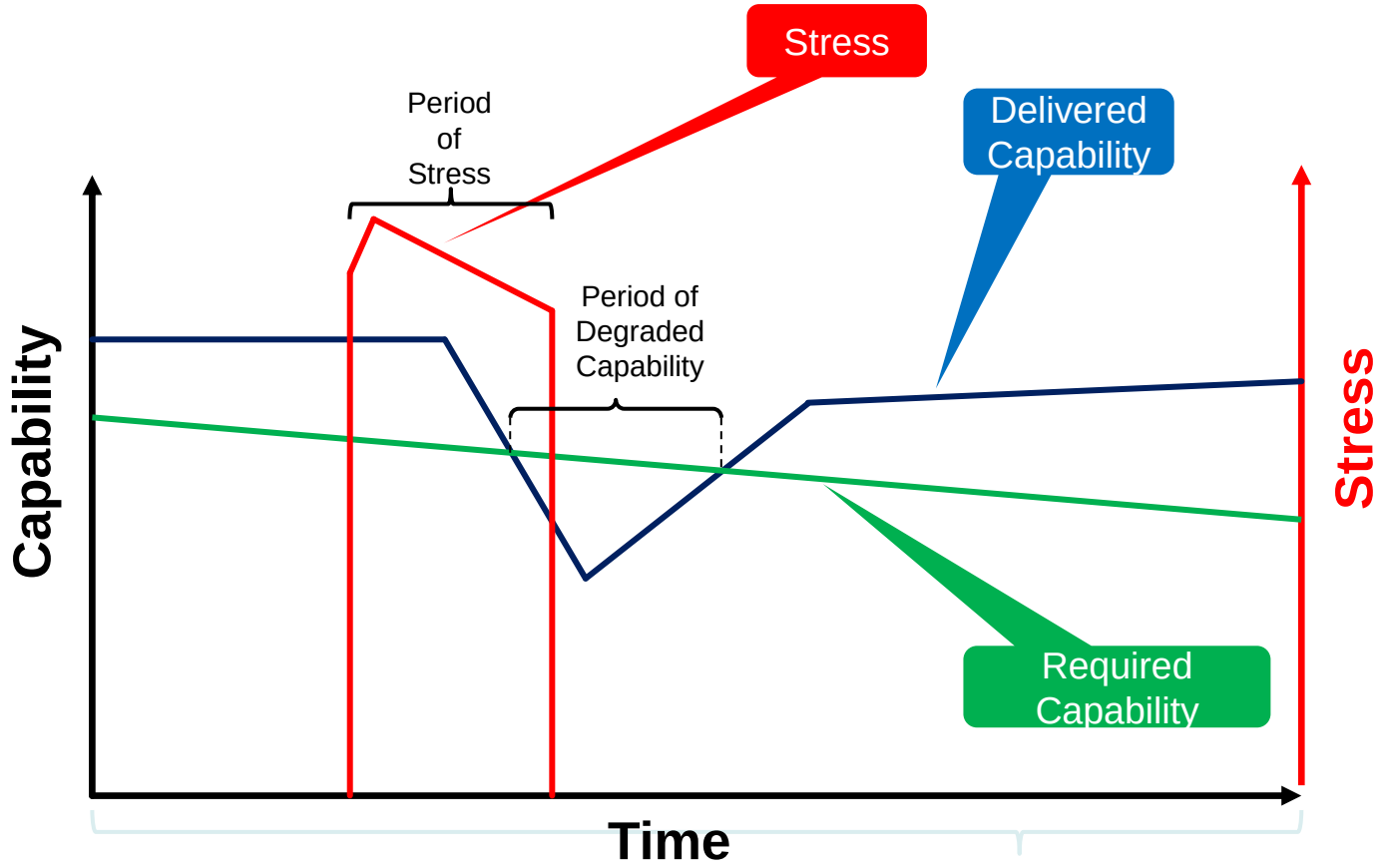
Causal Chains of Adversity may lead to Stress on the System



Source: John S. Brtis Paper #22 presented at 2022 Annual INCOSE Western States Regional Conference

System Resilience to Adversity (or Adversities)

Hypothetical Scenario over some Period of Interest



Source: John S. Brtis Paper #22 presented at 2022 Annual INCOSE Western States Regional Conference

Resilience Requirements

The following information is often part of a resilience requirement:

- **Capability(s) of interest with their metric(s) and units**
- **Target value(s); i.e., the required amount of the capability(s)**
- **System modes of operation, e.g., operational, training, exercise, maintenance, and update and related states for each mode of operation**
- **Adversity(s) being considered, their source, and type**
- **Potential stresses on the system, their metrics, units, and values**
- **Resilience-related scenario constraints, e.g., cost, schedule, policies, and regulations**
- **Timeframe and sub-timeframes of interest**
- **Resilience metric, units, determination methods, and resilience metric target**
  - **Example metrics: expected availability of required capability, maximum allowed degradation, maximum length of degradation, and total delivered capability**
  - **There may be multiple resilience targets, e.g., threshold and objective**
  - **Resilience metrics are often strains on the system; i.e., the effects of stress on the system**

Source: INCOSE Systems Engineering Body of Knowledge (SEBoK) https://sebokwiki.org/wiki/System_Resilience (see SEBoK System Resilience section references for more details)

Achieving System Resilience

- **The Three Objectives to obtain the Value of Resilience: (Taxonomy Layer 1)**
  - ***Avoid*** **adversity**
  - ***Withstand*** **adversity**
  - ***Recover*** **from adversity**
- **Means of achieving Objectives: (Taxonomy Layer 2)**

• *Adaptive Response*	• *Integrity*	• *Tolerance*
• *Agility*	• *Manage Complexity*	• *Transform*
• *Anticipation*	• *Prepare For*	• *Understand*
• *Constrain*	• *Prevent*	
• *Continuity*	• *Re-architect*	
• *Disaggregation*	• *Redeploy*	
• *Evolution*	• *Robustness*	
• *Graceful Degradation*	• *Situational Awareness*	

Source: INCOSE Systems Engineering Body of Knowledge (SEBoK) https://sebokwiki.org/wiki/System_Resilience (see SEBoK System Resilience section references for more details)

Achieving System Resilience (continued)

Taxonomy Layer 3: ***Architecture, Design, & Operational Techniques to Achieve Resilience Objectives***

- *absorption*
- *buffering*
- *defense in depth*
- *diversification*
- *dynamic representation*
- *internode interaction & interfaces*
- *modularity*
- *physical & functional redundancy*
- *protection*
- *repairability*
- *segmentation*
- *threat suppression*
- *analytic monitoring & modeling*
- *coordinated defense*
- *detection avoidance*
- *drift correction*
- *effect tolerance*
- *least privilege*
- *neutral state or safe state*
- *privilege restriction*
- *realignment*
- *replacement*
- *substantiated integrity*
- *unpredictability*
- *boundary enforcement*
- *deception*
- *distribution*
- *dynamic positioning*
- *human participation*
- *loose coupling*
- *non-persistence*
- *proliferation*
- *reconfiguring*
- *restructuring*
- *substitution*
- *virtualization*

Source: INCOSE Systems Engineering Body of Knowledge (SEBoK) https://sebokwiki.org/wiki/System_Resilience (see SEBoK System Resilience section references for more details)

Things that Potentially Frustrate Resilience (Sample)

Name	Description	Examples	How it Frustrates Resilience
Common mode failures	Failures of the same mode, failures that have an identical appearance or effect	Wind turbines: if one trips due to frozen blades it is likely that others will too	Undermines physical redundancy
Common cause failures	Failures having the same underlying cause	Texas cold snap caused wind turbines, natural gas, coal and nuclear power plants to fail due to sub-freezing temperatures	Undermines both physical and functional redundancy
Just in time resourcing	System consumables are delivered just-in-time, without buffering storage at the site of the system	Natural gas power stations went down because their fuel supply was interrupted	Lack of buffering leads to a fragile point of failure if supply is interrupted
Unnecessary complexity	Many systems do have some complex characteristics, but complexity in solutions that is not necessary to achieve system functions is likely to impair resilience	System "Work-around" solutions on top of prior "work-around" solutions to deal with design evolution due to parts obsolescence; design patches; fixing mis-matches due to changes in organization or operational needs	Unnecessary complexity can create unrecognized vulnerabilities or weaken the basic functionality under certain stressful conditions. In Complex systems, may also result in an increased incidence of detrimental emergent behavior, and thus loss of trust for use of that system

Source: INCOSE Resilient Systems Working Group (Work In Progress)

Potential Resilience Metrics for Modeling

- **Maximum adversity period and depth**
- **Expected value of capability: the probability-weighted average of capability delivered**
- **Threat resiliency-- the time integrated ratio of the capability provided divided by the minimum needed capability**
- **Expected availability of required capability-- the likelihood that for a given adverse environment the required capability level will be available**

$$R = \sum_{1}^{n} \left(\frac{P_i}{T} \int_{0}^{T} Cr(t)_i, dt \right)$$

R = Resilience of the required capability (*Cr*);
n = the number of exhaustive and mutually exclusive adversity scenarios within a context (*n* can equal 1);
P_i = the probability of adversity scenario *i*;
$Cr(t)_i$ = time wise availability of the required capability during scenario *i:* 0 if below the required level, 1 if at or above the required value. Where circumstances dictate this may take on a more complex, non-binary function of time;
T = length of the time of interest.

Source: INCOSE Systems Engineering Body of Knowledge (SEBoK) https://sebokwiki.org/wiki/System_Resilience (see SEBoK System Resilience section references for more details)

Potential Resilience Metrics for Modeling (continued)

- **Resilience levels-- the ability to provide required capability in a hierarchy of increasingly difficult adversity**
- **Cost to the opponent**
- **Cost-benefit to the opponent**
- **Resource resiliency-- the degradation of capability that occurs as successive contributing assets are lost**

Source: INCOSE Systems Engineering Body of Knowledge (SEBoK) https://sebokwiki.org/wiki/System_Resilience (see SEBoK System Resilience section references for more details)

Modeling, Measuring, & Evaluating System Resilience

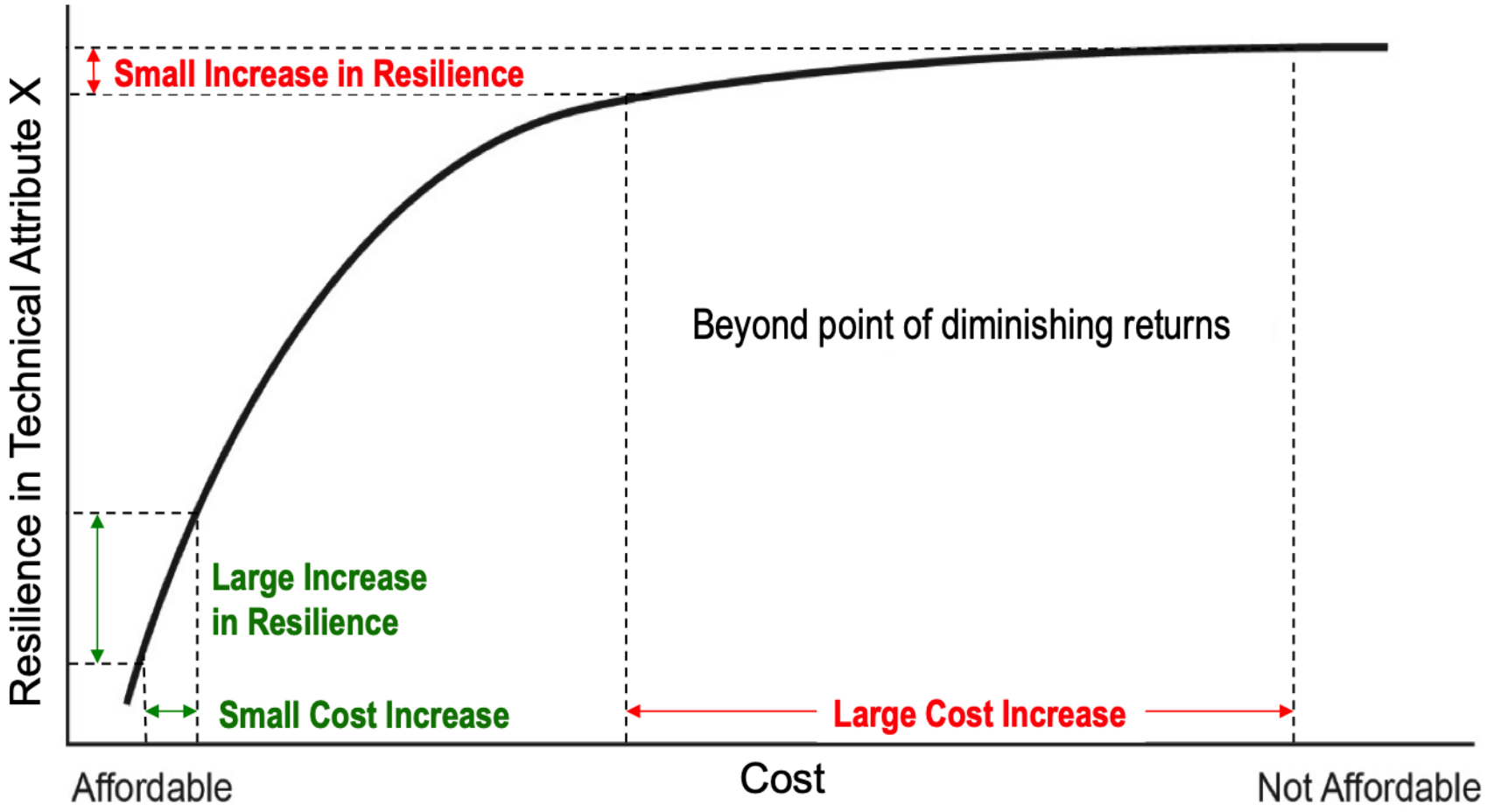
A system resilience model represents a selective abstraction of a system to provide the required capability when facing adversity within the system and its environment

Two representative resilience modeling techniques which could be applied to Model-Based Systems Engineering (MBSE), Digital Engineering (DE), and Digital Twins:

- **Formal Methods of Constructing Models for Systems Resilience—Resilience Contracts**
  - **Resilience Contracts (RC) are an upgrade to the widely used Contract-Based Design (CBD) approach**
  - **However, many modern systems do not always behave predictably-- To handle this, an RC is a mathematical model that extends CBD to account for uncertainty and unpredictability**
- **Application of System Dynamics**
  - **System Dynamics is suitable for resilience modeling because it captures behavior over time, and Resilience takes a behavior over time perspective (as shown on slide 6)**
  - **Modelling activities produce Causal Loop Diagrams which demonstrate the feedback structure in a system in which a change in one component can ripple through the other connected components in the design and return to the original part in a reinforcing way that can lead to catastrophic failure or in a balanced way that can lead to stability and recovery from adversity**

Source: INCOSE Systems Engineering Body of Knowledge (SEBoK) https://sebokwiki.org/wiki/Resilience_Modeling (forthcoming)
(see SEBoK Resilience Modeling section references for more details)

Affordable Resilience



Modified from Source: Marilee J. Wheaton "Resiliency and Affordability Attributes in a System Integration Tradespace" AIAA Space 2015 Pasadena, CA

Source: INCOSE Systems Engineering Body of Knowledge (SEBoK) https://sebokwiki.org/wiki/System_Resilience (see SEBoK System Resilience section references for more details)

Discipline Relationships

- **Resilience has commonality and synergy with a number of other quality areas**
- **Examples include availability, environmental impact, survivability, maintainability, reliability, operational risk management, safety, security and quality**
  - **This group of quality areas is referred to as loss-driven systems engineering (LDSE) because they all focus on potential losses involved in the development and use of systems**
  - **These areas frequently share the assets considered, losses considered, adversities considered, requirements, and architectural, design and process techniques**
  - **It is imperative that these areas work closely with one another and share information and decision-making in order to achieve a holistic approach**

Source: INCOSE Systems Engineering Body of Knowledge (SEBoK) https://sebokwiki.org/wiki/System_Resilience (see SEBoK System Resilience section references for more details)

Questions?

Contact Information: Ken Cureton kenneth.cureton@incose.net

For more information, please consult the INCOSE Resilient Systems Working Group web page at: https://www.incose.org/communities/working-groups-initiatives/resilient-systems