Resilience in Modular & Open Architectures

Presented by Mr. Kenneth Cureton to the Defense Acquisition University

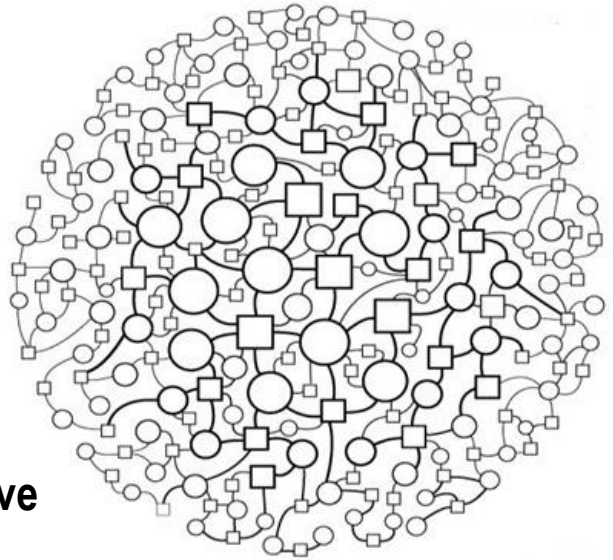
2024 May 09

INCOSE Resilient Systems Working Group and other sources as marked at the bottom of slides

Modular & Open Systems Approach (MOSA)

- **MOSA Provides Many Benefits, as Detailed by Other Presenters**
  - **But also a few challenges!**
- **Today's Presenter, Ken Cureton**
  - ***Not* an expert in MOSA!**
  - **But a Subject Matter Expert (SME) in valuable disciplines that pertain to MOSA, e.g.,**
    - **Resilient Systems Engineering**
    - **Interoperability of Technologies, People, & Processes e.g., MOSA Program Assessment & Rating Tool (PART)**
  - **Information presented is largely based on 40+ years of Systems Engineering experience**
    - **Please consider these as personal views unless cited at the bottom of slides**

Monolithic Approach from a Resilience Perspective



- **Traditional Systems Design**
  - Integration of many tightly coupled components
  - Strengths (from a Resilience perspective)
    - System Security may be stronger as attack surfaces "hidden" behind proprietary interfaces
  - Weaknesses (from a Resilience perspective)
    - Change of any component often requires extensive regression analysis of the whole system
    - Difficult to determine and verify true system performance margins (e.g., change in component technology due to obsolescence or vendors)
    - Challenges in accomplishing Root Cause Corrective Action (RCCA) analysis after system anomalies or failures
    - May constrain agile system development techniques (e.g., must consider system requirements all at once rather than through a discovery/maturity process)

Image Source: George J. Friedman & Phan Phan, "Constraint Theory – Multidimensional Mathematical Model Management" Second Edition, ISBN 978-3-319-54791-8 © Springer International Publishing AG 2005, 2017

MOSA Attributes from a Resilience Perspective (1 of 2)

- **Modular & Open Systems Approach**
  - **"A technical and business strategy for designing an affordable and adaptable system"**
    - **DoD preferred method for implementation of open systems-- required by U.S. Law**
  - **Drawbacks & Challenges**
    (from a Resilience perspective, more on these topics later)
    - ***Potential* Interoperability and System Security challenges due to use of Open Standards at component interfaces**
    - ***May* narrow focus away from the whole System and more on components ("Can't see the Forest through the Trees", "Whole system not in scope")**
    - ***May* result in a more Complicated or even Complex System due to number of modular "components"**
      - **Unlike the Monolithic approach (which may have multiple integrated functions accomplished by each component), MOSA component modules typically accomplish a specific set of small, composable function(s)**

Image Source: Internet Clipart Search

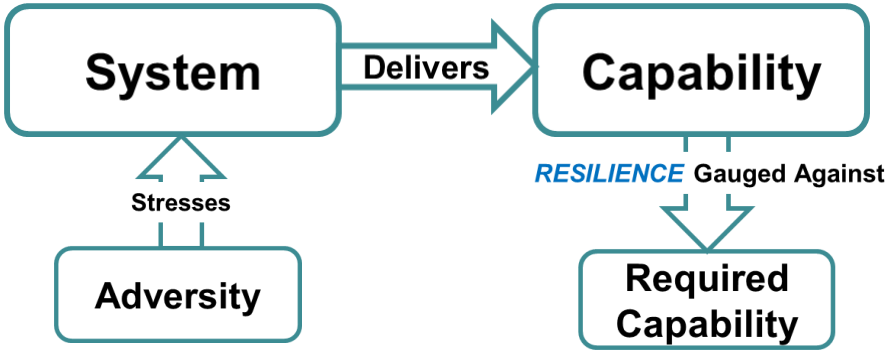
MOSA Attributes from a Resilience Perspective (2 of 2)

- **Modular & Open Systems Approach**
  - General Strengths
    - Open System approach often leverages a wider set of Industry experience & Open Standards
    - *Often* facilitates enhanced attention to details in (and resulting benefits of) Quality Characteristics (formerly known as Specialty Engineering or "Ilities"):
      - Producibility, Availability, Adaptability, Affordability, Interoperability, Reliability, etc.
      - Fault Tolerance (e.g., containment of fault propagation) & resulting Safety improvements
      - System Security (e.g., Defense in Depth)
      - ***System Resilience*** **(the emphasis of remainder of this presentation)**

Image Source: Internet Clipart Search

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 and organizational), infrastructures, concepts, and processes**
  - **INCOSE Systems Engineering Handbook (version 5) and Systems Engineering Body of Knowledge (SEBoK)**
  - **Forthcoming International Standards Organization (ISO) "Systems Resilience"**

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

What Adversities?

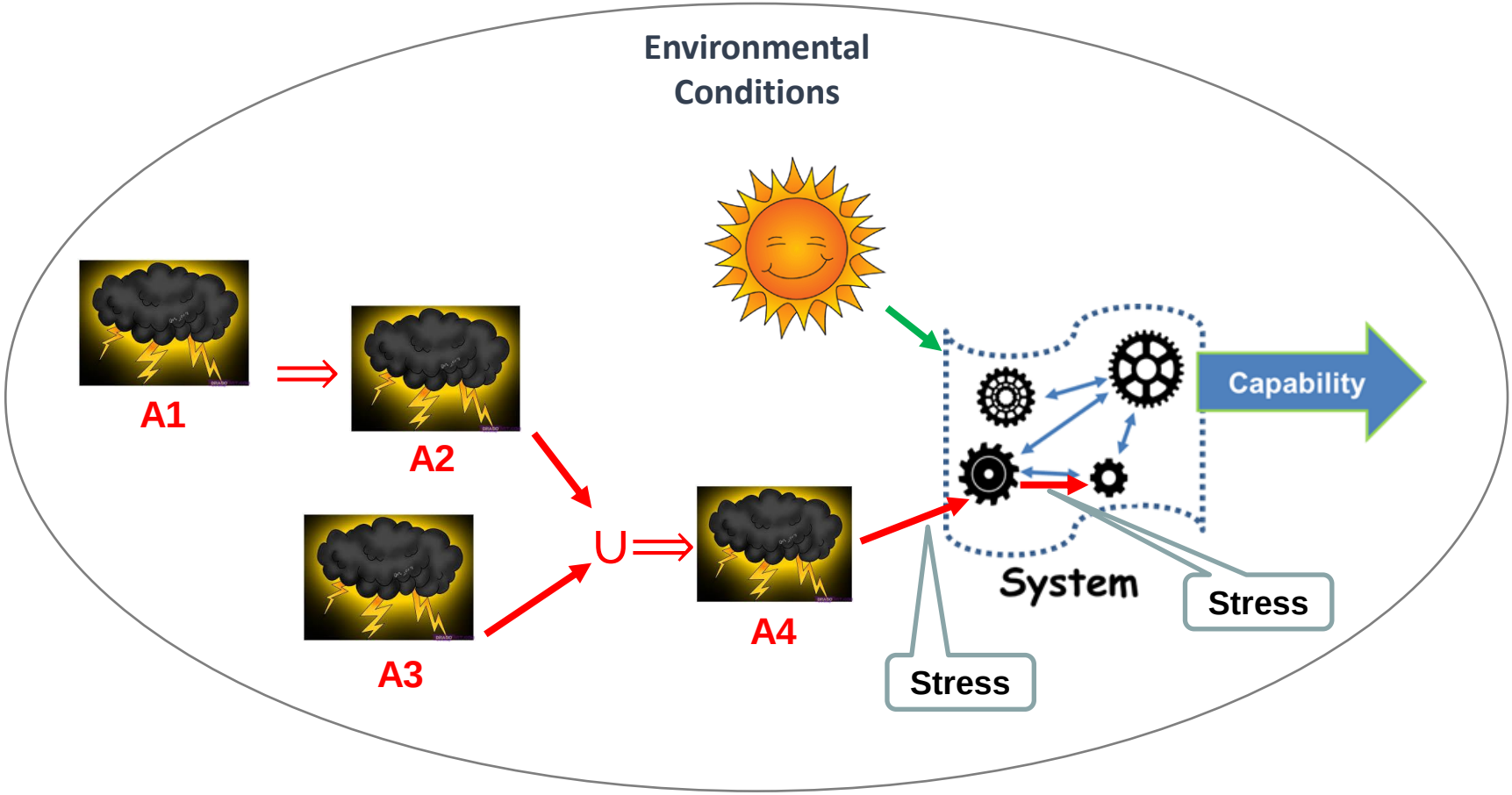
Adversity is ANY condition that may degrade the desired capability of a system

- **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)

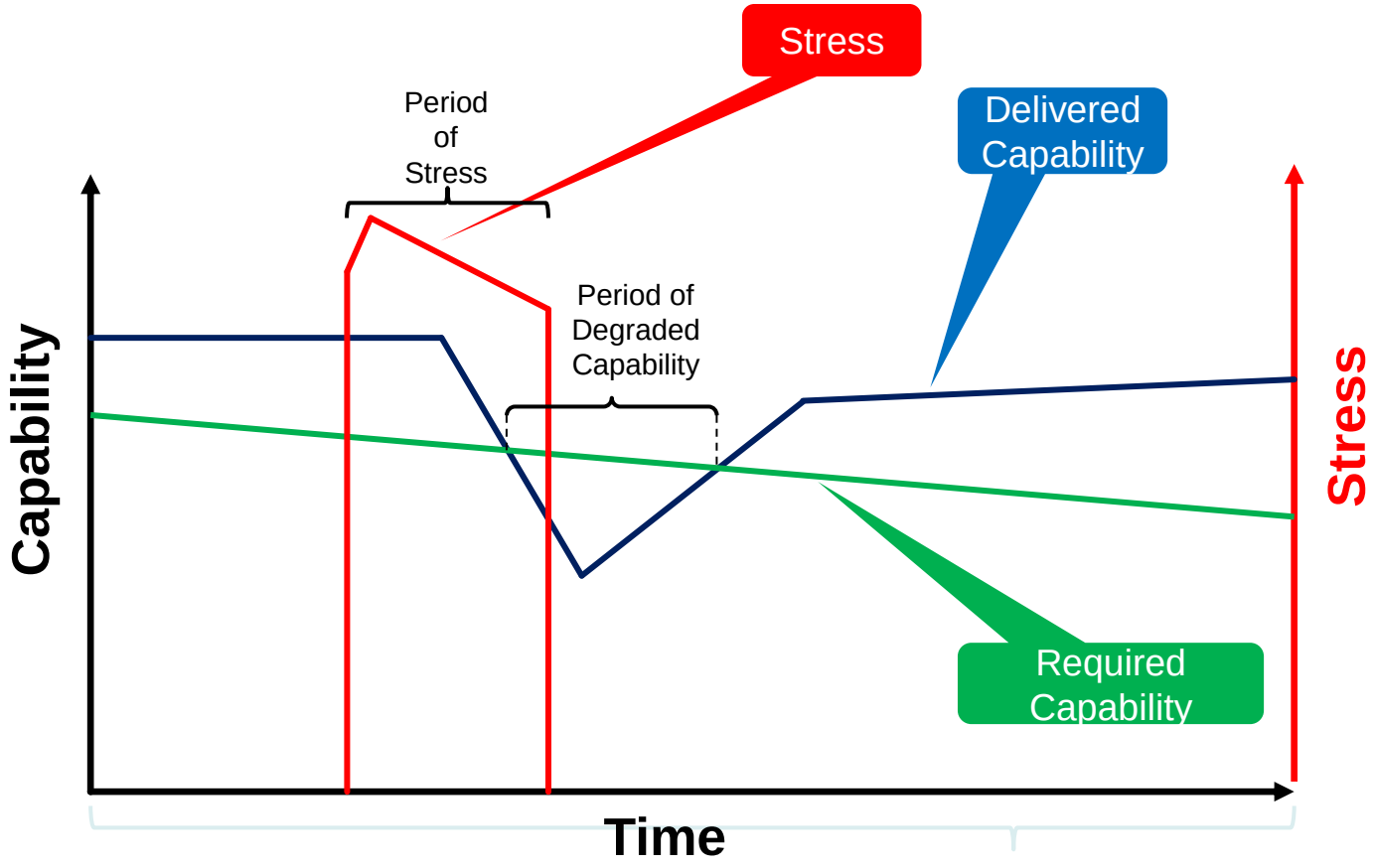
Causal Chains of Adversity may lead to Stress on the System



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

Achieving System Resilience

- **The Three Objectives to obtain the Value of Resilience: (Taxonomy Layer 1)**
  - ***Avoid*** **adversity**
  - ***Withstand*** **adversity**
  - ***Recover*** **from adversity**
- **Controversial!**
  - **Some technical disciplines insist that Resilience is limited to Recovery**
    - **They consider "Avoid" and "Withstand" as *Resistance* to adversity**
    - **Others argue that Resilience is just *Adaptation* to adversity**
- **This Presentation uses the INCOSE RSWG Definitions**

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

Means of Achieving Resilience Objectives (1 of 6)

Taxonomy Layer 2: Means of achieving Objectives

- ***Adaptive Response:*** **reacting appropriately and dynamically to the specific situation to limit consequences, avoid degradation of system capability**
- ***Agility:*** **ability of a system to adapt to deliver required capability in unpredictably evolving conditions**
  - **MOSA architectures allow "swapping out" of modular components over time to adapt the system to changing adversities, operational needs, changing environmental conditions, expanded System missions, evolving technologies (to provide expanded capabilities provided by new technologies or to replace obsolete technologies)**
- ***Anticipation:*** **establishing awareness of the nature of potential adversities, their likely consequences, and appropriate responses, prior to the adversity stressing the system**
- ***Constrain:*** **limit the propagation of damage within the system**
  - **MOSA architectures typically employ modular components with well-defined interfaces, which often provide extra attention to bounds-checking and fault containment methods**

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

Means of Achieving Resilience Objectives (2 of 6)

Taxonomy Layer 2: Means of achieving Objectives

- ***Continuity:*** **endurance of the delivery of required capability, while and after being stressed**
  - **MOSA architectures typically employ modular components with well-defined design techniques and interfaces, which often provide extra attention in characterizing performance margins and stress-handling methods**
- ***Disaggregation:*** **dispersing missions, functions, subsystems, or components across multiple systems or sub-systems**
  - **MOSA architectures "automatically" disperse functionality across modular components**
- ***Evolution:*** **restructuring the system to address changes to the adversity or needs over time**
  - **Same as Agility: MOSA architectures allow "swapping out" of modular components over time to adapt the system to changing adversities, operational needs, changing environmental conditions, expanded System missions, evolving technologies (to provide expanded capabilities provided by new technologies or to replace obsolete technologies)**
- ***Graceful Degradation:*** **ability of the system to transition to desirable states after damage**

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

Means of Achieving Resilience Objectives (3 of 6)

Taxonomy Layer 2: Means of achieving Objectives

- ***Integrity:*** **maintain quality of being complete and unaltered [ISO 13008:2012, 3.11]**
  - **MOSA architectures typically employ self-monitoring modular components that may detect unwanted modifications or loss of correct functionality through Contract-Based Design, Resilience Contracts, etc.**
- ***Manage Complexity:*** **leveraging value-added characteristics of complexity (e.g., Complex Adaptive Systems; Emergent Behavior) while suppressing their detracting characteristics**
  - **MOSA architectures with adaptive modular components (e.g., machine learning through learnable "self-training" neural networks) should employ Integrity-checking at their interfaces to detect loss of correct functionality through Contract-Based Design, Resilience Contracts, etc.**
  - ***Note need to consider advances in Artificial Intelligence / Machine Learning in MOSA principles!***
- ***Prepare:*** **develop & maintain courses of action that address predicted or anticipated adversity**
- ***Prevent:*** **deter or preclude the realization of adversity**

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

Means of Achieving Resilience Objectives (4 of 6)

Taxonomy Layer 2: Means of achieving Objectives

- ***Re-architect:*** **modify the architecture for improved resilience**
  - **Same as Agility: MOSA architectures allow "swapping out" of modular components over time to adapt the system to changing adversities, operational needs, changing environmental conditions, expanded System missions, evolving technologies (to provide expanded capabilities provided by new technologies or to replace obsolete technologies)**
- ***Redeploy:*** **restructure resources to provide capabilities after stress**
- ***Robustness:*** **damage insensitivity or ability of a structure to withstand adverse and unforeseen events or consequences of human errors without being damaged [ISO 8930:2021, 3.2.25]**
  - **Same as Integrity: MOSA architectures typically employ self-monitoring modular components that may detect unwanted modifications or loss of correct functionality through Contract-Based Design, Resilience Contracts, etc.**
- ***Situational Awareness:*** **perception of elements in the environment, and a comprehension of their meaning, and could include a projection of the future status of perceived elements and the risk associated with that status [ISO 17757:2019, 3.1.23]**

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

Means of Achieving Resilience Objectives (5 of 6)

Taxonomy Layer 2: Means of achieving Objectives

- ***Tolerance:*** **the ability of a material/structure to resist failure due to the presence of flaws for a specified period of unrepaired usage <damage tolerance> [ISO 21347:2005, 3.7]**
- ***Transform:*** **changing aspects of system behavior**
- ***Understand:*** **developing and maintaining useful representations of required system capabilities, how those capabilities are generated, the system environment, and the potential for degradation due to adversity**
  - **MOSA architectures typically have better/more detailed documentation or even models of modular components, if (and only if!) such documentation/models are kept up-to-date throughout the modular component life cycle**

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

Means of Achieving Resilience Objectives (6 of 6)

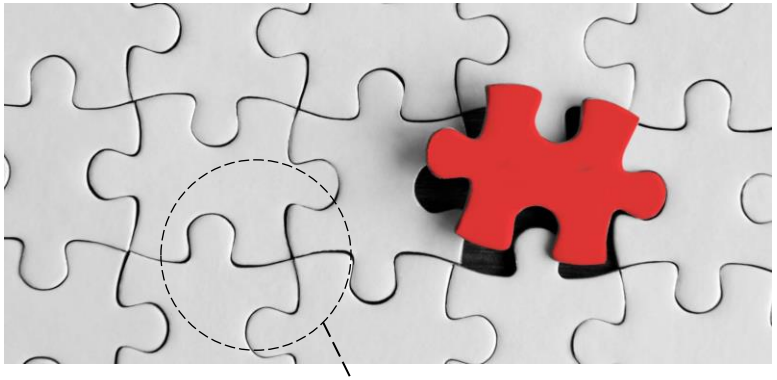
Taxonomy Layer 3: *Architecture, Design, & Operational Techniques to Achieve Resilience Objectives*

- 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

***RED** techniques are typically employed in MOSA architectures (note that most of these are Domain- or Application-specific, but could be incorporated in MOSA modular components)*

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

Interoperability Challenges of MOSA Modular Components



Modular Component Interfaces

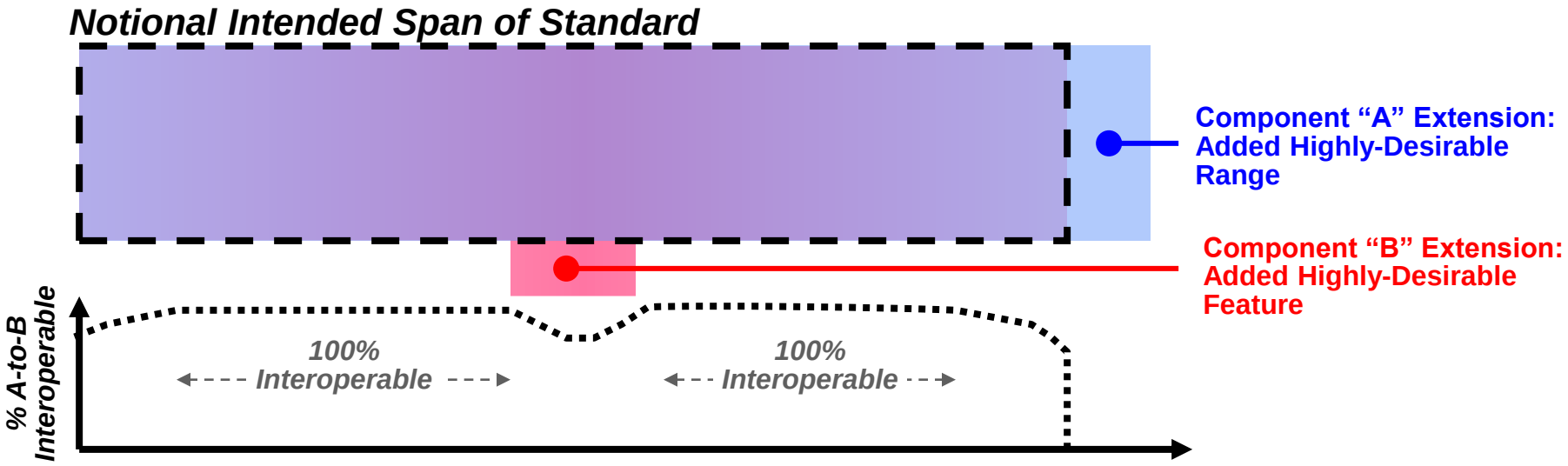
- **Must be WELL-DEFINED with careful consideration of:**
  - **Correct Standards**
    - **Preferably chosen to be long-lived and supported over the modular component life cycle**
    - **Preferably allowing some "performance margin" in Interfaces**
  - **Performance Margins chosen to avoid "brittle" designs due to changes:**
    - **Backward compatibility (e.g., USB Standards)**
    - **New functionality from new/improved Technologies**
    - **Replacement of obsolete technologies**
    - **Change in vendors/manufacturing techniques**
    - **Change in Maintenance procedures/personnel**

Image Source: Internet Clipart Search

Source: Network Centric Operations Industry Consortium (NCOIC) Interoperability Framework (NIF) briefing V1.0-2008-02-27 Released to the Public Domain

Interoperability Challenges of MOSA Modular Components

- **Many Standards Allow Options/Extensions**
  - **"Bad" Standard, or "Bad" Component Implementation?**
    - **Real-World Condition!**
  - **Typical Solution: Enforce consistent Guidance in use of Standards!**



Source: Network Centric Operations Industry Consortium (NCOIC) Interoperability Framework (NIF) briefing V1.0-2008-02-27
Released to the Public Domain

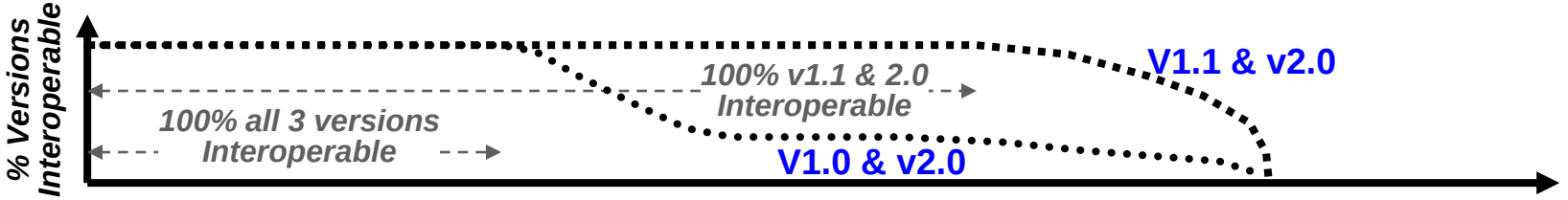
Interoperability Challenges of MOSA Modular Components

- **Many Standards Evolve over Time!**
  - **Is Each Component Running the Same Version of a Standard?**
    - **Real-World Condition! (Not necessarily a bad Standard)**
  - **Typical Solution: Enforce consistent Guidance in use of Standards!**

ORIGINAL Standard v1.0

UPDATED Standard v1.1

NEW Standard v2.0: "Backward Compatible"



Source: Network Centric Operations Industry Consortium (NCOIC) Interoperability Framework (NIF) briefing V1.0-2008-02-27
Released to the Public Domain

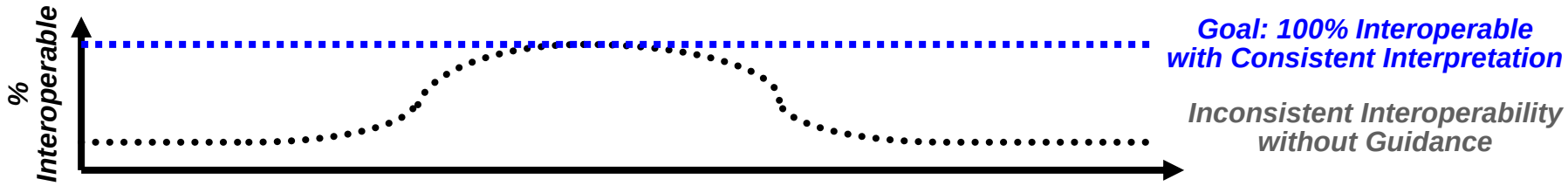
Interoperability Challenges of MOSA Modular Components

- **Inconsistent Interpretations of Standards!**
  - **Does Everyone Understand the Standard the Same Way?**
    - **Real-World Condition! (Not necessarily a bad Standard)**
    - **Requires Guidance to achieve goal of common understanding**
      - **Different Languages; different Cultural backgrounds**
      - **Same Standard applied in different Operational Domains**
      - **Same Standard implemented by designers with different levels of experience, different technical disciplines, different company rules**

Interpretation "A" of Standard

Interpretation "B" of Standard

Consistent Interpretation of Standard



Source: Network Centric Operations Industry Consortium (NCOIC) Interoperability Framework (NIF) briefing V1.0-2008-02-27
Released to the Public Domain

Summary

1. **System Resilience can be Strengthened via MOSA**
   - **Designers, Manufacturers, Operators, Maintainers, and Sustainers can apply specific techniques detailed in the INCOSE Resilience Taxonomy**
2. **Some MOSA Challenges can be Overcome via a Resilience Engineering approach**
   - **Accomplish deliberate emphasis on the Holistic System while considering MOSA component design and changes**
   - **Potentially reduce Interoperability issues by considering unintended consequences of component design Interface characteristics**

Questions?

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