PERSPECTIVE ON SYSTEM RESILIENCE

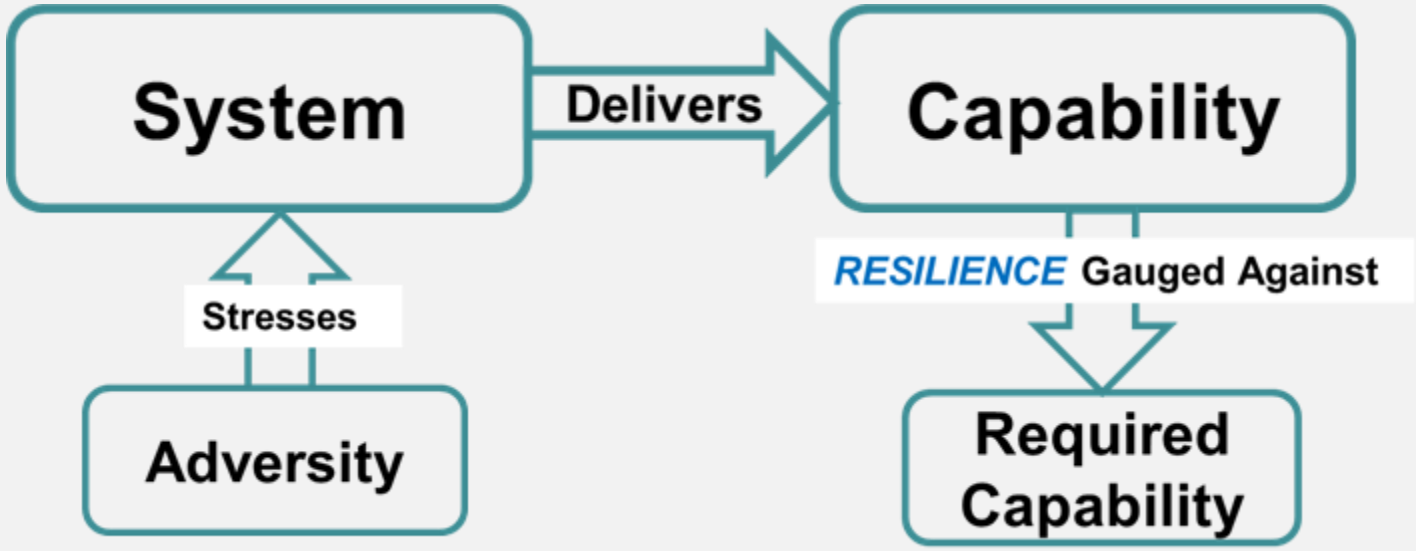
Delivery of Services by a System when encountering Adversity

It is a fact of life that engineered things will fail

We need the humility to accept that we cannot make unfailable systems – we need to find ways to accommodate the failure of items in a way that is tolerable

RESILIENCE

- Resilience is the ability to provide required capability when facing adversity



Copies from SEBoK: General Depiction of Resilience (Brtis & McEveley 2016,

PURPOSE OF SYSTEMS

- Systems are developed to provide service to owners and users
  - Focus is on the provision of service
  - Or on enabling projection of intent
- An engineered system is a means to enable the person leading deployment to effect intent
  - Therefore the engineered system is a means that enable capability

HEIDEGGER

- Heidegger, in *Being and Time*, introduced two ‘modes of being’
  - Pure Being – focus is on the properties and behaviour of the material of which tings ar made
    - Behaviour and properties of designed things can be predicted through knowledge of sciences and the configuration
  - Process Being – focus is on the entity as means to do something
    - If the entity can perform an action, then it is a useful
    - If it is broken it cannot perform its intended action – which reduces it to be just stuff – and to be known in terms of the pure being

APPROACH TO RESILIENCE

- The focus needs to be on the provision of the service
- Service can be provided by one very resilient instance of the system
  - Emphasis is on avoiding the system breaking
    - Reliability to protect from internal adversities
    - Robustness to withstand external adversities
    - Maintainability to ensure short outages (or diminutions of performance)
  - This approach is likely to be very expensive
  - This approach is necessary, and justified, for systems with very high consequence of major failure

APPROACH TO RESILIENCE

- Service can be provided by a fleet of reasonably resilient instances of the system
  - Emphasis is on understanding the availability of each instance of the system
    - Reliability must be understood
    - Robustness to withstand external adversities
    - Maintainability to ensure individual instance outages (or diminutions of performance) can be managed in the context of the support arrangements
  - This may be significantly cheaper than attempting to make each instance very reliable, maintainable and have high survivability
  - This approach is suitable for systems where it is possible to switch system instance that provides the service

MEASUREMENT OF RESILIENCE

- Measurement of anything requires clear description of the manifestation and its definition
- The challenge of measuring resilience involves the complications:
  - Achievement of resilience in different systems context manifests in different ways
    - A function of the nature of the system and its purpose
    - There is diversity of what is appropriate response to adversities
  - Resilience is a compounded manifestation involving:
    - Pre adversity encounter
    - Adversity encounter
    - Post adversity encounter
  - Phase
  - Resilience is observed in the actual life of a system – which in turn depends on the events that happen during the life
- These factors prevent an absolute measure of resilience
  - All is not lost – rational engineering action does not need an absolute scale

NO NEED FOR AN ABSOLUTE SCALE

- The engineering task is to develop systems for purposes
- During design various design ideas (alternatives) are generated
  - The question to ask is whether an alternative can deliver the resilience characteristics that matter for the situation
- Engineering decisions involve selection between alternatives
  - The alternatives that can be considered are the alternatives that have been proposed in the design process – i.e. what we have thought of
    - The best we can achieve is a selection of the best alternative we have thought of – there can be no assurance that the solution we choose is the best possible
- Consequence:
  - An engineering useful measure of resilience must be usable through analysis of expected performance of a system under adversity
    - This will provide a rational basis for choice of alternatives during design
  - Alternatives can be compared with each other
    - Resilience can be measured on an Ordinal Scale (Interval or Ratio scales are impossible)

MEASURING RESILIENCE

- In design it is normal to conduct a trade-off analysis of the performance of a system – e.g. using AHP
  - This reflects the multi-dimensional achievement of a system and the relative importance of each dimension and the value for scale of achievement in each dimension
    - This is a method of resolving multi-dimensional performance into a single measure of ‘goodness’, and enables alternatives to be compared
  - Traditionally this is done in the static situation of ‘if everything is working correctly’
- The AHP process reflects what is important to the stakeholders
- An Ordinal Scale of Resilience can be constructed by integrating the AHP process through the lifecycle
  - This needs:
    - Modelling of system performance with failures of each subsystem or component, taken singly or in combination
    - Estimation of the probability of each class of failure (all causes combined)
    - Estimation of time to restore failures
    - Modelling the lifecycle of failures and repairs using Monte Carlo analysis and a large number of lifecycles to determine a distribution of AHP outcomes
    - Compare alternatives by comparing the distributions to decide which distribution (which alternative) provides the most suitable outcome

THANK YOU