Lifecycle Models for Survivable Systems

Rick Linger

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Sponsored by the U.S. Department of Defense

Survivability Concepts

Survivability Defined

Survivability **is the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.**

No amount of security can guarantee systems will not be penetrated

Survivability focus is on mission continuity under adverse conditions

The “Three Rs” of Survivability

Resistance
- **capability to deter attacks**

Recognition
- **capability to recognize attacks and damage**

Recovery
- **capability to provide essential services during attack and recover full services after attack**

Survivable Network Analysis

SYSTEM: Essential services

Essential service usage scenarios

Essential architecture components

ENVIRONMENT: Intrusion strategies

Intrusion usage scenarios

Compromisible architecture components

- **Architecture softspots**
- **3Rs analysis**
- **Survivability Map recommendations**

Survivability Impact on Traditional Development Life Cycle

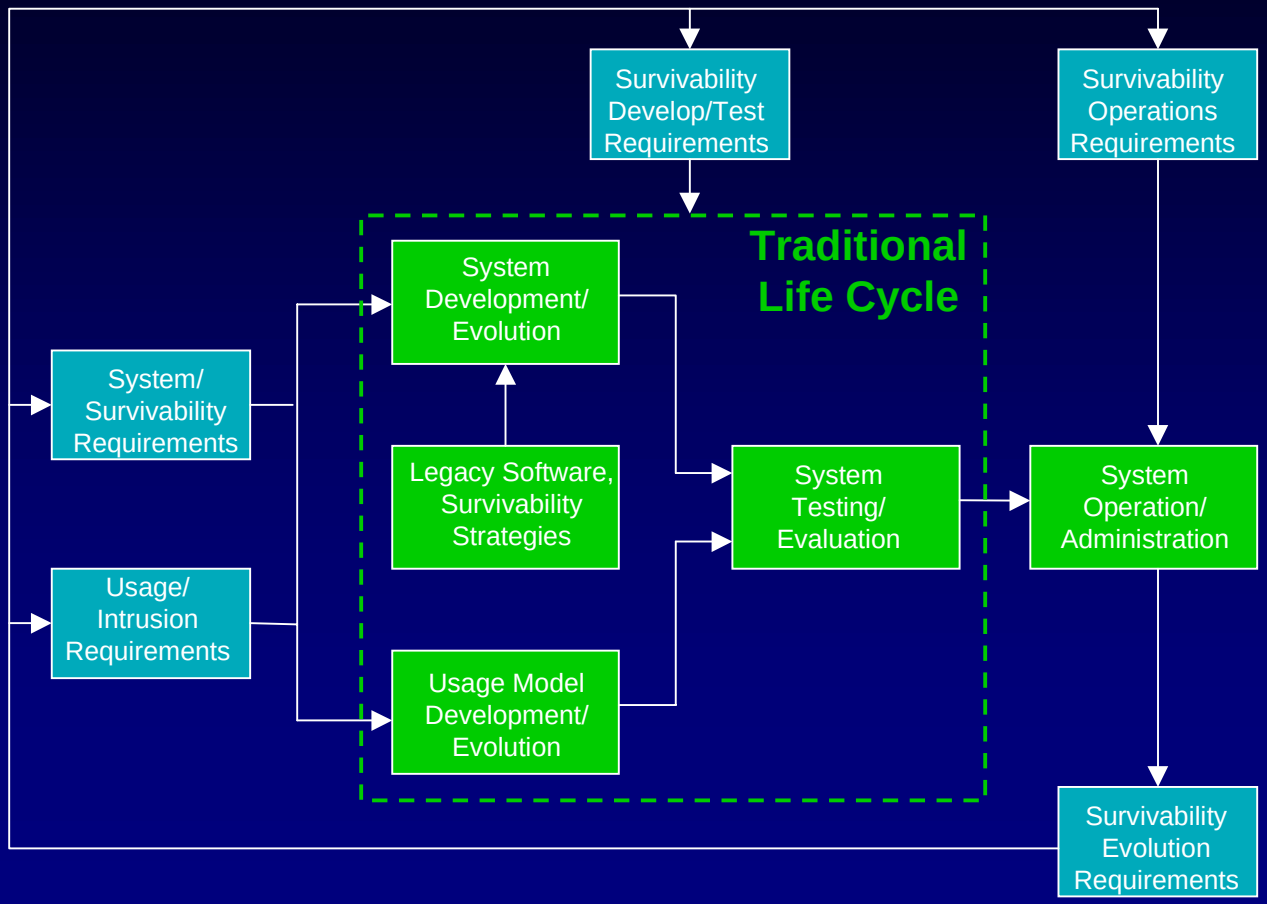
Survivability Impact - 1

Lifecycle Activities	Key Survivability Elements	Examples
Mission Definition	Analysis of mission criticality and consequences of failure	Estimation of cost impact of denial of service attacks
Concept of Operations	Definition of system capabilities in adverse environments	Enumeration of critical mission functions that must withstand attacks
Project Planning	Integration of survivability into lifecycle activities and work products	Identification of defensive coding techniques for implementation
Requirements Definition	Definition of survivability requirements from mission perspective	Definition of access requirements for critical system assets during attacks
System Specification	Specification of essential service and intrusion scenarios	Definition of steps that compose critical system transactions

Survivability Impact - 2

Lifecycle Activities	Key Survivability Elements	Examples
System Architecture	Integration of survivability strategies into architecture definition	Creation of network facilities for replication of critical data assets
System Design	Development and verification of survivability strategies	Correctness verification of data encryption algorithms
System Implementation	Application of survivability coding and implementation techniques	Definition of methods to avoid buffer overflow vulnerabilities
System Testing	Treatment of intruders as users in testing and certification	Addition of intrusion usage to usage models for statistical testing
System Evolution	Improvement of survivability to prevent degradation over time	Evolution of architecture in response to changing threat environment

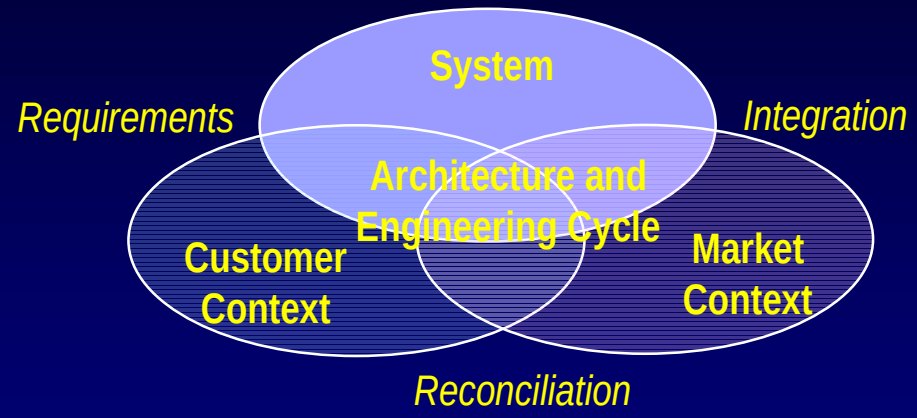
Survivability Requirements Impact



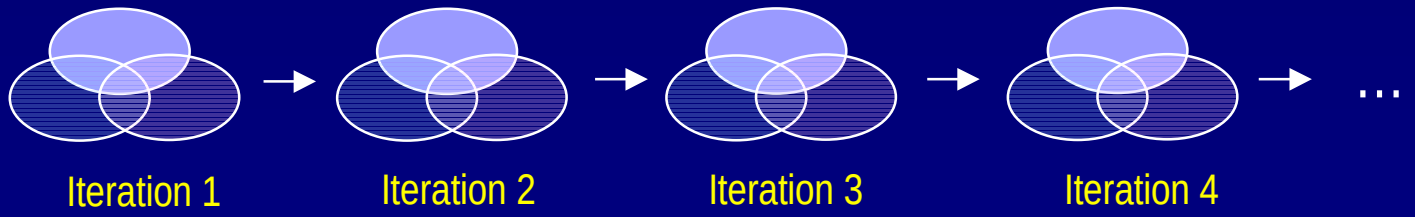
Survivability Impact on Contemporary Development Life Cycle

Contemporary Life Cycle

Iteration of customer requirements, COTS market capabilities, and system architecture



Life cycle of continuous system evolution



Survivability Impact

Reconcile mission survivability with COTS capabilities

Assess COTS vendors for survivability focus

Evaluate survivability of COTS products

Achieve survivability in system integration

Treat architecture as survivability integrator

Maintain survivability as COTS products evolve