Design Principles for Survivable System Architecture

1st IEEE Systems Conference
April 10, 2007

Matthew Richards
Research Assistant, MIT Engineering Systems Division

Daniel Hastings, Ph.D.
Professor, MIT Department of Aeronautics and Astronautics and Engineering Systems Division

Adam Ross, Ph.D.
Postdoctoral Associate, MIT Engineering Systems Division

Donna Rhodes, Ph.D.
Senior Lecturer, MIT Engineering Systems Division
Director, SEARI
Agenda

- Motivation
- Survivability Framework
- 12 Design Principles for Enhancing Survivability
- Passive vs. Active Survivability
- Conclusion
Motivation

• Despite increased geographic distribution, information technology has increased interdependence of engineering systems
• Interdependencies magnify risk from local disturbances that rapidly propagate within and among systems
• Risks exacerbated by emergence of new sources of disturbances
  – Physical: terrorism
  – Electronic: cyber-attacks
• Shortcomings associated with reductionist conventional approaches to survivability engineering
  – Limited to physical domain
  – Presuppose operating environments and hazards
  – Ineffective for managing emergent, context-dependent system properties

Research needed on how survivability should inform design decisions of system architectures
U.S. Army Research Laboratory report assesses state of architecting for survivability

- Scope: distributed systems, systems of systems
- Identifies several inadequacies with current paradigm

“Systems and networks with critical survivability requirements are extremely difficult to specify, develop, procure, operate, and maintain.”

“The currently existing evaluation criteria frameworks are not yet comprehensively suitable for evaluating highly survivable systems.”

“…there is almost no experience in evaluating systems having a collection of independent criteria that might contribute to survivability, and the interactions among different criteria subsets are almost unexplored outside of the context of this report.”

Identifies several challenges requiring future work, including:

- Generic mission models that can be readily tailored to specific systems to evaluate the adequacy of survivability requirements
- Families of systems and network topologies that are inherently robust to catastrophic failures

Enumeration of design principles for survivability would be a first step towards development of a generic survivability framework
Definition of Survivability

Ability of a system to minimize the impact of a finite disturbance on value delivery, achieved through either (1) the reduction of the likelihood or magnitude of a disturbance or (2) the satisfaction of a minimally acceptable level of value delivery during and after a finite disturbance.

Epoch:
Time period with a fixed context; characterized by static constraints, design concepts, available technologies, and articulated attributes (Ross 2006).

Type 2 Survivability

\[ V(t) \]

- original state
- recovered state
- disturbance
- actual recovery time \( \tau_r \)
- recovery
- \( V_e \) emergency value threshold
- \( V_x \) expected value threshold
- permitted recovery time \( T_r \)

Epoch 1a
Epoch 2
Epoch 1b
Type II : Direct Broadcast Satellite TV

Type II survivability is achieved here because $\tau_r < T_r$

In the case of DIRECTV, $\tau_r$ must be <0.3% of the time (about 25 hours each year)
Survivability Framework

Framework consists of the minimum set of elements to describe system
- Changes in elements will provide insights into survivability
- Used to enumerate 12 design principles for survivability
  - 6 identified for Type 1 survivability (reduction in susceptibility)
  - 6 identified for Type 2 survivability (reduction in vulnerability)
**Prevention (1.1)**

**Definition:** suppression of a future or potential future disturbance

Examples: aircraft suppression of enemy air defense (SEAD), 2nd Persian Gulf War

---

**Temporal Impact**

- **Observe**
- **Decide**
- **Act**

---

**Time**

- **Epoch 1a**
- **Epoch 2**
- **Epoch 1b**

---

**Node A**

- **Arc X**
- **Arc Y**

---

**Node B**

- **Arc Z**

---

**Node C**

---

**External Context**

- **Internal Context**

---

**External Change Agent**

---

**Internal Change Agent**
Mobility (1.2)

**Definition:** ability to relocate to avoid detection

examples: Navy TACAMO E-6 strategic communications aircraft, Scud launcher vehicles

Temporal Impact

V(t)

Epoch 1a

Epoch 1b

Epoch 2

time

mobility

external context

internal context

Node A

Node B

Node C

Arc X

Arc Y

Arc Z

internal change agent

external change agent

observe

decide

act
Concealment (1.3)

**Definition:** act of reducing the visibility of a system from an external change agent

examples: radar signature reduction on B-2 Spirit and F-117 Nighthawk

Temporal Impact

external context

internal context

Node A

Arc X

Node B

Arc Y

Arc Z

Node C

internal change agent

external change agent

observe

decide

act

Epoch 1a

Epoch 2

Epoch 1b

V(t)

V_x

V_e

T_r

time

concealment
Deterrence (1.4)

**Definition:** dissuasion of a rational external change agent from committing a disturbance; increases perceived costs above perceived benefits of attack

example: Mutually Assured Destruction

---

**Temporal Impact**

- **Epoch 1a**
- **Epoch 2**
- **Epoch 1b**

**Node A**

- **Arc X**
- **Arc Y**
- **Arc Z**

**Node B**

**Node C**

---

observe → decide → act

---

external context

internal context

---

internal change agent

external change agent
Preemption (1.5)

**Definition:** suppression of an imminent disturbance

example: missile defense, Israeli attack on Egyptian forces in 1967 Six Day War
Avoidance (1.6)

**Definition:** ability to maneuver away from a disturbance

Examples: aircraft missile evasion, precision landing on Mars Science Laboratory (MSL)
Type I Survivability Principles at Work

- Observe
- Decide
- Act

1.1 Prevention
1.2 Mobility
1.3 Concealment
1.4 Deterrence
1.5 Preemption
1.6 Avoidance

\( V(t) \) vs Time

Epoch 1a
Epoch 2
Epoch 1b

\( V_x \)
\( V_e \)
\( \tau_r \)
\( T_r \)
Hardness (2.1)

**Definition:** resistance of a system to deformation

examples: error correcting codes, Milstar satellite radiation hardening

![Diagram showing nodes A, B, and C with arcs X, Y, and Z.]

- **Node A**
  - Internal context
  - Internal change agent

- **Node B**
  - Arc X

- **Node C**
  - Arc Y
  - Arc Z

**Temporal Impact**
- V(t)
- V<sub>s</sub>
- T<sub>r</sub>

**Temporal examples:**
- error correcting codes
- Milstar satellite radiation hardening

observe  decide  act
Evolution (2.2)

**Definition:** alteration of system elements to reduce disturbance effectiveness (engineered mismatch)

example: post-deployment armor-plating of Humvees

Temporal Impact

Epoch 1a

Epoch 1b

Epoch 2

Observation

Decision

Action

Temporal Impact

Node A

Node B

Node C

external context

internal context

external change agent

internal change agent

Arc X

Arc Y

Arc Z

V(t)

V_e

V_s

T_r

Example: post-deployment armor-plating of Humvees
Redundancy (2.3)

**Definition:** duplication of critical system components to increase reliability

Examples: back-up GEO communications satellites, Space Shuttle avionics system of 5 identical general-purpose computers
Diversity (2.4)

**Definition:** variation in system elements (characteristic or spatial) to decrease effectiveness of homogeneous disturbances

example: heterogeneous operating systems decreases effectiveness of malware, separation of computers on spacecraft

Temporal Impact

Epoch 1a  Epoch 2  Epoch 1b

V(t)

observe  decide  act

time

external context

internal context

Node A

Node B

Node C

internal change agent

external change agent

Arc X

Arc Y

Arc Z

Temporal Impact

example: heterogeneous operating systems decreases effectiveness of malware, separation of computers on spacecraft
Replacement (2.5)

**Definition:** substitution of system elements to improve value delivery

Example: launch of XM-3 and XM-4 to replace XM-1 and XM-2 due to solar panel fogging that reduced Boeing 702 lifetimes from 15 to 6 years.
Repair (2.6)

**Definition:** restoration of system to improved state of value delivery

example: Hubble servicing missions

Temporal Impact

Epoch 1a Epoch 2 Epoch 1b

*V(t)*

Epoch 1b

**V**

**x**

**T**

**r**

Temporal Impact

example: Hubble servicing missions
Survivability Principles at Work

1.1 prevention
1.2 mobility
1.3 concealment
1.4 deterrence
1.5 preemption
1.6 avoidance
2.1 hardness
2.2 evolution
2.3 redundancy
2.4 diversity
2.5 replacement
2.6 repair

V(t)

V_x

V_e

\tau_r

\text{Epoch 1a}

\text{Epoch 2}

\text{Epoch 1b}

time

observe

decide

act

active

passive

\text{1.1 prevention}

\text{1.2 mobility}

\text{1.3 concealment}

\text{1.4 deterrence}

\text{1.5 preemption}

\text{1.6 avoidance}

\text{2.1 hardness}

\text{2.2 evolution}

\text{2.3 redundancy}

\text{2.4 diversity}

\text{2.5 replacement}

\text{2.6 repair}
## Passive vs. Active Survivability

<table>
<thead>
<tr>
<th>Philosophy</th>
<th>Passive Survivability</th>
<th>Active Survivability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Survivability</td>
<td>Survivability is something that a system <em>has</em></td>
<td>Survivability is something that a system <em>does</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Passive Survivability</th>
<th>Active Survivability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>proactive, resistant, robust</td>
<td>reactive, flexible, adaptive</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Design Principles</th>
<th>Passive Survivability</th>
<th>Active Survivability</th>
</tr>
</thead>
<tbody>
<tr>
<td>concealment, hardness, redundancy, diversity</td>
<td>prevention, mobility, deterrence, preemption, avoidance, evolution, replacement, repair</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Forecasting</th>
<th>Passive Survivability</th>
<th>Active Survivability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Presupposes knowledge of disturbance environment</td>
<td>Acknowledges uncertainty in projection of future disturbances</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Passive Survivability</th>
<th>Active Survivability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Closed (static)</td>
<td>Open (dynamic)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Design Focus</th>
<th>Passive Survivability</th>
<th>Active Survivability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Defensive barriers at system-level to resist disturbances</td>
<td>Architectural agility to avoid, deter, and recover from disturbances</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Failures</th>
<th>Passive Survivability</th>
<th>Active Survivability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Causal chain (often linear)</td>
<td>Tight couplings, functional resonance (nonlinear)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Relevant Disciplines</th>
<th>Passive Survivability</th>
<th>Active Survivability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Component reliability, safety engineering, risk analysis, domain-specific technologies</td>
<td>Real options, organizational theory, process design, domain-specific technologies</td>
</tr>
</tbody>
</table>
Conclusion

• Definition, framework, and enumeration of passive and active survivability design principles is only a first step
  – Helpful for understanding a larger set of survivability techniques
• Enumeration is not intended as a systems engineering checklist
  – Intended to provide designers with a portfolio of options from which to consider a larger tradespace of survivable designs
• Successful designs must balance investments in survivability with performance and cost
  – e.g., incorporate subset of the twelve principles with varying weights
• Future work
  – Development of quantitative metrics for each design principle
  – Incorporation of survivability as an attribute in an existing satellite tradespace