

# INTRODUCTION

Different definitions for survivability

From AIAA (American Institute of Aeronautics and Astronautics).

- » <http://www.aiaa.org>
- » survivability is defined for aircrafts as “the capability of an aircraft to avoid or withstand hostile environments, including both man-made and naturally occurring environments, such as lightning strikes, mid-air collisions, and crashes”



# National Communication System Technology and Standards Division

- » Federal Standard 1037C, Telecommunications: Glossary of telecommunication terms, 1996
- » survivability of telecommunication systems is “the property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance; e.g., nuclear burst”.

From [M.S. Deutsch and R.R. Willis 1988].

- » survivability of software systems is  
“The degree to which essential functions are still available even though some part of the system is down”.



From Ellison et.al.

Tech Report CMU/SEI-97-TR-013, May 1999

» “We define survivability as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents. We use the term system in the broadest possible sense, including networks and large-scale systems of systems.”

## From June 2000 Neumann Report

- » ability of a computer-communication system-based application to satisfy and to continue to satisfy certain critical requirements (e.g., specific requirements for security, reliability, real-time responsiveness, and correctness) in the face of adverse conditions.
- » Survivability must be defined with respect to the set of adversities that are supposed to be withstood.
- » Types of adversities might be typically include hardware faults, software flaws, attacks on systems and networks perpetrated by malicious users, and electromagnetic interference



## From TIAI.2 Working Group

- » Network survivability is:
  - » (i) the ability of a network to maintain or restore an acceptable level of performance during network failures by applying various restoration techniques, and
  - » (ii) the mitigation or prevention of service outages from network failures by applying preventative techniques.

Liu & Trivedi capture the definition of TIAI.2 as

» Suppose a measure of interest  $M$  has the value  $m_0$  just before a failure occurs. The survivability behavior can be depicted by the following attributes:  $m_a$  is the value of  $M$  just after the failure occurs,  $m_u$  is the maximum difference between the value of  $M$  and  $m_a$  after the failure,  $m_r$  is the restored value of  $M$  after some time  $t_r$ , and  $t_R$  is the time for the system to restore the value of  $m_0$ .



Table 1: Laprie's view on dependability and survivability [1]

Concept	Dependability	Survivability
Goal	<ol style="list-style-type: none"> <li>1) ability to deliver service that can justifiably be trusted</li> <li>2) ability of a system to avoid failures that are more frequent or more severe, and outage durations that are longer, than is acceptable to the user(s)</li> </ol>	<p>capability of a system to fulfill its mission in a timely manner</p>
Threats present	<ol style="list-style-type: none"> <li>1) design faults (e.g., software flaws, hardware errata, malicious logics)</li> <li>2) physical faults (e.g., production defects, physical deterioration)</li> <li>3) interaction faults (e.g., physical interference, input mistakes, attacks, including viruses, worms, intrusions)</li> </ol>	<ol style="list-style-type: none"> <li>1) attacks (e.g., intrusions, probes, denials of service)</li> <li>2) failures (internally generated events due to, e.g., software design errors, hardware degradation, human errors, corrupted data)</li> <li>3) accidents (externally generated events such as natural disasters)</li> </ol>

Knight & Sullivan 2000 in “On the Definition of Survivability” assumes that “a system is survivable if it complies with its survivability specifications”

–Survivability Specifications:

» a four-tuple,  $\{E, R, P, M\}$



»  $\{E, R, P, M\}$  where:

- $E =$  A statement of the assumed operating environment for the system.
- $R =$  A set of specifications each of which is a complete statement of a tolerable form of service that the system must provide.
- $P =$  A probability distribution across the set of specifications,  $R$ .

## » {E, R, P, M} where:

- M = A finite-state machine denoted by the four-tuple  $\{S, s_0, V, T\}$  with the following meanings:
  - S: A finite set of states each of which has a unique label which is one of the specifications defined in R.
  - $s_0$ :  $s_0$  in S is the initial or preferred state for the machine.
  - V: A finite set of customer values.
  - T: A state transition matrix.
- We will discuss this later in more detail...