

Resilient and Survivable Networking

The University of Kansas EECS 983

Dependability – Spring 2008

James P.G. Sterbenz

Department of Electrical Engineering & Computer Science
Information Technology & Telecommunications Research Center
The University of Kansas



jpgs@eecs.ku.edu

<http://www.ittc.ku.edu/~jpgs/courses/rsnets>

Resilient and Survivable Networking

Dependability

DE.1 Faults, errors, failures

DE.2 Dependability: availability and reliability

Dependability

DE.1 Faults, Errors, Failures

DE.1 Faults, errors, failures

DE.2 Dependability: availability and reliability

Basic Definitions

Faults, Errors, Failures

- *Fault*
 - cause of an *error*
 - *dormant* (or latent) when it does not yet cause an error
 - *active* when it causes an error
 - may be internal or external to a given system
- *Vulnerability*
 - internal fault that allows an external fault to cause an error

[Laprie-1994], [Avizienis-Laprie-Randell-Landwehr-2004TR]

Basic Definitions

Types of Faults

- *Fault*
 - see Figs. 4 and 6

[Laprie-1994], [Avizienis-Laprie-Randell-Landwehr-2004TR]

Basic Definitions

Faults, Errors, Failures

- *Error*
 - stochastic event in either space (system) or time
 - manifestation of a fault
 - system state that may lead to a subsequent failure
- *Failure*
 - deviation from service

[Laprie-1994], [Avizienis-Laprie-Randell-Landwehr-2004TR]

Basic Definitions

Faults, Errors, Failures

- Service *failure*
 - deviation of delivered service from service specification
 - transition from correct to incorrect service state
 - *service outage*: incorrect service state
 - *timing failure*: performance degradation
 - *content failure*: incorrect information
- Service *restoration*
 - transition from incorrect to correct service state

[Laprie-1994], [Avizienis-Laprie-Randell-Landwehr-2004TR]

Basic Definitions

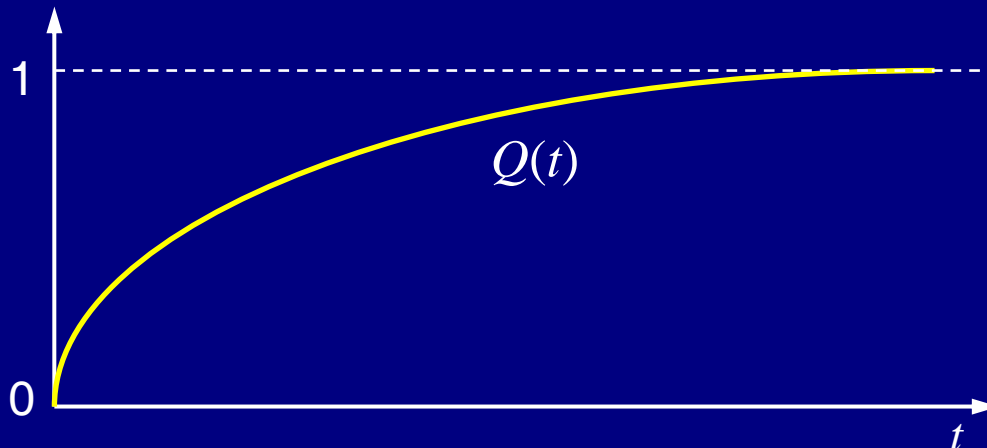
Types of Failures

- *Failure*
 - see Figs. 8 and 9

Basic Definitions

Failure Distribution Function

- Failure probability density
 $f(t) \triangleq$ time to failure from operational state
- Failure CDF (cumulative distribution function)
 $Q(t) \triangleq \Pr[\text{one or more failures in } [0, t]]$



Basic Definitions

Fault Tolerance

- *Fault tolerance*
 - avoid service *failures* in the presence of *faults*
- Mature discipline
 - generally assumes *independent random* faults
 - traditional fault models do *not* hold under
 - malicious attack and large-scale natural disaster

Basic Definitions

Byzantine Fault Tolerance

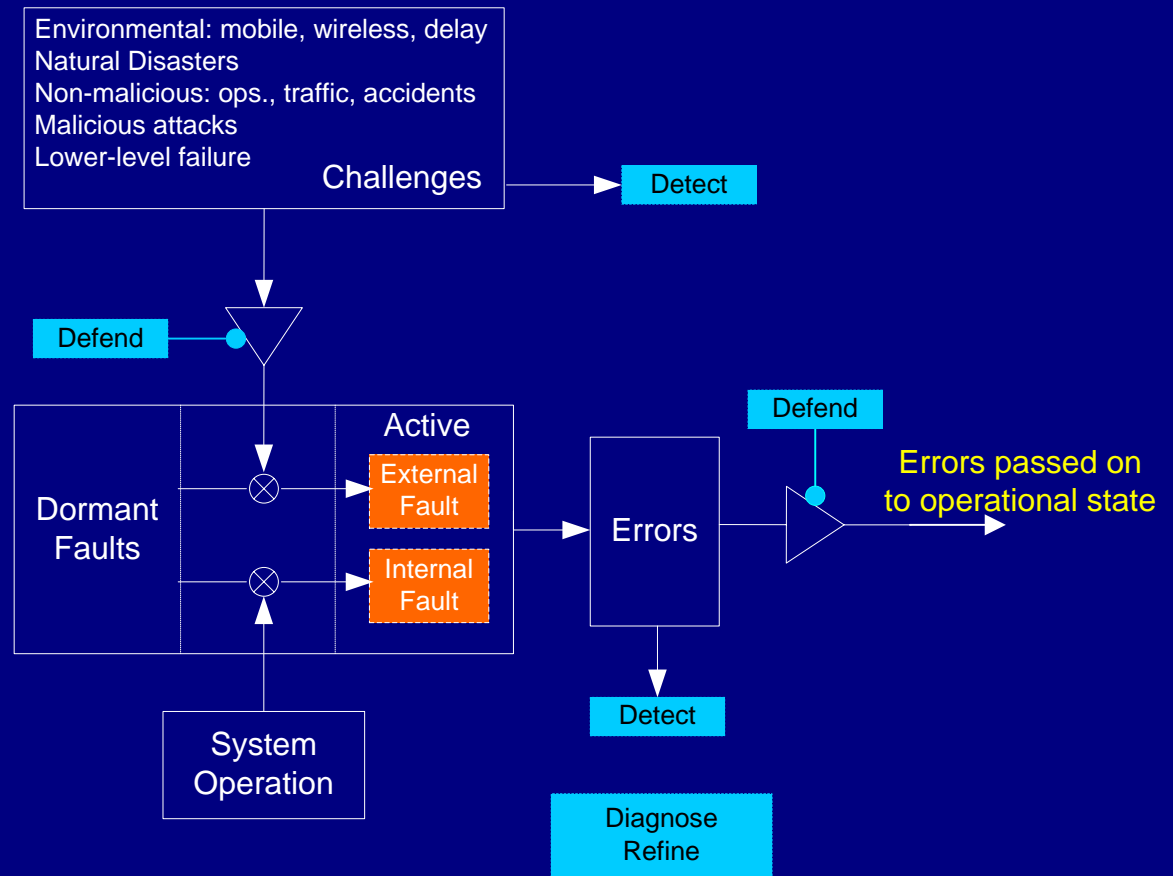
- Conflicting information to different parts of system
 - may be malicious
- *Byzantine fault tolerance*
 - avoid *failures* in the presence of *Byzantine faults*
- Preventing Byzantine failures
 - less than 1/3 Byzantine components if not authentication

[Lamport-Shostak-Pease-1982]

Basic Definitions

Fault → Error → Failure Chain

- **Challenge**
 - may trigger dormant fault
- **Active fault**
 - may cause error (activation)
- **Error**
 - may be observed as failure (propagation)



Challenges

Definition

- *Challenges to normal operation*
 - unintentional misconfiguration or operational mistakes
 - malicious attacks
 - large-scale natural disasters
 - environmental challenges
 - mobility
 - weak and episodic channels (typically wireless)
 - unpredictably long delay
 - unusual but legitimate traffic (e.g. flash crowd)
 - service failure at a lower level

Dependability

DE.2 Availability and Reliability

DE.1 Faults, errors, failures

DE.2 Dependability: availability and reliability

Dependability

Definition

- *Dependability*
 - reliance can be placed on delivered service
- Dependability aspects
 - *availability*: readiness for usage
 - *reliability*: continuity of service
 - *safety*: non-occurrence of catastrophic consequences
 - *integrity*: non-occurrence of improper information alterations
 - *maintainability*: aptitude to undergo repairs and evolution

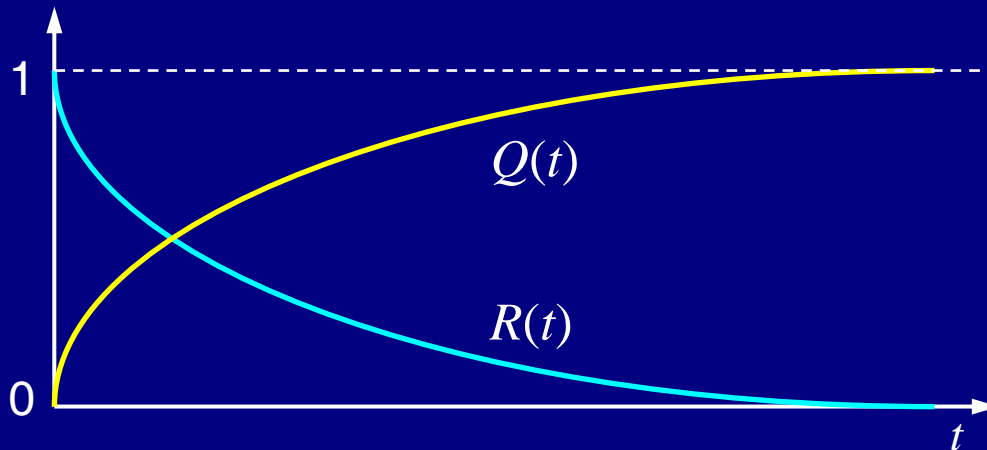
Security Definition

- *Security*
 - **availability**: readiness for usage
 - confidentiality: non-occurrence of unauthorised disclosure
 - **integrity**: non-occurrence of improper information alterations
 - accountability: availability and integrity of identity
 - authenticity: integrity of message content and origin
 - nonrepudiability: availability & integrity of origin or reception

Reliability and Availability

Reliability Definition

- *Reliability*
 - probability of a of system performing its purpose adequately
 - for the period of time intended
 - under the operating conditions intended
- $R(t) \triangleq \Pr[\text{no failure in } [0,t]] = 1 - Q(t)$



Reliability and Availability

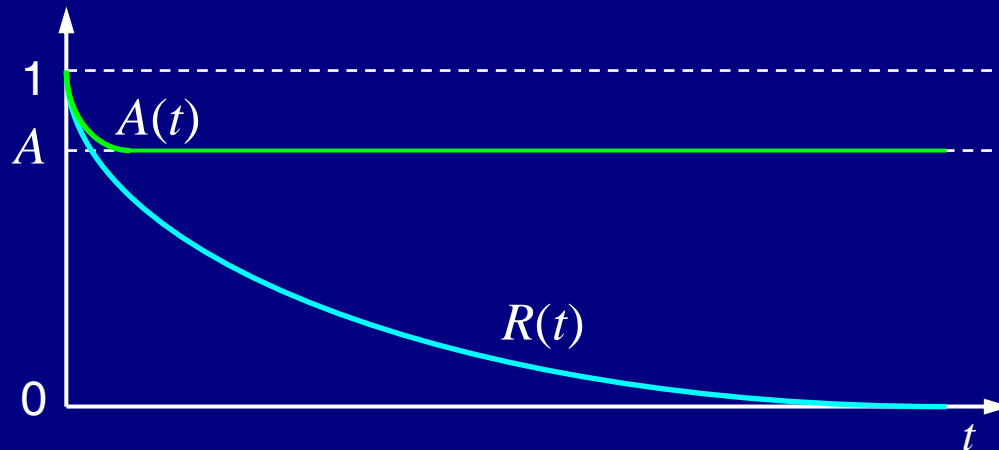
Mean Time to Failure

- *MTTF* (mean time to failure)
 - expected value of failure density function $f(t)$
- *MTTR* (mean time to repair)
 - expected value of repair density function
- *MTBF* (mean time between failures)
- $MTBF = MTTF + MTTR$

Reliability and Availability

Availability Definition

- *Availability*
 - probability of a of system operational at a given time
 - initially follows $R(t)$ but then repairs keep availability higher
 - steady state: uptime / observation time
- $A = \text{MTTF} / \text{MTBF}$



System Availability

Series and Parallel Composition

- Series availabilities multiply: $A(t) = \prod R_i(t)$
 - conservative approximation as sum of unavailabilities
 $U(t) = \sum U_i(t)$
- Parallel availabilities: $A(t) = 1 - \prod [1 - R_i(t)]$
 - exact product of unavailabilities
 $U(t) = \prod U_i(t)$
- Series-parallel iterative reductions
 - not possible for many network topologies (diagonals)

Graph Reliability

Definition

- Model network as a *graph* $G = (V, E)$
 - set of vertices $V = \{v_1, v_2, \dots\}$ correspond to links
 - set of edges $E = \{e_1, e_2, \dots\}$ correspond to nodes
- Reliability
 - probability of
 - graph remaining connected
 - path existing between pair of nodes (2-terminal reliability)
 - path existing between set of nodes (k -terminal reliability)
 - given failures of
 - edges (links)
 - vertices (nodes)

Graph Reliability

Definition

- Reliability of a graph dependent on
 - reliability of components: edges and vertices
 - topology
- Resilient topology requires *biconnected* graph
 - every pair of vertices connected by at least 2 disjoint paths
 - disjoint edges
 - disjoint vertices (no articulation points)

Dependability

References and Further Reading

- References at wiki.ittc.ku.edu/resilinet/Dependability

End of Foils