Chapter 1- 4: Embedded Computing

Soo-Ik Chae

Topics

- Reliability, safety, and security.
- Consumer electronics.

Related disciplines

- Reliable/dependable system design creates systems that function even in the face of internal or external errors.
- Security concentrates on malicious attacks.
- Safety-critical system design develops methods to ensure that systems operate safely under a wide variety of error conditions.

Dependability and security

After Avizienis et al. [Avi04]

Attributes of dependability and security (Avizienis et al.)

- Availability of correct service.
- Continuity of correct service.
- Safety from catastrophic consequences.
- Integrity from improper system alterations.
- Maintainability through modification or repairs.
- Confidentiality of information.

Reliability requirements on embedded systems

- Safety-critical or high-reliability applications:
  - Automotive.
  - Aviation.
  - Medicine.
  - Critical communications.
- Many high-reliability applications require distributed embedded systems.
- Embedded systems may be vulnerable to new types of attacks.

Faults

- Faults may cause errors; reliable systems recover from faults.
- A fault may be transient or permanent.
- Types of faults:
  - Physical faults from manufacturing defects, radiation hazards, etc.
  - Design faults.
  - Operational faults from human error, security breaches, etc.

System reliability metrics

- Mean time to failure (MTTF) is the expected time for first system to fail:

$$MTTF \stackrel{?}{=} \int_0^\infty R(t)dt$$

- Reliability function describes the probability that the system will operate correctly in the time interval [0,t].
- Hazard function is the failure rate of components:

$$z(t) = \frac{pdf}{1 - CDF}.$$

System reliability metrics

- **pdf** **$f(x)= \theta e^{-\theta x}$**
  where $x \geq 0$ and $\theta > 0$ is a constant
- **cdf** **$F(x)= P(X \leq x) = 1- e^{-\theta x}$**
- **Reliability $= 1 - F(x) = e^{-\theta x}$**
- **Failure Rate = θ**
- **MTBF or MTTF = $1/\theta$ =**
- Where the reliability of the component at x, R(x), is equal to the probability that the process or component performs its designed use at (time) x.

Common fault distributions

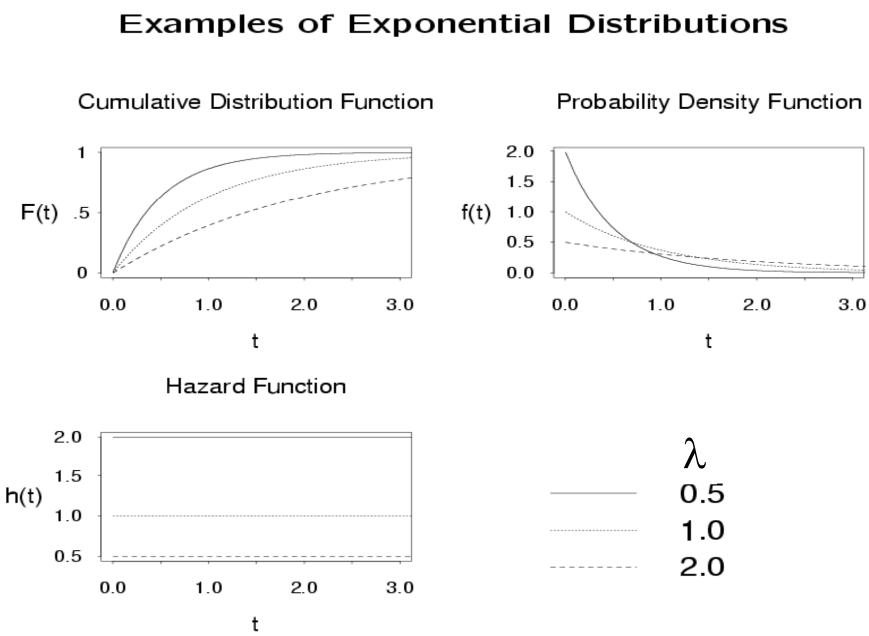
- Exponential distribution.
- Weibull distribution.
- Bathtub distributions

Exponential distribution

- Hazard function $h(t) = \lambda$
- PDF $f(t) = \lambda e^{-\lambda t}$
- Survival function

$$P(T > t) = S(t) = \int_t^{\infty} h e^{-hu}\, du = -e^{-hu}\Big|_t^{\infty} = 0 - -e^{-ht} = e^{-ht}$$

f(t), F(t), S(t), and h(t) for different exponential distributions:



Weibull distribution

- The Weibull distribution is unique in that it takes on the shape which best fits the data. The more typical situation is where data is "force fitted" into a standard type of distribution, such as the Normal, Exponential, or other.
- For example, a Weibull shape factor of 1.00 represents an exponential distribution.
- A Weibull shape factor of about 3.25 or above represents an approximately normal distribution.
- In addition, use of any of the Weibull analysis routines to accomplish estimates of population characteristics, is simply a recognition of the fact that populations are rarely 100% normal, binomial, or exponential and so on.

Weibull distribution

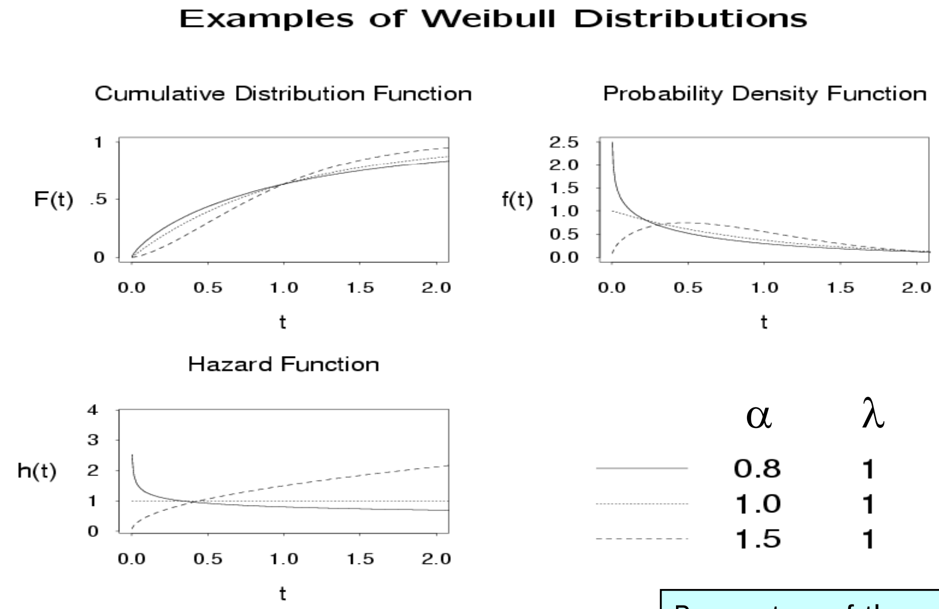
- Hazard function
  - Shape parameter: α
  - Scaling parameter: λ
- PDF
- Survival function

$$h(t) = \alpha\lambda(\lambda t)^{\alpha-1}$$

$$f(t) = \alpha\lambda(\lambda t)^{\alpha-1} e^{-(\lambda t)^{\alpha}}$$

$$P(T > t) = S(t) = \int_{e^{-(\lambda t)^{\alpha}}}^{\infty} e^{-u} du = e^{-(\lambda t)^{\alpha}}$$

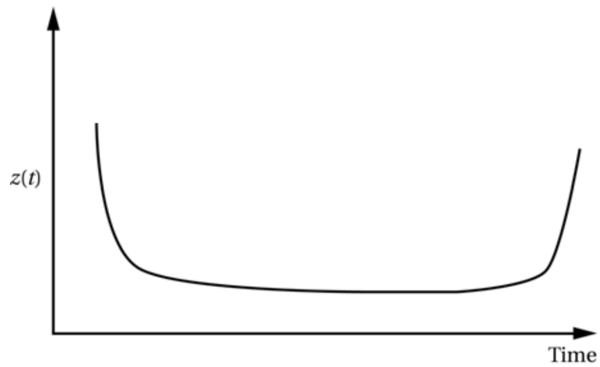
f(t), F(t), S(t), and h(t) for different Weibull distributions:



Parameters of the Weibull distribution

Bathtub distributions

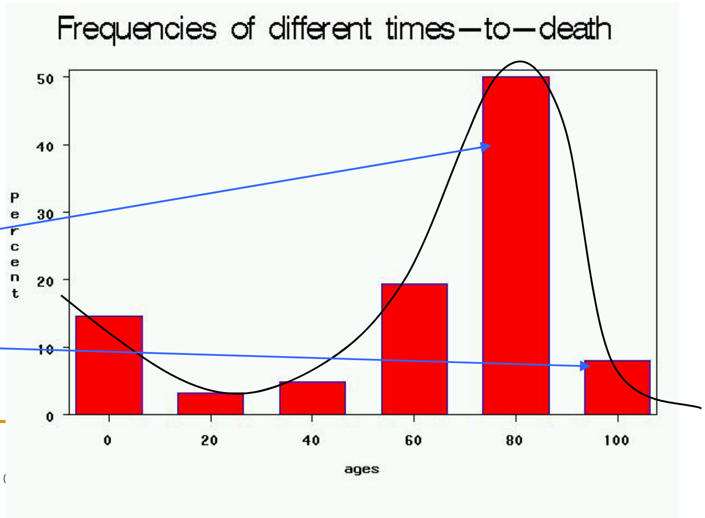
- Bathtub distributions are often empirically observed.
  - High failure rates at beginning, end of component life.



(Death) Probability density function: f(t)

In the case of human longevity, T_i is unlikely to follow a normal distribution, because the probability of death is not highest in the middle ages, but at the beginning and end of life.

Hypothetical data:

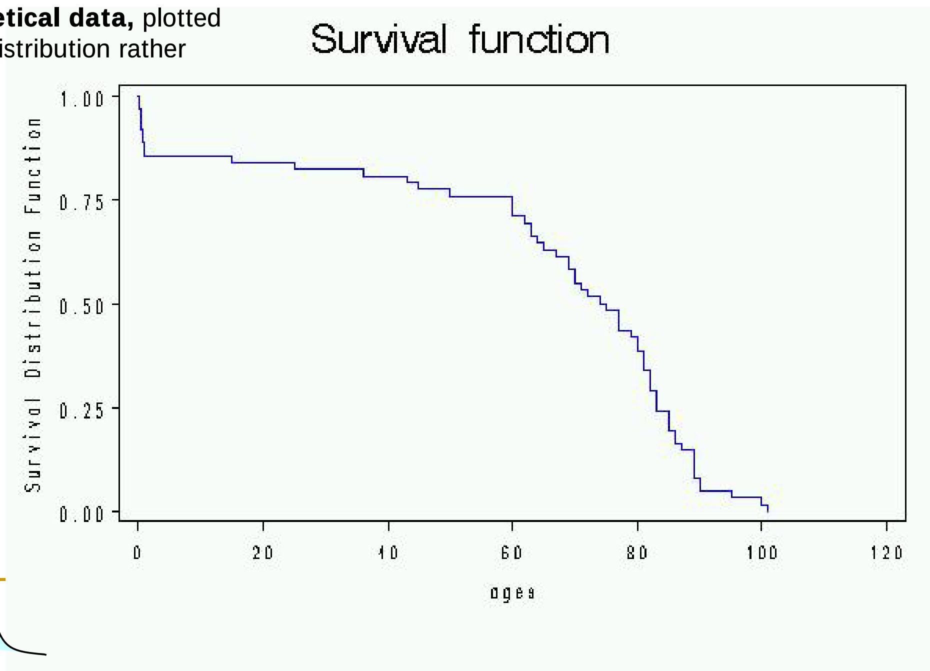


People have a high chance of dying in their 70's and 80's;

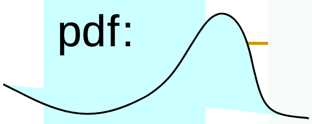
BUT they have a smaller chance of dying in their 90's and 100's, because few people make it long enough to die at these ages.

Cumulative survival

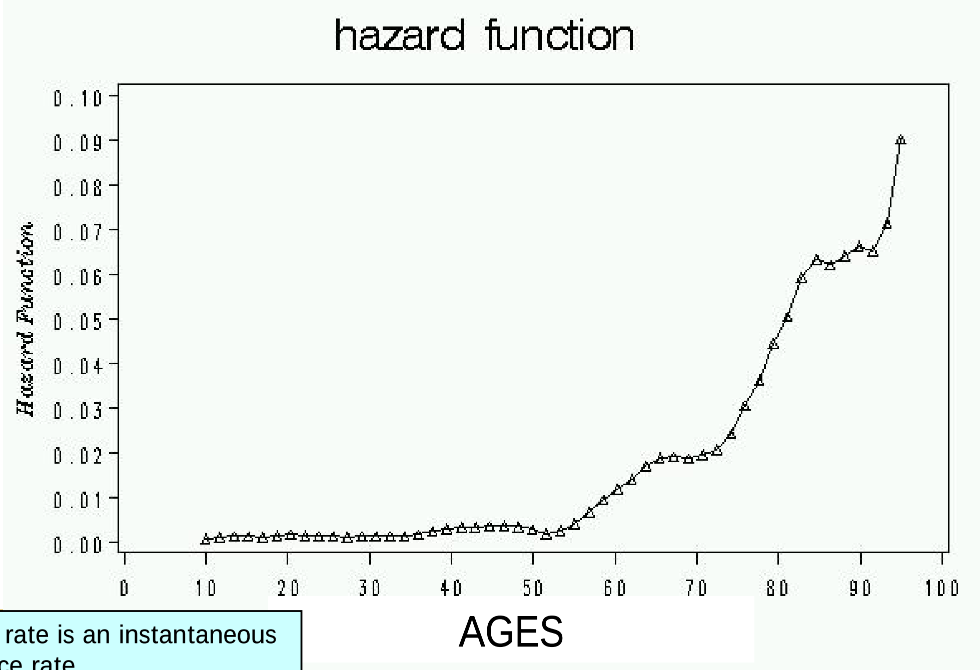
Same hypothetical data, plotted as cumulative distribution rather than density:



Recall pdf:



Hazard Function



Hazard rate is an instantaneous incidence rate.

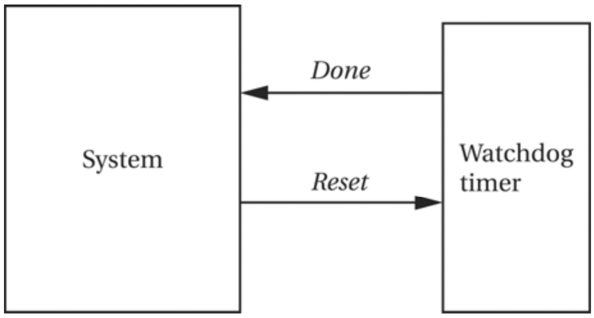
Possible actions after a fault

- Fail: without trying to even detect an error
- Detect: diagnostic information is useful even if the system stops
- Correct: memory errors are routinely corrected
- Recover: more than a simple correction which may cause a noticeable pause in system operation.
- Contain: steps to ensure that a failure does not corrupt a large part of the system
- Reconfigure: disable a faulty unit and enable another unit
- Restart: good for transient errors and software errors
- Repair: for either HW or SW components

Reliability methods

- Error-correction codes.
- Voting systems.
  - Triple-modular redundancy (TMR) uses majority voting.
- Watchdog timer must be periodically reset by system to show that system operates correctly.
- Design diversity uses redundancy implemented in different types of components.

- A done signal should be attached to an error interrupt in the system
- When running properly, it always resets the timer before it roll over.



Novel attacks and countermeasures

- Embedded systems provide physical access, a key avenue for attack.
- Internet-enabled embedded systems provide remote access to attackers.
  - Example: Internet-enabled automobiles.
- Battery attacks exercise the system to wear out a battery.
- Quality-of-service attacks interfere with real-time behavior.

Sensor network attacks (Wood and Stankovic)

- Physical layer: jamming, tampering.
- Link layer: collision, exhaustion, unfairness.
- Network and routing layers: neglect and greed, horning, misdirection, authorization, probing, redundancy.
- Transport layer: flooding, desynchronization.

Power attack

- Developed by Kocher et al.
- Measure CPU current to determine instructions, data.
  - Simple power analysis: inspect a trace manually to determine program action.
  - Differential power analysis: uses correlation to identify action and key bits. It was originally aimed at smart cards, which draw their power form the external card reader.
- High-leakage devices are less vulnerable to power attacks.

Consumer electronics architectures

- Consumer electronics pushes the edge of the envelope in several directions:
  - Complex functionality and high performance.
  - Often battery-powered.
  - Very low cost.
- Generally include one or more standards.

Bluetooth

- Personal-area network.
  - 2.5 GHz band.
  - Generally within 2 meters, may be extended to 30 meters.
- Basic network is master-slave, but higher levels of protocol stack provide peer-to-peer operation.

Bluetooth stack

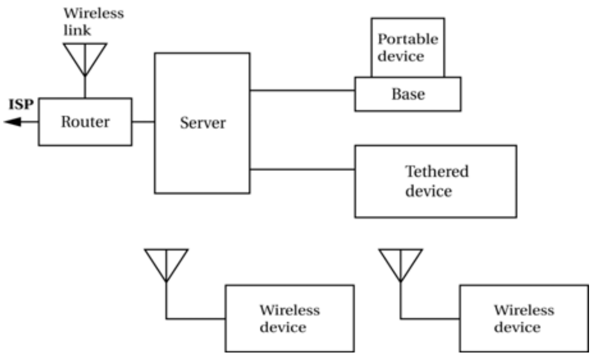
Logical link control and adaptation (L2CAP)
Link Manager
Baseband
Physical

Bluetooth middleware group protocols

- RFCOMM provides serial interface; compatible with RS-232.
- Service discovery protocol discovers services (printing, etc.) on the network.

Networked consumer appliances

- PC acts as a host.
- Some devices are semipermanently connected (USB); others are on wired Ethernet; others are on wireless networks.
- Devices must be configured properly with the system.

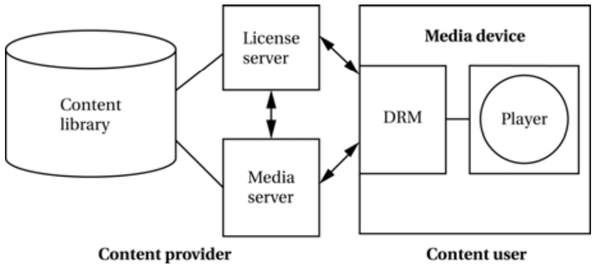


High-level services

- Service discovery allows the device to find another device on the network that will provide a service (for example, printing).
  - Jini lookup services hold service proxies.
  - Jini uses join protocol to add a service.
  - Jini client obtains a lease for a given service.

Digital rights management

- Digital rights management (DRM) is used to ensure that copyrighted material is used within the terms required by owner.
  - Devices that can play material.
  - Number of times material can be played.
  - Expiration date.



System overview : typical DRM model