ETLS 509 - Validation & Verification
University of St. Thomas

John Engelman

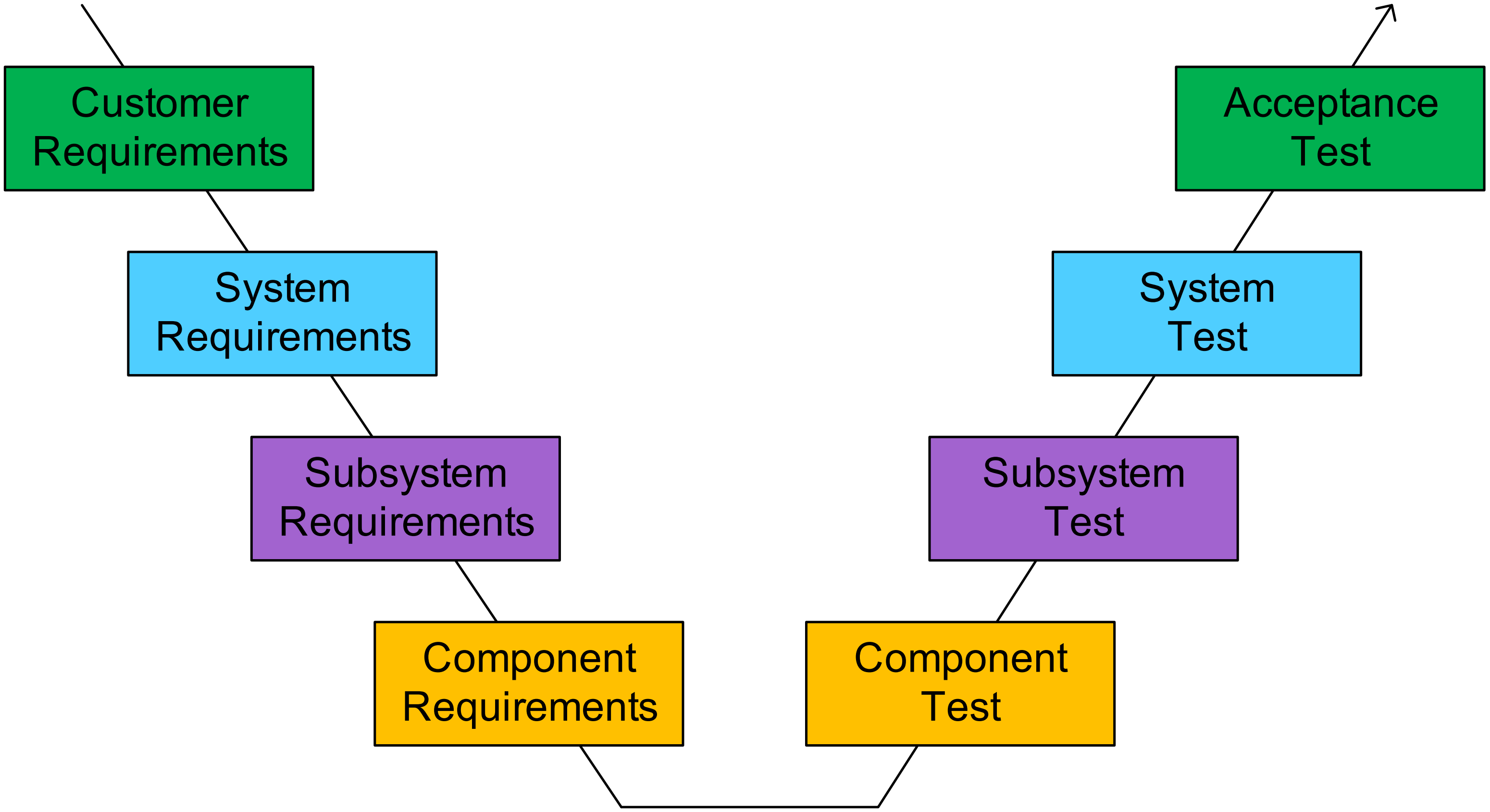
Fall 2016

Agenda

- Review
- Reliability, Maintainability, Availability

ETLS 509 - Session 9

- **Requirements Definition RM&A**



Definitions

- **Reliability - the probability that a system or product will accomplish its designated mission in a satisfactory manner for a given period when used under specified operating conditions.**
  - Note that time is inherent in the definition of reliability
- **Maintainability - is the ability of the system to be maintained, it is a design-dependent parameter.**
- **Availability - the probability that a system or equipment, when used under stated conditions in an ideal support environment, will operate satisfactorily an any point in time as required.**

Reliability, Maintainability, Availability

- **Reliability, Maintainability, and Availability (RMA) are intertwined aspects of any system**
  - To increase the reliability of a system may involve trade-offs that also increase the routine maintenance
    - Auto manufactures will sometime include changing items such as a timing belt after a specific number of miles, even though the timing belt has not failed
      - The belt is replaced prior to an expected failure thereby increasing the overall reliability of the vehicle at the potential cost of increased maintenance
      - The increased routine maintenance can have both positive and negative effects on availability.
        - » While the maintenance is being done the vehicle is not available thereby decreasing the availability.
        - » A failure while driving could result in a significantly longer loss of use of the vehicle than the routine maintenance and as such the preventative maintenance can also have a positive effect on availability

Failure Rates

The failure rate λ $\lambda = \dfrac{\textit{number of failures}}{\textit{total operating hours}}$

- **The failure rate for a system, subsystem, or component may be determined via operating history**
  - When operating history is not available, then λ will be calculated.
- **If the distribution of failures in a system is an exponential distribution, then the mean time between failures (MTBF) is**

$$\mathrm{MTBF} = \frac{1}{\lambda}$$

  - If λ=0.0001 failures/hour the MTBF = 10000 hours

Failure Rates - continued

- **Failure rates can also be associate with missions or mission duration -**

$$\lambda = \frac{number\ of\ failures}{total\ mission\ time}$$

Here the units on λ are failures per mission hour with maintenance done following mission

$$\lambda = \frac{number\ of\ failures}{number\ of\ missions}$$

Here the units on λ are failures per mission with maintenance done following each mission

- **A failure is defined to be something that causes the system to not be operating within a specified set of parameters**
  - It does not matter if the failure is hardware or software, if a person is an integral part of the system the failure can also be human error. Failure rates usually do not take human error as a failure mechanism – the system design is to be "robust against human errors."

Failures - continued

- **Scheduled maintenance does not count as a failure**
  - Changing oil in a vehicle
  - Filling up with gasoline
- **Failure to perform scheduled maintenance may result in a system not operating within a specified set of parameters; however, failures due to this are not system failures and need to be separated out from system failures.**
  - Similarly, operating a system outside of its defined limits may result in failures, e.g., operating the system at higher temperatures than specified. These failures will not be taken into account in determine failure rates of MTBF.

Reliability

- ***R(t)=1-F(t)***
  - *R(t)* is the reliability function
  - *F(t)* is the probability that a system will fail by time *t*

$$F(t)=\int_0^t f(t)dt \qquad R(t)=1-F(t)=\int_t^\infty f(t)dt$$

where *f(t)* is the failure distribution function

- **Failure distribution density functions are a function of the types of failure modes and systems. There are many different density distribution functions**
- **If f(t) is an exponential density function, a common type then**

$$f(t)=\frac{1}{\theta}e^{-\frac{t}{\theta}} \quad \textbf{and} \quad R(t)=\int_t^\infty \frac{1}{\theta}e^{-\frac{t}{\theta}}dt=\left[-e^{-\frac{t}{\theta}}\right]_t^\infty=e^{-\frac{t}{\theta}}$$

Determining Reliability of a System Composed of Multiple Subsystems/Components

- **For a serial system, i.e., a system where the failure of any individual item results in the system no longer operating within its operational parameters**
  - If the system is composed of n items each with reliability R_i for $1 \le i \le n$ then the reliability of the system

$$R = \prod_{i=1}^{n} R_i$$

where R is the reliability of the system.

- **The failure rates for a serial system are additive, given each component i has *MTBF***

$$\lambda_i = \frac{1}{MTBF_i} \quad \text{then } \lambda = \sum_{i=1}^{n} \lambda_i$$

An Example

- **Suppose a system is serial and has 4 subsystems, A, B, C, D**

  $MTBF_A$= 25,000 hours, $MTBF_B$= 125,000 hours

  $MTBF_C$= 5,000 hours, $MTBF_D$= 10,000 hours

  Then λ_A = 0.00004 failures/hour, λ_B = 0.000008 failures/hour,

  λ_C = 0.0002 failures/hour, λ_D = 0.0001 failures/hour,

  $\lambda = \lambda_A + \lambda_B + \lambda_C + \lambda_D$

  = 0.000348 failures/hour

  The system MTBF is 2873 hours

Parallel Systems

- **To increase overall reliability systems are frequently built with parallel components so that if one parallel component fails, normal system operation may continue.**
  - Although having the additional hardware/software increases the number of “hardware/software” failures, these failures are not system failures and do not effect the system reliability.
- **The reliability of a parallel network is**

$$R = 1 - \prod_{i=1}^{n} (1 - R_i)$$

where R_i is the reliability of the ith parallel component.

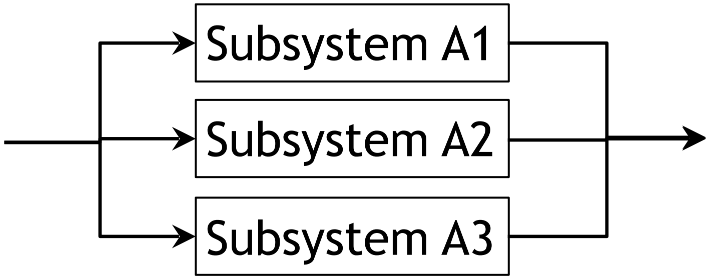
Reliability in Parallel Systems

- **The reliability of a parallel network is**

$$R = 1 - \prod_{i=1}^{n} (1 - R_i)$$

where R_i is the reliability of the ith parallel component. R_i=1-λ_i and λ_i is failure rate of the ith parallel component.

- **Consider the flowing set of 3 subsystems where if any one of the subsystems is operational, the system as a whole is operational. subsystem**

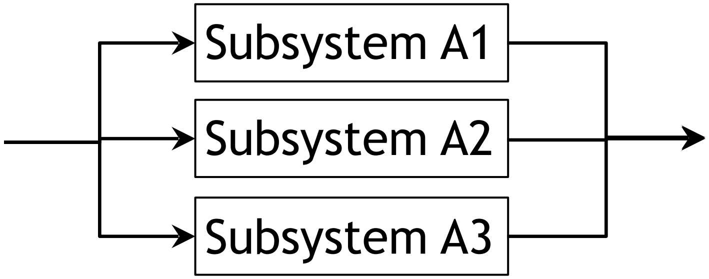


If R_{A1} = R_{A2} = R_{A3} = 0.9, then $R = 1 - (1 - .9)^3 = 0.999$

The parallel network has resulted in probably of a failure during a mission going from 1/10 to 1/1000

Parallel Systems Another Example

Consider



where

$$R_{A1} = 0.9999, \quad R_{A2} = 0.9995 \quad \text{and} \quad R_{A3} = 0.999$$

then

$$R = 1 - (1 - 0.9999)(1 - 0.9995)(1 - 0.999) = 0.0000000005$$

Or the probably of a system failure with just subsystem A1 went from 1 out of 10,000 to 1 out of 2,000,000,000.

To put in perspective, the 777 has 9 parallel flight computer. Even if each had only had a reliability of 0.99, this subsystem would have a reliability with 18 9’s

Combining Parallel and Serial Systems

- **In some systems there may be subsystems that are subject to higher failure rates and as such may need to be parallelized to obtain a sufficiently high system reliability while other system may not.**

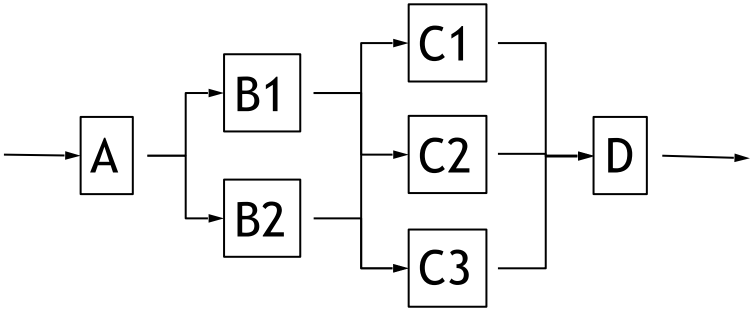
If a system has serial components *S_1* … *S_m* with reliabilities R_{Si} and parallel subsystems *P_1* … *P_n* and parallel subsystem *P_i* is composed of *i_k* components in parallel with reliabilities $R_{P_{i_j}}$

the reliability of the system is

$$R = \left(\prod_{j=1}^{m} R_{S_j} \right) \prod_{i=1}^{n} \left[1 - \prod_{h=1}^{i_k} \left(1 - R_{P_{i_h}} \right) \right]$$

A Combined Parallel/Serial Reliability Example

- **Suppose a system as two sets of redundant subsystems along with two serial subsystems.**
  - Serial subsystem A and D have reliabilities of .99999 and .99995 respectively.
  - The first set of parallel subsystems consists of two identical subsystems B1 & B2 each with a reliability of .995
  - The second set of parallel subsystems consists of three identical subsystems C1, C2, C3 with reliability .97



$$R_A = 0.99999\ ,\ \ R_B = 1-(1-R_{B1})(1-R_{B2}) = 1-.005^2 = 0.999975$$

$$R_C = 1-(1-R_{C1})(1-R_{C2})(1-R_3) = 1-.03^3 = 0.999973\quad ,\quad R_D = 0.99995$$

$$R = R_A R_B R_C R_D = 0.99999 * 0.999975 * 0.999973 * 0.99995 = 0.999913$$

Reliability Allocation

- **Overall system reliability is a frequent requirement**
  - Reliability is allocated to each of the subsystems, i.e., a subsystem will receive a reliability allocation of the form:
the reliability will be greater than or equal to an allocation
  - Reliability allocations are frequently done in terms of failure rates or MTBFs, i.e. Failure rate $\leq$ n failures/hour, MTBF $\geq$ m hours.
    - MTBF is frequently determined by observation of components/subsystems that have been previously used.

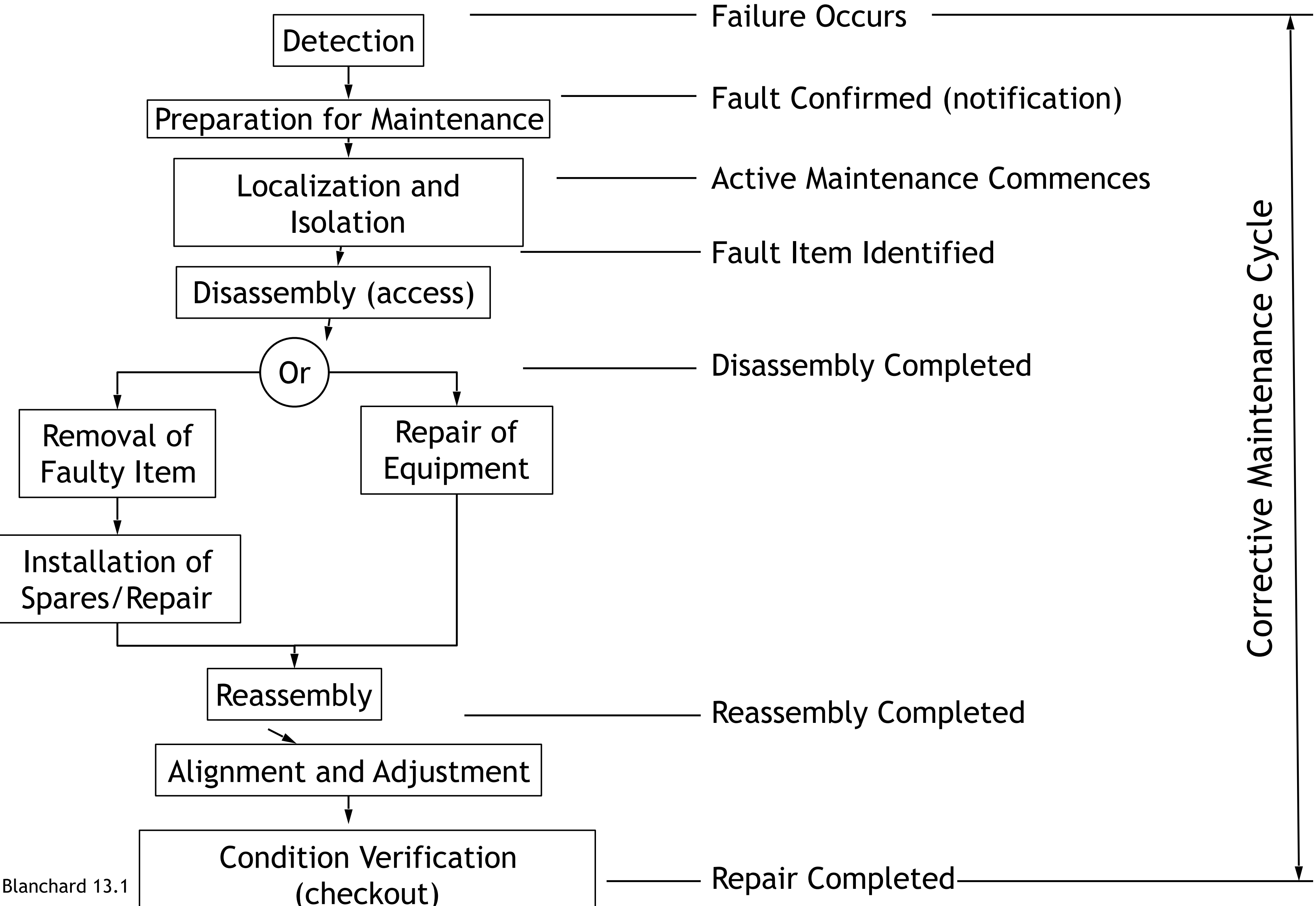
Reliability Test and Evaluation

- **Many different techniques are utilized for reliability test and evaluation**
  - For example the DOD has multiple documents defining reliability testing, the site - http://www.weibull.com/knowledge/milhdbk.htm has dozens of the DOD reliability testing documents, e.g.,
    - MIL-STD-883E Test Method Standard Microcircuits
    - MIL-HDBK-781 Handbook for Reliability Test Methods, Plans and Environments for Engineering, Development, Qualification, and Production

Maintainability

- **Maintenance breaks into broad categories**
  - Corrective Maintenance – fix something that is broken, i.e., that has failed
    - Fix a flat tire
  - Condition Based Maintenance - accomplished based on a set of operational conditions (changing fluids based on level of contaminants).
  - Preventative Maintenance – maintenance preformed to avoid potential failures, e.g., changing timing belt in an auto after a given number of miles have been driven
- **These types of maintenance apply to software as well as hardware**
  - Addition of new features via software is frequently referred to in the industry as “maintenance.” Since this is adding functionality, e.g., going beyond the stated functionality of the system, this type of “maintenance” is sometimes referred to as “adaptive maintenance.”
    - Many commercial software companies may offer a “maintenance” package with the software that included corrective maintenance as well as enhancements – additional functionality or improved performance

Corrective Maintenance Action



Detection

Preparation for Maintenance

Localization and Isolation

Disassembly (access)

Or

Removal of Faulty Item

Repair of Equipment

Installation of Spares/Repair

Reassembly

Alignment and Adjustment

Condition Verification (checkout)

Failure Occurs

Fault Confirmed (notification)

Active Maintenance Commences

Fault Item Identified

Disassembly Completed

Reassembly Completed

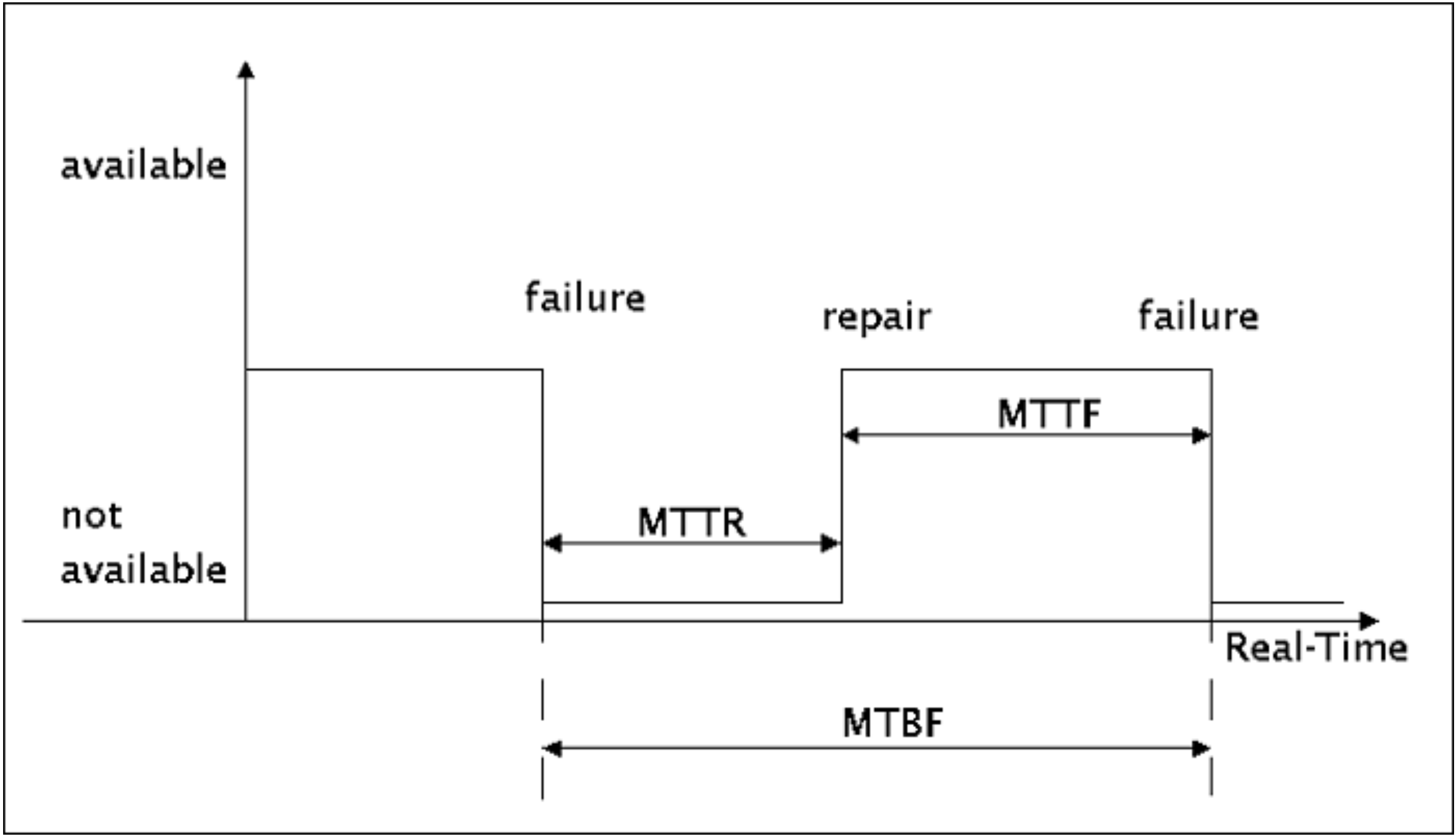
Repair Completed

Corrective Maintenance Cycle

Blanchard 13.1

Quantifying Maintenance

- **Mean Time To Repair (MTTR)**
  - Average time to repair over the set of corrective maintenance actions weighted by their frequency of occurrence. MTTR does not include preventative maintenance actions
    - If there were two corrective maintenance actions, A and B, with A occurring 75% of the time and B occurring 25% of the time and A took 1 hour and B took 4 hours, the MTTR would be 1.75 hours
  - MTTR can be miss leading if the number of possible maintenance actions is small with widely varying times
  - MTTRs will frequently be given according to the problem being corrected
    - Repairing items on automobiles will have a “book time”
      - A well trained mechanic will take this amount of time to perform the repair.
  - MTTRs are one reflection of how well maintainability was designed into a system.


available
not available
failure
repair
failure
MTTF
MTTR
Real-Time
MTBF

Preventative Maintenance

- **Mean Preventative Maintenance Time (MPMT) is the preventative maintenance required to keep a system at its specified level of performance**

$$\overline{\mathrm{M}}\mathrm{pt} = \mathrm{MTMP} = \frac{\sum \left(\mathrm{fpt_i}\right)\left(\mathrm{Mpt_i}\right)}{\sum \left(\mathrm{fpt_i}\right)}$$

Where fpt_i is the frequency of the ith preventative maintenance action and Mpt_i is elapsed time for the ith preventative maintenance action. MTMP or $\overline{\mathrm{M}}\mathrm{pt}$ is summed over all preventative maintenance actions.

Average Maintenance Time

- Mean Active Maintenance Time or $\overline{\mathrm{M}}$ is the mean elapsed time required to perform preventative maintenance and corrective maintenance

$$\overline{\mathrm{M}} = \frac{(\lambda)\mathrm{MTTR} + (\mathrm{fpt})\overline{\mathrm{M}}\mathrm{pt}}{\lambda + \mathrm{fpt}}$$

Where λ is the corrective maintenance rate and fpt is the preventative maintenance rate

Additional Maintenance Measures

- **Mean Time Between Replacement (MTBR)**
  - This is the average time between when a component will need to be replaced. It is a major determining factor for spares for a system
- **Mean Time Between Maintenance**

$$\mathrm{MTBM} = \frac{1}{1/\mathrm{MTBM}_{\mu} + 1/\mathrm{MTBM}_{s}}$$

Where MTBM_{μ} is the time between unscheduled (corrective maintenance) and MTBM_{s} is the time between scheduled maintenance

Elements of Effectiveness

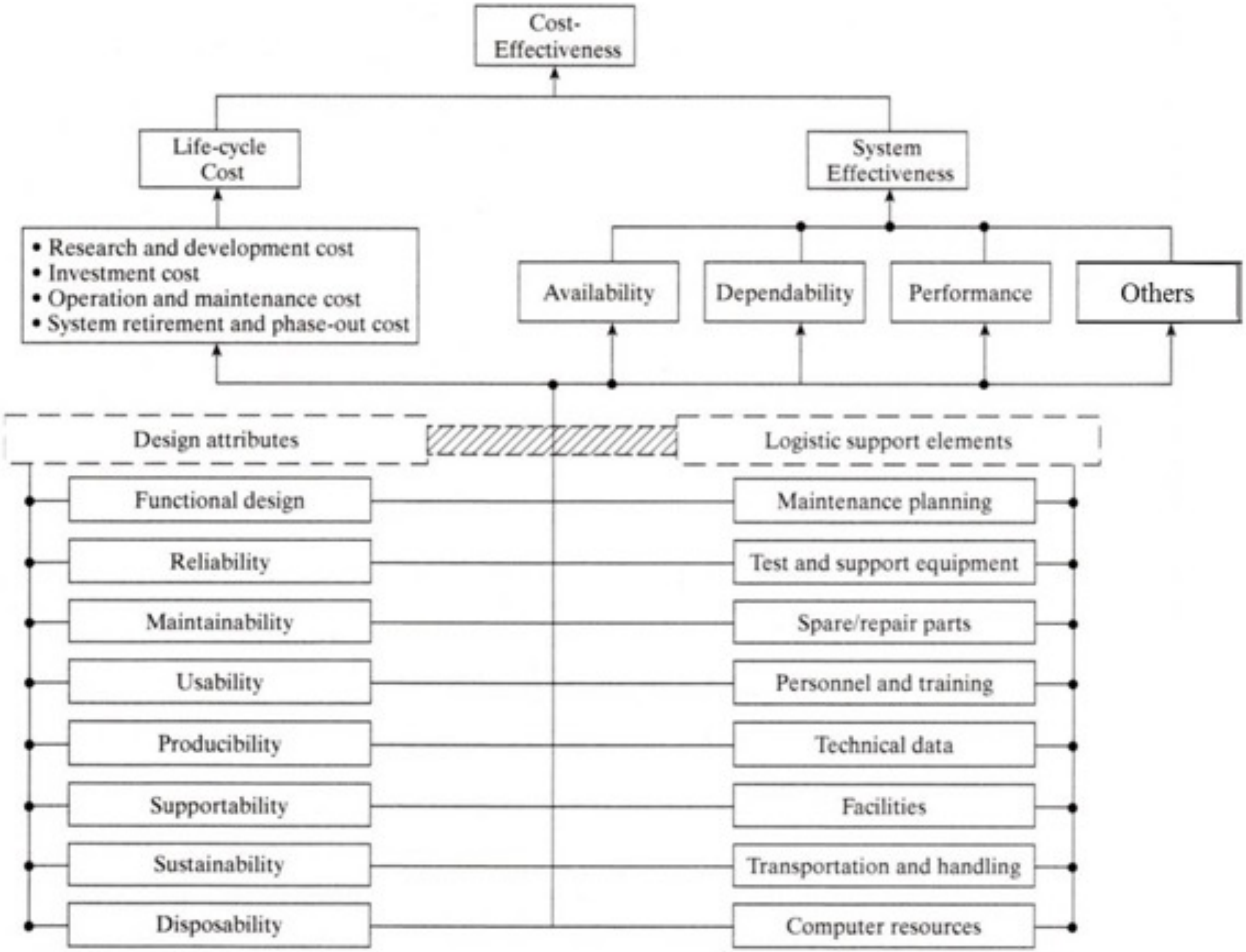


Figure 13.9 Blanchard

How important is maintenance?

Additional Maintenance Considerations

- **Two additional factors that are not included in the previously defined maintenance times that occur in reality are**
  - Logistical Delay Time (LDT) – this is the system down time while waiting for a spare, test equipment or maintenance staff to become available.
  - Administrative Delay Time (ADT) – this is the delay time that occurs for administrative reasons, e.g., approval to repair, funding.
- **Maintenance Down Time (MDT)**
  - This is the total amount of elapsed time to repair a non-operational system to full operational status. It includes $\overline{\mathrm{M}}$
    the mean active maintenance time, LDT and ADT

Maintainability Requirements Allocation

- **Maintainability, as with any other aspect of a complete system, will have requirements at a system level that need to be allocated to achieve overall system performance**
  - Different aspects of maintainability, e.g., preventative maintenance versus corrective maintenance, will have significantly different effects on different parts of a system
    - Moving mechanical components may have lubrication requirements. This can be dramatically effected by design
      - Autos made in the 1960's required bearings to have grease applied regularly, e.g., whenever oil was changed. Design improvements and changes eliminated the need for this thereby having a significant impact on preventative/scheduled maintenance
  - Maintainability is also about how maintenance of an item will be done if required. Poor design and have a dramatic effect on the cost of preforming maintenance and the associated down time.

Verification of Repair Times

- **Maintenance verification is typically performed via demonstrations**
  - Purpose of the demonstrations is to show that MTTR requirements are satisfied and to demonstrate that faults are detected.
- **Demonstration methods**
  - Failure is induced into the equipment without knowledge of the test team.
    - The test team is then responsible for finding and repairing the failure
    - The time for the process is recorded
    - The process is repeated over a range of possible faults to obtain statistics on the equipment as a whole
  - Test team will be asked to replace components to determine the actual time required to replace components.
    - This is a method of testing maintenance times that is especially appropriate if the time to diagnose a fault is minimal, e.g., replacing a broken axel on a vehicle
- **How is system maintenance validation approached?**

Availability

- **The availability of a system, whether explicitly stated as a design requirement or not is one of the most important aspects of a system**
- **A number of different availability measures are discussed as certain systems may require significant amounts of non-failure related maintenance and it may not be desirable, on the users part, to include this type of maintenance in the availability numbers**
  - Consider the maintenance on the former space shuttles that was required after each flight. This maintenance was know and factored into the total number of space shuttles in the fleet.

Availability

- **A_i is the inherent availability of a system**
  - the probability that a system or equipment, when used under stated conditions in an ideal support environment, will operate satisfactorily an any point in time as required

$$A_i = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

  Where MTBF is the mean time between failures and MTTR is the mean time to repair

  - A_i is what is normally referred to as availability

Achieved Availability

- **A_a or the availability achieved by a system is the probability that a system when used in an ideal support environment. It includes the preventative maintenance that is not included in A_i the inherent availability of a system**

$$A_a = \frac{\text{MTBM}}{\text{MTBM} + \overline{\overline{\text{M}}}}$$

Where MTBM is the mean time between maintenance and

$\overline{\text{M}}$ is mean active maintenance time

Operational Availability

- **Operational Availability (A_o) is the probability that a system when used under stated conditions in an actual operational environment will operate satisfactorily when called upon**

$$A_o = \frac{\text{MTBM}}{\text{MTBM} + \text{MDT}}$$

Where MTBM is the mean time between maintenance and MDT is the mean maintenance down time

- **A_o is the availability number that is of the most interest to a user of a system as it represents what is likely to be expected.**

Final Thoughts

- **RMA (Reliability, Maintainability, Availability) models for a system are general not know**
  - There may be historical data on portions and building blocks of a system. These building blocks provide a basis for RMA predictions.
  - RMA is statistical in nature and the answers to general RMA questions are generally answered with statistics
    - We predict how long a component will last, this is probabilistic by its very nature
  - Design techniques are utilized to increase the overall availability of a system by allowing faults to happen without degrading system performance
    - One power plant going off-line, e.g., a fault causing it to have to be taken off-line, does (should not) impact the availability of electricity
- **The RMA associate with a system on initial fielding can and usually does improve with time and design changes**