RISK-INFORMED OPERATIONAL DECISION MANAGEMENT

RELIABILITY AND AVAILABILITY

Michael W. Golay
Professor of Nuclear Engineering
Massachusetts Institute of Technology

Component States and Populations

Successful — N_s

Failure ↓ ↑ Repair

Failed — N_f

Consider a population, N_{so}, of successful components and, N_{fo}, failed components placed into service at the same time.

At time, t, progresses, some of these components will fail and some of the failed components will be repaired and returned to service.

The expected populations of components vary in time as:

Expected Successful Components:	$N_s = N_o P_s(t)$	
Expected Failed Components:	$N_f = N_o P_f(t)$	and
Probability Conservation:	$P_s(t) + P_f(t) = 1$	and
Component Conservation:	$N_s(t) + N_f(t) = N_o$	

COMPONENT FAILURE PROBABILITY

Component (Conditional) Failure Rate, $\lambda(t)$,

$$\frac{1}{P_s(t)}\frac{dP_s(t)}{dt} = \frac{1}{N_s(t)}\frac{dN_s(t)}{dt} = -\lambda(t)$$

where

$P_s(t)$ = probability that an individual component will be successful at time, t;

$N_s(t)$ = expected number of components surviving at time, t (note that $N_s(t=0) = N_{so}$);

$\lambda(t)$ = time-dependent (conditional) failure rate function.

Mean-Time-To-Failure (MTTF) = $1/\lambda = \tau_f$,

for λ = constant.

COMPONENT REPAIR PROBABILITY

Component Repair Coefficient, $\mu(t)$,

$$\frac{1}{P_f(t)}\frac{dP_f(t)}{dt} = \frac{1}{N_f(t)}\frac{dN_f(t)}{dt} = -\mu(t)$$

where

$P_f(t)$ = probability that an individual component will be failed at time, t;

$N_f(t)$ = expected number of components failed at time, t (note that $N_f(t=0) = N_{fo}$);

$\mu(t)$ = time-dependent (conditional) repair rate function.

Mean-Time-To-Repair (MTTR) = $1/\mu = \tau_R$,

for μ = constant.

Combined Repair and Failure

$$\frac{dN_s}{dt} = -\lambda N_s(t) + \mu N_f(t)$$

$$\frac{dN_f}{dt} = \lambda N_s(t) - \mu N_f(t)$$

can express as matrix equation

$$\frac{d\overline{N}}{dt} = M\overline{N} \ ,$$

where

$$\overline{N} = \begin{pmatrix} N_s(t) \\ N_f(t) \end{pmatrix} \ , \ \text{and} \ \ M = \begin{pmatrix} -\lambda & \mu \\ \lambda & -\mu \end{pmatrix} \ .$$

This is the relationship for a Markov process, where for a single component:

$$\frac{d\overline{P}(t)}{dt} = M\overline{P}(t) \ ,$$

where

$$\overline{P}(t) = \ \text{state vector of the component} = \begin{pmatrix} P_s(t) \\ P_f(t) \end{pmatrix} \ .$$

For initial condition $P_s(t=0) = 1$ and $P_f(t=0) = 0$,

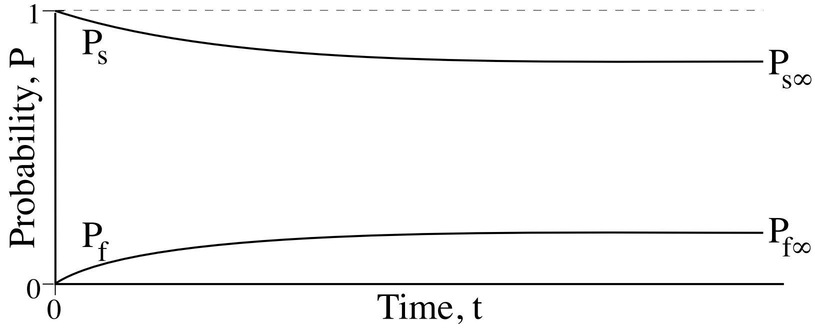
Solution is:

$$P_s(t) = \frac{\mu}{\lambda + \mu} + \left(\frac{\lambda}{\lambda + \mu}\right) e^{-(\lambda+\mu)t}$$

$$P_f(t) = \left(\frac{\lambda}{\lambda + \mu}\right)\left[1 - e^{-(\lambda+\mu)t}\right] .$$

Asymptotic result: (i.e., as $t \rightarrow \infty$)

$$P_{s_\infty} = \left(\frac{\mu}{\lambda + \mu}\right) , \qquad P_{f_\infty} = \left(\frac{\lambda}{\lambda + \mu}\right) .$$



COMPONENT CYCLE: RUN-TO-FAILURE, REPAIR AND RETURN-TO-SERVICE

Consider that total mean cycle time is τ_{cycle} for:

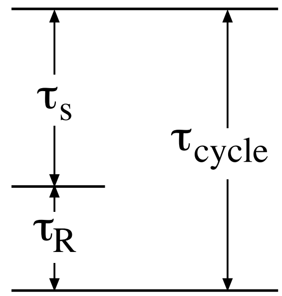
<u>Component Status</u>

a) Service $= \tau_s$ (= MTTF)

b) Failure

c) Waiting for repair $= \tau_R$ (= MTTR)

d) Repaired to service



$$\tau_{cycle} = \tau_s + \tau_R = \frac{1}{\lambda} + \frac{1}{\mu} = \frac{\mu + \lambda}{\lambda\mu}$$

$$P_{s_\infty} = \frac{\tau_s}{\tau_{cycle}} = \frac{\mu}{\mu + \lambda}$$

$$P_{f_\infty} = \frac{\tau_R}{\tau_{cycle}} = \frac{\lambda}{\mu + \lambda}$$

EFFECTS OF COMPONENT TESTING AND INSPECTION

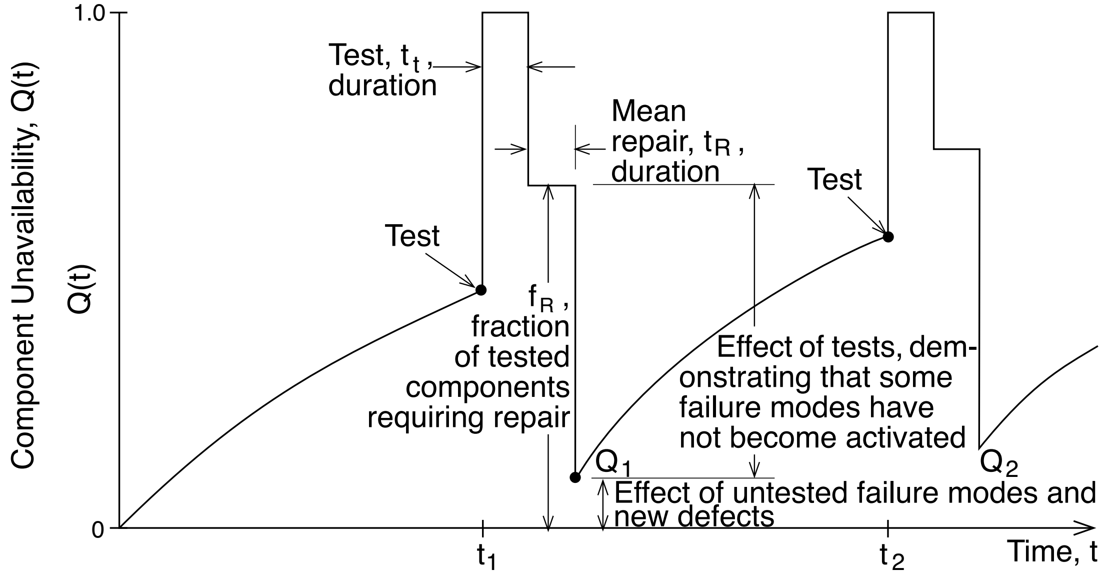
BENEFICIAL

- Verify That Component Is Operable
- Reveal Failures That Can Be Repaired
- Exercise Component and Maintain Operability
- Maintain Skills of Testing Team

HARMFUL

- Removal From Service Can Result in Complete Component Unavailability
- Wear and Tear Due to Testing (Wear, Fatigue, Corrosion, …)
- Introduction of New Defects (e.g., via Damage During Inspection, Fuel Depletion)
- Acceleration of Dependent Failures
- Damage or Degradation of Component via Incorrect Restoration to Service
- Human Error Can Cause Wrong Component to Be Removed From Service

TIME DEPEDENCE OF STANDBY COMPONENT UNAVAILABILITY, INCLUDING TEST AND REPAIR



t_1 = time of first test

t_i = time of i-th test

POST-TEST UNAVAILABILITY

CAUSED BY

- Failures Requiring Repairs, Caused by Tests
- Defects Introduced by Tests, Resulting in Later Failures
- Incorrect Component (and Supporting System) Disengagement, Re-Engagement
- Incorrect Component Having Been Tested

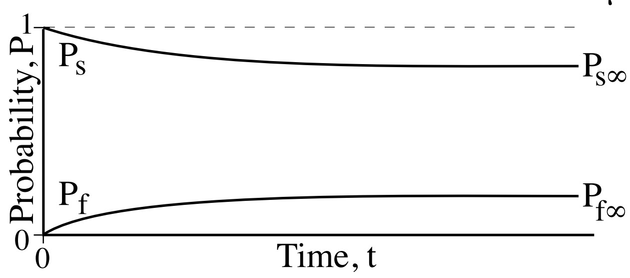
MEAN AVAILABILITY, <Q>, UNDER DIFFERENT COMBINATIONS OF TESTING AND REPAIR: CASES TO BE CONSIDERED (λ = CONSTANT)

CASES

1. Asymptotic Component Unavailability as Function of μ, λ
2. Mean Component Unavailability During Standby Interval
3. Cycle Mean Unavailability Due to
   - Defects randomly introduced during standby,
   - Unavailability due to testing and repairs
4. Cycle Mean Unavailability Due to
   - Pre-existing defects,
   - Defects introduced during standby, and
   - Unavailability due to testing and repairs
5. Standby Interval That Minimizes <Q>

CASE 1. ASYMPTOTIC AVAILABILITY WHEN FAILURES ARE MONITORED AND REPAIRED

$$\text{Asymptotic Availability}: \quad A_\infty = P_{s_\infty} = \frac{\mu}{\mu + \lambda}$$



Note that MTTR $= \frac{1}{\mu} = T_D$ (T_D = repair-related down-time)

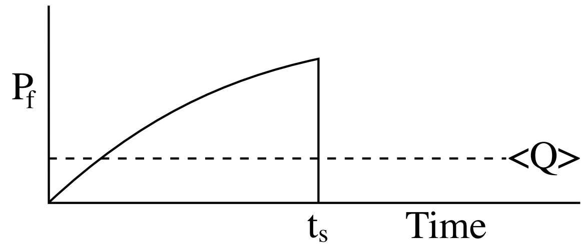
$$\Rightarrow \boxed{A = \frac{1}{1 + \lambda T_D}} \quad \text{and} \quad \boxed{Q = 1 - A = \frac{\lambda T_D}{1 + \lambda T_D}}$$

$$\boxed{\text{also,} \quad Q \approx \lambda T_D}$$

CASE 2. MEAN UNAVAILABILITY DURING STANDBY PERIOD, t_s

During Standby: $Q(t) = P_f(t) = 1 - e^{-\lambda t_s} \approx 1 - (1 - \lambda t_s)$

$Q(t) \approx \lambda t_s$



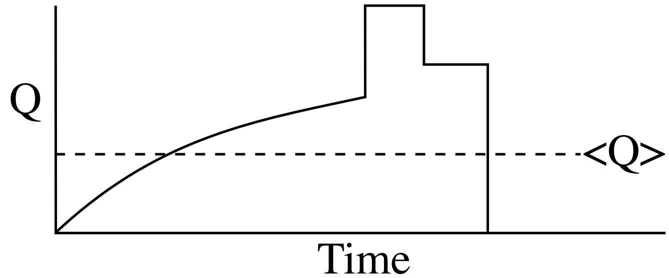
$$\langle Q \rangle = \frac{\int_0^{t_s} Q(t')dt'}{t_s} = \frac{\int_0^{t_s} \lambda(t')dt'}{t_s} = \lambda \frac{t_s^2}{2t_s}$$

$$\boxed{\langle Q \rangle = \lambda \frac{t_s}{2}}$$

CASE 3. MEAN CYCLE UNAVAILABILITY, INCLUDING TESTING AND REPAIR

For the Entire Testing Cycle Can Evaluate Expected Unavailability, <Q>, Due to Defects Introduced Randomly During Standby and Unavailability Due to Testing and Repairs as:

$$\langle Q \rangle = \frac{1}{t_c}\int_0^{t_c} Q(t)dt\,, \qquad \text{where}$$



CASE 3. MEAN CYCLE UNAVAILABILITY (continued)

DOWNTIME: $t_D = t_{D_s} + t_{D_t} + t_{D_R}$

During Standby: $t_{D_s} = \frac{\lambda t_s^2}{2}$

During Testing: $t_{D_t} = t_t$

During Repair: $t_{D_R} = f_R t_R$

f_R = repair frequency, the fraction of tests for which a repair is required

CYCLE TIME: $t_c = t_s + t_t + t_R$
(cycle = standby + testing + repair)

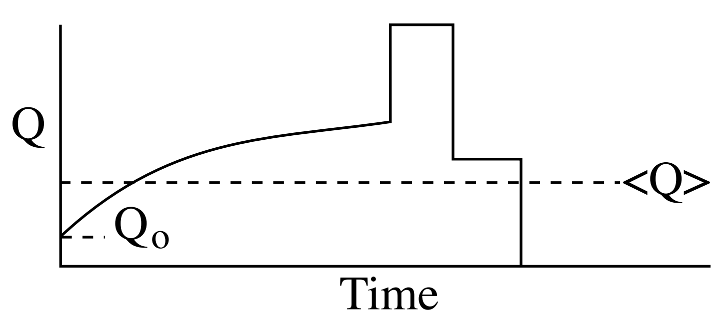
AVERAGE UNAVAILABILITY:

$$\langle Q \rangle = \frac{t_D}{t_c} = \frac{1}{t_c} * \left(\frac{\lambda t_s^2}{2} + t_t + f_R t_R \right)$$

CASE 4. MEAN CYCLE UNAVAILABILITY, INCLUDING PRE-EXISTING UNAVAILABILITY, Q_o

Evaluate Expected System Unavailability, <Q>, Due to

- Pre-Existing Defects
- Defects Introduced Randomly During Standby and
- Unavailability Due to Testing and Repairs as:



CASE 4. MEAN CYCLE UNAVAILABILITY, INCLUDING PRE-EXISTING UNAVAILABILITY, Q_o (continued)

DOWNTIME: $t_D = t_{D_s} + t_{D_t} + t_{D_R}$

During Standby: $t_{D_s} = Q_o t_s + \frac{\lambda}{2} t_s^2 (1 - Q_o)$

Q_o = expected unavailability due to pre-existing defects (i.e., those not interrogated during testing)

During Testing: $t_{D_t} = t_t$

During Repair: $t_{D_R} = f_R t_R$

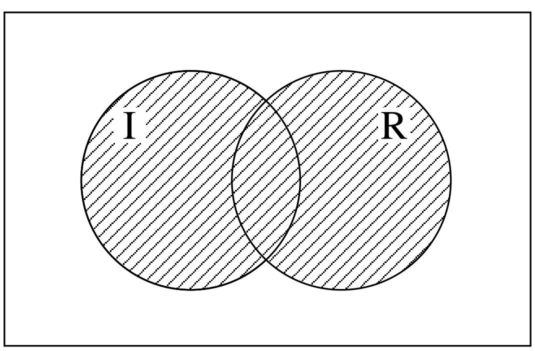
For Entire Cycle: $t_D = Q_o t_s + (1 - Q_o) \frac{\lambda}{2} t_s^2 + t_t + f_R t_R$

CYCLE TIME: $\underset{\text{cycle}}{t_c} = \underset{\text{standby}}{t_s} + \underset{\text{testing}}{t_t} + \underset{\text{repair}}{t_R}$

AVERAGE UNAVAILABILITY:

$$\langle Q \rangle = \frac{t_D}{t_c} = \frac{1}{t_c} \left\{ \left[Q_o t_s + (1 - Q_o) \frac{\lambda}{2} t_s^2 \right] + t_t + f_R t_R \right\}$$

COMBINED CASE OF EFFECT UPON STANDBY SYSTEM FAILURE OF PRE-EXISTING FAULT AND RANDOMLY INTRODUCED FAULT



I = Pre-existing fault event

R = Random fault event

F = I+R = Component fault

$$P(F) = P(I + R) = P(I) + P(R) - P(I) \cdot P(R)$$

$$P(F) = Q_o + \frac{\lambda t_s}{2} - Q_o \cdot \frac{\lambda t_s}{2}$$

$$P(F) = Q_o + (1 - Q_o) \frac{\lambda t_s}{2}$$

CASE 5. STANDBY INTERVAL THAT MINIMIZES <Q>

For a Good System: $t_t + f_R t_R << t_s$

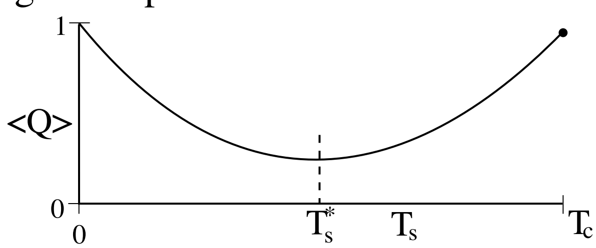
$$Q_o << 1$$

$$\Rightarrow \quad \langle Q \rangle \approx \frac{1}{t_c}\left(Q_o t_s + \frac{\lambda}{2} t_s^2 + t_t + f_R t_R \right)$$

The value of t_s which minimizes $\langle Q \rangle$, t_s^*, is obtained from $\frac{\partial \langle Q \rangle}{\partial t_s} = 0$ as

$$t_s^* = \left[\frac{2\left(t_t + f_R t_R\right)}{\lambda} \right]^{1/2} = \left[2\tau_f \left(t_t + f_R t_R\right) \right]^{1/2}$$

τ_f = random defects contribution
$(t_t + f_R t_R)$ = testing and repair contribution



CASE 5. STANDBY INTERVAL THAT MINIMIZES <U>

For a Good System: $t_t + f_R t_R << t_s$

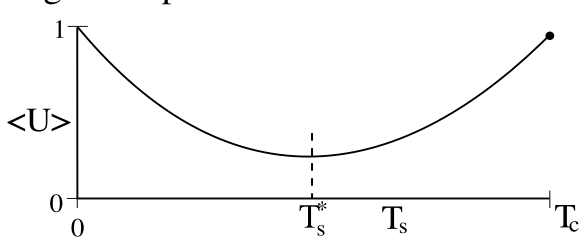
$$U_o << 1$$

$$\Rightarrow \quad \langle U \rangle \approx \frac{1}{t_c}\left(U_o t_s + \frac{\lambda}{2} t_s^2 + t_t + f_R t_R \right)$$

The value of t_s which minimizes $\langle U \rangle$, t_s^*, is obtained from $\frac{\partial \langle U \rangle}{\partial t_s} = 0$ as

$$t_s^* = \left[\frac{2\left(t_t + f_R t_R\right)}{\lambda} \right]^{1/2} = \left[2\tau_f \left(t_t + f_R t_R\right) \right]^{1/2}$$

τ_f = random defects contribution
$(t_t + f_R t_R)$ = testing and repair contribution



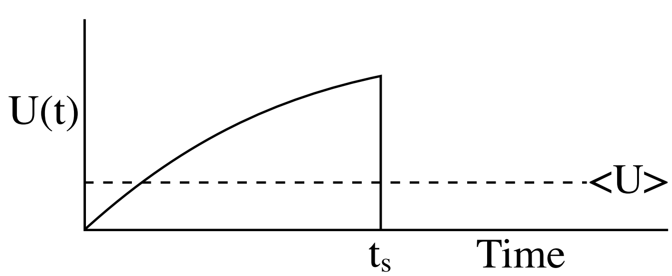
UNAVAILABILITY

- Failure density $f_T(t) = \lambda e^{-\lambda t} \quad t \geq 0$
- Cumulative Density Function (CDF): $F_T(t) = P(T \leq t) = \int_0^t f_T(t)dt$
- Unavailability $U(t)$:
  probability that system is down at time t,

$$U(t) = F_T(t) = \int_0^t f_T(t)dt = 1 - e^{-\lambda t} \approx 1 - (1 - \lambda t)$$

$$U(t) \approx \lambda t$$

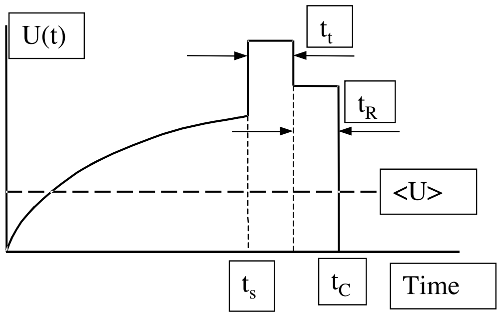
MEAN UNAVAILABILITY DURING STANDBY PERIOD, t_s



$$< U >= \frac{1}{t_s}\int_0^{t_s} U(t)dt \approx \int_0^{t_s} \lambda t dt = \lambda \frac{t_s^2}{2t_s}$$

$$< U > \approx \lambda \frac{t_s}{2}$$

MEAN CYCLE UNAVAILABILITY, INCLUDING TESTING AND REPAIR



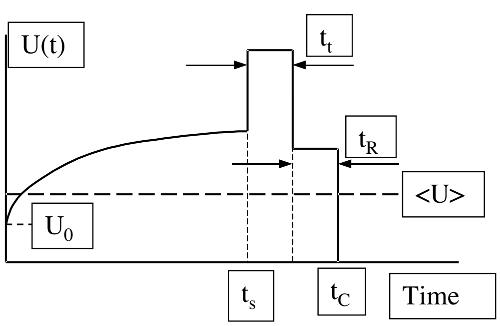
$$U(t) = \begin{cases} \lambda t & (0 \le t \le t_s) \\ 1 & (t_s < t \le t_s + t_t) \\ f_R & (t_s + t_t < t \le t_C) \end{cases}$$

$$< U > = \frac{1}{t_C} \times \int_0^{t_C} U(t)dt$$

$$= \frac{1}{t_C} \times \left[\int_0^{t_s} \lambda t dt + \int_{t_s}^{t_s + t_t} dt + \int_{t_s + t_t}^{t_c} f_R dt \right]$$

$$= \frac{1}{t_C} \times \left[\frac{\lambda}{2} t_s^2 + t_t + f_R t_R \right]$$

MEAN CYCLE UNAVAILABILITY INCLUDING PRE-EXISTING UNAVAILABILITY, U_0



$$U(t) = \begin{cases} U_0 + (1 - U_0)\lambda t & (0 \le t \le t_s) \\ 1 & (t_s < t \le t_s + t_t) \\ f_R & (t_s + t_t < t \le t_C) \end{cases}$$

$$< U > = \frac{1}{t_C} \times \int_0^{t_C} U(t)dt$$

$$= \frac{1}{t_C} \times \left[\int_0^{t_s} U_0 + (1 - U_0)\lambda t dt + \int_{t_s}^{t_s + t_t} dt + \int_{t_s + t_t}^{t_c} f_R dt \right]$$

$$= \frac{1}{t_C} \times \left[\left(U_0 t_s + (1 - U_0) \frac{\lambda}{2} t_s^2 \right) + t_t + f_R t_R \right]$$

STANDBY INTERVAL, t_s^*, THAT MINIMIZES <U>

- $< U >= \frac{1}{t_C} \times \left[\left(U_0 t_s + (1 - U_0) \frac{\lambda}{2} t_s^2 \right) + t_t + f_R t_R \right]$
- For a good system $\begin{cases} t_t + f_R t_R << t_s \\ U_0 << 1 \end{cases} \Rightarrow \begin{cases} t_C = t_s + t_t + t_R \approx t_s \\ (1 - U_0) \approx 1 \end{cases}$

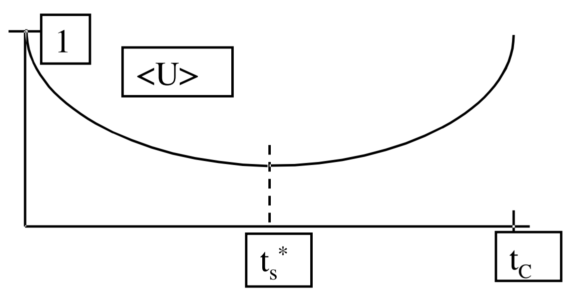
$$\Rightarrow < U > \approx \frac{1}{t_s} \times \left[\left(U_0 t + \frac{\lambda}{2} t_s^2 \right) + t_t + f_R t_R \right]$$

$$\frac{\partial < U >}{\partial t_s} (t_s^*) = 0$$

$$\frac{\partial < U >}{\partial t_s} (t_s^*) = \frac{\lambda}{2} - (t_t + f_R t_R) \times \frac{1}{t_s^{*2}} = 0$$

$$\Rightarrow t_s^* = \left[\frac{2(t_t + f_R t_R)}{\lambda} \right]^{1/2}$$

STANDBY INTERVAL, t_s^*, THAT MINIMIZES <U> (continued)



$$t_s^* = \left[\frac{2(t_t + f_R t_R)}{\lambda} \right]^{1/2} = \left[2\tau_f \left(t_t + f_R t_R \right) \right]^{1/2}$$

t_f = random defects contribution

$(t_t + f_R t_R)$ = testing and repair contribution

MEAN UNAVAILABILITY, EXAMPLES

- Mean unavailability during standby period t_s:

$$t_s = 10^3 \text{hr}, \lambda = 10^{-4} \text{hr}^{-1}$$

$$< U >= \lambda \frac{t_s}{2} = 10^{-4} \times \frac{10^3}{2} = 0.05$$

- Mean cycle unavailability, including testing and repair:

$$t_s = 10^3 \text{ hr}, \quad \lambda = 10^{-4} \text{ hr}^{-1}, \quad t_t = 25 \text{ hr}, \quad t_R = 60 \text{ hr}, \quad f_R = 0.01$$

$$< U > = \frac{1}{t_C} \left[\frac{\lambda t_s^2}{2} + t_t + f_R t_R \right]$$

$$= \frac{1}{10^3 + 25 + 60} \left[\frac{10^{-4} \times 10^{3\times2}}{2} + 25 + 0.01 \times 60 \right] \approx 0.07$$

MEAN UNAVAILABILITY, EXAMPLES (continued)

- Mean cycle unavailability including U_0:

$$t_s = 10^3 \text{ hr}, \quad \lambda = 10^{-4} \text{ hr}^{-1}, \quad t_t = 25 \text{ hr}, \quad t_R = 60 \text{ hr}, \quad f_R = 0.01, \quad U_0 = 0.02$$

$$< U > = \frac{1}{t_C} \left[U_0 t_s + (1 - U_0) \frac{\lambda t_s^2}{2} + t_t + f_R t_R \right]$$

$$= \frac{1}{10^3 + 25 + 60} \left[0.02 \times 10^3 + (1 - 0.02) \frac{10^{-4} \times 10^{3\times2}}{2} + 25 + 0.01 \times 60 \right] \approx 0.087$$

- Optimum standby interval t_s:

$$t_s^* = \left[\frac{2(t_t + f_R t_R)}{\lambda} \right]^{1/2} = \left[\frac{2(25 + 0.01 \times 60)}{10^{-4}} \right]^{1/2} \approx 715.54 \text{ hr}$$

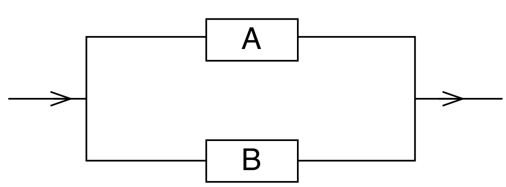
EXAMINATION OF SEQUENCING OF TESTS

EXAMPLE OF TWO PARALLEL INDENTICAL COMPONENTS

A) Successive Testing

B) Staggered Testing

FOR REDUNDANT SYSTEMS CAN COMBINE INDIVIDUAL COMPONENT UNAVAILABILITY VALUES TO OBTAIN OVERALL SYSTEM UNAVAILABILITY, CONSIDER A 1/2 PARALLEL SYTEM (e.g., Two Parallel EDGs), WHERE SUCCESS OF ONE COMPONENT IS SUFFICIENT FOR SYSTEM SUCCESS



$$Q_{system} = Q_A \cdot Q_B \qquad \text{(ignoring dependencies)}$$

In Standby:

$$Q_s(t) = \left(1 - e^{-\lambda_A t_A}\right)\left(1 - e^{-\lambda_B t_B}\right) \approx \lambda_A t_A \cdot \lambda_B t_B = \lambda_A \lambda_B t_A t_B$$

t_A = time that component A has been on standby
t_B = time that component B has been on standby

Note, effects of downtime for repair omitted from this analysis.

FOR REDUNDANT SYSTEMS CAN COMBINE INDIVIDUAL COMPONENT UNAVAILABILITY VALUES TO OBTAIN OVERALL SYSTEM UNAVAILABILITY, CONSIDER A 1/2 PARALLEL SYTEM (e.g., Two Parallel EDGs), WHERE SUCCESS OF ONE COMPONENT IS SUFFICIENT FOR SYSTEM SUCCESS (continued)

With Unit A in Testing: $Q_s = 1 \cdot \left(1 - e^{-\lambda_B t_B}\right) \approx \lambda_B t_B$

With Unit B in Testing: $Q_s = \left(1 - e^{-\lambda_A t_A}\right) \cdot 1 \approx \lambda_A t_A$

With Unit A in Repair: $Q_s = f_{R_A} \left(1 - e^{-\lambda_B t_B}\right) \approx f_{R_A} \cdot \lambda_B t_B$

where f_{R_A} = repair frequency of Unit A

With Unit B in Repair: $Q_s = f_{R_B} \left(1 - e^{-\lambda_A t_A}\right) \approx f_{R_B} \cdot \lambda_A t_A$

where f_{R_B} = repair frequency of Unit B

ILLUSTRATION OF INDIVIDUAL COMPONENT (e.g., EDG) UNRELIABILITIES FOR A 1/2 PARALLEL SYSTEM GIVEN A STRATEGY OF TESTING EACH COMPONENT AT SUCCESSIVE INTERVALS (e.g., TESTING BOTH COMPONENTS DURING SAME OUTAGE)

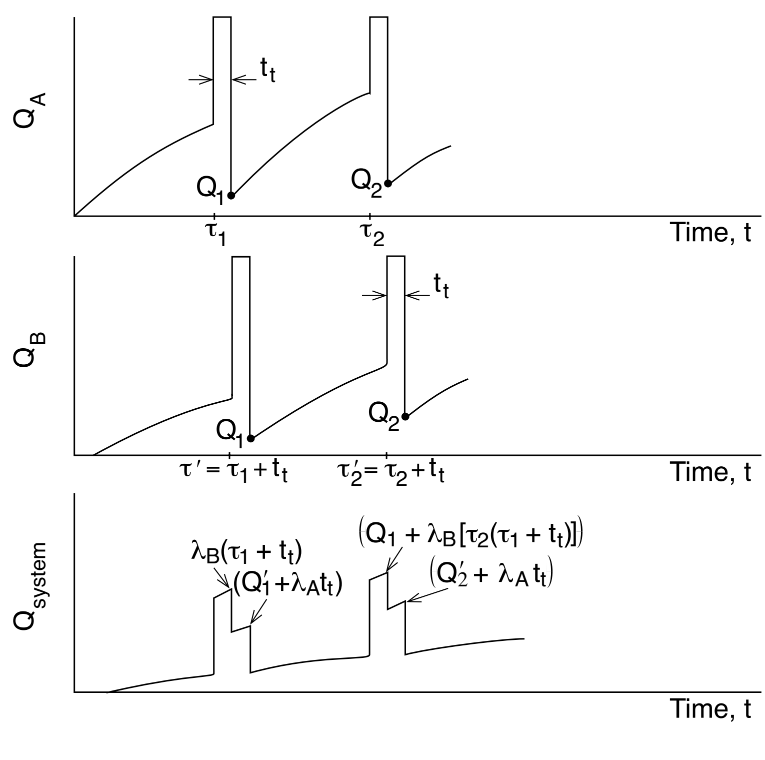
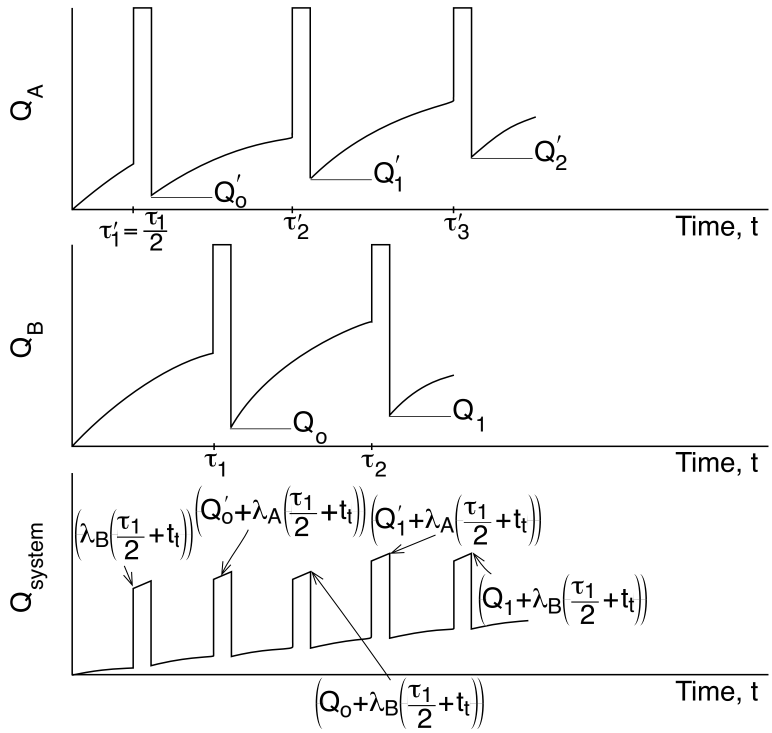


ILLUSTRATION OF INDIVIDUAL COMPONENT (e.g., EDG) UNRELIABILITY FOR A 1/2 PARALLEL SYSTEM GIVEN A STRATEGY OF TESTING EACH COMPONENT AT EVENLY STAGGERED



COMPARISON OF MAXIMUM AND AVERAGE VALUES OF Q, FIRST CYCLE OF TESTING

	Q_{max}
Successive Testing:	$\lambda_B(\tau_1 + t_t) \approx \lambda_B \tau_1$
Staggered Testing:	$\lambda_B\left(\frac{\tau_1}{2} + t_t\right) \approx \lambda_B \frac{\tau_1}{2}$

	$<Q>_{cycle}$
Successive Testing:	$\approx \lambda_B t_t$
Staggered Testing:	$\approx (\lambda_A + \lambda_B)\frac{t_t}{3}$

HUMAN ERRORS ARE TYPICALLY MOST IMPORTANT

Also, taking into account human errors committed during tests and repair and failure modes not tested previously.

Q_o = unavailability due to defects existing at the start of the next testing cycle

$$Q_o = Q_U + Q_H \ , \quad \text{where}$$

Q_U = unavailability due to failure modes not interrogated during the tests performed, and those activated upon demand

$Q_H = \lambda_t t_t + \lambda_R t_R$, and

λ_t = rate of introduction of defects due to human errors during tests (e.g., system realignment errors), hr^{-1}

λ_R = rate of introduction of defects due to human errors during repairs (e.g., incorrectly installed gaskets, tools or debris left within a component), hr^{-1}