Υπολογιστικά Συστήματα Υψηλής Αξιοπιστίας

Εισαγωγή στην αξιοπιστία συστημάτων

Δρ. Γκάμας Βασίλειος

Επιστημονικός Συνεργάτης
vgkamas@uniwa.gr

Πανεπιστήμιο Δυτικής Αττικής
Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών

Σκοπός παρουσίασης

- Να εισάγει τους φοιτητές στην έννοια της αξιοπιστίας (reliability) των υπολογιστικών συστημάτων και στην σχετική ορολογία

Εισαγωγή (1/4)

- **Αξιοπιστία**: εκφράζει το μέτρο της ικανότητας ενός συστήματος να λειτουργεί χωρίς αστοχίες
- Αποτελεί ποσοτική δήλωση της πιθανότητας ενός συστήματος να λειτουργεί στο περιβάλλον για το οποίο έχει σχεδιαστεί χωρίς αστοχίες, για ένα συγκεκριμένο χρονικό διάστημα

Σε ποιο απλουστευμένη διατύπωση, η αξιοπιστία εκφράζει την πιθανότητα επιτυχίας ενός συστήματος

Εισαγωγή (2/4)

- **Σύστημα**: συλλογή από επιμέρους τμήματα ή υποσυστήματα τα οποία έχουν συναρμολογηθεί με σκοπό την εκτέλεση μιας συγκεκριμένης διεργασίας
- Τυπικές αρχιτεκτονικές συστημάτων
  - Σειριακά (serial)
  - Παράλληλα (parallel)
  - Συνδυαστικά (serial + parallel)

Εισαγωγή (3/4)

- Η ακριβής εκτίμηση της αξιοπιστίας των σύγχρονων υπολογιστικών συστημάτων είναι εξαιρετικά δύσκολη διαδικασία για δυο βασικούς λόγους
  - Ο πρώτος λόγος είναι ο μεγάλος βαθμός αλληλεξάρτησης μεταξύ του υλικού και του λογισμικού
  - Ο δεύτερος λόγος είναι πως τα υποσυστήματα λογισμικού εξαιτίας της δυναμικής τους φύσης δεν επιδέχονται εύκολα την μαθηματική ανάλυση που απαιτείται για την διατύπωση ενός μοντέλου που θα περιγράφει την συμπεριφορά τους όσον αφορά την αξιοπιστία τους

Εισαγωγή (4/4)

- Παράμετροι που χρειάζεται να καθοριστούν για τον καθορισμό της αξιοπιστίας
  - Τι κάνει το σύστημα;
  - Ποια είναι η προδιαγεγραμμένη απόδοση του συστήματος;
  - Για πόσο διάστημά το σύστημα θα πρέπει να λειτουργεί;
  - Ποιες είναι οι συνθήκες κάτω από τις οποίες το σύστημα λειτουργεί;

Ανάγκη για αξιοπιστία

- Προβλήματα υλικού, π.χ.
  - Υπερθέρμανση, spike τάσης
  - Προβλήματα στον συγχρονισμό, crosstalk
  - Εξωτερικές παρεμβολές
- Προβλήματα λογισμικού, π.χ.
  - Υπερχείλιση μετρητή ή buffer
  - Μη αποδεκτή είσοδος στο πρόγραμμα
  - Ατέρμονος βρόχος

Σχεδιασμός αξιοπιστίας

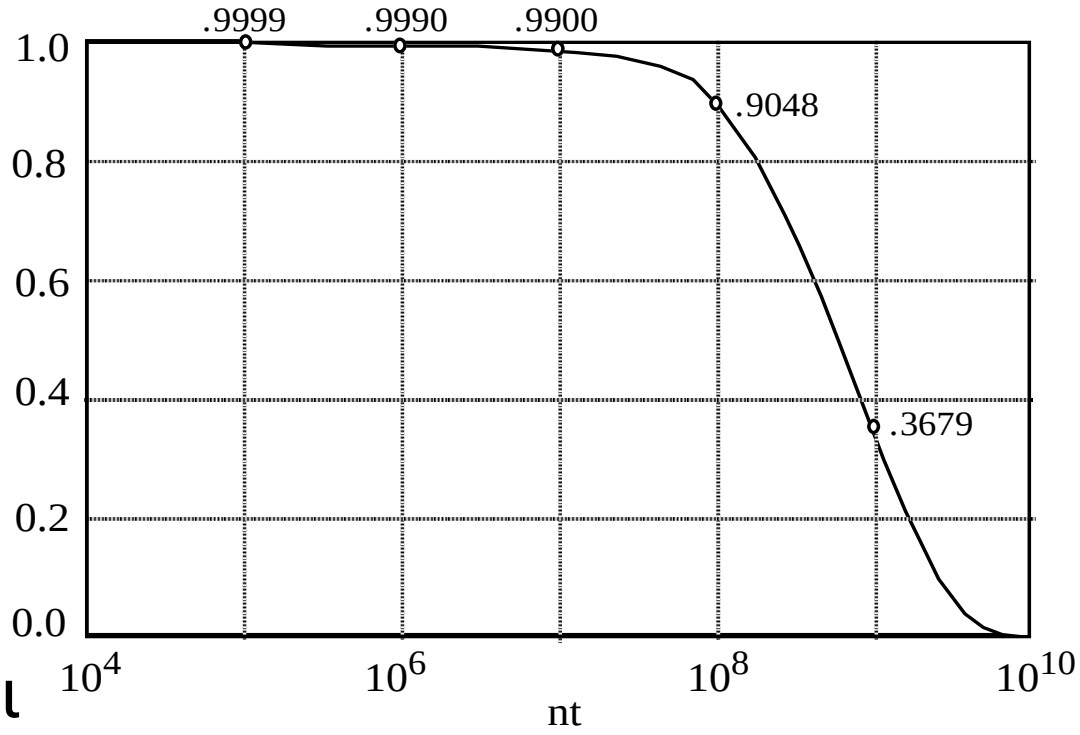
- Το επίπεδο αξιοπιστίας ενός συστήματος καθορίζεται κατά την διαδικασία του σχεδιασμού
- Η διαδικασία σχεδιασμού υπαγορεύει την παραμετροποίηση ενός συστήματος η οποία επηρεάζει το επίπεδο αξιοπιστίας
- Ο μηχανικός σχεδίασης του συστήματος θα πρέπει να είναι εξοικειωμένος με τις βασικές έννοιες της ανάλυσης της αξιοπιστίας οι οποίες μπορούν να χρησιμοποιηθούν για την αξιολόγηση του σχεδιασμού

Αξιοπιστία συστημάτων

- Η αξιοπιστία ενός συστήματος *n*-transistors κάθε ένα από τα οποία έχει ένα ρυθμό βλαβών λ δίνεται από την σχέση $e^{-n\lambda t}$

$$R(t) = e^{-n\lambda t}$$

- Υπάρχουν μόνο 3 τρόποι για να γίνει το σύστημα πιο αξιόπιστο
  - Να μειωθεί το λ
  - Να μειωθεί το n
  - Να μειωθεί το t

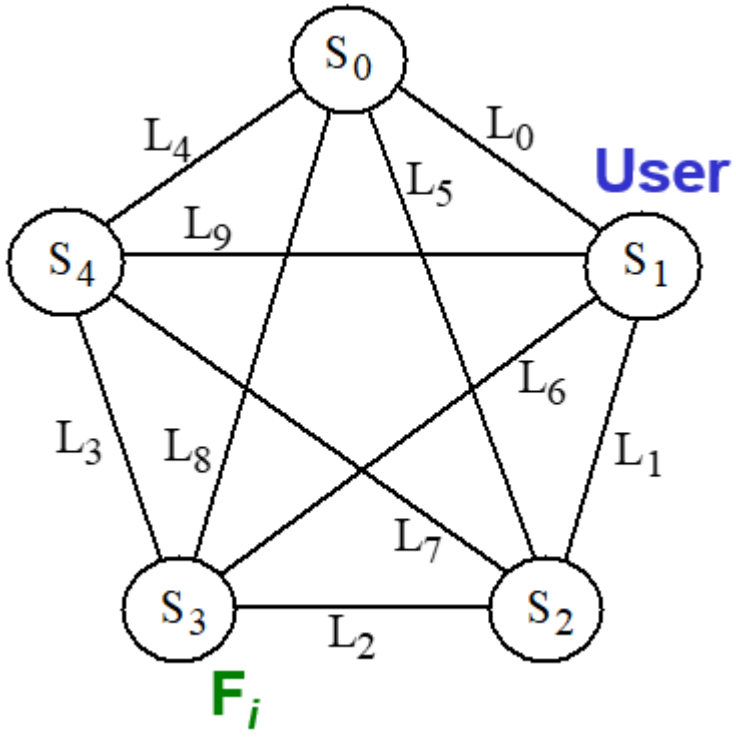


Ενναλακτική λύση

Αλλαγή του τρόπου υπολογισμού της αξιοπιστίας εισάγοντας στοιχεία πλεονασμού στο σύστημα!

Βελτιώνοντας την διαθεσιμότητα ενός συστήματος (1/3)

- Κατανεμημένη βάση δεδομένων με 5 sites
- Πλήρης διασύνδεση με αφιερωμένα κυκλώματα
- Τα sites και τα links μπορεί να εμφανίσουν δυσλειτουργία
- Ο πλεονασμός βελτιώνει την διαθεσιμότητα της βάσης δεδομένων



S: Πιθανότητα το site να είναι διαθέσιμο = 99%
L: Πιθανότητα το link να είναι διαθέσιμο = 95%

Single-copy availability = *SL*
Unavailability = 1 – *SL* = 1 – 0.99 × 0.95 = 5.95%

Βελτιώνοντας την διαθεσιμότητα ενός συστήματος (2/3)

- Data Duplication: Home και Mirror Sites

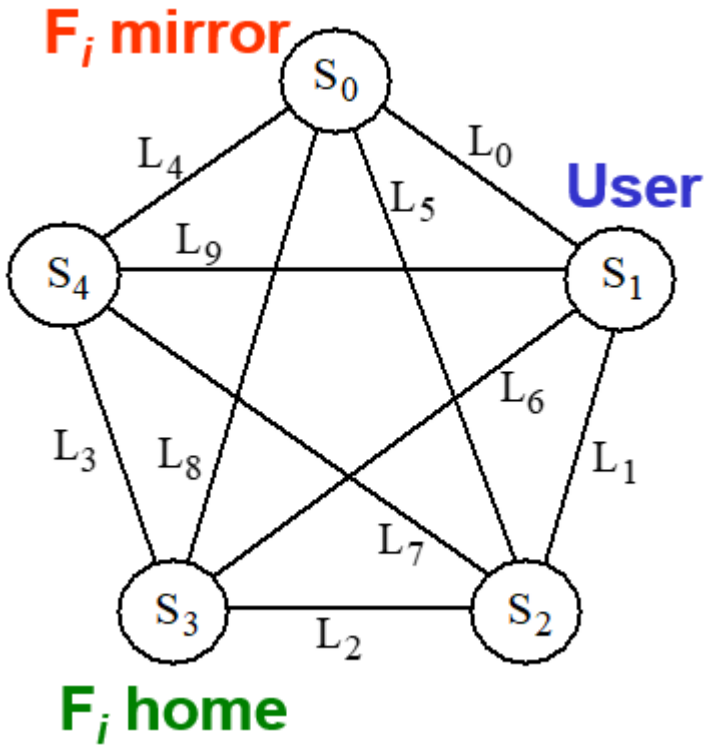
$$A = SL + (1 - SL)SL$$

Primary site can be reached

Mirror site can be reached

Primary site inaccessible

Duplicated availability = $2SL - (SL)^2$
Unavailability = $1 - 2SL + (SL)^2$ = 0.35%



Η μη διαθεσιμότητα δεδομένων μειώθηκε από το 5.95% στο 0.35%

Η διαθεσιμότητα βελτιώθηκε από το ≈ 94% στο 99.65%

Βελτιώνοντας την διαθεσιμότητα ενός συστήματος (3/3)

- Data Triplication: Home και 2 Backups

$$A = SL + (1 - SL)SL + (1 - SL)^2SL$$

Primary site can be reached

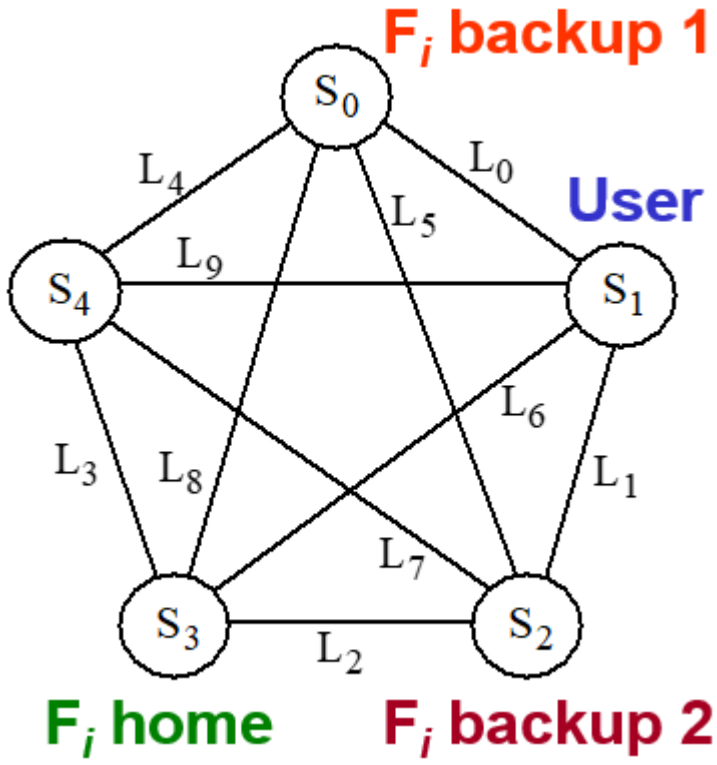
Primary site inaccessible

Backup 1 can be reached

Primary and backup 1 inaccessible

Backup 2 can be reached

Triplicated avail. = $3SL - 3(SL)^2 - (SL)^3$
Unavailability = $1 - 3SL - 3(SL)^2 + (SL)^3 = 0.02\%$



Η μη διαθεσιμότητα δεδομένων μειώθηκε από το 5.95% το 0.02%

Η διαθεσιμότητα βελτιώθηκε από το ≈ 94% το 99.98%

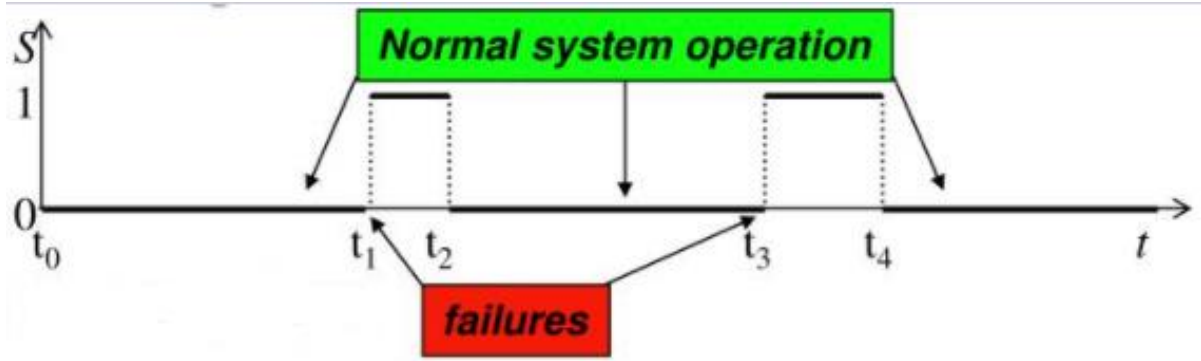
Ερωτήματα που αγνοήθηκαν στο προηγούμενο παράδειγμα (1/2)

- Πώς διατηρούνται συνεπή τα πλεονάζων αντίγραφα δεδομένων;
  - Όταν ένας χρήστης τροποποιεί δεδομένα πως ενημερώνονται τα αντίγραφά τους με γρήγορο τρόπο και αποφεύγεται η χρήση μη ενημερωμένων δεδομένων;
- Πως καθορίζονται τα μη λειτουργικά sites και links;
  - Η διάγνωση των σφαλμάτων θα πρέπει να είναι γρήγορη
- Πως γίνεται η ανάκτηση δεδομένων όταν ένα μη λειτουργικό site / link επιστρέφει σε κανονική λειτουργία;
  - Το site θα πρέπει να ενημερωθεί σχετικά με τις αλλαγές που έχουν πραγματοποιηθεί
- Πως εντοπίζονται σφάλματα που προκλήθηκαν στα δεδομένα;
  - Αυτό είναι αρκετά πιο δύσκολο σε σχέση με την ανίχνευση τυχαίων σφαλμάτων

Ερωτήματα που αγνοήθηκαν στο προηγούμενο παράδειγμα (2/2)

- Το προηγούμενο παράδειγμα καταδεικνύει ότι:
  - Υπάρχουν διάφορες λύσεις για την βελτίωση της αξιοπιστίας ενός συστήματος
  - Οι εναλλακτικές λύσεις θα πρέπει να αξιολογηθούν μέσω μοντελοποίησης
  - Θα πρέπει να επιλεγεί η πιο κοστοστρεφή λύση

Υπολογισμός αξιοπιστίας συστήματος



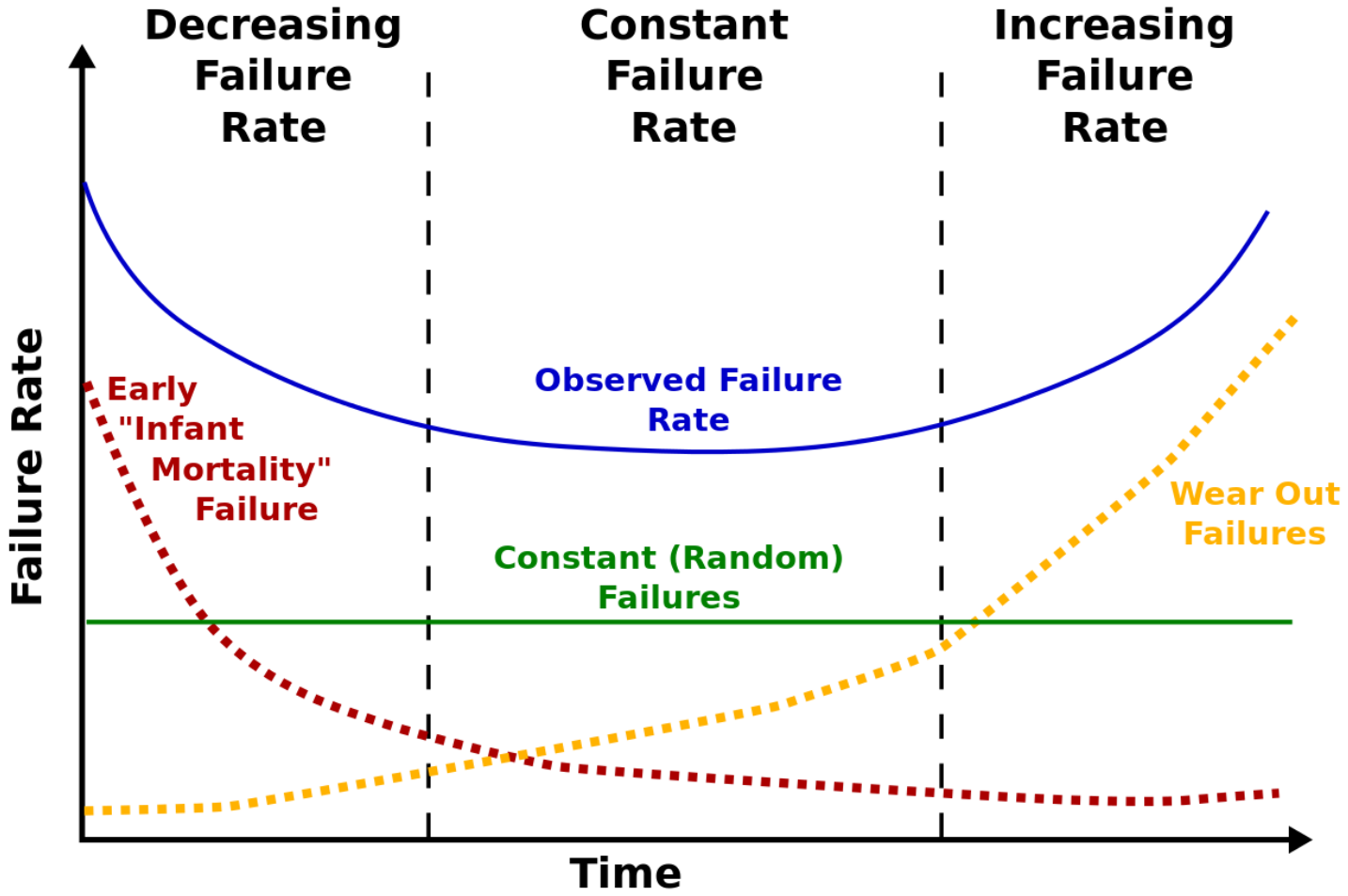
- Η χρονική διάρκεια κανονικής λειτουργίας (T_n) ενός συστήματος είναι τυχαίος αριθμός με εκθετική κατανομή
- Η πιθανότητα κανονικής λειτουργίας ενός συστήματος μέχρι την χρονική στιγμή t (δηλαδή η αξιοπιστία) είναι

$$R(t) = P(T_n > t) = e^{-\lambda t}$$

- Ο ρυθμός βλαβών (failure rate) λ ενός συστήματος είναι το άθροισμα του ρυθμού βλαβών λ_i των επιμέρους στοιχείων του συστήματος

$$\lambda = \sum_{i=0}^{k} \lambda_i$$

Καμπύλη Bathtub



Δείτε επίσης

Αξιοπιστία συστημάτων: Βασικοί δείκτες (1/3)

- Μέσος χρόνος μεταξύ βλαβών (Mean Time Between Failures)

$$MTBF = \int_0^\infty e^{-\lambda t} dt = \frac{1}{\lambda}$$

- Ο χρόνος επισκευής (repair time, *R*) ακολουθεί εκθετική κατανομή

$$P(R > t) = e^{-\mu t}$$

όπου *μ* ο ρυθμός επισκευής

Αξιοπιστία συστημάτων: Βασικοί δείκτες (2/3)

- Μέσος χρόνος αποτυχίας (Mean Time To Failure)

$$MTTF = \frac{1}{n}\sum_{i=1}^{n} T_i$$

όπου T_i είναι η διάρκεια ζωής του στοιχείου *i* και n είναι το πλήθος των στοιχείων του συστήματος

Αξιοπιστία συστημάτων: Βασικοί δείκτες (3/3)

- Μέσος χρόνος μέχρι την επισκευή (Mean Time To Repair)

$$MTTR = \frac{1}{\mu}$$

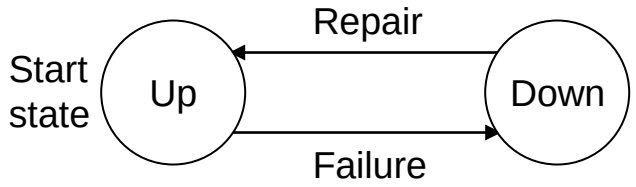
- Διαθεσιμότητα συστήματος

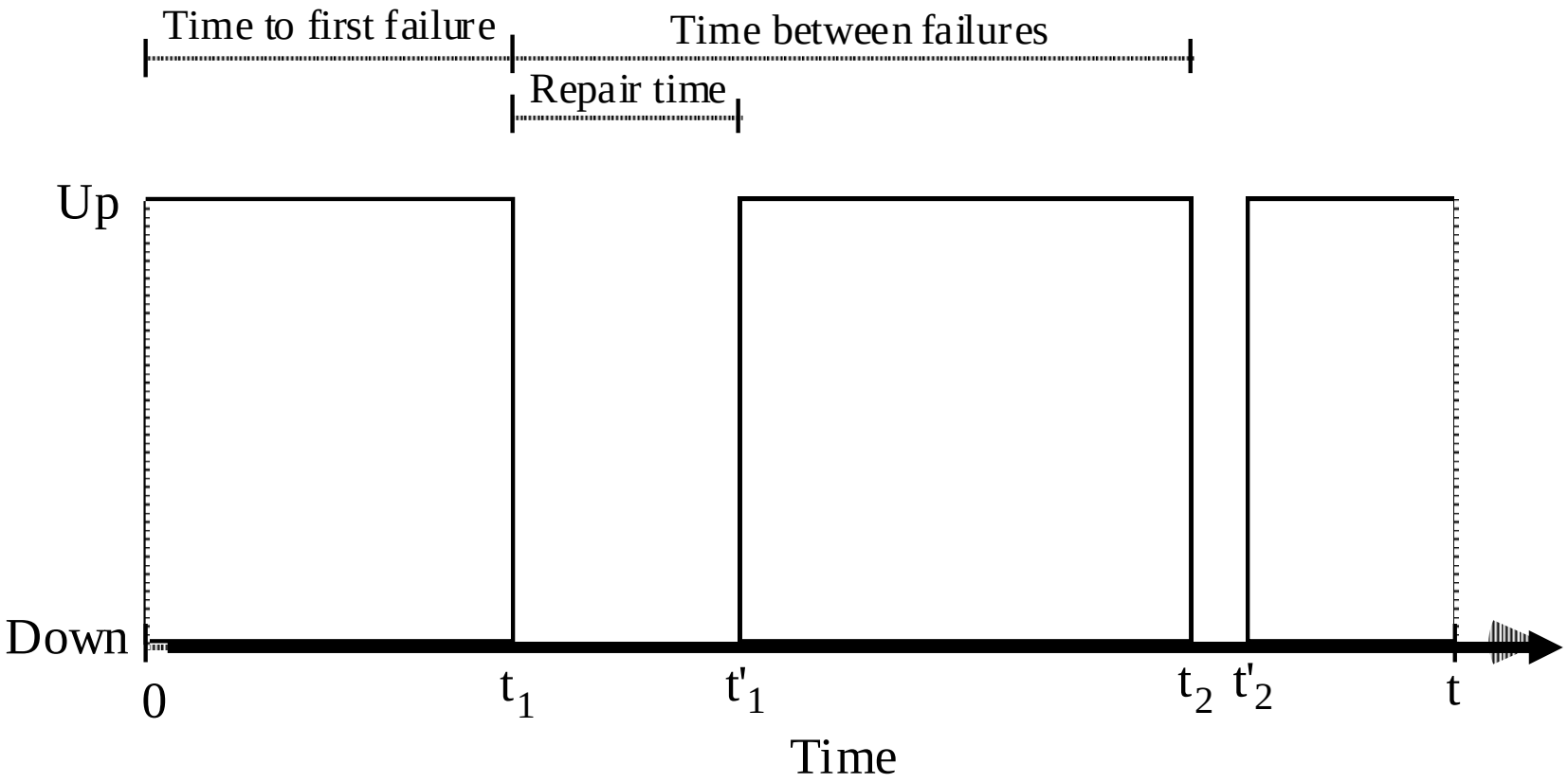
$$Availability = \frac{MTBF}{MTBF + MTTR}$$

- Συστήματα υψηλής αξιοπιστίας έχουν διαθεσιμότητα μεγαλύτερη του 0.9999 (“four 9 systems”)

Λειτουργία συστήματος και downtimes

Μικροί χρόνοι επιδιόρθωσης σημαίνει καλή **συντηρισιμότητα**





Αξιοπιστία σειριακών συστημάτων (1/4)

- Σε ένα σειριακό σύστημα, όλα τα τμήματα ή υποσυστήματά του θα πρέπει να λειτουργούν για να λειτουργεί το σύστημα
- Αν κάποιο από τα τμήματα ή υποσυστήματα αποτύχει τότε αποτυγχάνει όλο το σύστημα

$$R_s(t) = R_1(t)\, R_2(t)\, R_3(t) \ldots R_n(t) = \prod_{i=1}^{n} R_i(t)$$

Αξιοπιστία σειριακών συστημάτων (2/4)

- Η αξιοπιστία ενός σειριακού συστήματος δεν μπορεί να είναι μεγαλύτερη από την μικρότερη αξιοπιστία των επιμέρους τμημάτων του.

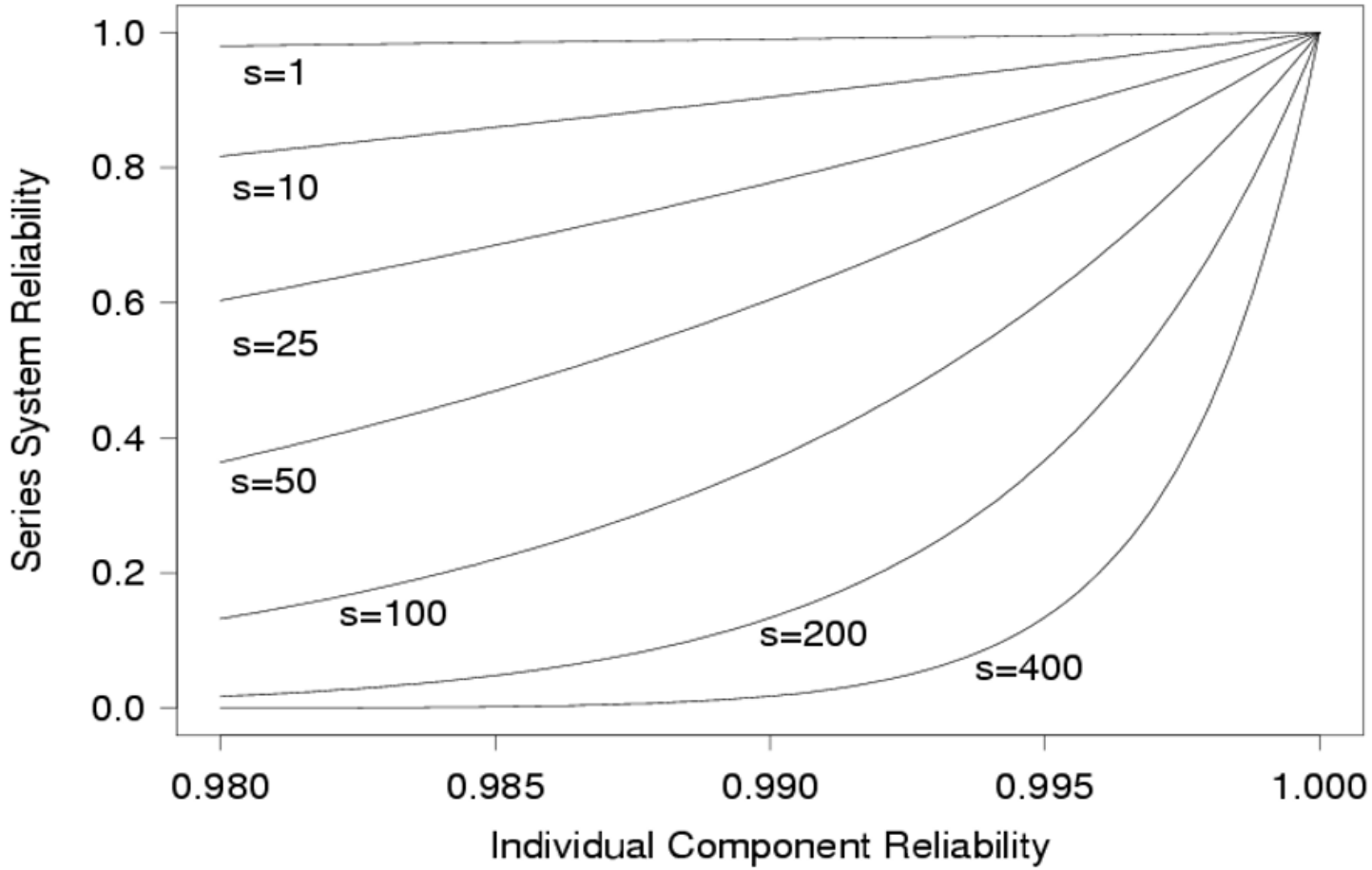
$$R_s(t) \leq \min\{R_1(t), R_2(t), \dots, R_n(t)\}$$

- Είναι σημαντικό όλα τα επιμέρους τμήματα να έχουν υψηλή αξιοπιστία ειδικά όταν το σύστημα αποτελείται από έναν υψηλό αριθμό επιμέρους τμημάτων.

Αξιοπιστία σειριακών συστημάτων (3/4)

- Η αξιοπιστία ενός σειριακού συστήματος καθορίζεται από δύο παραμέτρους
  - Το επίπεδο αξιοπιστίας των επιμέρους τμημάτων
  - Το πλήθος των τμημάτων
- Η αξιοπιστία ενός σειριακού συστήματος μπορεί να βελτιωθεί με τους παρακάτω τρόπους
  - Αυξάνοντας την αξιοπιστία των επιμέρους τμημάτων
  - Μειώνοντας το πλήθος των επιμέρους τμημάτων σε σειρά

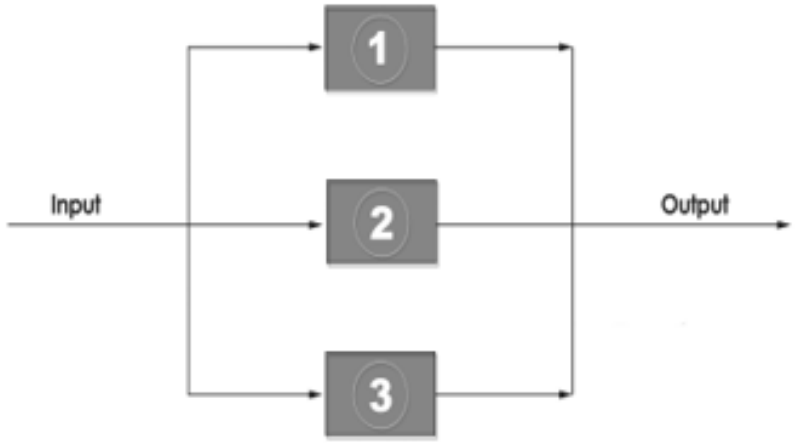
Αξιοπιστία σειριακών συστημάτων (4/4)



Αξιοπιστία συστήματος s τμημάτων σε σειρά

Αξιοπιστία παράλληλων συστημάτων (1/4)

- Σε ένα παράλληλο σύστημα θα πρέπει να αποτύχουν όλα τα τμήματα ή υποσυστήματά του για να αποτύχει το σύστημα
- Το παράλληλο σύστημα λειτουργεί όσο λειτουργεί ένα από τα υποσυστήματά του (εισαγωγή στοιχείων πλεονασμού)



$$R_s(t) = 1 - \prod_{i=1}^{n} [1 - R_i(t)]$$

Αξιοπιστία παράλληλων συστημάτων (2/4)

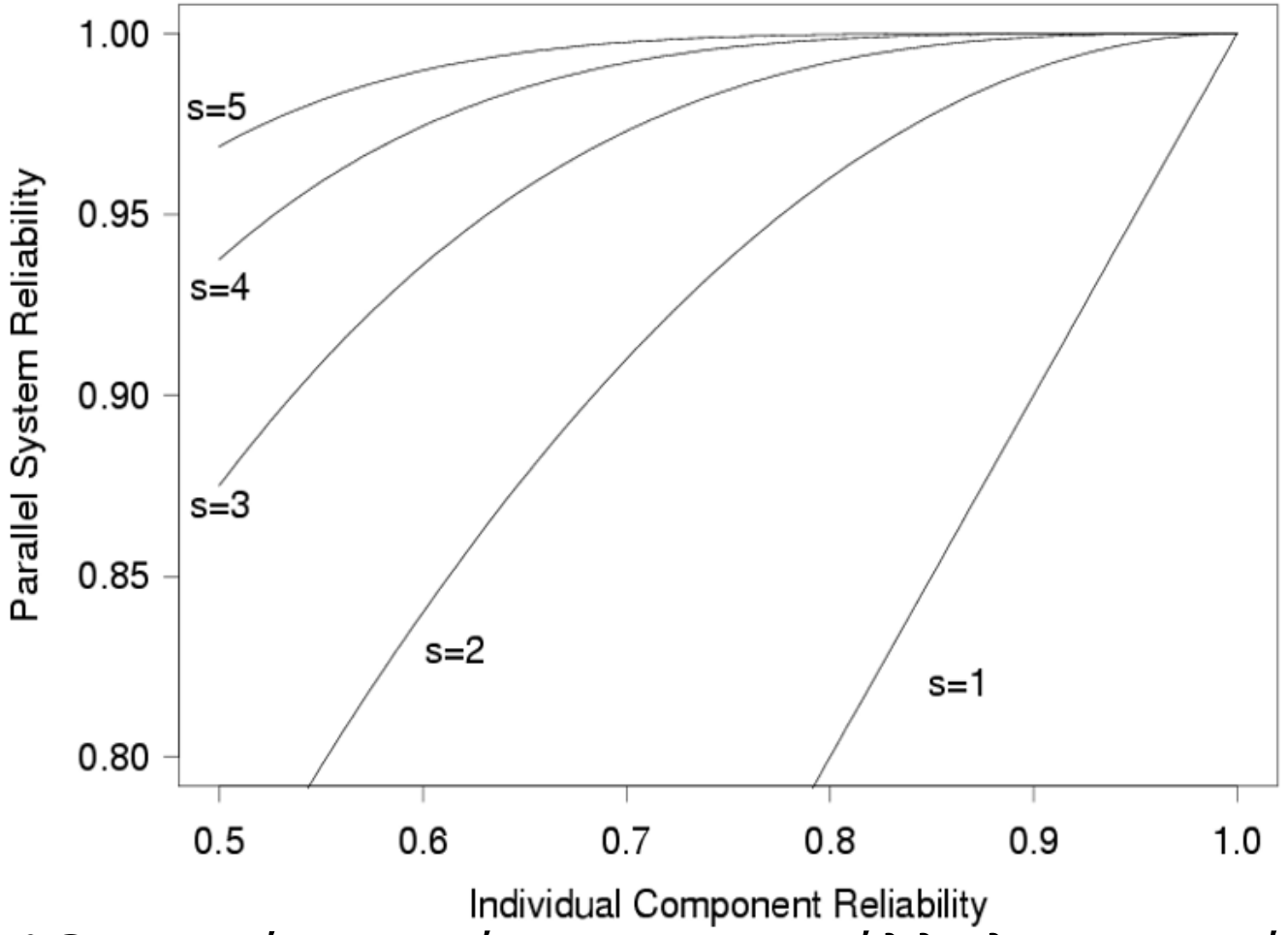
- Η αξιοπιστία ενός παράλληλου συστήματος δεν μπορεί να είναι μικρότερη από την μέγιστη αξιοπιστία μεταξύ των διαφορετικών τμημάτων του

$$R_s(t) \geq max\{R_1(t), R_2(t), \dots, R_n(t)\}$$

Αξιοπιστία παράλληλων συστημάτων (3/4)

- Πλεονεκτήματα
  - Βελτιωμένη αξιοπιστία του συστήματος χρησιμοποιώντας στοιχεία πλεονασμού
  - Μικρότερα downtimes καθώς οι εργασίες συντήρησης μπορούν να πραγματοποιηθούν χωρίς να χρειαστεί να τεθεί το σύστημα εκτός λειτουργίας (μόνο συγκεκριμένα τμήματά του τίθενται εκτός λειτουργίας)
- Μειονεκτήματα
  - Μπορεί να μην είναι εφικτές για τον σχεδιασμό ορισμένων συστημάτων
  - Σε συστήματα υψηλής αξιοπιστίας τα οφέλη που προκύπτουν μπορεί να είναι μικρά
  - Το κόστος μπορεί να είναι απαγορευτικό
  - Η κατανάλωση ενέργειας μπορεί να αυξηθεί

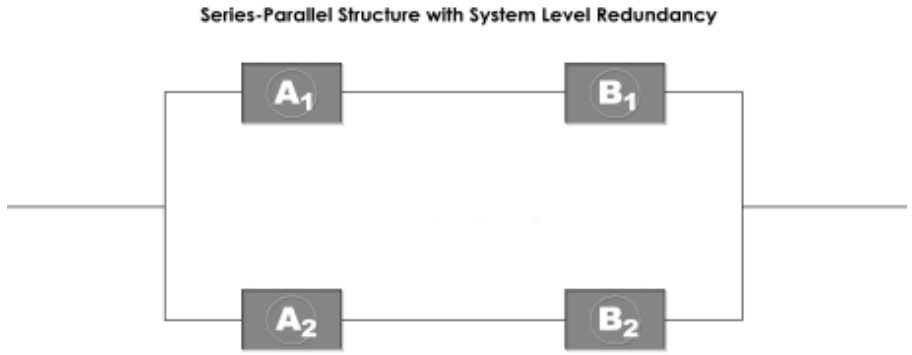
Αξιοπιστία παράλληλων συστημάτων (4/4)

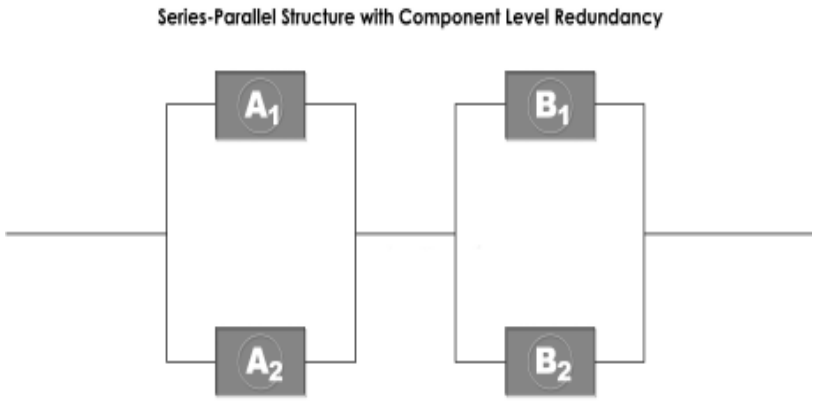


Αξιοπιστία συστήματος s παράλληλων τμημάτων

Σειριακές-παράλληλες αρχιτεκτονικές

- Έστω ένα απλό σύστημα που αποτελείται από δύο τμήματα Α και Β.
- Δύο ενναλακτικές σειριακές-παράλληλες αρχιτεκτονικές
  - Σειριακή-Παράλληλη αρχιτεκτονική με πλεονασμό σε επίπεδο συστήματος (ή πλεονασμό υψηλού επιπέδου)
  - Σειριακή-Παράλληλη αρχιτεκτονική με πλεονασμό σε επίπεδο τμήματος (ή πλεονασμό χαμηλού επιπέδου)
- Αν θέλουμε να βελτιώσουμε την αξιοπιστία ενός συστήματος εισάγοντας στοιχεία πλεονασμού, τότε αυτά θα πρέπει να εισαχθούν στο χαμηλότερο επίπεδο του σχεδιασμού
- Ποια από τις 2 αρχιτεκτονικές έχει την υψηλότερη αξιοπιστία;

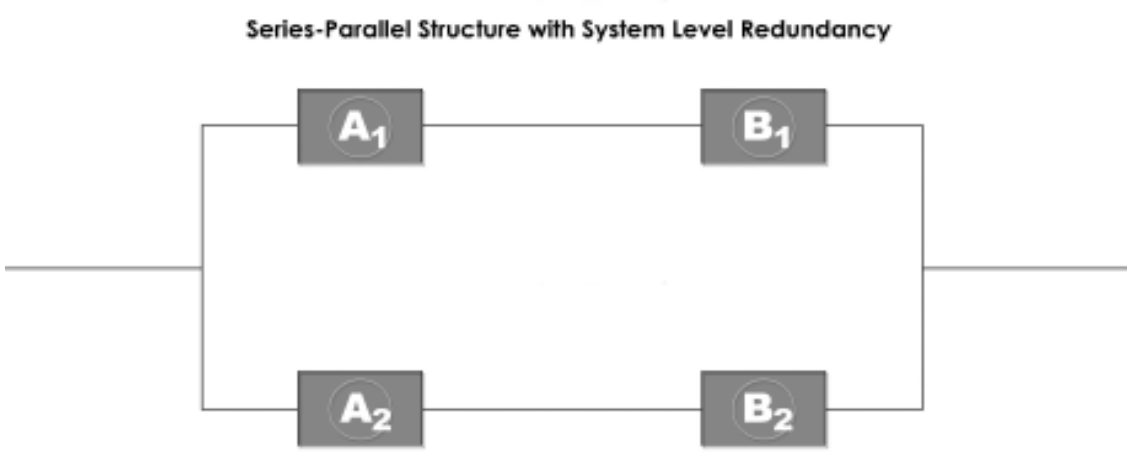




Υψηλού επιπέδου πλεονασμός

- Παραδείγματα
  - Υποθαλάσσια καλώδια οπτικών ινών
  - Σύστημα πέδησης αυτοκινήτου
- Αξιοπιστία του συστήματος

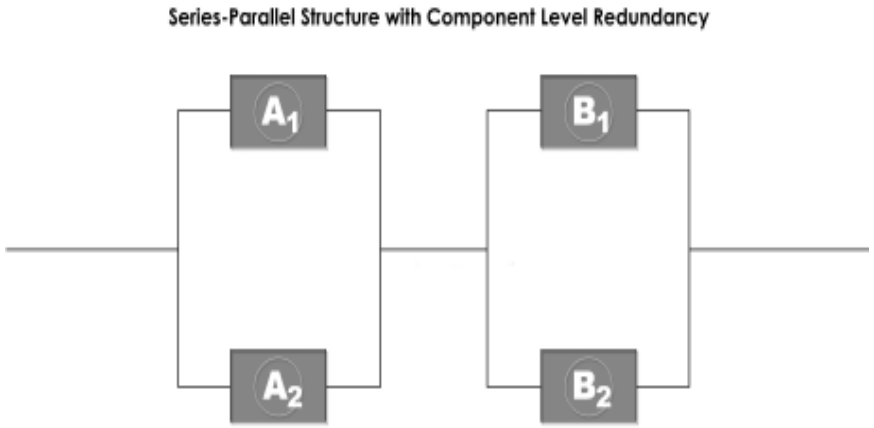
$$R_{high} = 1 - (1 - R_A R_B)(1 - R_A R_B)$$



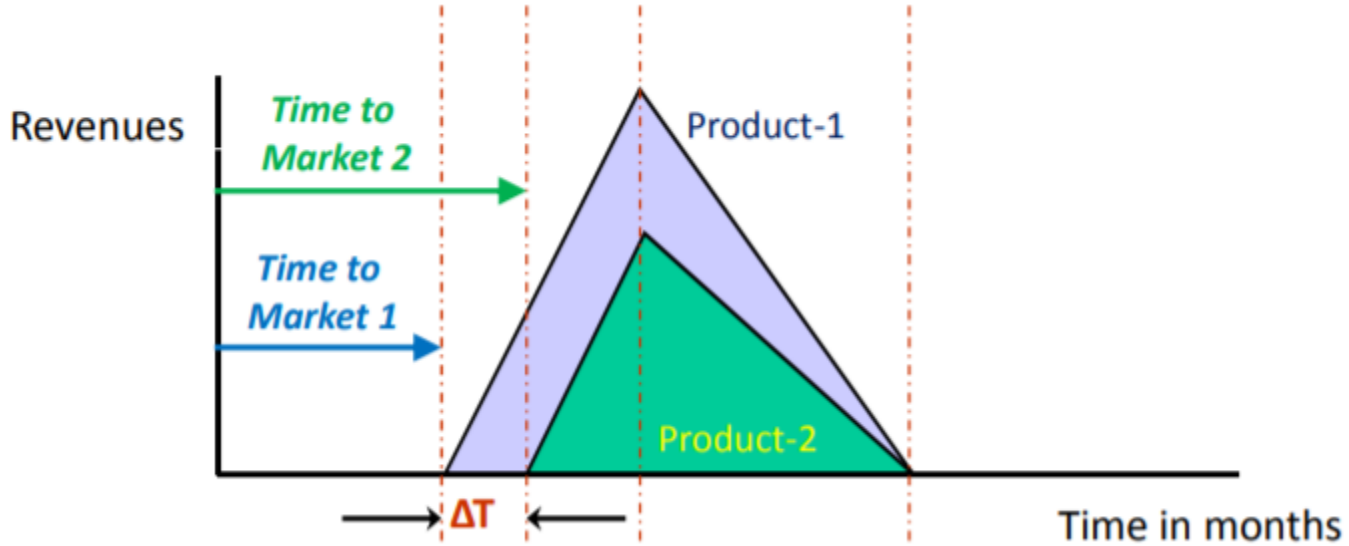
Χαμηλού επιπέδου πλεονασμός

- Παραδείγματα
  - Διπλοί επαναλήπτες σε υποθαλάσσια καλώδια οπτικών ινών
- Αξιοπιστία του συστήματος

$$R_{low} = (1 - (1 - R_A)^2)(1 - (1 - R_B)^2)$$



Αξιοπιστία και time-to-market



- Ένα αξιόπιστο προϊόν με ένα μικρό διάστημα time-to-market έχει περισσότερα έσοδα σε σχέση με ένα προϊόν με μεγαλύτερο time-to-market
- Απαιτούνται διαδικασίες δοκιμής με το ελάχιστο δυνατό κόστος και χρόνο!

Ασκήσεις

Άσκηση 1

Συγκρίνετε την διαθεσιμότητα των παρακάτω 2 εξυπηρετητών:

- Ο εξυπηρετητής uniwa έχει δηλώσει MTBF 1000 ώρες και μπορεί να επισκευαστεί από έναν μηχανικό σε 3 ώρες κατά μέσο όρο.
- Ο εξυπηρετητής uoa έχει MTBF 500 ωρών και μπορεί να επισκευαστεί από τους κατασκευαστές σε 45 λεπτά

Άσκηση 1 - Λύση

- Διαθεσιμότητα εξυπηρετητή uniwa

$$Availability = \frac{MTBF}{MTBF + MTTR} = \frac{1000}{1000 + 3} = 99{,}70\%$$

Διαθεσιμότητα εξυπηρετητή uoa

$$Availability = \frac{MTBF}{MTBF + MTTR} = \frac{500}{500 + 0{,}75} = 99{,}85\%$$

Άσκηση 2

- Ένα δείγμα από 10 λαμπτήρες πυρακτώσεως έχει την ακόλουθη διάρκεια ζωής σε ώρες: 204, 1473, 650, 697, 1737, 558, 723, 215, 526, 1850. Ποια είναι η τιμή του MTTF;

Άσκηση 2 - Λύση

- Η τιμή του MTTF δίνεται από την σχέση

$$MTTF = \frac{204+1473+650+697+1737+558+723+215+526+1850}{10} = 863$$

Άσκηση 3

- Ο αριθμός των βλαβών ενός συστήματος εντός χρονικού διαστήματος 10^9 ωρών είναι μια μονάδα (καλείται FITS) που χρησιμοποιείται στους υπολογισμούς της αξιοπιστίας. Υπολογίστε το MTBF ενός συστήματος με 500 στοιχεία, καθένα από τα οποία έχει ρυθμό βλαβών 1000 FITS.

Άσκηση 3 - Λύση

- Ο ρυθμός βλαβών λ είναι το άθροισμα του ρυθμού βλαβών λ_i των επιμέρους στοιχείων του συστήματος

$$\lambda = \sum_{i=0}^{k} \lambda_i \text{ όπου } \lambda_i = \frac{1000}{10^9} \text{ οπότε } \lambda = 500 \times \frac{1000}{10^9} = 5 \times 10^{-4}$$

$$MTBF = \frac{1}{\lambda} = 2000 \text{ ώρες}$$

Άσκηση 4

- Ας υποθέσουμε ένα σειριακό σύστημα το οποίο αποτελείται από 5 τμήματα με ρυθμό βλαβών 0.2 ανά ώρα. Να υπολογιστεί η αξιοπιστία και το MTTF του συστήματος

Άσκηση 4 - Λύση

- Ο ρυθμός βλαβών λ είναι το άθροισμα του ρυθμού βλαβών λ_i των επιμέρους στοιχείων του συστήματος

$$\lambda = \sum_{i=0}^{k} \lambda_i \text{ όπου } \lambda_i = 0.2 \text{ οπότε } \lambda = 5 \times 0.2 = 1$$

- Η αξιοπιστία του συστήματος δίνεται από την σχέση

$$R(t) = e^{-\lambda t} = e^{-t}$$

- Το MTTF του συστήματος δίνεται από την σχέση

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

Άσκηση 5

- Υποθέστε ένα σειριακό σύστημα το οποίο αποτελείται από 4 τμήματα. Τα πρώτα δύο τμήματα έχουν 90% αξιοπιστία την χρονική στιγμή t = 1 έτος και τα υπόλοιπα δύο έχουν 80% αξιοπιστία την χρονική στιγμή t = 1 έτος. Ποια είναι η αξιοπιστία του σειριακού συστήματος στην διάρκεια του ενός έτους;

Άσκηση 5 - Λύση

- Η πιθανότητα το σύστημα να λειτουργεί επιτυχώς στην διάρκεια ενός έτους, δηλαδή η αξιοπιστία του, δίνεται από την παρακάτω σχέση:

$$R_s(t)=R_1(t)\,R_2(t)\,R_3(t)\,R_4(t)=(0.9)^2(0.8)^2=51.84\%$$

Άσκηση 6

- Μία γραμμή παραγωγής μιας μηχανής αποτελείται από 5 διαφορετικά ρομπότ συναρμολόγησης τα οποία έχουν τοποθετηθεί σε σειριακή διάταξη
  - Αν κάθε ρομπότ έχει 95% αξιοπιστία, ποια είναι η αξιοπιστία της γραμμής παραγωγής;
  - Για να επιτύχουμε 95% αξιοπιστία στην γραμμή παραγωγής, ποια πρέπει να είναι η αξιοπιστία κάθε επιμέρους ρομπότ;

Άσκηση 6 - Λύση

- Η αξιοπιστία της γραμμής παραγωγής δίνεται από την παρακάτω σχέση:

$$R_s(t)=R_1(t)\ R_2(t)\ R_3(t)\ R_4(t)=(0.9)^5=59.04\%$$

- Για να επιτύχουμε 95% αξιοπιστία στην γραμμή παραγωγής η αξιοπιστία κάθε επιμέρους ρομπότ θα υπολογιστεί ως εξής:

$$0.95 = R_i^5 \text{ οπότε } R_i = 98.98\%$$

Άσκηση 7

- Υποθέστε ένα παράλληλο σύστημα το οποίο αποτελείται από 4 τμήματα. Τα πρώτα 2 τμήματα έχουν 90% αξιοπιστία την χρονική στιγμή t = 1 έτος και τα υπόλοιπα δύο 80% αξιοπιστία την χρονική στιγμή t = 1 έτος. Ποια είναι η αξιοπιστία του παράλληλου συστήματος στην διάρκεια του ενός έτους;

Άσκηση 7 - Λύση

- Η πιθανότητα το σύστημα να λειτουργεί επιτυχώς στην διάρκεια ενός έτους, δηλαδή η αξιοπιστία του, δίνεται από την παρακάτω σχέση:

$$R_s(t)=1-[(1-0.9)^2(1-0.8)^2]=99.6\%$$

Πηγές

- Behrooz Parhami, “Dependable Computing”.

Ερωτήσεις