

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

Αποτίμηση αξιοπιστίας διατάξεων συστημάτων για μακροχρόνια ψηφιακή διατήρηση

Μερόπη Σ. Πετράκη

Μεταπτυχιακή Εργασία

Ηράκλειο, Φεβρουάριος 2005

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

**Αποτίμηση αξιοπιστίας διατάξεων συστημάτων για
μακροχρόνια ψηφιακή διατήρηση**

Εργασία που υποβλήθηκε από την

Μερόπη Σ. Πετράκη

ως μερική εκπλήρωση των απαιτήσεων για την απόκτηση

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΔΙΠΛΩΜΑΤΟΣ ΕΙΔΙΚΕΥΣΗΣ

Συγγραφέας:

Μερόπη Πετράκη, Τμήμα Επιστήμης Υπολογιστών

Εισηγητική Επιτροπή:

Πάνος Κωνσταντόπουλος, Καθηγητής, Επόπτης

Martin Doerr, Ερευνητής του Ινστιτούτου Πληροφορικής ΙΤΕ, Μέλος, Επιβλέπων

Μαρία Παπαδοπούλη, Επίκουρος Καθηγήτρια, Μέλος

Δεκτή:

Δημήτρης Πλεξουσάκης, Αναπληρωτής καθηγητής

Πρόεδρος Επιτροπής Μεταπτυχιακών Σπουδών

Ηράκλειο, Φεβρουάριος 2005

Αποτίμηση αξιοπιστίας διατάξεων συστημάτων για μακροχρόνια ψηφιακή διατήρηση

Μερόπη Σ. Πετράκη

Μεταπτυχιακή Εργασία

Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης

Περίληψη

Το ψηφιακό υλικό είναι ευάλωτο σε απώλειες και φθορές καθώς αποθηκεύεται σε μαγνητικά και οπτικά μέσα που μπορεί να αστοχήσουν από έκθεση σε ζέστη, υγρασία, περιβαλλοντική μόλυνση ή ελαττωματικές συσκευές ανάγνωσης και εγγραφής. Οργανισμοί που στην αποστολή τους περιλαμβάνεται η διαφύλαξη της πληροφορίας και της πολιτισμικής κληρονομιάς έχουν ιδιαίτερα υψηλές απαιτήσεις αξιοπιστίας για τα συστήματα διατήρησης του ψηφιακού υλικού. Ουσιαστικά το πρόβλημα είναι να επιτευχθούν δεδομένοι στόχοι αξιοπιστίας με ελάχιστο κόστος.

Η παρούσα εργασία εξετάζει την αποτελεσματικότητα διατάξεων συστημάτων που εξασφαλίζουν την διατήρηση ψηφιακών δεδομένων χρησιμοποιώντας αναλυτικές τεχνικές μοντελοποίησης για την αποτίμηση της αξιοπιστίας των διατάξεων αυτών. Τα αποτελέσματα που προκύπτουν είναι χρήσιμα για την υποστήριξη αποφάσεων όπως πόσα αντίγραφα πρέπει να διατηρούνται για κάθε ψηφιακό έγγραφο, πόσο συχνά απαιτείται να ελέγχονται τα αντίγραφα για αλλοιώσεις, ποια αποθηκευτικά σχήματα είναι αποτελεσματικά για διατήρηση δεδομένων, ποιες στρατηγικές είναι αποτελεσματικές για ανάκαμψη από σφάλματα και επιδιορθώσεις, πόσες τοποθεσίες πρέπει να χρησιμοποιούνται για πρόληψη απώλειας από φυσικές καταστροφές όπως

πυρκαγιά, πλημμύρα, σεισμός. Διεξήχθησαν αναλύσεις ευαισθησίας μιας σειράς κριτηρίων αξιοπιστίας σε αντιπροσωπευτικές περιπτώσεις ως προς τις παραμέτρους των μοντέλων. Οι αναλύσεις ευαισθησίας φάνηκαν ιδιαίτερα χρήσιμες στο να διαπιστωθούν «μείζονες» παράγοντες που μπορεί να επηρεάσουν την αξιοπιστία και κατ' επέκταση το κόστος κάθε διάταξης. Τα παραδείγματα δείχνουν ότι η διαίσθηση μπορεί να αποδειχθεί εσφαλμένη στη εκτίμηση αυτών των παραγόντων.

Επόπτης: Πάνος Κωνσταντόπουλος,

Καθηγητής

Evaluating the reliability of system configurations for long term digital preservation

Meropi S. Petraki

Master's Thesis

Computer Science Department, University of Crete

Abstract

Digital material is vulnerable to loss and corruption as it is stored in magnetic and optical media that can fail because of exposure to heat, humidity, airborne contaminants or because of faulty reading and writing devices. Organizations whose mission encompasses the preservation of information and cultural heritage have very high reliability requirements for their digital preservation systems. The problem essentially is to achieve given reliability goals with minimal cost.

In this work we study the effectiveness of various system configurations for digital preservation by applying analytical modelling techniques to evaluate the reliability of those configurations. The results are useful in supporting such decisions as how many copies to retain for each document, how frequently to check these copies for corruptions, what storage schemes are most effective for data preservation, what strategies are most effective for error recovery and repair, how many sites should be used in order to prevent loss from natural disasters such as flood, fire, earthquake. We have conducted sensitivity analysis of a set of reliability criteria with respect to model parameters in representative cases. Sensitivity analysis has proved especially helpful in finding 'major' factors that influence the reliability and cost of each

configuration. The examples show that intuition may fail to estimate such factors.

Supervisor: Panos Constantopoulos,

Professor

*Αφιερωμένο σε όλους εκείνους που ήταν δίπλα μου
σε αυτό το δύσκολο αγώνα*

Ευχαριστίες

Στο σημείο αυτό θα ήθελα να ευχαριστήσω όλους όσους άμεσα ή έμμεσα με βοήθησαν στην ολοκλήρωση αυτής της εργασίας. Θερμές ευχαριστίες στον επίοπτη καθηγητή μου, κ. *Πάνο Κωνσταντόπουλο* που με στήριξε και έδειξε εμπιστοσύνη στο πρόσωπο μου σε όλη την διάρκεια της συνεργασίας μας. Τον ευχαριστώ ιδιαίτερα για τις χρήσιμες συμβουλές και την καθοδήγηση του, που υπήρξε αποτελεσματική στο να βρεθεί η άκρη του νήματος που οδήγησε τελικά στην ολοκλήρωση αυτής της εργασίας. Ευχαριστώ ιδιαίτερα και τον κ. *Martin Doerr*, επιβλέποντα της εργασίας μου, που με τις ιδέες και προτάσεις του έδωσε μια διαφορετική πνοή σε αυτή την εργασία, χωρίς την πολύτιμη συμβολή του η ολοκλήρωση αυτής της εργασίας θα ήταν αδύνατη.

Επίσης θα ήθελα να ευχαριστήσω την *Μαρία Παπαδοπούλη* που δέχτηκε τόσο πρόθυμα να είναι μέλος της εισηγητικής επιτροπής και μου έδωσε ιδέες και συμβουλές για πιθανές επεκτάσεις αυτής της δουλειάς.

Ένα μεγάλο ευχαριστώ στους φίλους μου που με ανέχτηκαν τόσο καιρό και ιδιαίτερα στην φίλη-αδελφή μου *Βάσω* που με στήριξε ψυχολογικά σε όλη την διάρκεια αυτού του δύσκολου και μακρύ αγώνα.

Πρωτίστως, οφείλω ένα ευχαριστώ στους γονείς μου *Σπύρο* και *Ευανθία* που αν και ζουν τόσα χρόνια μακριά πάντα στηρίζουν τις επιλογές μου και με εμπιστεύονται, και τα αδέρφια μου *Χρύσα* και *Μιχάλη* που με την αγάπη και την υποστήριξη τους είναι πάντα κοντά μου.

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1	1
ΕΙΣΑΓΩΓΗ	1
1.1 Ψηφιακή διατήρηση και αρχειοθέτηση: ένα ευρύ πρόβλημα	1
1.2 Ανασκόπηση των ερευνητικών προκλήσεων στην ψηφιακή διατήρηση.....	4
1.3 Αντικείμενο της εργασίας	6
1.4 Οργάνωση της εργασίας	8
ΚΕΦΑΛΑΙΟ 2	10
ΑΠΩΛΕΙΑ ΨΗΦΙΑΚΗΣ ΠΛΗΡΟΦΟΡΙΑΣ: ΠΡΟΒΛΗΜΑΤΑ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ	11
2.1 Κατηγορίες γεγονότων που οδηγούν στην απώλεια ψηφιακής πληροφορίας.....	11
2.2 Τρόποι αντιμετώπισης	12
2.2.1 Τεχνικές για την μείωση πιθανότητας εμφάνισης αστοχιών	12
2.2.2 Τεχνικές ανάκαμψης αστοχιών	13
ΚΕΦΑΛΑΙΟ 3	17
ΚΡΙΤΗΡΙΑ ΑΠΟΤΙΜΗΣΗΣ ΑΞΙΟΠΙΣΤΙΑΣ ΚΑΙ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ	17
3.1 Εισαγωγή	17
3.2 Βασικοί ορισμοί και ορολογία.....	19
3.2.1 Κριτήρια ολικής αξιοπιστίας	19
3.2.1.1 Κριτήρια αξιοπιστίας	19
3.2.1.2 Κριτήρια διαθεσιμότητας.....	20
3.2.2 Καθορισμός παραμέτρων σε μοντέλα ολικής αξιοπιστίας.....	21
3.2.2.1 Ρυθμός αστοχίας (Failure Rate).....	22
3.2.2.2 Ρυθμός επισκευής (Repair rate)	24
3.2.2.3 Πιθανότητες κάλυψης	24
3.3 Κατηγορίες μοντέλων ολικής αξιοπιστίας.....	25
3.3.1 Διαγράμματα μπλοκ αξιοπιστίας (Reliability Block Diagrams-RBDs)	27
3.3.2 Δέντρα σφαλμάτων (Fault trees)	28
3.3.3 Γράφοι αξιοπιστίας (Reliability Graphs-RGs)	29
3.4 Η εκθετική κατανομή	30
3.5 Τεχνικές μοντελοποίησης αξιοπιστίας και διαθεσιμότητας: Μοντέλα Markov	32

3.5.1	Αλυσίδες Markov συνεχούς χρόνου	33
3.6	Μετασχηματισμοί Laplace.....	39
3.7	SHARPE: Υποστηρικτικό λογισμικό των τεχνικών μοντελοποίησης	40
3.7.1	Εισαγωγή	40
3.7.2	Εργαλείο SHARPE.....	41
3.7.3	SHARPE: Αλυσίδες Markov.....	42
ΚΕΦΑΛΑΙΟ 4	45
ΑΠΟΤΙΜΗΣΗ ΑΞΙΟΠΙΣΤΙΑΣ ΔΙΑΤΑΞΕΩΝ ΣΥΣΤΗΜΑΤΩΝ ΓΙΑ ΜΑΚΡΟΧΡΟΝΙΑ ΨΗΦΙΑΚΗ ΔΙΑΤΗΡΗΣΗ.....		45
4.1	Εισαγωγή	45
4.2	Υποθέσεις που εισάγονται στην μελέτη	47
4.3	Βασικές συνιστώσες διατάξεων για ψηφιακή διατήρηση.....	48
4.3.1	Εξοπλισμός φύλαξης δεδομένων (Data storage equipment)	48
4.3.2	Τοποθεσία μιας διάταξης.....	50
4.4	Ένα απλό παράδειγμα διάταξης για ψηφιακή διατήρηση	51
4.4.1	Περιγραφή του μοντέλου	51
4.4.2	Υπολογισμός μαθηματικού τύπου για το μέσου χρόνου αποτυχίας (MTTF) της αλυσίδας Markov για ένα ζεύγος δίσκων	55
4.4.3	Σχεδίαση ιεραρχικού μοντέλου στο SHARPE	58
4.4.4	Ανάλυση ευαισθησίας.....	60
4.4.5	Αξιοπιστία της διάταξης.....	67
4.5	Επέκταση της διάταξης: Προσθήκη αντιγράφου ασφαλείας.....	68
4.5.1	Περιγραφή του μοντέλου	68
4.5.2	Σχεδίαση ιεραρχικού μοντέλου στο SHARPE	72
4.5.3	Ανάλυση ευαισθησίας.....	74
4.5.4	Αξιοπιστία της διάταξης.....	80
4.5.5	Ασφάλεια της διάταξης για μεγάλα χρονικά διαστήματα.....	81
4.5.6	Επιρροή εξωτερικών γεγονότων καταστροφής στην αξιοπιστία διατάξεων συστημάτων για ψηφιακή διατήρηση.....	82
4.6	Επικύρωση αποτελεσμάτων με αντίστοιχα παραδείγματα στο ArchSim.....	87
4.7	Επέκταση διάταξης: Μελέτη διάταξης με τέσσερα αντίγραφα ασφαλείας.....	88
4.7.1	Περιγραφή του μοντέλου	88
4.7.2	Ασφάλεια της διάταξης για μεγάλα χρονικά διαστήματα.....	91
4.8	Επέκταση διάταξης: Μελέτη αξιοπιστίας αρχιτεκτονικών παρατάξεων δίσκων (RAID) 91	
4.8.1	RAID επιπέδου 1.....	93
4.8.2	RAID επιπέδου 3, 4, 5.....	94
4.8.3	Γενικό μοντέλο αξιοπιστίας.....	95
4.8.4	Σχεδίαση ιεραρχικού μοντέλου αξιοπιστίας RAID 3,4,5 με περιορισμένο πλήθος εφεδρικών δίσκων (cold & hot spares).....	97
4.8.5	Ενδεικτικά αριθμητικά αποτελέσματα	101

ΚΕΦΑΛΑΙΟ 5	103
ΕΠΙΛΟΓΟΣ ΚΑΙ ΜΕΛΛΟΝΤΙΚΗ ΕΡΓΑΣΙΑ.....	103
5.1 Επίλογος.....	103
5.2 Μελλοντική εργασία.....	104
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	109

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

1.1 Ψηφιακή διατήρηση και αρχειοθέτηση: ένα ευρύ πρόβλημα

Η σημαντική πρόοδος στην τεχνολογία των υπολογιστών και τις πληροφορίες παρέχει στην κοινωνία μας ισχυρά εργαλεία για την δημιουργία, οργάνωση και διανομή ψηφιακών πόρων, ανεγείροντας ταυτόχρονα νέες και πολύπλοκες προκλήσεις στην διατήρηση της ψηφιακής πληροφορίας για μεγάλα χρονικά διαστήματα. Η ανάγκη αναφοράς στο πρόβλημα μακροβιότητας της ψηφιακής πληροφορίας γίνεται όλο και περισσότερο επιτακτική εξαιτίας του γεγονότος ότι οι αποθήκες ψηφιακής πληροφορίας έχουν ξεπεράσει σε μέγεθος και σπουδαιότητα τα υπάρχοντα φυσικά αρχεία. Η δυνατότητα διατήρησης του ψηφιακού υλικού αποτελεί μια σοβαρή πρόκληση για κυβερνητικές αποστολές, αποθήκες γνώσεων επιστημονικών δεδομένων, βιβλιοθήκες, αρχεία, μουσεία και γενικότερα οποιουδήποτε οργανισμού που απαιτεί συνεχή πρόσβαση στην πληροφορία που διαθέτει [NSF+].

Αν και το ενδιαφέρον γύρω από την δυνατότητα της κοινωνίας να διατηρήσει την ψηφιακή πληροφορία στο κοντινό και απώτερο μέλλον δεν είναι καινούργια, οι προκλήσεις για ψηφιακή αρχειοθέτηση και διατήρηση είναι πιεστική εξαιτίας τις αυξανόμενης τάσης οι ψηφιακές τεχνολογίες και η ψηφιακή πληροφορία να παραμένουν στο κέντρο τις έρευνας, τις κυβερνητικής διαχείρισης, του ηλεκτρονικού εμπορίου, της μόρφωσης, της διασκέδασης και των τεχνών. Στην διάρκεια των τελευταίων ετών τόσο κυβερνητικά πρακτορεία, ερευνητικές βιβλιοθήκες αλλά και εταιρίες και ιδιοκτήτες έχουν συγκεντρώσει

τεράστιες ποσότητες ψηφιακής πληροφορίας μεγάλο μέρος από την οποία προβλέπεται να είναι πολύτιμη στο προβλεπόμενο μέλλον. Όλο και περισσότεροι οργανισμοί όλων των ειδών έχουν ανάγκη να εξασφαλίσουν ότι οι αξιόλογοι ψηφιακοί πόροι που δημιουργούν σήμερα θα είναι διαθέσιμοι και κατανοητοί στο μέλλον.

Ωστόσο παρατηρείται έντονα η τάση όλο και περισσότερο ψηφιακό περιεχόμενο είναι διαθέσιμο και αξιόλογο για διατήρηση. Έτσι για παράδειγμα στη βιοιατρική έρευνα ομάδες ερευνητών σε πανεπιστήμια αλλά και σε βιομηχανίες βασίζουν την έρευνα τους στη πρόσβαση τεραστίων βάσεων δεδομένων όπως οι βάσεις δεδομένων του ανθρώπινου γενετικού υλικού, για να ανιχνεύσουν την θεμελίωση για αναρίθμητες ασθένειες και να επιταχύνουν την ανακάλυψη αποτελεσματικών θεραπειών. Ομοίως ο όγκος πληροφορίας που πρέπει να διαχειρίζεται σε άλλα επιστημονικά πρακτορεία είναι τεράστιος και αυξάνει συνεχώς. Σημαντικές αναλύσεις επίσης απαιτούν την διατήρηση των μοντέλων, προσομοιώσεων και των εργαλείων οπτικοποίησης. Σε πολλά πεδία οι ερευνητές δεν ενδιαφέρονται να δημοσιεύσουν μόνο τα αποτελέσματα αλλά και τα δεδομένα πάνω στα οποία βασίζονται οι μελέτες ώστε η επιστημονική έρευνα να μπορεί να ελέγχεται για την εγκυρότητα της, να μπορεί να αναπαράγεται και να γίνονται επεκτάσεις.

Ένα άλλο σημαντικό πρόβλημα αποτελεί το γεγονός ότι οι ψηφιακές συλλογές αυξάνονται με τέτοιο ρυθμό που καταστούν αδύνατη την δυνατότητα διαχείρισης και διατήρησης τους. Τα πρακτορεία σε όλα τα κυβερνητικά επίπεδα έχουν καταπονηθεί από την ταχεία αύξηση τις ποσότητας και τις πολυπλοκότητας των δεδομένων που συλλέγουν και τις αυξανόμενες απαιτήσεις του κοινού για πρόσβαση σε αυτούς του ψηφιακούς πόρους. Έντονα προβλήματα αντηχούν από στατιστικά γραφεία όπως το γραφείο απογραφής, το εθνικό κέντρο στατιστικής στην υγεία που δημιουργούν μακροχρόνια σύνολα δεδομένων που οι ερευνητές εκμεταλλεύονται για να κατανοήσουν τάσεις στην

απασχόληση, τους μισθούς, την δημόσια υγεία, την στέγαση, μόρφωση κ.λ.π ή χρησιμοποιούνται για αναλύσεις αποτελεσμάτων γύρω από κυβερνητικές πολιτικές και τις μεγάλες κοινωνικές επενδύσεις που στοχεύουν στην βελτίωση της κοινωνικής ευημερίας. Ιδιωτικές εταιρίες επίσης συλλέγουν ψηφιακά δεδομένα ως μέρος της βασικής του αποστολής τους, όπως για παράδειγμα για την ανάπτυξη νέων φαρμάκων από φαρμακευτικές εταιρίες, για την εξερεύνηση των πόρων πετρελαίου, φυσικού αερίου, νερού. Ψηφιακά βίντεο, ήχος, κινούμενα σχέδια και τα συνοδευόμενα κείμενα είναι μείζον πόροι της βιομηχανίας διασκέδασης αλλά επίσης αποτελούν σημαντικούς πολιτιστικούς πόρους για το κοινό. Η μετατόπιση χρήσης ψηφιακών πόρων πέρα από ακαδημαϊκή χρήση εξειδικευμένων βάσεων δεδομένων έχει σαν αποτέλεσμα πολλά είδη οργανισμών ακόμα και απλοί πολίτες να αντιμετωπίζουν προκλήσεις ψηφιακής διατήρησης. Η εκτεταμένη χρήση ηλεκτρονικής διακυβέρνησης και του ηλεκτρονικού εμπορίου έχει σαν αποτέλεσμα την δημιουργία ηλεκτρονικών συναλλαγών που αποθηκεύονται σε βάσεις δεδομένων και χρειάζεται να υποστηρίζονται τουλάχιστον όσο καιρό απαιτείται για ικανοποιηθούν ζητήματα εξέταση λογιστικών βιβλίων, φορολογικά καθώς και μια σειρά από άλλες απαιτήσεις ευθύνης. Ιατρικοί φάκελοι που παρακολουθούν ατομικά ιατρικά ιστορικά γίνονται επίσης ψηφιακοί. Πόροι πολιτιστική κληρονομιάς και ζωντανές αποδείξεις της ανθρώπινης δημιουργικότητας στα ψηφιακά χρόνια, παράγονται, διαμοιράζονται και χρησιμοποιούνται σε ψηφιακή μορφή κυρίως μέσα από τον Παγκόσμιο Ιστό. Ακόμα και απλοί πολίτες συγκεντρώνουν αξιόλογους πόρους όπως ηλεκτρονική αλληλογραφία και ψηφιακές φωτογραφίες.

Στην πραγματικότητα λίγοι είναι οι τομείς της κοινωνίας που δεν έχουν επαφή με κάποιο τρόπο από την ανάγκη αύξησης της μακροζωίας των ψηφιακών πόρων και την μείωση του ρίσκου καταστροφικής απώλειας τους.

1.2 Ανασκόπηση των ερευνητικών προκλήσεων στην ψηφιακή διατήρηση

Η διατήρηση της ψηφιακής πληροφορίας είναι πολύ πιο δύσκολη από την διατήρηση παραδοσιακού χαρτιού, ταινιών και πληροφορίας ήχου και βίντεο. Πρώτα από όλα η προοπτική μακροχρόνιων περιόδων ανεγείρει από μόνη της ξεχωριστές προκλήσεις. Τα ψηφιακά αρχεία έχουν σαν στόχο την διατήρηση δεδομένων για δεκαετίες, αιώνες ή ακόμα μεγαλύτερα διαστήματα. Ωστόσο τα αποθηκευτικά μέσα, οι συσκευές εισόδου-εξόδου, οι γλώσσες προγραμματισμού, οι εφαρμογές λογισμικού καθώς και τα πρότυπα που είναι απαραίτητα για την ανάκτηση και την ερμηνεία της ψηφιακής πληροφορίας αναθεωρούνται και αντικαθίστανται κάθε λίγα χρόνια. Δεδομένης της σημερινής ταχείας καινοτομίας στην τεχνολογία της πληροφορίας, η ψηφιακή πληροφορία που δημιουργείται σήμερα ίσως να μην είναι προσιτή ή αδύνατον να ερμηνευτεί σε λίγα χρόνια από τώρα [NSF+].

Η φυσική αναπαράσταση της ψηφιακής πληροφορίας μπορεί να διαχειρίζεται αντιγράφοντας τις ροές των δυαδικών ψηφίων από ένα φορέα σε έναν άλλο. Αναμφίβολα το πιο προκλητικό πρόβλημα είναι η διατήρηση της λογικής αναπαράστασης της πληροφορίας – η δυνατότητα ουσιαστικά παρουσίασης της ροής δυαδικών ψηφίων με τρόπους που έχουν σημασία, έτσι ώστε άνθρωποι και υπολογιστές να μπορούν να ερμηνεύουν, να χρησιμοποιούν και να την κατανοούν σε οποιαδήποτε χρονικό σημείο στο μέλλον. Η λογική διατήρηση είναι ένα δύσκολο πρόβλημα καθώς άνθρωποι και οργανισμοί χρησιμοποιούν όλο και περισσότερο πολύπλοκα εργαλεία λογισμικού, μοντέλα δεδομένων, σημασιολογία και έννοιες για την σύλληψη, αναπαράσταση, παρουσίαση και ανάλυση πολλών διαφορετικών ειδών πληροφορίας. Μορφοποιήσεις, πρότυπα, λογισμικό και σημασιολογία αναπτύσσονται με διαφορετικούς ρυθμούς για τα διαφορετικά είδη της ψηφιακής πληροφορίας επαυξάνοντας την πολυπλοκότητα σχεδίασης και επιλογής αποτελεσματικών στρατηγικών διατήρησης για μεγάλα

χρονικά διαστήματα.

Ένα επιπλέον πρόβλημα στην διατήρηση για μεγάλα χρονικά διαστήματα που καλύπτουν χρονικά διαστήματα δεκαετιών, γενεών ή και αιώνων είναι η απειλή τις διακοπτόμενης διαχείρισης των ψηφιακών αντικείμενων που είναι κρίσιμη. Σε αντίθεση με πολλά φυσικά αντικείμενα που αντέχουν περιόδους αμέλειας χωρίς να έχουν σαν αποτέλεσμα την ολική απώλεια, κάτι τέτοιο δεν ισχύει για τα ψηφιακά αντικείμενα που απαιτούν μόνιμη διατήρηση και εκπόνηση συστημάτων «ζωτικής υποστήριξης» για να επιβιώσουν. Ο πλεονασμός, πολλαπλά αντίγραφα και ασφάλεια απέναντι σε επιθέσεις σε συστήματα αρχειοθέτησης και κατά αστοχιών τις τεχνολογία αποτελούν κρίσιμες απαιτήσεις για την διατήρηση για μεγάλα χρονικά διαστήματα, όπως επίσης η προοδευτική μετάβαση (migration) [H01].

Επιπλέον οι προκλήσεις για ψηφιακή διατήρηση είναι μοναδικές εξαιτίας τις κλίμακας και ποικιλίας της πληροφορίας που έχει επί-μακράν αξία. Τα ψηφιακά αντικείμενα που είναι αξιόλογα για διατήρηση περιλαμβάνουν βάσεις δεδομένων, έγγραφα, καταγραφές ήχου και βίντεο, φωτογραφικό υλικό και δυναμικά πολυμεσικά προϊόντα. Οι οντότητες αυτές δημιουργούνται σε πολλά διαφορετικά είδη μέσων και αποθηκεύονται σε ευρεία ποικιλία από μορφοποιήσεις. Παρά την σταθερή πτώση στο κόστος αποθήκευσης η πρόσφατη μαζική άφιξη ψηφιακής πληροφορίας και η αυξανόμενη πολυπλοκότητα ξεπερνάει τις δυνατότητες αρχειοθέτησης των περισσότερων οργανισμών. Αυτό συμβαίνει κυρίως λόγω του γεγονότος ότι η ψηφιακή αρχειοθέτηση και διατήρηση για μεγάλα χρονικά διαστήματα απαιτεί πολύ περισσότερα σε σχέση με την αποθήκευση πολύ μεγάλων ποσοτήτων από ακατέργαστα δυαδικά ψηφία πληροφορίας. Οι ψηφιακές συλλογές απαιτούν υποστήριξη και επεξεργασία για να εξασφαλιστεί η μακροβιότητα, προστασία της ακεραιότητας και εμπλουτισμός της αξίας για μελλοντική χρήση. Οι τρέχουσες μεθοδολογίες διατήρησης απαιτούν εντατική ανθρώπινη παρέμβαση που δεν προβλέπεται να

είναι ανεκτή για μεγάλη χρονική διάρκεια καθώς θα είναι αδύνατον να κλιμακωθεί προς το ογκώδες μέγεθος πολλών ψηφιακών συλλογών. Επιπλέον δεν υπάρχουν επαρκώς αναπτυγμένες μεθοδολογίες για την διατήρηση πολλών σημερινών πολύπλοκων ειδών δεδομένων και μορφοποιήσεων.

Η ανάπτυξη υποδομής για ψηφιακή αρχειοθέτηση καθοδηγείται δυναμικά από την ανάγκη υποστήριξης πολλαπλών κοινοτήτων. Κάθε κοινότητα έχει τις δικές της απαιτήσεις που προβλέπεται να επηρεάσουν το περιεχόμενο, την οργάνωση, σχεδίαση και τις υπηρεσίες των ψηφιακών αρχείων. Δεδομένης της ποικιλίας του ψηφιακού υλικού που χρειάζεται να συντηρηθεί και των διαφορετικών ενδιαφερόμενων στην διαδικασία διατήρηση και των αποτελεσμάτων αυτής, γίνεται φανερό ότι δεν υπάρχει μια μοναδική προσέγγιση που να ανταποκρίνεται σε όλες τις προκλήσεις ψηφιακής διατήρησης. Αντιθέτως, απαιτείται έρευνα σε ένα ευρύ φάσμα λύσεων που επεκτείνονται από εργαλεία που μπορεί να χρησιμοποιήσει ένας απλός πολίτης για να διατηρήσει την φωτογραφική συλλογή του μέχρι συστήματα μεγάλων ψηφιακών αποθηκών για ερευνητικές βάσεις, εικόνες και καταγεγραμμένους ήχους. Η δημιουργία υποδομής που θα καθιστά εφικτή και υποφερτή την διατήρηση ψηφιακών συλλογών για μεγάλα χρονικά διαστήματα επίσης απαιτεί την αναγνώριση *εννοιών, μεθοδολογιών και τεχνολογιών* που να ικανοποιούν κοινές απαιτήσεις για αποθήκευση, διαχείριση και πρόσβαση.

1.3 Αντικείμενο της εργασίας

Το πρόβλημα της ψηφιακής διατήρησης επικεντρώνεται στο να εξασφαλίσει ότι ψηφιακά έγγραφα που δημιουργούνται σήμερα από υπολογιστικά συστήματα και εφαρμογές να μπορούν να παραμένουν διαθέσιμα, χρηστικά και αυθεντικά σε δέκα ακόμα και εκατό χρόνια όταν πλέον οι εφαρμογές και τα συστήματα τα οποία χρησιμοποιήθηκαν για την δημιουργία και την ερμηνεία αυτών των ψηφιακών εγγράφων δεν θα είναι πλέον διαθέσιμα.

Υπάρχουν δυο σημαντικές συνιστώσες που πρέπει να μελετηθούν στην διατήρηση των ψηφιακών εγγράφων:

- Διατήρηση της ροής δυαδικών ψηφίων που αποτελούν ένα ψηφιακό έγγραφο (data preservation)
- Διατήρηση του νοήματος ενός ψηφιακού εγγράφου (meaning preservation).

Η παρούσα μελέτη επικεντρώνεται στο πρώτο πρόβλημα, και συγκεκριμένα στη σχεδίαση διατάξεων συστημάτων για την διατήρηση ψηφιακών δεδομένων (διατήρηση της ροής των δυαδικών ψηφίων). Μια σειρά από αναλυτικές τεχνικές θα χρησιμοποιηθούν για την ανάπτυξη μοντέλων αξιοπιστίας με στόχο την υποστήριξη στη λήψη αποφάσεων που εμπλέκονται στην σχεδίαση αξιόπιστων διατάξεων συστημάτων, που είναι κατάλληλα για την μακροχρόνια φύλαξη ψηφιακών δεδομένων. Ερωτήματα όπως πόσα αντίγραφα ασφαλείας για κάθε ψηφιακό έγγραφο απαιτείται να κρατάει μια διάταξη για να πετύχει ένα δεδομένο στόχο αξιοπιστίας, πόσο συχνά απαιτείται να γίνεται έλεγχος στα αντίγραφα για τυχόν σφάλματα, ποια αποθηκευτικά μέσα είναι κατάλληλα για την αποθήκευση ψηφιακών δεδομένων, τι επιρροή μπορεί να έχουν φυσικά γεγονότα καταστροφής (όπως πυρκαγιά, πλημμύρα και σεισμοί) στην αξιοπιστία μιας προτεινόμενης διάταξης καθώς και εναλλακτικές διατάξεις που διατηρούν αντίγραφα σε διαφορετικές τοποθεσίες, εξετάζονται.

Μια σειρά από αναλύσεις ευαισθησίας εκτελούνται και καταγράφουν τις μεταβολές στα κριτήρια αξιοπιστίας των προτεινόμενων διατάξεων σε συναρτήσει των μεταβολών στις παραμέτρους εισόδου. Οι αναλύσεις ευαισθησίας είναι ιδιαίτερα χρήσιμες στο να εστιάσουν στις παραμέτρους που επηρεάζουν σε σημαντικό βαθμό την αξιοπιστία και το κόστος των διατάξεων («μειζονες» παράγοντες) και παράλληλα μπορεί να δώσουν απαντήσεις στα σημαντικά ερωτήματα που όπως αναφέραμε εμπλέκονται στην σχεδίαση

διατάξεων συστημάτων για ψηφιακή διατήρηση.

1.4 Οργάνωση της εργασίας

Η οργάνωση της συγκεκριμένης μεταπτυχιακής εργασίας έχει ως εξής:

- Στο Κεφάλαιο 2 περιγράφονται συνοπτικά οι τρόποι με τους οποίους μπορεί να χαθεί ψηφιακή πληροφορία καθώς και κάποιες βασικές τεχνικές και στρατηγικές για την αντιμετώπιση πιθανών αστοχιών ώστε να μην έχουν ως αποτέλεσμα την απώλεια πληροφορίας.
- Στο Κεφάλαιο 3 παρουσιάζεται το θεωρητικό υπόβαθρο για την αποτίμηση της αξιοπιστίας και διαθεσιμότητας υπολογιστικών συστημάτων. Με μια σύντομη ανασκόπηση εισάγονται βασικές ορολογίες, ορισμοί και καθώς και οι παράμετροι που εμφανίζονται σε μοντέλα ολικής αξιοπιστίας. Ιδιαίτερη έμφαση δίνεται στα μοντέλα Markov και στην θεωρία πάνω στην οποία στηρίζονται καθώς αποτελούν την τεχνική μοντελοποίησης που χρησιμοποιείται για την μελέτη της αξιοπιστίας προτεινόμενων διατάξεων συστημάτων για ψηφιακή διατήρηση. Στο τέλος του κεφαλαίου υπάρχει μια σύντομη ανασκόπηση των δυνατοτήτων του λογισμικού SHARPE που χρησιμοποιείται στη διάρκεια της παρούσας εργασίας για την ανάλυση των μοντέλων και την παραγωγή αριθμητικών αποτελεσμάτων.
- Στο Κεφάλαιο 4 περιγράφεται ο τρόπος μοντελοποίησης μιας σειράς προτεινόμενων διατάξεων συστημάτων για ψηφιακή διατήρηση και ταυτόχρονα γίνεται και η αποτίμηση της αξιοπιστίας τους. Μια σειρά από αναλύσεις ευαισθησίας εκτελούνται και εξετάζουν πιθανές επιρροές των παραμέτρων εισόδου σε κριτήρια αξιοπιστίας των διατάξεων συστημάτων για ψηφιακή διατήρηση.
- Το Κεφάλαιο 5 καταλήγει την συγκεκριμένη μεταπτυχιακή εργασία,

ανακεφαλαιώνοντας την προσφορά της και δίνει μια σειρά από κατευθύνσεις για μελλοντική εργασία

ΚΕΦΑΛΑΙΟ 2

Απώλεια ψηφιακής πληροφορίας: προβλήματα και αντιμετώπιση

2.1 Κατηγορίες γεγονότων που οδηγούν στην απώλεια ψηφιακής πληροφορίας

Ένα αρχικό βήμα στη μελέτη διατάξεων συστημάτων για μακροχρόνια φύλαξη ψηφιακών δεδομένων αποτελεί η κατανόηση του τρόπου με τον οποίο χάνεται πληροφορία καθώς και των τεχνικών που υπάρχουν για την μείωση του κινδύνου αυτών των απωλειών.

Οι κυριότερες κατηγορίες ανεπιθύμητων γεγονότων που μπορεί να οδηγήσουν στην απώλεια ενός ψηφιακού εγγράφου είναι [C03]:

- Αλλοίωση και αστοχία του φορέα δεδομένων: Η διαδικασία φυσικής φθοράς μπορεί να καταστήσει ένα φορέα ψηφιακής πληροφορίας μη αναγνώσιμο. Ένα πολύ χαρακτηριστικό παράδειγμα είναι η μαγνητική εξασθένιση (media decay) που συμβαίνει όταν ένας φορέας χάσει την ικανότητα να κρατάει τα δυαδικά ψηφία που κωδικοποιούν ένα ψηφιακό έγγραφο¹. Επίσης ένας δίσκος μπορεί να αστοχήσει και να χάσει τα δεδομένα του λόγω συντριβής της κεφαλής του δίσκου, αστοχίας ηλεκτρονικών κυκλωμάτων ελέγχου ή ελαττωμάτων στην διάρκεια κατασκευής του.
- Παλαίωση συνιστωσών πρόσβασης: Ένα ψηφιακό έγγραφο μπορεί να

¹ Με τον όρο ψηφιακό έγγραφο θα αναφερόμαστε στην μονάδα πληροφορίας που διαχειρίζεται ένα σύστημα ψηφιακής διατήρησης.

χαθεί λόγω παλαιώσης των συνιστωσών που υποστηρίζουν την πρόσβαση σε αυτό. Χαρακτηριστικό παράδειγμα είναι η κατάργηση της μορφοποίησης που ακολουθεί ένα ψηφιακό έγγραφο, που συμβαίνει όταν το σύστημα δεν είναι πλέον σε θέση να ερμηνεύσει τα δυαδικά ψηφία που είναι αποθηκευμένα σε ένα φορέα.

- Ανθρώπινα λάθη και λάθη λογισμικού: Ψηφιακά έγγραφα μπορεί να χαλάσουν και να χαθούν τόσο από ανθρώπινα λάθη όσο και από σφάλματα λογισμικού.
- Εξωτερικά γεγονότα: Εξωτερικά γεγονότα όπως πυρκαγιά, πλημμύρα, σεισμοί κ.α. μπορεί επίσης να προκαλέσουν καταστροφή ψηφιακής πληροφορίας. Τέτοια γεγονότα προκαλούν μάλιστα ολικές απώλειες καταστρέφοντας για παράδειγμα πολλαπλούς δίσκους και ίσως όλα τα διαθέσιμα αντίγραφα ασφαλείας των ψηφιακών εγγράφων.

2.2 Τρόποι αντιμετώπισης

Δυο γνωστοί τρόποι για την αντιμετώπιση αστοχιών σε υπολογιστικά συστήματα είναι είτε η μείωση των πιθανοτήτων να συμβούν οι αστοχίες που περιγράψαμε στην προηγούμενη ενότητα είτε η σχεδίαση των συστημάτων να γίνεται με τέτοιο τρόπο ώστε ακόμα και αν συμβαίνουν αστοχίες να μην έχουν σαν αποτέλεσμα την απώλεια ψηφιακών εγγράφων. Στη συνέχεια της ενότητας θα κάνουμε μια σύντομη ανασκόπηση των τεχνικών που ανήκουν σε αυτές τις δυο κατηγορίες.

2.2.1 Τεχνικές για την μείωσης πιθανότητας εμφάνισης αστοχιών

Για την αντιμετώπιση του κινδύνου φυσικής φθοράς των φορέων πληροφορίας προτείνετε η επιλογή πιο αξιόπιστων συνιστωσών με μεγαλύτερη διάρκεια ζωής καθώς και η φύλαξη των φορέων σε ελεγχόμενες περιβαλλοντικές συνθήκες χωρίς μεταβολές σε θερμοκρασία και υγρασία. Ιδίως ο έλεγχος του περιβάλλοντος λειτουργίας ενός συστήματος έχει δείξει ότι μειώνει σημαντικά την πιθανότητα

ξαφνικών αστοχιών [NML03, B95, AES28-1997, DPGN03].

Το πρόβλημα της παλαιώσης των συνιστωσών πρόσβασης σε ψηφιακά έγγραφα είναι πολύπλοκο καθώς κανείς δεν μπορεί να προβλέψει με ακρίβεια ποια λειτουργικά συστήματα, μορφότυποι δεδομένων και συσκευές θα συνεχίζουν να υποστηρίζονται στο μέλλον. Ωστόσο έχουν προταθεί τεχνικές που βοηθάνε να αντιμετωπιστεί το πρόβλημα όπως για παράδειγμα η χρήση προτύπων και η διατήρηση της τεχνολογίας [H02]. Η επιστημονική κοινότητα που ασχολείται με τη ψηφιακή διατήρηση έχει δώσει ιδιαίτερη σημασία στην χρήση προτύπων για την μορφοποίηση των ψηφιακών δεδομένων καθώς τα πρότυπα είναι καλά τεκμηριωμένα και επιτρέπουν ακόμα και την επαναδημιουργία λογισμικού για την ερμηνεία των ψηφιακών εγγράφων. Στην βιβλιογραφία δίνεται ιδιαίτερα έμφαση στην πρότυπη γλώσσα XML που για πολλούς θεωρείται η πιο υποσχόμενη τωρινή λύση μορφοποίηση δεδομένων για αρχειοθέτηση και διαλειτουργικότητα και εξετάζεται σαν μια ξεχωριστή στρατηγική προσέγγιση για ψηφιακή διατήρηση [H02]. Η διατήρηση της τεχνολογίας αποτελεί επίσης μια τεχνική για την αντιμετώπιση της παλαιώσης των συνιστωσών. Ωστόσο είναι δαπανηρή και από τεχνολογικής άποψης εξαιρετικά πολύπλοκη.

Για την μείωση της πιθανότητας απωλειών ψηφιακής πληροφορίας λόγω ανθρώπινων λαθών, υπάρχουν οδηγίες για την σχεδίαση διεπαφών ώστε να παρεμποδίζονται για παράδειγμα λαθεμένες ενέργειες διαγραφής. Αντίστοιχα για τα λάθη λογισμικού που μπορεί να οδηγήσουν σε απώλεια δεδομένων έχουν προταθεί έλεγχοι ασφάλειας στο υλικό απαγορεύοντας για παράδειγμα εγγραφή στην μνήμη από μη εξουσιοδοτημένα προγράμματα λογισμικού.

2.2.2 Τεχνικές ανάκαμψης αστοχιών

Μετάβαση (Migration)

Ένα ευρέως αποδεκτός ορισμός του όρου μετάβαση δόθηκε το 1996 από το Task Force on the Archiving of Digital Information [CPA-RLG96]:

«Η μετάβαση είναι ένα σύνολο από οργανωμένα καθήκοντα σχεδιασμένα για την εκτέλεση περιοδικής μεταφοράς του ψηφιακού υλικού από μια διάταξη υλικού-λογισμικού σε άλλη ή από μια γενεά τεχνολογίας υπολογιστών στην επόμενη γενεά»

Ο συγκεκριμένος ορισμός είναι αρκετά ευρύς και διαφορετικές ομάδες και άτομα έχουν προτείνει μια σειρά από διαφορετικές τεχνικές προσεγγίσεις για στρατηγικές μετάβασης. Το National Preservation Office [NPO] διαχωρίζει τη μετάβαση σε τέσσερα διαφορετικά νήματα:

- *Αλλαγή φορέα:* Συχνά απαιτείται να γίνεται αλλαγή του φορέα των ψηφιακών εγγράφων σε συνδυασμό με άλλες ενέργειες διατήρησης ώστε να εξασφαλιστεί η μακροχρόνια ερμηνεία της ροής δυαδικών ψηφίων.
- *Προς τα πίσω συμβατότητα:* Βασίζεται κυρίως στους δημιουργούς λογισμικού να κάνουν νέες εκδόσεις εφαρμογών συμβατές με προκατόχους τους. Ωστόσο τέτοιου είδους συμβατότητες διαρκούν συνήθως για λίγες γενεές και βασίζονται και στα συμφέροντα των δημιουργών του αντίστοιχου λογισμικού.
- *Δια-λειτουργικότητα:* Απαιτεί την δυνατότητα μετακίνησης των ψηφιακών αντικειμένων από μια πλατφόρμα ή εφαρμογή στην επόμενη. Εδώ είναι αναγκαία η λήψη μέτρων ώστε να εξασφαλιστεί ότι δεν θα υπάρχουν απώλειες της αυθεντικότητας, πληροφορίας ή λειτουργικότητας.
- *Μετατροπή σε πρότυπες μορφοποιήσεις:* Δυνατότητα μετακίνησης των αντικειμένων από αρχικούς μορφότευπους που εξαρτώνται από τις εφαρμογές που χρησιμοποιήθηκαν για την δημιουργία τους, σε πρότυπους μορφότευπους μη ιδιοκτησιακού χαρακτήρα.

Τα τελευταία χρόνια η μετάβαση αποτελεί μια ευρέως διαδεδομένη στρατηγική διατήρησης καθώς προσφέρει την πιο απλή τεχνολογικά προσέγγιση για την εξασφάλιση συνεχής πρόσβασης σε ψηφιακά έγγραφα. Στην βιβλιογραφία

υπάρχει πλούσιο υλικό για την τρέχουσα έρευνα γύρω από την εφαρμογή στρατηγικών μετάβασης [LKR+00, DPC, H01].

Πανομοιότυπη επανάληψη (Replication)

Η τεχνική της πανομοιότυπης επανάληψης αντιμετωπίζει αστοχίες με την δημιουργία πολλαπλών αντιγράφων ή νέων στιγμιότυπων ενός ψηφιακού εγγράφου ώστε να εξασφαλίζεται η μακρόχρονη επιβίωση του. Έτσι για παράδειγμα σε περίπτωση αστοχίας ενός δίσκου, έχοντας πανομοιότυπα αντίγραφα των εγγράφων σε ίδια ή διαφορετικά αποθηκευτικά μέσα είναι δυνατή η ανακατασκευή των περιεχομένων του δίσκου. Η τεχνική αυτή μπορεί να χρησιμοποιηθεί και για την αντιμετώπιση του προβλήματος παλαίωσης των συνιστωσών πρόσβασης καθώς για ένα ψηφιακό αντίγραφο είναι δυνατόν να διατηρούνται πολλαπλά αντίγραφα σε διαφορετικές μορφοποιήσεις ώστε να μειώνεται ο κίνδυνος ένα έγγραφο να μην μπορεί να ερμηνευτεί πια λόγω ξεπερασμένης μορφοποίησης. Η πανομοιότυπη επανάληψη έχει χρησιμοποιηθεί σε πολλά συστήματα, μεταξύ άλλων τα εξής: Computer Research Repository, The Archival Intermemory Project, Stanford Archival Fault [HL93, CCM00].

Εξομοίωση (Emulation)

Η εξομοίωση περιλαμβάνει την επαναδημιουργία σε μια νέα πλατφόρμα, όλων των συνιστωσών που απαιτούνται για την πρόσβαση σε ένα ψηφιακό έγγραφο. Η εξομοίωση μπορεί να γίνει σε πολλά επίπεδα: υλικού, λειτουργικού συστήματος ή λογισμικού εφαρμογής. Το βασικό μειονέκτημα αυτής της προσέγγισης είναι το κατά πόσο είναι επιτεύξιμη καθώς πρόκειται για διαδικασία εξαιρετικά πολύπλοκη που απαιτεί λεπτομερείς γνώσεις για το αρχικό περιβάλλον. Στην ουσία δεν υπάρχει καμία εγγύηση ότι θα είναι εφικτή η αναδημιουργία ενός πλήρους υπολογιστικού περιβάλλοντος σε κάποιο μελλοντικό υπολογιστή. Ωστόσο, η εξομοίωση έχει δοκιμαστεί σε κάποια πεδία με επιτυχία και ίσως αποτελεί μοναδικό τρόπο για την υποστήριξη πολύπλοκων

βάσεων δεδομένων και πολυμεσικών αντικειμένων.

Μια παραλλαγή της εξομοίωσης προτάθηκε από τον Raymond Lorie της IBM [L01] που πρότεινε την ιδέα ενός “Γενικού Ιδεατού Υπολογιστή” (Universal Virtual Computer - UVC). Για την ερμηνεία αρχείων δεδομένων στο μέλλον προτείνει να γράφεται ένα πρόγραμμα που να εκτελεί την ερμηνεία των εγγραφών στη γλώσσα μηχανής του UVC. Η συγκεκριμένη προσέγγιση έχει πολλά κοινά με τις αρχές που χρησιμοποιεί η Java πλατφόρμα για να πετύχει δια-λειτουργικότητα μεταξύ των προγραμμάτων της.

Γρήγορη ανίχνευση σφαλμάτων και επισκευή

Η γρήγορη ανίχνευση και επισκευή είναι σημαντικός παράγοντας για την βελτίωση της αξιοπιστίας διατάξεων συστημάτων για ψηφιακή διατήρηση. Ωστόσο τα σφάλματα δεν είναι εύκολο να ανιχνεύονται άμεσα καθώς συχνά πρώτα συμβαίνει ένα σφάλμα και στη συνέχεια εκδηλώνεται. Σε ένα σύστημα που περιλαμβάνει μεγάλο πλήθος από συνιστώσες δεν είναι πάντα εύκολα να ελέγχονται όλες για πιθανά σφάλματα. Συνήθως γίνεται επιλεκτική επιλογή τους με δειγματοληψία ή χρησιμοποιούνται ειδικά συστήματα προειδοποίησης αστοχιών όταν μια συνιστώσα πλησιάζει στο τέλος της ζωής της (τεχνολογία S.M.A.R.T [HFM+02]).

Πάντως είναι πολύ σημαντικό να σημειωθεί ότι σε περίπτωση ανίχνευσης αστοχίας μιας συνιστώσας (για παράδειγμα ενός δίσκου) είναι σημαντικό να γίνεται άμεσα η επισκευή της. Όπως θα αποδείξουμε στο κεφάλαιο 4, μεγάλες αναμονές μέχρι την επισκευή, αυξάνει σημαντικά το κίνδυνο μια δεύτερη αστοχία να οδηγήσει σε απώλεια της πληροφορίας.

ΚΕΦΑΛΑΙΟ 3

Κριτήρια αποτίμησης αξιοπιστίας και διαθεσιμότητας

3.1 Εισαγωγή

Η ραγδαία ανάπτυξη υπολογιστών και υπολογιστικών συστημάτων σε διάφορα πεδία έχει φέρει στο επίκεντρο την ανάγκη βásiμων και αξιόπιστων συστημάτων. Και ενώ στο παρελθόν το ενδιαφέρον επικεντρωνόταν στην απόδοση συστημάτων, η ολική αξιοπιστία των συστημάτων (system dependability) αποκτάει όλο και περισσότερη σημασία. Ο Laprie [L85] ορίζει την «ολική αξιοπιστία συστημάτων» ως την δυνατότητα ενός συστήματος ή προϊόντος να παρέχει το προσδοκώμενο επίπεδο υπηρεσιών στους χρήστες ειδικά υπό το φως αστοχιών και άλλων συμβάντων που έχουν επιπτώσεις στο επίπεδο των παρεχόμενων υπηρεσιών. Συνεπώς μπορούμε να θεωρήσουμε ότι ο όρος «ολική αξιοπιστία» αποτελεί το γενικό όρο που περικλείει και μελετά την αξιοπιστία, διαθεσιμότητα, ασφάλεια και συντηρησιμότητα συστημάτων. Ανάλογα με το περιβάλλον εφαρμογής, ένα ή περισσότερα από αυτά τα χαρακτηριστικά αποτελούν κατάλληλη προβολή της συμπεριφοράς του συστήματος. Έτσι για παράδειγμα, σε ένα περιβάλλον πληροφοριακών συστημάτων διαχείρισης, η αναλογία χρόνου που είναι ικανό το σύστημα να προσφέρει τις προσδοκώμενες υπηρεσίες (διαθεσιμότητα του συστήματος) αποτελεί ένα σημαντικό κριτήριο. Σε ένα σύστημα ελέγχου πτήσης αεροσκαφών, οι αστοχίες του συστήματος μπορεί να είναι καταστροφικές. Συνεπώς η δυνατότητα του συστήματος να παρέχει συνεχώς υπηρεσίες χωρίς καταστροφικές αστοχίες (αξιοπιστία του συστήματος) είναι μεγαλύτερης σημασίας.

Ο Heimann [HMT89] αναφέρει τρεις διαφορετικούς λόγους για την χρήση της ολικής αξιοπιστίας στην αποτίμηση συστημάτων:

- Η ολική αξιοπιστία επιτρέπει σύγκριση μεταξύ διαφορετικών σχεδιαστικών επιλογών, ταυτόχρονα με το κόστος και την απόδοση. Μαζί με το κόστος και την απόδοση, η ολική αξιοπιστία είναι το τρίτο κρίσιμο κριτήριο πάνω στο οποίο λαμβάνονται αποφάσεις σχετικές με το σύστημα.
- Η ολική αξιοπιστία εστιάζει κατάλληλα στην προσπάθεια βελτίωσης ενός προϊόντος. Η αποτίμηση της ολικής αξιοπιστίας επιτρέπει να προσδιοριστούν οι όψεις της συμπεριφοράς του συστήματος, όπως η αξιοπιστία υποσυστημάτων, κάλυψη σφαλμάτων, στρατηγικές συντήρησης που παίζουν κρίσιμο ρόλο στον καθορισμό της γενικής αξιοπιστίας του συστήματος.
- Η ολική αξιοπιστία λαμβάνει υπόψη θέματα που αφορούν την ασφάλεια και κινδύνους. Η αποτίμηση της ολικής αξιοπιστίας επιτρέπει να προσδιοριστούν επισφαλής καταστάσεις και κίνδυνοι που εμπλέκονται με το σύστημα και καθιστούν αδύνατη την παροχή των προσδοκώμενων υπηρεσιών.

Παραδοσιακά, τα διαγράμματα μπλοκ αξιοπιστίας και τα δέντρα σφαλμάτων είχαν χρησιμοποιηθεί για την ανάλυση αξιοπιστίας και διαθεσιμότητας συστημάτων. Αυτά τα είδη μοντέλων επιτρέπουν μια περιεκτική περιγραφή του συστήματος υπό μελέτη και μπορούν να αποτιμηθούν αποτελεσματικά, ωστόσο δεν μπορούν εύκολα να αναπαραστήσουν εξαρτήσεις που απαντώνται σε πραγματικά συστήματα. Τα μοντέλα Markov από την άλλη μεριά είναι ικανά να συλλάβουν διάφορα είδη εξαρτήσεων που απαντώνται σε μοντέλα αξιοπιστίας και διαθεσιμότητας.

Σκοπός αυτής της ενότητας είναι να δώσει μια εποπτεία για τις τεχνικές και τα εργαλεία που υπάρχουν για την αποτίμηση της ολικής αξιοπιστίας.

3.2 Βασικοί ορισμοί και ορολογία

Αρχικά θα επικεντρωθούμε σε βασικούς ορισμούς και ορολογία που χρησιμοποιείται συχνά στην αποτίμηση της ολικής αξιοπιστίας ενός συστήματος. Θα ορίσουμε μια σειρά από κριτήρια ολικής αξιοπιστίας και στη συνέχεια στην ενότητα 3.3 θα παρουσιάσουμε μια σειρά από τεχνικές μοντελοποίησης που χρησιμοποιούνται συχνά τόσο για την αναπαράσταση της συμπεριφορά συστημάτων σε επίπεδο ολικής αξιοπιστίας όσο και στην αποτίμηση των κριτηρίων ολικής αξιοπιστίας που παρουσιάζουν ενδιαφέρον.

3.2.1 Κριτήρια ολικής αξιοπιστίας

Τα κριτήρια ολικής αξιοπιστίας μπορούμε να θεωρήσουμε ότι ανήκουν σε δυο μεγάλες κατηγορίες: την αξιοπιστία συστημάτων και την διαθεσιμότητα συστημάτων. Ανάλογα με την περίπτωση που εξετάζουμε ένα ή περισσότερα από αυτά τα κριτήρια μπορεί να είναι κατάλληλο. Το κριτήριο της αξιοπιστίας συστημάτων συνήθως είναι σχετικό σε περιπτώσεις συστημάτων που είναι ευαίσθητα σε αστοχίες και διακοπές λειτουργίας. Η διαθεσιμότητα συστημάτων αποτελεί κριτήριο για συστήματα όπου σύντομες διακοπές είναι ανεκτές. Κυρίως οι εμπορικές εφαρμογές υπολογιστικών συστημάτων, όπως συστήματα τραπεζικών αναλήψεων ή συστήματα κράτησης εισιτηρίων ανήκουν σε αυτή την κατηγορία.

3.2.1.1 Κριτήρια αξιοπιστίας

Ορισμός 3.1: Η αξιοπιστία $R(t)$ ενός συστήματος το χρόνο t είναι η πιθανότητα να μην έχει συμβεί αστοχία στο σύστημα στο χρονικό διάστημα $[0, t)$. Αν X είναι η τυχαία μεταβλητή που αναπαριστά το χρόνο εμφάνισης μιας αστοχίας του συστήματος τότε ισχύει $R(t) = P(X > t)$.

Η αξιοπιστία χρησιμοποιείται πολύ συχνά ως κριτήριο για την αποτίμηση

συστημάτων κρίσιμων αποστολών. Μπορούμε επίσης να υπολογίσουμε την αναξιοπιστία του συστήματος ως $1 - R(t)$. Ένα κριτήριο που παρουσιάζει επίσης ενδιαφέρον είναι ο μέσος χρόνος μέχρι την αστοχία ενός συστήματος $MTTF$.

Ορισμός 3.2: Ο μέσος χρόνος μέχρι την αστοχία ενός συστήματος $MTTF$ είναι ο αναμενόμενος χρόνος μέχρι να συμβεί η πρώτη αστοχία του συστήματος. Αν X είναι η τυχαία μεταβλητή που αναπαριστά το χρόνο μέχρι την εμφάνιση μιας αστοχίας του συστήματος, τότε $MTTF = E[X]$.

Δοσμένης της αξιοπιστίας του συστήματος $R(t)$, ο $MTTF$ μπορεί να υπολογιστεί ως:

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

3.2.1.2 Κριτήρια διαθεσιμότητας

Τα κριτήρια διαθεσιμότητας συστημάτων είναι ιδιαίτερα κατάλληλα για συστήματα που επιδέχονται επισκευή και σύντομες διακοπές στη λειτουργία τους είναι ανεκτές. Αναλόγως με το χρονικό ορίζοντα που ενδιαφέρει, τα κριτήρια διαθεσιμότητας συστήματος εκφράζονται με τρεις διαφορετικούς τρόπους.

Ορισμός 3.3: Η στιγμιαία διαθεσιμότητα $A(t)$ ενός συστήματος το χρόνο t είναι η πιθανότητα το σύστημα να λειτουργεί σωστά το χρόνο t .

Σε ορισμένες εφαρμογές είναι καλύτερο να υπολογίζεται η μη-διαθεσιμότητα του συστήματος $U(t) = 1 - A(t)$

Ορισμός 3.4: Η διαθεσιμότητα ενός διαστήματος (interval availability) $\bar{A}(t)$ ενός συστήματος στο $[0, t)$ είναι η αναμενόμενη αναλογία χρόνου εντός του διαστήματος κατά την οποία το σύστημα λειτουργούσε σωστά.

Πρέπει να σημειώσουμε ότι ισχύει:
$$\bar{A}(t) = \frac{1}{t} \int_0^t A(x) dx$$

Ορισμός 3.5: Η οριακή διαθεσιμότητα διαστήματος (limiting interval availability) είναι το αναμενόμενο κλάσμα χρόνου κατά το οποίο το σύστημα είναι λειτουργικό $\bar{A} = \lim_{t \rightarrow \infty} \bar{A}(t)$

Ορισμός 3.6: Η διαθεσιμότητα σταθερής κατάστασης (steady-state availability) A_{ss} αναπαριστά την πιθανότητα μεγάλης διάρκειας στην οποία το σύστημα είναι διαθέσιμο $A_{ss} = \lim_{t \rightarrow \infty} A(t)$.

Η μη-διαθεσιμότητα σταθερής κατάστασης του συστήματος δίνεται από την σχέση $U_{ss} = 1 - A_{ss}$.

Άλλα κατάλληλα κριτήρια για την διαθεσιμότητα συστήματος είναι: αθροιστική συνάρτηση διαθεσιμότητας (cumulative availability distribution), διαθεσιμότητα ανοχής (tolerance availability), capacity-oriented availability, tolerance capacity-oriented availability, degraded-capacity time [HMT89].

3.2.2 Καθορισμός παραμέτρων σε μοντέλα ολικής αξιοπιστίας

Για την επίλυση και χρήση μοντέλων ολικής αξιοπιστίας είναι ανάγκη να

μελετηθούν μια σειρά από θεμελιώδης παράμετροι. Οι παράμετροι ομαδοποιούνται σε τέσσερις κατηγορίες: ρυθμοί αστοχίας (λ), πιθανότητα κάλυψης σφάλματος (c), ρυθμοί επισκευής (μ), reward rate (r).

3.2.2.1 Ρυθμός αστοχίας (Failure Rate)

Η δεσμευμένη πιθανότητα μια συνιστώσα να μην επιβιώσει για ένα επιπλέον χρονικό διάστημα x δεδομένου ότι έχει επιβιώσει μέχρι το χρόνο t γράφεται ως εξής:

$$G_Y(x|t) = \frac{P(t < X \leq t+x)}{P(X > t)} = \frac{F(t+x) - F(t)}{R(t)}$$

Ορισμός 3.7 (Στιγμιαίου ρυθμού αστοχίας)

Ο στιγμιαίος ρυθμός αστοχίας $h(t)$ κατά το χρόνο t ορίζεται ως

$$h(t) = \lim_{x \rightarrow 0} \frac{1}{x} \frac{F(t+x) - F(t)}{R(t)} = \lim_{x \rightarrow 0} \frac{R(t) - R(t+x)}{xR(t)} \quad h(t) = \frac{f(t)}{R(t)}$$

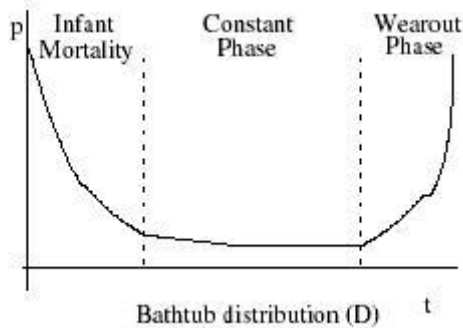
Συνεπώς, το γινόμενο $h(t) \cdot \Delta t$ αναπαριστά την δεσμευμένη πιθανότητα μια συνιστώσα που έχει επιβιώσει μέχρι το χρόνο t , να αστοχήσει στο διάστημα $(t, t + \Delta t]$. Η εκθετική κατανομή που εισάγεται στην ενότητα 3.4 χαρακτηρίζεται από σταθερό ρυθμός αστοχίας και ανεξάρτητο από την ηλικία t της συνιστώσας.

Αν θεωρήσουμε συνιστώσες που παλαιώνουν με την έννοια ότι η δεσμευμένη πιθανότητα επιβίωσης μειώνεται με την ηλικία της συνιστώσας t αυτό σημαίνει ότι $R_i(y)$ είναι φθίνουσα στο διάστημα $0 < t < \infty$ για όλα τα $y \geq 0$. Αυτό έχει σαν αποτέλεσμα ο στιγμιαίος ρυθμός αστοχίας της συνιστώσας να είναι αύξουσα συνάρτηση ως προς το t για $t \geq 0$. Η αντίστοιχη συνάρτηση κατανομής $F(t)$ ονομάζεται κατανομή με αύξοντα χρόνου αστοχίας.

Αν η ηλικία της συνιστώσας είναι ευεργετική με την έννοια ότι η δεσμευμένη πιθανότητα επιβίωσης αυξάνεται με την ηλικία της συνιστώσας, τότε ο στιγμιαίος

ρυθμός αστοχίας της συνιστώσας είναι φθίνουσα συνάρτηση ως προς το t για $t \geq 0$ και η αντίστοιχη συνάρτηση κατανομής $F(t)$ ονομάζεται κατανομή φθίνοντα χρόνου αστοχίας (decreasing failure rate distribution-DFR).

Η συμπεριφορά του ρυθμούς αστοχίας ως συνάρτηση της ηλικίας είναι γνωστή



Εικόνα 1: Καμπύλη αστοχίας

και ως καμπύλη αστοχίας (Εικόνα 1). Στην αρχική περίοδο ζωής (περίοδος διόρθωσης λαθών), οι αστοχίες είναι ενδογενής και προκύπτουν από ενυπάρχοντα ελαττώματα του συστήματος που αποδίδονται σε λαθεμένο σχεδιασμό, λάθη στην κατασκευή ή συναρμολόγηση. Στην διάρκεια αυτής της περιόδου αναμένεται ο ρυθμός αστοχίας να μειώνεται με την ηλικία. Μετά την περίοδο διόρθωσης λαθών το σύστημα, είναι επιρρεπές σε τυχαίες αστοχίες που καλούνται και εξωγενής. Τέτοιες αστοχίες σχετίζονται κυρίως με τις συνθήκες περιβάλλοντος στο οποίο λειτουργεί το σύστημα. Είναι αποτέλεσμα σοβαρών και μη προβλέψιμων εντάσεων που προκύπτουν από απότομες περιβαλλοντικές διαταραχές και ο ρυθμός αστοχίας καθορίζονται από την ταλαιπωρία που επιβάλλεται λόγω του περιβάλλοντος. Στην διάρκεια της χρήσιμης περιόδου, συνήθως ο ρυθμός αστοχίας προσεγγιστικά θεωρείται σταθερός και μπορεί να γίνει η υπόθεση ότι ο χρόνος μέχρι την αστοχία της συνιστώσας είναι εκθετικά κατανομημένος. Όταν η συνιστώσα αρχίζει να φτάνει την «αναμενόμενη διάρκεια ζωής» της ο ρυθμός αστοχίας αρχίζει να αυξάνει και ουσιαστικά η

συνιστώσα είναι στην φάση της φθοράς.

3.2.2.2 Ρυθμός επισκευής (*Repair rate*)

Ο ρυθμός επισκευής πρέπει να λαμβάνεται υπόψη σε ακριβή μοντέλα αξιοπιστίας συστημάτων. Ωστόσο είναι δύσκολη η αναπαράσταση της δραστηριότητας επισκευής με αναλυτικό τρόπο [SS98]. Υπάρχουν πολλοί παράγοντες που επηρεάζουν τον ρυθμό με τον οποίο συμβαίνει η επισκευή περιλαμβάνοντας ανθρώπινη επιδεξιότητα, απαιτούμενο χρόνο μετακίνησης, δυνατότητα διάγνωσης και την διαθεσιμότητα εξαρτημάτων. Παρά την έλλειψη θεωρητικής γνώσης σε βάθος, τα πιθανοτικά μοντέλα κάνουν υποθέσεις για τον ρυθμό επισκευής με ανάλογο τρόπο του ρυθμού αστοχίας.

Για την επίλυση μοντέλων αξιοπιστίας που περιλαμβάνει τόσο ρυθμό αστοχίας και ρυθμό επισκευής απαιτείται η χρήση μοντέλων Markov που αναλύονται σε επόμενες ενότητες. Σε αυτά τα μοντέλα συνήθως γίνεται η υπόθεση ότι η επισκευή ενός συστήματος που έχει αστοχήσει επαναφέρει το σύστημα με τέτοιο τρόπο ώστε ο ρυθμός αστοχίας του συστήματος να παραμένει ο ίδιος σαν να μην είχε συμβεί κάποια αστοχία [SS98]. Στην περίπτωση εκθετικού μοντέλου (σταθερό ρυθμό αστοχίας) κάτι τέτοιο ισχύει και ο ρυθμός επισκευής συνδέεται με το αναμενόμενο χρόνο επισκευής (*MTTR*-Mean time to repair) ενός συστήματος ή μιας συνιστώσας που έχει αστοχήσει με την σχέση $MTTR = \frac{1}{\mu}$. Αυτή η υπόθεση είναι λιγότερο έγκυρη για την Weibull διαδικασία αλλά γίνεται για να επιτυγχάνονται αναλυτικές λύσεις [SS98].

3.2.2.3 Πιθανότητες κάλυψης

Σε μια ανάλυση της αξιοπιστίας σε επίπεδο συστήματος, είναι πολύ σημαντικό να γνωρίζουμε πόσο καλά ένα σύστημα σαν σύνολο μπορεί να λειτουργήσει όταν αστοχήσει ένα από τα υποσυστήματα του. Αν το σύστημα μπορεί να λειτουργήσει χωρίς προβληματικές επιρροές ή με μια αποδεκτή υποβίβαση των λειτουργιών του, τότε θεωρείται ότι η αστοχία έχει καλυφθεί. Αν όμως η αστοχία

προκαλέσει αναστολή τις λειτουργίας ολόκληρου του συστήματος, τότε θεωρείται ότι η αστοχία δεν έχει καλυφθεί. Η κάλυψη είναι η πιθανότητα το σύστημα να ανακάμψει επιτυχώς από ένα συγκεκριμένο είδος αστοχίας. Συχνά η κάλυψη είναι η πιθανότητα μια συγκεκριμένη κλάση σφάλματος να ανιχνεύεται επιτυχώς πριν συμβεί πλήρης φθορά στο σύστημα. Είναι επίσης γνωστό ότι ακόμα και μικρές αλλαγές στην τιμή της πιθανότητας κάλυψης μπορεί να προκαλέσει μάλλον μεγάλες αλλαγές στα αποτελέσματα του μοντέλου [SS98].

3.3 Κατηγορίες μοντέλων ολικής αξιοπιστίας

Μια σειρά από κατηγορίες μοντέλων χρησιμοποιούνται τόσο για να αναπαραστήσουν την συμπεριφορά πολύπλοκων συστημάτων ότι αφορά την ολική αξιοπιστία τους και για να ληφθούν διάφορα κριτήρια ολικής αξιοπιστίας. Τα μοντέλα αυτά ευρέως κατηγοριοποιούνται σε δυο είδη [MFT00]: (1) Μοντέλα χωρίς χώρο καταστάσεων, και (2) Μοντέλα με χώρο καταστάσεων, ανάλογα με την φύση των δομικών στοιχείων τους και τις τεχνικές επίλυσης. Στα μοντέλα χωρίς χώρο καταστάσεων δεν απαιτείται η απαρίθμηση των καταστάσεων του συστήματος, ενώ στις τεχνικές μοντελοποίησης με χώρο καταστάσεων απαιτείται η συλλογή μεταβλητών των οποίων οι τιμές καθορίζουν την κατάσταση του συστήματος σε ένα δεδομένο σημείο. Τα μοντέλα χωρίς χώρο καταστάσεων επιτρέπουν περιεκτικές περιγραφές του υπό μελέτη συστήματος και μπορούν να αποτιμηθούν αποτελεσματικά, ωστόσο αδυνατούν να αναπαραστήσουν εξαρτήσεις εντός του συστήματος που απαντώνται συχνά σε πραγματικά συστήματα, σε αντίθεση με τα μεθόδους που βασίζονται σε χώρο καταστάσεων.

Τα μοντέλα χώρου καταστάσεων μπορεί να έχουν φύση ντετερμινιστική ή στοχαστική. Τα μοντέλα χαρακτηρίζονται ντετερμινιστικά αν τα δομικά τους στοιχεία είναι επαρκώς καθορισμένα έτσι ώστε η συμπεριφορά του μοντέλου να καθορίζεται με ακρίβεια. Στοχαστικά μοντέλα, από την άλλη, έχουν πιθανοτική φύση και δεν καθορίζουν αριθμητικές τιμές για τις μεταβλητές όπως συμβαίνει

στα ντετερμινιστικά. Συνήθως στα στοχαστικά μοντέλα καθορίζουν πιθανότητες (and/or moments) που σχετίζονται με την κατάσταση του συστήματος και τις μεταβλητές εξόδου. Οι πιθανότητες των καταστάσεων υπολογίζονται και στην συνέχεια προσδιορίζονται τα κριτήρια ολικής αξιοπιστίας που παρουσιάζουν ενδιαφέρον.

Στοχαστικά μοντέλα είναι η μέθοδος που επιλέγεται όταν μοντελοποιείται η ολική αξιοπιστία υπολογιστικών συστημάτων αφού συχνά απαιτείται να αναπαρασταθούν φαινόμενα που περικλείουν σημαντική αβεβαιότητα και μη-προβλέψιμη μεταβλητότητα (έμφυτη στο σύστημα ή στις μεταβλητές εισόδου). Μέσα από την πιθανοτική προσέγγιση, η απήχηση των αβεβαιοτήτων στην επίλυση του μοντέλου μπορεί ξεκάθαρα να αποδειχθεί.

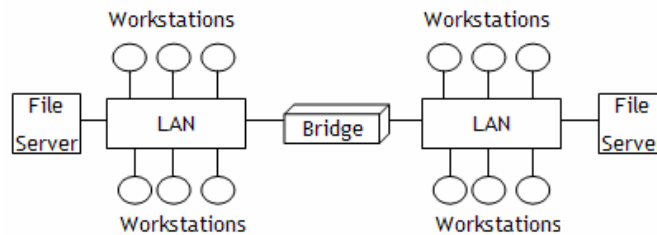
Στην πράξη, τα στοχαστικά μοντέλα κατηγοριοποιούνται παραπέρα σε Markovian και non-Markovian [MFT00]. Ο διαχωρισμός βασίζεται στην συνάρτηση κατανομής των τυχαίων μεταβλητών (joint distribution) της υποκείμενης στοχαστικής διαδικασίας. Τα Markov μοντέλα που θα παρουσιάσουμε εκτεταμένα στην ενότητα 3.4, έχουν χρησιμοποιηθεί για την αποτίμηση ολικής αξιοπιστίας υλικού και λογισμικού υπολογιστικών συστημάτων. Ο λόγος που τα μοντέλα Markov είναι δημοφιλή είναι ότι περιλαμβάνουν την δυνατότητα να συλλάβουν μια σειρά από εξαρτήσεις που υπάρχουν στο σύστημα επίσης επιτρέπουν εξίσου τον υπολογισμό κριτηρίων όπως σταθερής κατάστασης, μεταβατικής και αθροιστικά μεταβατικής και με την επέκταση σε Markov reward μοντέλα είναι χρήσιμα στην ανάλυση επιδόσεων συστημάτων (performability analysis). Ένα μεγάλο εύρος προβλημάτων εμπίπτουν στην κυριότητα των μοντέλων Markov (ομοιογενών και μη-ομοιογενών). Ωστόσο, υπάρχουν σημαντικές πλευρές στην συμπεριφορά συστημάτων στα στοχαστικά μοντέλα που δεν είναι εύκολο να συλληφθούν από ένα μοντέλο Markov. Το κοινό χαρακτηριστικό που μοιράζονται αυτά τα προβλήματα είναι ότι η Markov ιδιότητα δεν είναι έγκυρη σε όλα τις χρονικές

στιγμές. Αυτές οι κατηγορίες προβλημάτων αναφέρονται από κοινού ως non-Markovian μοντέλα. Τα non-Markovian μοντέλα αναλύονται με την βοήθεια συμπληρωματικών μεταβλητών ή επεκτάσεις του χώρου καταστάσεων του μοντέλου σε φάσεις. Μια εισαγωγή των non-Markovian μοντέλων υπάρχει στο [MFT00].

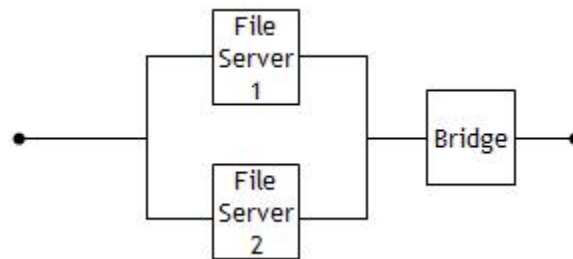
3.3.1 Διαγράμματα μπλοκ αξιοπιστίας (Reliability Block Diagrams-RBDs)

Σε ένα μοντέλο διαγράμματος μπλοκ αξιοπιστίας οι συνιστώσες και τα υπό-συστήματα αναπαρίστανται από μπλοκ. Οι διασυνδέσεις μεταξύ των μπλοκ απεικονίζουν την λειτουργική εξάρτηση του συστήματος που υπάρχει μεταξύ των συνιστωσών και των υπό-συστημάτων. Οι συνιστώσες για τις οποίες υπάρχει η απαίτηση να λειτουργούν όλες ώστε να είναι λειτουργικό και το (υπό)σύστημα είναι συνδεδεμένες σε σειρά. Τα μπλοκ των συνιστωσών είναι συνδεδεμένα παράλληλα αν και μόνο αν η αστοχία όλων έχει σαν αποτέλεσμα την αστοχία του (υπό) συστήματος. Σε αυτή την κατηγορία των μοντέλων υποθέτουμε ότι οι ξεχωριστές συνιστώσες είναι ανεξάρτητες μεταξύ τους, συνεπώς η αστοχία μιας συνιστώσας δεν επηρεάζει την συμπεριφορά αστοχίας οποιασδήποτε άλλης συνιστώσας. Τα RBD's είναι η προσέγγιση στη μοντελοποίηση συστημάτων που απεικονίζει την πιθανότητα επιτυχίας. Η δομή των μπλοκ στα διαγράμματα μπλοκ αξιοπιστίας μπορεί επίσης να είναι της μορφής κ-από-ν (k OF n), δηλαδή ένα μπλοκ με n συνιστώσες είναι λειτουργικό αν τουλάχιστον k σε πλήθος συνιστώσες είναι λειτουργικές. Το διάγραμμα μπλοκ αξιοπιστίας για το παράδειγμα 3-1 που περιγράφεται στη συνέχεια υπάρχει στην Εικόνα 3

Παράδειγμα 3.1: Θεωρούμε ένα δικτυωμένο σύστημα που αποτελείται από δυο τοπικά LAN τμήματα που συνδέονται μεταξύ τους με μια γέφυρα. Κάθε τμήμα LAN έχει τοπικά ένα εξυπηρετητή διαχείρισης αρχείων (file server) και παρέχει δεδομένα σε σταθμούς εργασίας. Τα δεδομένα στους εξυπηρετητές αρχείων είναι πανομοιότυπα μεταξύ τους έτσι ώστε ακόμα και αν ένας από τους εξυπηρετητές αστοχήσει να μπορούν να συνεχίζουν οι σταθμοί εργασίας να λαμβάνουν τα δεδομένα τους. Η γέφυρα είναι η κρίσιμη συνιστώσα που φροντίζει να υπάρχει συνέπεια ανάμεσα στα δεδομένα των δυο εξυπηρετητών. Συνεπώς το σύστημα που περιγράψαμε είναι λειτουργικό αρκεί ένας από τους εξυπηρετητές και η γέφυρα να λειτουργούν.



Εικόνα 2: Παράδειγμα δικτυωμένου συστήματος

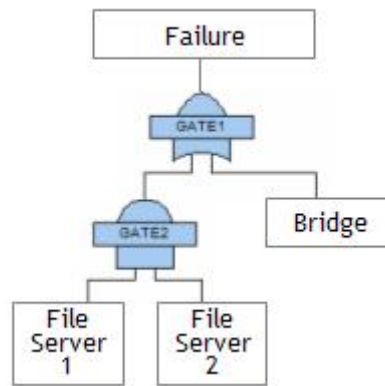


Εικόνα 3: Παράδειγμα διαγράμματος μπλοκ αξιοπιστίας

3.3.2 Δέντρα σφαλμάτων (Fault trees)

Τα δέντρα σφαλμάτων σε αντίθεση με τα RBDs, απεικονίζουν την πιθανότητα αστοχίας στην μοντελοποίηση συστημάτων. Στα δέντρα σφαλμάτων

χρησιμοποιούνται πύλες Boolean (AND και OR πύλες) για να αναπαραστήσουν την λειτουργική εξάρτηση των συνιστώσων του συστήματος. Σε περίπτωση αστοχίας της συνιστώσας, η αντίστοιχη είσοδος της πύλης γίνεται αληθής. Για πύλες OR ισχύει ότι αν οποιαδήποτε από τις εισόδους γίνει αληθής τότε και η έξοδος της πύλης γίνεται αληθής. Οι εισοδοί των πύλων OR είναι οι συνιστώσες που απαιτείται να λειτουργούν όλες ώστε να λειτουργεί το (υπό)σύστημα. Αντίθετα, οι εισοδοί των πύλων AND, είναι εκείνες οι συνιστώσες για τις οποίες απαιτείται να αστοχήσουν όλες για να αστοχήσει και το (υπό)σύστημα. Οποτεδήποτε η έξοδος της ανώτατης πύλης γίνει αληθής το σύστημα έχει αστοχήσει. Το δέντρο σφαλμάτων για το παράδειγμα 3.1 υπάρχει στην Εικόνα 4.



Εικόνα 4. Παράδειγμα δέντρου σφαλμάτων

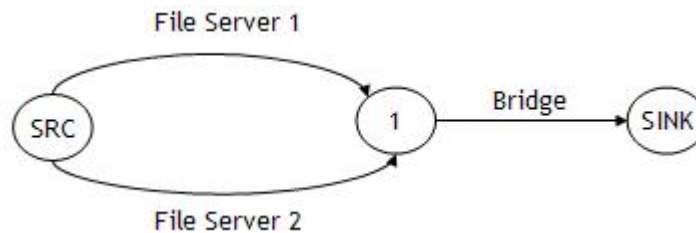
Μια σειρά από επεκτάσεις έχουν γίνει στα δέντρα σφαλμάτων περιλαμβάνοντας την χρήση της πύλης NOT, XOR, Priority AND, kOFn πύλες. Μια επιπλέον επέκταση αποτελούν τα δέντρα σφαλμάτων όπου επιτρέπεται η χρήση επαναλαμβανόμενων γεγονότων. Στην περίπτωση αυτή επιτρέπεται σε διαφορετικές πύλες να μοιράζονται εισόδους μεταξύ τους [CL02].

3.3.3 Γράφοι αξιοπιστίας (Reliability Graphs-RGs)

Ένα γράφος αξιοπιστίας $G = (U, V)$ αποτελεί ένα ειδικό τύπο ακυκλικού γράφου όπου U αναπαριστά το σύνολο των κόμβων και V το σύνολο των ακμών του

γράφου. Μια συνιστώσα αναπαριστάται από μια κατευθυνόμενη ακμή μέσα στο γράφο που συνδέει δυο κόμβους. Μερικές ειδικές ακμές που ονομάζονται ∞ -ακμές αναπαριστούν συνιστώσες που δεν αστοχούν. Υπάρχουν δυο ειδικοί κόμβοι στο γράφο που χαρακτηρίζονται ως κόμβος αρχής (source node) και κόμβος απορροφητικός (sink node). Ο κόμβος αρχής δεν έχει ακμές που εισέρχονται σε αυτόν ενώ ο απορροφητικός κόμβος δεν έχει εξερχόμενες ακμές. Το σύστημα θεωρείται λειτουργικό εφόσον υπάρχει τουλάχιστον ένα κατευθυνόμενο μονοπάτι από το κόμβο αρχής προς τον απορροφητικό κόμβο.

Ο γράφος αξιοπιστίας για το παράδειγμα 3-1 φαίνεται στην Εικόνα 5.



Εικόνα 5. Παράδειγμα γράφου αξιοπιστίας

3.4 Η εκθετική κατανομή

Αυτή η κατανομή που ενίοτε αποκαλείται και αρνητική εκθετική κατανομή (negative exponential distribution), απαντάται συχνά στην θεωρία αξιοπιστίας. Ο λόγος για την χρήση αυτής της κατανομής είναι η ιδιότητα «χωρίς μνήμη» (memoryless property) που έχει και η συνεπαγόμενη δυνατότητα αναλυτικής παρακολούθησης της, καθώς και η σχέση που την συνδέει με την (διακριτή) κατανομή Poisson. Συνεπώς οι ακόλουθες τυχαίες μεταβλητές συχνά να μοντελοποιούνται ως εκθετικές:

- Ο χρόνος μεταξύ δυο διαδοχικών αφίξεων εργασιών σε ένα εξυπηρετητή (interarrival time).
- Ο χρόνος μέχρι την αστοχία μιας συνιστώσας.
- Ο χρόνος που απαιτείται για την επισκευή μιας συνιστώσας που έχει

υποστεί βλάβη.

Η συνάρτηση πυκνότητας (pdf), η αθροιστική συνάρτηση κατανομής (cdf), η συνάρτηση αξιοπιστίας και η συνάρτηση ρυθμού αστοχίας για την εκθετική κατανομή δίνονται στο Πίνακας 1

Συνάρτηση πυκνότητας	Αθροιστική συνάρτηση κατανομής	Συνάρτηση αξιοπιστίας	Συνάρτηση ρυθμού αστοχίας
$f(t) = \begin{cases} \lambda e^{-\lambda t}, & \text{αν } t > 0 \\ 0, & \text{διαφορετικά} \end{cases}$	$F(t) = \begin{cases} 1 - e^{-\lambda t}, & \text{αν } 0 \leq t < \infty \\ 0, & \text{διαφορετικά} \end{cases}$	$R(t) = \lambda e^{-\lambda t}$	$z(t) = \lambda$

Πίνακας 1: Συναρτήσεις εκθετικής κατανομής

Ας εξετάσουμε την ιδιότητα «χωρίς μνήμη» της εκθετικής κατανομής. Ας υποθέσουμε ότι γνωρίζουμε ότι η τ.μ. X υπερβαίνει μια δεδομένη τιμή t , δηλαδή ισχύει $X > t$. Για παράδειγμα, ας θεωρήσουμε ότι το X περιγράφει το χρόνο ζωής μιας συνιστώσας, και υποθέτουμε ότι έχουμε παρατηρήσει ότι αυτή ήδη λειτουργεί για t ώρες. Ενδιαφερόμαστε για την κατανομή της τυχαίας μεταβλητής $Y = X - t$ του υπόλοιπου χρόνου ζωής. Υποθέτουμε ότι η δεσμευμένη πιθανότητα της $Y \leq y$ δεδομένου ότι $X > t$ συμβολίζεται ως $G_y(y|t)$. Όπως αποδεικνύεται [T02] η $G_y(y|t)$ είναι ανεξάρτητη του t και ταυτίζεται με την αρχική εκθετική κατανομή του X . Ουσιαστικά η κατανομή του υπόλοιπου χρόνου ζωής της συνιστώσας δεν εξαρτάται από το πόσο μεγάλο ήταν το χρονικό διάστημα της μέχρι τώρα λειτουργίας της συνιστώσας. Συνεπώς η συνιστώσα δεν παλαιώνει (είναι πάντα σαν καινούργια ή ξεχνάει το διάστημα που έχει ήδη λειτουργήσει) και πιθανή βλάβη λειτουργίας είναι αποτέλεσμα κάποιας ξαφνικής εμφάνισης μιας αστοχίας, και όχι βαθμιαίας αλλοίωσης.

3.5 Τεχνικές μοντελοποίησης αξιοπιστίας και διαθεσιμότητας: Μοντέλα Markov

Ένα αποτελεσματικό εργαλείο για την μοντελοποίηση συστημάτων που συνθέτονται από διαφορετικές διαδικασίες, όπως διαδικασίες αστοχίας και επισκευής, είναι τα μοντέλα Markov. Τα μοντέλα Markov αποτελούν βασικά εργαλεία για την μοντελοποίηση αξιοπιστίας και διαθεσιμότητας.

Μια διαδικασία Markov (Markov process) είναι μια στοχαστική διαδικασία που η δυναμική συμπεριφορά της είναι τέτοια ώστε οι κατανομές πιθανοτήτων για την μελλοντική ανάπτυξη της εξαρτάται μόνο από την παρούσα κατάσταση και όχι από το πώς η διαδικασία έφτασε σε αυτή την κατάσταση. Αν υποθέσουμε ότι ο χώρος καταστάσεων I είναι διακριτός (πεπερασμένος ή άπειρα μετρήσιμος) τότε η Markov διαδικασία είναι γνωστή ως αλυσίδα Markov [T02]. Αν επιπλέον θεωρήσουμε ότι ο χώρος παραμέτρου T είναι επίσης διακριτός, τότε έχουμε αλυσίδα Markov διακριτού χρόνου (*discrete-time Markov Chain-DTMC*) ενώ αν ο χώρος της παραμέτρου T είναι συνεχής $T = [0, \infty)$ τότε έχουμε αλυσίδα Markov συνεχούς χρόνου (*continuous-time Markov Chain-CTMC*) [T02].

Δυο είναι οι κεντρικές έννοιες στα μοντέλα Markov: η έννοια της κατάστασης και η έννοια της μετάβασης κατάστασης. Η κατάσταση σε μια αλυσίδα Markov περιγράφει πλήρως οτιδήποτε πρέπει να γνωρίζουμε κάθε χρονική στιγμή για τις συνιστώσες και τα υπό-συστήματα που αποτελούν το σύστημα. Στα μοντέλα αξιοπιστίας κάθε κατάσταση περιγράφει ένα ξεχωριστό συνδυασμό λειτουργικών και μη-λειτουργικών μονάδων. Αν κάθε μονάδα μπορεί να βρίσκεται σε μια από τις συνθήκες - λειτουργική, μη λειτουργική τότε ολόκληρο το μοντέλο για ένα σύστημα n μονάδων έχει 2^n καταστάσεις. Με το πέρασμα του χρόνου το σύστημα μεταβαίνει από κατάσταση σε κατάσταση καθώς οι μονάδες αστοχούν και επισκευάζονται. Οι αλλαγές καταστάσεων ονομάζονται μεταβάσεις.

3.5.1 Αλυσίδες Markov συνεχούς χρόνου

Στις αλυσίδες Markov συνεχούς χρόνου $\{X(t) | t > 0\}$, στις οποίες επικεντρώνεται η παρούσα μελέτη, οι μεταβάσεις από μια δεδομένη κατάσταση σε μια άλλη μπορεί να συμβούν σε οποιαδήποτε χρονική στιγμή και επίσης περιορίζουμε την προσοχή μας σε διαδικασίες διακριτών καταστάσεων. Αυτό συνεπάγεται ότι αν και η παράμετρος t έχει συνεχές πεδίο τιμών, το σύνολο των τιμών $X(t)$ είναι διακριτό. Ας θεωρήσουμε $I = \{0,1,2,\dots\}$ ότι είναι ο χώρος καταστάσεων της διαδικασίας, και $T = [0, \infty)$ ο χώρος παραμέτρων.

Μια στοχαστική διαδικασία, διακριτών καταστάσεων συνεχούς χρόνου $\{X(t) | t > 0\}$ ονομάζεται αλυσίδα Markov αν για $t_0 < t_1 < t_2 < \dots < t_n < t$ με t και $t_r \geq 0$ ($r = 0,1,\dots,n$) η συνάρτηση δεσμευμένης πιθανότητας ικανοποιεί την σχέση:

$$\begin{aligned} P(X(t) = x | X(t_n) = x_n, X(t_{n-1}) = x_{n-1}, \dots, X(t_0) = x_0) \\ = P(X(t) = x | X(t_n) = x_n) \end{aligned}$$

Η συμπεριφορά της διαδικασίας χαρακτηρίζεται:

(1) από το διάνυσμα πιθανοτήτων αρχικής κατάστασης που δίνονται από την συνάρτηση πιθανότητας της $X(t_0)$

$$P(X(t_0) = k), k = 0,1,2,\dots$$

Τύπος 1

(2) από τις πιθανότητες μετάβασης

$$p_{ij}(u, t) = P(X(t) = j | X(u) = i)$$

Τύπος 2

Η αλυσίδα Markov $\{X(t) | t > 0\}$ ονομάζεται χρονικά ομοιογενής αν $p_{ij}(u, t)$

εξαρτάται μόνο από την χρονική διαφορά $(t - u)$.

Για μια αλυσίδα Markov συνεχούς χρόνου μπορούμε να ορίσουμε τον infinitesimal generator matrix [T02] που δίνεται ως $Q = [q_{ij}]$ όπου q_{ij} , $i \neq j$ αναπαριστά τους ρυθμούς μετάβασης από την κατάσταση i στην κατάσταση j , και τα διαγώνια στοιχεία του πίνακα είναι $q_{ii} = -q_i = -\sum_{j \neq i} q_{ij}$.

Στη συνέχεια δίνονται μια σειρά από συστήματα διαφορικών εξισώσεων που μπορούν να χρησιμοποιηθούν για την ανάλυση της συμπεριφοράς μιας αλυσίδας Markov [MFT00]. Αναλυτικά οι αποδείξεις και τα βήματα για την παραγωγή αυτών των εξισώσεων υπάρχουν στο [T02].

Στιγμιαία προσωρινή ανάλυση (Instantaneous Transient Analysis)

Έστω η πιθανότητα κατάστασης το χρόνο t ότι δίνεται $\pi_j = P(X(t) = j)$ και αναπαριστά την μη-δεσμευμένη πιθανότητα η αλυσίδα Markov συνεχούς χρόνου να βρίσκεται στην κατάσταση i το χρόνο t . Το διάνυσμα $\pi(t) = [\pi_1(t), \pi_2(t), \dots, \pi_n(t)]$ αναπαριστά το διάνυσμα πιθανοτήτων προσωρινής κατάστασης (transient state probability vector). Η συμπεριφορά της αλυσίδας περιγράφεται από την ακόλουθη Kolmogorov εξίσωση:

$$\frac{d\pi(t)}{dt} = \pi(t) \cdot Q$$

Τύπος 3

δοσμένου του διανύσματος αρχικών πιθανοτήτων $\pi(0) = [\pi_0(0), \pi_1(0), \dots]$ το χρόνο $t = 0$.

Αθροιστική μεταβατική ανάλυση (Cumulative Transient Analysis)

Ορίζοντας $L_j(t) = \int_0^t \pi_j(x) dx$, μπορεί να αποδειχτεί ότι το $L_j(t)$ είναι ο αναμενόμενος αθροιστικός χρόνος που καταναλώνεται από την CTMC στην

κατάσταση j στο χρονικό διάστημα $(0,t]$. Αν θεωρήσουμε το διάνυσμα $L(t) = [L_j(t)]$ τότε με ολοκλήρωση της σχέσης που περιγράφει ο Τύπος 3 προκύπτει:

$$\frac{dL(t)}{dt} = L(t) Q + \pi(0)$$

Ανάλυση σταθερής κατάστασης (Steady-state analysis)

Έστω π_i η πιθανότητα σταθερής κατάστασης για την κατάσταση i μια αλυσίδας Markov συνεχούς χρόνου, και έστω $\pi = [\pi_0, \pi_1, \dots]$ το διάνυσμα των πιθανοτήτων σταθερής κατάστασης. Γνωρίζουμε ότι στην σταθερή κατάσταση ισχύει [T02]:

$$\lim_{t \rightarrow \infty} \frac{d\pi_j(t)}{dt} = 0$$

Τύπος 4

Αντικαθιστώντας στο Τύπος 4 προκύπτει το ακόλουθο σύστημα γραμμικών ομοιογενών εξισώσεων (μια για κάθε κατάσταση j):

$$0 = \sum_{i \neq j} \pi_i q_{ij} - \pi_j q_j \quad \text{ή σε μορφή πινάκων } \pi Q = 0. \text{ Επιπλέον ισχύει } \sum_j \pi_j = 1$$

Θα ολοκληρώσουμε την ενότητα δίνοντας μια ταξινόμηση των καταστάσεων για αλυσίδες Markov συνεχούς χρόνου καθώς ένα παράδειγμα αλυσίδας Markov συνεχούς χρόνου.

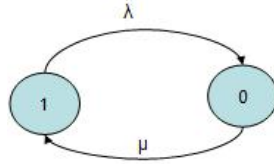
Για την μελέτη της συμπεριφοράς μια αλυσίδας Markov, οι καταστάσεις κατηγοριοποιούνται ανάλογα με τον αν το σύστημα τις επισκέπτεται άπειρα συχνά ή πεπερασμένο πλήθος φορές. Η κατηγοριοποίηση διαφέρει σε κάποιο βαθμό για αλυσίδες Markov συνεχούς και διακριτού χρόνου [T02]. Παρακάτω δίνουμε κατηγορίες καταστάσεων που ενδιαφέρουν την παρούσα μελέτη.

- Μια κατάσταση i ονομάζεται *μεταβατική* (transient) αν και μόνο αν υπάρχει θετική πιθανότητα ότι η διαδικασία δεν επιστρέφει σε αυτή την

κατάσταση

- Μια κατάσταση i ονομάζεται *απορροφητική* (absorbing state) εάν ισχύει $q_{ij} = 0$ για όλα $j \neq i$, έτσι ώστε η αλυσίδα μόλις εισέρχεται σε αυτή την κατάσταση προορίζεται να παραμείνει σε αυτή καθώς δεν προβλέπονται μεταβάσεις.
- Μια κατάσταση j λέγεται ότι είναι *επιτεύξιμη* (reachable) από μια κατάσταση i αν $t > 0$ και ισχύει $p_{ij}(t) > 0$. Μια αλυσίδα Markov συνεχούς χρόνου ονομάζεται *ανάγωγη* (irreducible) αν κάθε κατάσταση της είναι επιτεύξιμη από οποιαδήποτε άλλη

Παράδειγμα 3-2: Ας θεωρήσουμε μια απλή αλυσίδα Markov συνεχούς χρόνου δυο καταστάσεων ενός συστήματος. Το σύστημα βρίσκεται στην κατάσταση 1 όταν είναι λειτουργικό ενώ μεταβαίνει στην κατάσταση 0 όταν αστοχήσει με ρυθμό λ , από την κατάσταση 0 επανέρχεται με επισκευή στην κατάσταση 1 με ρυθμό επισκευής μ . Το μοντέλο που περιγράψαμε φαίνεται στην Εικόνα 6.



Εικόνα 6

Ας υποθέσουμε ότι $\pi_1(t), \pi_0(t)$ είναι οι πιθανότητες το μοντέλο να βρίσκεται στην λειτουργική κατάσταση και κατάσταση επισκευής αντίστοιχα. Ο πίνακας μεταβάσεων δίνεται ως:

$$Q = \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix}$$

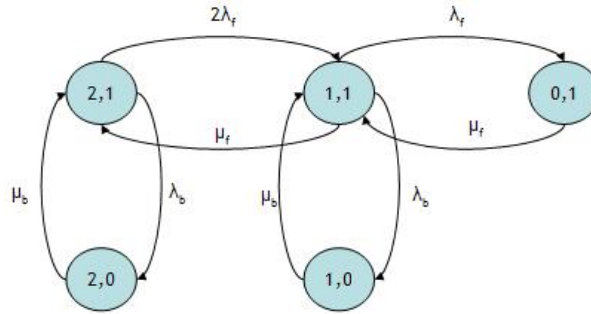
Συνεπώς οι διαφορικές εξισώσεις που περιγράφουν τις πιθανότητες $\pi_1(t), \pi_0(t)$ (οι εξισώσεις Charman-Kolmogorov) είναι:

$$\begin{aligned} \frac{d\pi_1(t)}{dt} &= -\lambda\pi_1(t) + \mu\pi_0(t) \\ \frac{d\pi_0(t)}{dt} &= -\mu\pi_0(t) + \lambda\pi_1(t) \end{aligned}$$

Τύπος 5

Για την λύση των διαφορικών εξισώσεων μπορεί να χρησιμοποιηθούν μετασχηματισμοί Laplace. Μια σύντομη εισαγωγή παρουσιάζεται στην ενότητα 3.6.

Παράδειγμα 3-3: Ας θεωρήσουμε το παράδειγμα 3-1, το δικτυωμένο σύστημα που αποτελείται από δυο τοπικά LAN τμήματα που συνδέονται μεταξύ τους με μια γέφυρα (το παρουσιάσαμε στην ενότητα 3.3.1). Η συμπεριφορά του συστήματος μαζί με τις εξαρτήσεις που ισχύουν ότι αφορά τις αστοχίες και την επισκευή μπορούν να αναπαρασταθούν από μια αλυσίδα Markov συνεχούς χρόνου όπως φαίνεται στην Εικόνα 7.



Εικόνα 7: Παράδειγμα αλυσίδας Markov συνεχούς χρόνου

Οι καταστάσεις της αλυσίδας (i, j) ερμηνεύονται ως εξής: i αναπαριστά το πλήθος των εξυπηρετητών διαχείρισης αρχείων που είναι λειτουργικοί και j είναι 0 ή 1 ανάλογα με αν η γέφυρα είναι λειτουργική ή έχει αστοχήσει. Οι ρυθμοί αστοχίας και επισκευής για όλες τις συνιστώσες που μοντελοποιούνται είναι ανεξάρτητες από το χρόνο και ερμηνεύονται στο πίνακα παρακάτω.

Ρυθμοί		
Αστοχίας	Επισκευής	Σημασία
λ_f	μ_f	Σταθεροί ρυθμοί για τους εξυπηρετητές διαχείρισης αρχείων
λ_b	μ_b	Σταθεροί ρυθμοί για την γέφυρα

Πίνακας 2

Όπως παρατηρούμε το σύστημα είναι λειτουργικό στις καταστάσεις (2,1) και (1,1) συνεπώς για να υπολογίσουμε την διαθεσιμότητα σταθερής κατάστασης του συστήματος αρκεί να προσθέσουμε τις πιθανότητες σταθερής κατάστασης αυτών των δυο καταστάσεων: $A_{ss} = \pi_{(2,1)} + \pi_{(1,1)}$. Οι πιθανότητες σταθερής κατάστασης $\pi_{(2,1)}, \pi_{(1,1)}$ υπολογίζονται επιλύοντας το ομοιογενές γραμμικό σύστημα που παρουσιάσαμε στην αρχή αυτής της ενότητας.

3.6 Μετασχηματισμοί Laplace

Το σύνολο των εξισώσεων που χρησιμοποιήθηκαν στο παράδειγμα 3-2 μπορούν να επιλυθούν με την χρήση μετασχηματισμών Laplace της συνάρτησης χρονικού πεδίου ορισμού που δίνεται από:

$$L\{f(t)\} = f^x(s) = \int_0^{\infty} f(t)e^{-st} dt$$

Οι μετασχηματισμοί Laplace ανάγουν κοινές, γραμμικές διαφορικές εξισώσεις με σταθερούς συντελεστές σε αλγεβρικές εκφράσεις στο s . Οι αλγεβρικές εκφράσεις επιλύονται και μετασχηματίζονται πίσω στο χρονικό πεδίο ορισμού. Στο [T02] υπάρχουν οι πιο συνηθισμένοι μετασχηματισμοί Laplace.

Λαμβάνοντας τους μετασχηματισμούς για τις εξισώσεις του παραδείγματος 3-2 (Τύπος 5) προκύπτει:

$$\begin{aligned} sp_0^x - p_0(0) &= -\lambda p_0^x(s) + \mu p_1^x(s) \\ sp_1^x - p_1(0) &= \lambda p_0^x(s) - \mu p_1^x(s) \end{aligned}$$

Τύπος 6

όπου $p_0(0)$ είναι τιμή του $p_0(t)$ για $t = 0$. Οι αλγεβρικές εκφράσεις του Τύπος 6 επιλύονται με την βοήθεια οποιασδήποτε τεχνικής επίλυσης γραμμικών εξισώσεων όπως κανόνας Kramer ή Gaussian απαλοιφή. Ωστόσο σε πρακτικά προβλήματα οι αλυσίδες Markov που προκύπτουν είναι αρκετά μεγάλες ώστε η χρήση των μετασχηματισμών Laplace να γίνεται δύσκολη ακόμα και αδύνατη. Όπως θα δούμε στην Ενότητα 4.4.2 υπάρχει τρόπος υπολογισμού του μέσου χρόνου αστοχίας $MTTF$ ενός συστήματος που περιγράφεται με ένα μοντέλο Markov συνεχούς χρόνου με την βοήθεια επίλυσης ενός γραμμικού συστήματος εξισώσεων.

3.7 SHARPE: Υποστηρικτικό λογισμικό των τεχνικών μοντελοποίησης

3.7.1 Εισαγωγή

Μια σειρά από πακέτα λογισμικού έχουν αναπτυχθεί για την απλοποίηση της ανάλυσης πολύπλοκων συστημάτων. Αυτά τα πακέτα υποστηρίζουν τις κυριότερες τεχνικές μοντελοποίησης: συνδυαστικά και Markov. Σε αυτή την ενότητα θα κάνουμε μια σύντομη εισαγωγή των δυνατοτήτων του λογισμικού SHARPE που χρησιμοποιήθηκε στην ανάλυση της αξιοπιστίας διατάξεων συστημάτων για ψηφιακή διατήρηση.

Στην διάρκεια σχεδίασης ενός υπολογιστικού συστήματος ακόμα και μέτριας πολυπλοκότητας είναι δύσκολα να γίνουν προβλέψεις σχετικά με τα χαρακτηριστικά αξιοπιστίας και απόδοσης που πρόκειται να έχει το σύστημα. Συνήθως η κατασκευή του συστήματος και η λήψη μετρήσεων αποτελεί πολυδάπανη λύση. Αλλά ακόμα και αν κάτι τέτοιο δεν αποτελεί πρόβλημα, επιχειρηματολογείτε [STP93] ότι μετρήσεις που καθοδηγούνται από ένα μοντέλο συστήματος αποτελούν μια πιο αποτελεσματική μεθοδολογία σχεδίασης. Ιδιαίτερα αν το μοντέλο είναι μια καλή αφαίρεση του συστήματος, δίνει την δυνατότητα στους αναλυτές να εκτελέσουν “trade-off” μελέτες, να απαντήσουμε σε ερωτήσεις του τύπου «τι θα ήταν το αποτέλεσμα αν», να εκτελέσουν αναλύσεις ευαισθησίας και να συγκρίνουν εναλλακτικές σχεδίασης. Συνεπώς ένα εργαλείο που δίνει την δυνατότητα για εύκολο καθορισμό και γρήγορη επίλυση στοχαστικών μοντέλων αποτελεί σημαντική βοήθεια για τον σχεδιαστή του συστήματος.

Ο πιο συνηθισμένος τύπος στοχαστικών μοντέλων που χρησιμοποιούνται στην πράξη είναι η προσομοίωση διακριτών γεγονότων, καθώς καλύπτεται αρκετά λεπτομερώς η συμπεριφορά τους συστήματος σε τέτοια μοντέλα. Ωστόσο οι προσομοιώσεις είναι αρκετά χρονοβόρες και μια πιο χρήσιμη λύση για τους σχεδιαστές συστημάτων αποτελεί η χρήση αναλυτικών μοντέλων αντί για

προσομοιώσεις ή συνδυασμό τους. Οι πρόσφατες επεκτάσεις στην δημιουργία μοντέλων, ιεραρχίες μοντέλων και τεχνικών επίλυσης καθώς και η υλοποίηση τους σε εργαλεία όπως το SHARPE επιτρέπουν την ανάπτυξη και μελέτη μεγάλων και ρεαλιστικών μοντέλων. Στην διάρκεια της μοντελοποίησης μπορεί να χρησιμοποιηθούν μια σειρά από μοντέλα ή συνδυασμοί μοντέλων ιεραρχικά για τα διάφορα φυσικά επίπεδα ή επίπεδα αφαίρεσης του συστήματος. Επίσης μπορεί να χρησιμοποιηθούν διαφορετικά μοντέλα για την επικύρωση αποτελεσμάτων.

3.7.2 Εργαλείο SHARPE

Το πακέτο SHARPE υπάρχει εδώ και 13 χρόνια και είναι ευρέως γνωστό στο πεδίο της αξιοπιστίας και ανάλυσης απόδοσης. Αποτελεί ένα εργαλείο λογισμικού για την ανάλυση στοχαστικών μοντέλων [ST92].

Τα μοντέλα που περιλαμβάνει η SHARPE (Symbolic Hierarchical Automated Reliability and Performance Evaluator) μηχανή είναι [STP93]:

- Συνδυαστικά μοντέλα αξιοπιστίας: διαγράμματα μπλοκ αξιοπιστίας, δέντρα σφαλμάτων, γράφους αξιοπιστίας
- Κατευθυνόμενος, ακυκλικός γράφος προτεραιοτήτων καθηκόντων (Directed Task Precedence Graphs)
- Μοντέλα Markov, semi-Markov, Markov reward
- Product-form queuing networks
- Generalized Stochastic Petri Nets

Το SHARPE δίνει την δυνατότητα υποστήριξης πολλαπλών τύπων μοντέλων, παρέχει ευέλικτους μηχανισμούς για συνδυασμό αποτελεσμάτων έτσι ώστε τα μοντέλα να μπορούν να χρησιμοποιηθούν σε ιεραρχικούς συνδυασμούς. Το SHARPE επιτρέπει στους χρήστες την κατασκευή και ανάλυση μοντέλων για

απόδοση, αξιοπιστία και διαθεσιμότητα. Η πρόσβαση στα μοντέλα είναι άμεση και πλήρης χωρίς υποθέσεις για το πεδίο εφαρμογής.

Λεπτομέρειες για τις δυνατότητες του SHARPE για τους τύπους μοντέλων που υποστηρίζονται υπάρχουν στη βιβλιογραφία [HSZ+00, ST92, T99]. Στη συνέχεια τις ενότητες θα επικεντρωθούμε στις δυνατότητες που παρέχει για τα μοντέλα Markov που ενδιαφέρουν την μελέτη και θα χρησιμοποιηθούν στη συνέχεια. Επίσης θα εισάγουμε την δυνατότητα δημιουργίας ιεραρχικών μοντέλων στο SHARPE.

3.7.3 SHARPE: Αλυσίδες Markov

Το SHARPE επιτρέπει την ανάλυση των ακόλουθων αλυσίδων Markov [ST92]:

1. **Ακυκλική (acyclic)**. Μια αλυσίδα ονομάζεται ακυκλική αν επισκέπτεται κάθε κατάσταση το πολύ μια φορά (ο γράφος της αλυσίδας δεν έχει κύκλους).
2. **Ανάγωγη (irreducible)**. Μια αλυσίδα ονομάζεται ανάγωγη αν από κάθε κατάσταση έχουμε πρόσβαση σε κάθε άλλη κατάσταση. Για ανάγωγες αλυσίδες υπολογίζεται η πιθανότητα σταθερής κατάστασης και είναι ανεξάρτητη από τις αρχικές πιθανότητες.
3. **Phase-type**. Μια αλυσίδα ονομάζεται phase-type όταν δεν είναι ούτε ακυκλική ούτε ανάγωγη. Έχει μια ή περισσότερες απορροφητικές καταστάσεις και μια ή περισσότερες μεταβατικές καταστάσεις. Συνεπώς εγγυάται ότι η διαδικασία τελικά θα φτάσει σε μια από τις απορροφητικές καταστάσεις.

Η δομή της αλυσίδας Markov καθορίζεται στο SHARPE δίνοντας κάθε πιθανή μετάβαση κατάστασης μαζί με τους στιγμιαίους ρυθμούς μετάβασης. Το SHARPE δίνει την δυνατότητα να υπολογιστούν οι ακόλουθες συναρτήσεις και πιθανότητες:

- συνάρτηση κατανομής του χρόνου μέχρι η διαδικασία να φτάσει σε μια συγκεκριμένη απορροφητική κατάσταση (δεν ισχύει για ανάγωγες αλυσίδες).
- συνάρτηση κατανομή του χρόνου μέχρι η διαδικασία να φτάσει στην απορρόφηση ανεξάρτητα από την κατάσταση απορρόφησης στην οποία θα συμβεί (δεν ισχύει για ανάγωγες αλυσίδες).
- μεταβατική συνάρτηση πιθανότητας με παράμετρο t , δοσμένης της πιθανότητας ότι βρίσκεται σε μια συγκεκριμένη κατάσταση το χρόνο t .
- μεταβατική πιθανότητα (όχι συνάρτηση αλλά αριθμητική τιμή) να βρίσκεται σε μια κατάσταση σε συγκεκριμένο χρόνο t .
- Πιθανότητα να επισκεφτεί μια συγκεκριμένη κατάσταση (δεν ισχύει για ανάγωγες αλυσίδες για την οποία ισχύει ότι η πιθανότητα είναι 1 για κάθε κατάσταση).
- Πιθανότητα σταθερής κατάστασης για μια συγκεκριμένη κατάσταση (μόνο για ανάγωγες αλυσίδες)
- συνάρτηση κατανομής του χρόνου μέχρι να συμβεί μια συγκεκριμένη μετάβαση (μόνο για ακυκλικές αλυσίδες)

ΚΕΦΑΛΑΙΟ 4

Αποτίμηση αξιοπιστίας διατάξεων συστημάτων για μακροχρόνια ψηφιακή διατήρηση

4.1 Εισαγωγή

Έχοντας ορίσει το πρόβλημα της ψηφιακής διατήρησης καθώς και μια σειρά από αναλυτικές τεχνικές μοντελοποίησης, επόμενο βήμα στην παρούσα εργασία αποτελεί η ανάπτυξη αναλυτικών μοντέλων για την μελέτη της αξιοπιστίας διατάξεων συστημάτων για τη φύλαξη ψηφιακών δεδομένων. Αρχικός μας στόχος είναι να δώσουμε μέσα από αντιπροσωπευτικά παραδείγματα περιπτώσεων, μια αποτελεσματική προσέγγιση γενικότερα στο πρόβλημα μελέτης διατάξεων συστημάτων για μακροχρόνια φύλαξη ψηφιακών δεδομένων. Συνεπώς τα μοντέλα που αναλύονται σε αυτό το κεφάλαιο επιδέχονται παραπέρα γενικεύσεις, επεκτάσεις, και εισαγωγή επιπλέον παραμέτρων. Ένας δεύτερος εξίσου σημαντικός στόχος της μελέτης είναι να προκύψουν «μείζονες» παράγοντες που παίζουν πολύ σημαντικό ρόλο στην σχεδίαση και υλοποίηση τέτοιων διατάξεων. Για την ανάδειξη αυτών των σημαντικών παραγόντων εκτελούνται μια σειρά από αναλύσεις ευαισθησίας που διαφοροποιούν τις τιμές στις παραμέτρους εισόδου των μοντέλων ενώ καταγράφονται οι μεταβολές που συμβαίνουν αντίστοιχα στα κριτήρια αξιοπιστίας. Τα αποτελέσματα είναι ιδιαίτερα χρήσιμα για την υποστήριξη αποφάσεων όπως πόσα αντίγραφα απαιτούνται για κάθε ψηφιακό έγγραφο για να επιτευχθεί μια συγκεκριμένη απαίτηση αξιοπιστίας, πόσο συχνά απαιτείται να ελέγχονται τα έγγραφα για

πιθανές αλλοιώσεις και σφάλματα, πόσες τοποθεσίες πρέπει να χρησιμοποιούνται για πρόληψη από φυσικές καταστροφές κ.α.

Η μελέτη της συμπεριφοράς των προτεινόμενων παραδειγμάτων που δίνονται επεκτείνεται σε πολύ μεγάλα χρονικά διαστήματα της τάξης των 1000 ετών. Τέτοιοι χρονικοί ορίζοντες εξαιρετικά μεγάλοι παρουσιάζουν ενδιαφέρον για Μουσεία και οργανισμούς που έχουν ως βασικό πολιτικό τους στόχο την διατήρηση του ψηφιακού υλικού τους για τέτοια μεγάλα χρονικά διαστήματα τουλάχιστον.

Ένας τρόπος μοντελοποίησης τέτοιων διατάξεων συστημάτων μπορεί να γίνει με την χρήση προσομοίωσης διακριτών γεγονότων. Η προσομοίωση ουσιαστικά είναι ένα πρόγραμμα που μιμείται την δυναμική συμπεριφορά του συστήματος που μοντελοποιεί και δίνει μια σειρά μετρήσεις της συμπεριφοράς του. Αν και η προσομοίωση μπορεί να καλύψει την συμπεριφορά ενός συστήματος με αρκετή λεπτομέρεια έχει το μειονέκτημα ότι χρειάζεται αρκετό χρόνο για να εκτελεστεί. Αυτό μπορεί να αποτελεί πρόβλημα ιδιαίτερα για μοντέλα που χρειάζεται να αλλάζουν συχνά τις τιμές των παραμέτρων τους. Στη μελέτη του [C03] έχει αναπτυχθεί το εργαλείο προσομοίωσης ArchSim για την αποτίμηση μοντέλων για αρχειακές αποθήκες (AR-Archival Repository). Το ArchSim λαμβάνει ως είσοδο ένα AR μοντέλο, καθώς και το χρόνο προσομοίωσης και δίνει ως αποτέλεσμα το μέσο χρόνο μέχρι την αστοχία του AR και ένα διάστημα αξιοπιστίας (confidence interval) για αυτό το χρόνο. Το ArchSim χρησιμοποιεί μια βιβλιοθήκη με προκαθορισμένες κατανομές αστοχίας που μπορεί να χρησιμοποιηθούν για την περιγραφή των συνιστωσών του AR.

Εναλλακτικά για την μελέτη συμπεριφοράς συστημάτων μπορεί να χρησιμοποιηθούν αναλυτικά μοντέλα. Ένα αναλυτικό μοντέλο αποτελεί μια αφαίρεση του συστήματος που περιγράφεται από ένα σύνολο τύπων και εξισώσεων. Η επίλυση αυτών των εξισώσεων δίνει αποτελέσματα που περιγράφουν την συμπεριφορά του συστήματος. Συχνά για την λύση των

εξιώσεων απαιτείται να εκτελεστεί αριθμητική επίλυση. Για την σχεδίαση αναλυτικών μοντέλων είναι σημαντικό να επιλέγονται καλές αφαιρέσεις του συστήματος που μοντελοποιείται, να δίνεται προσοχή στην παραμετροποίηση του μοντέλου και στην επικύρωση του. Το μεγάλο πλεονέκτημα ωστόσο των αναλυτικών μοντέλων είναι ότι από την στιγμή που δημιουργούνται είναι εύκολο και γρήγορο στην συνέχεια να γίνουν “trade off” μελέτες, να απαντηθούν “what if” ερωτήσεις και να εκτελεστούν αναλύσεις ευαισθησίας που συγκρίνουν εναλλακτικές σχεδίασης [STP93].

Για τις μαθηματικές προβλέψεις της αξιοπιστίας των μοντέλων που θα αναπτυχθούν στην συνέχεια χρησιμοποιείται το εργαλείο SHARPE [HSZ+00, T99, STP93, ST92].

4.2 Υποθέσεις που εισάγονται στην μελέτη

Μια βασική υπόθεση που θα κάνουμε στην παρούσα μελέτη είναι ότι οι αστοχίες των συνιστωσών που εξετάζουμε είναι ολικές. Δηλαδή θα θεωρήσουμε ότι δεν υπάρχει δυνατότητα επισκευής μιας συνιστώσας ή μερικής ανάκτησης της πληροφορίας μετά από ένα γεγονός αστοχίας. Έτσι για παράδειγμα όταν μιλάμε για αστοχία ενός δίσκου θα εννοούμε πάντα την ολική καταστροφή του δίσκου χωρίς δυνατότητα επανάκτησης των περιεχομένων του. Η παραδοχή αυτή γίνεται κυρίως για το λόγο ότι σε συστήματα ψηφιακής διατήρησης μας ενδιαφέρει η ανάκαμψη από γεγονότα μαζικής καταστροφής πληροφορίας. Η μερική καταστροφή πληροφορίας σε υπολογιστικά συστήματα είναι ένα πρόβλημα που έχει αντιμετωπιστεί εδώ και χρόνια με την εφαρμογή στρατηγικών δημιουργίας εφεδρικών μονάδων και δεν εξετάζεται στην παρούσα προσέγγιση.

Μια δεύτερη σημαντική παραδοχή αφορά απώλειες ψηφιακών εγγράφων που προέρχονται από ξεπερασμένους μορφότευπους δεδομένων. Στην παρούσα μελέτη θεωρούμε ότι δεν υπάρχουν απώλειες ψηφιακών δεδομένων λόγω

απαρχαίωσης του μορφότυπου που ακολουθούν τα ψηφιακά έγγραφα.

Η τρίτη παραδοχή αφορά τις περιβαλλοντικές συνθήκες κάτω από τις οποίες λειτουργεί το σύστημα. Μελέτες στην βιβλιογραφία [NML03, SS98, B95, AES28-1997, DPGN03] έχουν δείξει ότι αυξημένες θερμοκρασίες και μεταβολές στην υγρασία μπορεί να οδηγήσουν στην επιτάχυνση του ρυθμού αστοχίας των αποθηκευτικών μέσων. Στην αρχική προσέγγιση θα θεωρήσουμε ότι οι συνθήκες λειτουργίας του συστήματος είναι ιδανικές και δεν αποτελούν επιβαρυντικό παράγοντα στην εμφάνιση πιθανών αστοχιών των αποθηκευτικών μονάδων.

4.3 Βασικές συνιστώσες διατάξεων συστημάτων για ψηφιακή διατήρηση

Οι κύριες συνιστώσες που θα εξετάσουμε στις διατάξεις συστημάτων για μακροχρόνια φύλαξη ψηφιακών δεδομένων είναι:

- Τα αποθηκευτικά μέσα
- Τοποθεσία στην οποία βρίσκεται η διάταξη

Παρακάτω παραθέτουμε τα χαρακτηριστικά που έχουν οι συνιστώσες αυτές και μας ενδιαφέρουν να μοντελοποιήσουμε με σκοπό την εξαγωγή συμπερασμάτων για τον ρόλο και την επιρροή τους στην αξιοπιστία των υπό-μελέτη διατάξεων.

4.3.1 Εξοπλισμός φύλαξης δεδομένων (Data storage equipment)

Η βιομηχανία παραγωγής μαζικών μέσων αποθήκευσης βασίζεται σε τρεις βασικές τεχνολογίες αποθήκευσης δεδομένων [NML03]:

- σκληροί δίσκοι
- μαγνητικές ταινίες
- οπτικοί δίσκοι

Τουλάχιστον στο άμεσα προβλεπόμενο μέλλον θεωρείται απίθανο να υπάρξει

μια ανερχόμενη τεχνολογία που να μπορεί να παίξει σημαντικό ρόλο στην μαζική αποθήκευση δεδομένων.

Ότι αφορά την ακεραιότητα των δεδομένων στα αποθηκευτικά μέσα, η τεχνολογία σήμερα έχει πολύ μεγάλη ακρίβεια και δίνει προϊόντα με εξαιρετική αξιοπιστία. Έτσι με βάση τα στοιχεία του National Media Lab [NML03], σε ένα κανονικό περιβάλλον γραφείου με θερμοκρασίες 18-23°C και σχετική υγρασία 30-55%, οι μαγνητικές ταινίες καταγράφουν απώλειες του σήματος εξόδου περίπου 2db για ένα χρόνο αποθήκευσης περίπου 50 χρόνια. Οι οπτικοί δίσκοι είναι πιο ανθεκτικοί σε υψηλότερες τιμές υγρασίας σε σχέση με τις μαγνητικές ταινίες καθώς περιβάλλονται από ειδικό προστατευτικό κάλυμμα που προστατεύει από την υγρασία. Με σχετική υγρασία μέχρι και 80% μπορεί να μην προκαλέσει επιβλαβή αποτελέσματα αρκεί η περίοδος έκθεσης να είναι μικρότερη από 15 ημέρες. Οι σκληροί δίσκοι υψηλής πυκνότητας υφίσταται μεγαλύτερη απώλεια σήματος και με βάση τα κριτήρια σχεδίασης των βιομηχανιών τα εγγεγραμμένα δεδομένων έχουν απώλειες σήματος περίπου 1db ή μικρότερη ανά 10ετία ή 2db ανά 20ετία όπου 2db απώλεια σχετίζεται συνήθως με 10πλάσια αύξηση του ρυθμός σφάλματος μπιτ (BER-Bit Error Rate) ή λιγότερη και εμπίπτει στις δυνατότητες του συστήματος διόρθωσης λαθών που είναι ενσωματωμένες σε όλες τις συσκευές αποθήκευσης.

Οι σημερινές τάσεις δείχνουν ότι για την μαζική αποθήκευση δεδομένων για σκοπούς αρχειοθέτησης γίνεται χρήση κυρίως από μαγνητικές ταινίες. Το ίδιο ισχύει και για την δημιουργία αντιγράφων ασφαλείας που αποτελεί ένα σημαντικό πεδίο περί αποθήκευσης. Τα μηχανήματα εγγραφής μαγνητικών ταινιών με διαφορετικά επίπεδα απόδοσης και δυνατότητες αποτελούν τα κύρια μέσα για την λειτουργία των αντιγράφων ασφαλείας. Πρόσφατα οι κατασκευαστές οπτικών δίσκων έχουν ξεκινήσει να προάγουν την χρήση εγγραφόμενων DVD για αυτό το σκοπό. Έτσι παρόλο που στο τομέα αποθήκευσης δεδομένων των καταναλωτών οι οπτικοί δίσκοι διαφαίνεται να

εκτοπίσουν τους μαγνητικούς δίσκους τα επόμενα 10 χρόνια, είναι μάλλον απίθανο να συμβεί και το ίδιο για εφαρμογές αποθήκευσης στο τομέα της βιομηχανίας και του εμπορίου.

Ένα άλλο ενδιαφέρον στοιχείο για τα αποθηκευτικά μέσα αποτελεί το γεγονός της σύγκλισης των τιμών που παρατηρείται. Στο τέλος του έτους 2002 το κόστος των μέσων αποθήκευσης και για τις τρεις τεχνολογίες (μαγνητικές ταινίες, εγγραφόμενοι οπτικοί δίσκοι και σκληροί δίσκοι) σύγκλινε μεταξύ \$1.00 και \$2.00 ανά GB [NML03]. Επιπλέον μείωση κατά 50% αναμένεται για τα επόμενο 2-3 χρόνια. Ωστόσο το κόστος αυξάνει όταν τα αποθηκευτικά μέσα είναι ενσωματωμένα σε συστήματα αποθήκευσης. Η αύξηση αυτή κυμαίνεται με ένα συντελεστή 2 έως 5 για κανονικά συστήματα αποθήκευσης.

Για τους σκοπούς αυτής της μελέτης θα θεωρήσουμε ότι τα ψηφιακά δεδομένα που διαχειρίζεται η διάταξη αποθηκεύονται σε απλούς σκληρούς δίσκους. Επιπλέον θα χρησιμοποιήσουμε μαγνητικές ταινίες που παρουσιάζουν μεγαλύτερη αξιοπιστία σε σχέση με τους δίσκους για μακροχρόνια φύλαξη αντιγράφων ασφαλείας. Ένας κοινά αποδεκτός τρόπος για την μέτρηση της αξιοπιστίας των δίσκων και των μαγνητικών ταινιών αποτελεί ο αναμενόμενος χρόνος ζωής του δίσκου ή ο μέσος χρόνος μέχρι την αστοχία του δίσκου (Mean Time to Failure- *MTTF*). Μια συνήθης τιμή του *MTTF* για ένα κοινό δίσκο είναι ο χρόνος εγγύησης που δίνουν οι κατασκευαστές (3 έως 5 χρόνια). Μια απλή προσέγγιση για την μοντελοποίηση του χρόνου ζωής ενός δίσκου είναι η χρήση της εκθετικού μοντέλου [MT93] που συνεπάγεται σταθερούς ρυθμούς αστοχίας.

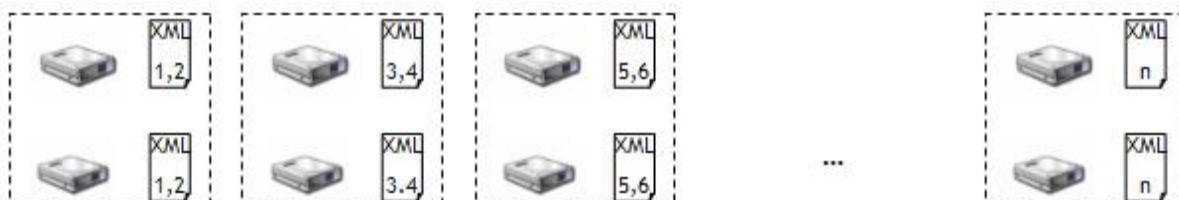
4.3.2 Τοποθεσία μιας διάταξης

Στην σχεδίαση μιας διάταξης για ψηφιακή διατήρηση είναι σημαντικό να απεικονιστούν οι επιρροές που υπάρχουν από τυχόν εξωτερικά γεγονότα που μπορεί να καταστρέψουν την τοποθεσία στην οποία υπάρχει μια διάταξη ή μέρος αυτής. Καταστροφές μεγάλης έκτασης που προκαλούνται από σεισμούς,

ισχυρούς τυφώνες και πλημμύρες μεγάλης έκτασης μπορεί να απαντώνται σπάνια, ωστόσο καταστροφές μπορεί να εκδηλωθούν με πολλούς διαφορετικούς τρόπους όπως για παράδειγμα μια ρήξη σωλήνα νερού ή εκδήλωση πυρκαγιάς σε κτήριο από ανθρώπινο λάθος. Συνεπώς τέτοιου είδους κίνδυνοι καταστροφής ψηφιακής πληροφορίας είναι απαραίτητο να ληφθούν υπόψη στην σχεδίαση διατάξεων συστημάτων για ψηφιακή διατήρηση. Σαν μια πρώτη απλή προσέγγιση θα υποθέσουμε την εκθετική κατανομή ως το μοντέλο που περιγράφει το χρόνο μέχρι την αστοχία μιας τοποθεσίας από ένα φυσικό γεγονός καταστροφής.

4.4 Ένα απλό παράδειγμα διάταξης συστήματος για ψηφιακή διατήρηση

4.4.1 Περιγραφή του μοντέλου



Εικόνα 8: N ζεύγη δίσκων της διάταξης

Ένα απλό παράδειγμα διάταξης συστήματος για ψηφιακή διατήρηση θα μπορούσε να περιγραφεί ως εξής:

Ας θεωρήσουμε ότι έχουμε ένα σύνολο από ψηφιακά έγγραφα. Για απλοποίηση του προβλήματος θα θεωρήσουμε ότι τόσο το περιεχόμενο όσο και το πλήθος των εγγράφων δεν μεταβάλλεται.

Τα αποθηκευτικά μέσα τα οποία χρησιμοποιούμε για την φύλαξη των εγγράφων είναι μια σειρά από απλοί σκληροί δίσκοι με τα ίδια κατασκευαστικά χαρακτηριστικά. Για κάθε ένα από τα ψηφιακά έγγραφα που διαχειρίζεται το σύστημα δημιουργείται ταυτόχρονα και ένα αντίγραφο σε ένα δεύτερο σκληρό

δίσκο. Με αυτό τον τρόπο εξασφαλίζουμε ότι σε περίπτωση αστοχίας ενός δίσκου, είναι δυνατή η αντικατάσταση του και η ανακατασκευή του περιεχομένου από τον δεύτερο δίσκο. Συνεπώς η διάταξη περιλαμβάνει N ζεύγη δίσκων όπως φαίνεται στην Εικόνα 8. Το πλήθος από ζεύγη δίσκων N που απαιτείται καθορίζεται ανάλογα με το πλήθος των ψηφιακών εγγράφων που διαχειρίζεται η διάταξη και τον απαιτούμενο αποθηκευτικό χώρο. Θεωρούμε ότι η διάταξη αστοχεί αν οποιοδήποτε από τα ζεύγη των δίσκων αστοχήσει με αποτέλεσμα την απώλεια ψηφιακών εγγράφων.

Μπορούμε να θεωρήσουμε ότι κάθε ζεύγος δίσκων λειτουργεί ανεξάρτητα από τα υπόλοιπα πράγμα που επιτρέπει την μοντελοποίηση τους με ένα διάγραμμα μπλοκ αξιοπιστίας. Συνεπώς με βάση τις παραπάνω υποθέσεις, μπορούμε να κατασκευάσουμε ένα ιεραρχικό μοντέλο αξιοπιστίας δυο επιπέδων. Η γενική αξιοπιστία της διάταξης που αποτελείται από N ζεύγη δίσκων μοντελοποιείται από ένα διάγραμμα μπλοκ αξιοπιστίας. Κάθε μπλοκ εσωτερικά μοντελοποιείται με την βοήθεια μιας αλυσίδας Markov που θα παρουσιάσουμε αναλυτικά στην συνέχεια της ενότητας. Η παραπάνω ανάλυση υποστηρίζεται από το εργαλείο SHARPE καθώς επιτρέπει την ανάλυση ιεραρχικών μοντέλων. Η επίλυση του μοντέλου της διάταξης στο SHARPE υπάρχει αναλυτικά στην ενότητα 4.4.3.

Αν $R_i(t)$ είναι η αξιοπιστία για κάθε ζεύγος δίσκων τότε η αξιοπιστία της διάταξης δίνεται από το τύπο:

$$R_{config} = \prod_{i=1}^N R_i(t)$$

Αντίστοιχα ο μέσος χρόνος για την αστοχία ενός ζεύγους δίσκων δίνεται από τον τύπο:

$$MTDL_i = \int_0^{\infty} R_i(t) dt$$

Τύπος 7

ενώ ο τύπος που μας δίνει το μέσο χρόνο μέχρι την αστοχία ολόκληρης της διάταξης (Mean Time to Data Loss-MTDL) δίνεται από τον τύπο:

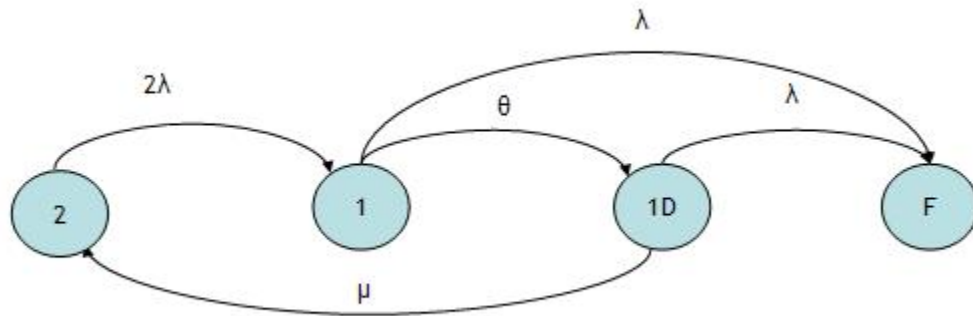
$$MTDL_{config} = \int_0^x R_{config}(t) dt$$

Τύπος 8

Κάθε ζεύγος δίσκων που υπάρχει στην διάταξη μοντελοποιείται με μια αλυσίδα Markov συνεχούς χρόνου, διακριτών καταστάσεων (CTMC). Το διάγραμμα καταστάσεων καθώς και οι ρυθμοί μετάβασης φαίνονται στην Εικόνα 9. Η κατάσταση i αντιστοιχεί στον αριθμό δίσκων που είναι λειτουργικοί. Η αρχική κατάσταση αντιστοιχεί σε $i=2$ καθώς όπως αναφέραμε η διάταξη έχει δυο δίσκους που διατηρούν ταυτόσημα αντίγραφα για κάθε ψηφιακό έγγραφο. Η κατάσταση $\{1D\}$ αντιστοιχεί στην κατάσταση ανίχνευσης ενός σφάλματος. Ουσιαστικά το σύστημα μεταβαίνει στην κατάσταση $\{1\}$ όταν συμβεί κάποιιο σφάλμα σε ένα δίσκο που δεν έχει ανιχνευτεί ακόμα. Η μετάβαση από την κατάσταση $\{1\}$ στην κατάσταση $\{1D\}$ (με ρυθμό θ) υποδηλώνει ότι βρέθηκε το σφάλμα και συνεπώς μπορεί να ξεκινήσει η διαδικασία επισκευής του δίσκου, όπως υποδηλώνεται στην Εικόνα 9 με την μετάβαση από την κατάσταση $\{1D\}$ στην κατάσταση $\{2\}$ με σταθερό ρυθμό επισκευής μ . Η κατάσταση $\{1D\}$ υποδηλώνει την χρονική καθυστέρηση που υπάρχει από την στιγμή που θα συμβεί ένα σφάλμα σε ένα δίσκο μέχρι την στιγμή που ανιχνεύεται. Ωστόσο υπάρχει δυνατότητα στην διάρκεια ανίχνευσης ενός σφάλματος να συμβεί και ένα δεύτερο σφάλμα, δηλαδή να χαθεί και δεύτερος δίσκος. Συνεπώς υπάρχουν μεταβάσεις από τις καταστάσεις $\{1\}$, $\{1D\}$ στην κατάσταση $\{F\}$ που είναι η απορροφητική κατάσταση της αλυσίδας Markov και υποδηλώνει την κατάσταση στην το ζεύγος των δίσκων και κατά επέκταση η διάταξη έχει χάσει πλέον ψηφιακά έγγραφα.

Για το μοντέλο Markov υποθέτουμε ότι έχουμε σταθερό ρυθμό αστοχίας του

δίσκου $\lambda = 1/MTTF_{disk}$ με αναμενόμενο χρόνο ζωής του δίσκου ($MTTF_{disk}$) στα 3 χρόνια που αντιστοιχεί στην εγγύηση που συνήθως δίνουν οι κατασκευαστές. Άλλες ενδεικτικές τιμές για τον αναμενόμενο χρόνο ζωής ενός σκληρού δίσκου είναι τα 5 χρόνια για δίσκους που σταματάνε και ξεκινάνε να περιστρέφονται πολύ συχνά, ενώ 10-20 χρόνια για δίσκους που είναι αδρανείς [C03].



Εικόνα 9. Μοντέλο Markov διάταξης με ένα ζεύγος δίσκων

Για την αντικατάσταση ενός δίσκου που έχει αστοχήσει θα θεωρήσουμε ότι απαιτούνται 50 ώρες σε περίπτωση που η διάταξη έχει άμεσα διαθέσιμους εφεδρικούς δίσκους για τους οποίους υποθέτουμε ότι δεν αστοχούν μέχρι να τεθούν σε λειτουργία (cold spare) ενώ 74 ώρες όταν δεν υπάρχουν εφεδρικοί δίσκοι καθώς υποθέτουμε ότι χρειάζονται επιπλέον 24 ώρες για την παραγγελία και παραλαβή του δίσκου [MT93]. Ο χρόνος αντικατάστασης περιγράφεται με την βοήθεια του εκθετικού μοντέλου με παράμετρο $\mu = 1/MTTR_{disk}$. Επίσης θα θεωρήσουμε ότι ο μέσος χρόνος που απαιτείται για την ανίχνευση μια αστοχίας του δίσκου ($MTTFD_{disk}$) είναι εκθετικά κατανομημένος με παράμετρο $\theta = 1/MTTFD$. Μια αρχική υποθετική τιμή για το $MTTFD_{disk}$ είναι 14 ημέρες. Ενδεικτικά ο έλεγχος ενός δίσκου για τον εντοπισμό απώλειας δεδομένων απαιτεί να εξεταστούν όλα τα ψηφιακά έγγραφα για πιθανές απώλειες. Όπως αναφέρει ο Crespo [C03] με χρήση 3% του ρυθμού μετάδοσης του δίσκου ένας

τέτοιος έλεγχος για μια διάταξη με 200.000 έγγραφα απαιτεί περίπου 60 ημέρες για να ολοκληρωθεί. Για να βρεθούν πιθανές απώλειες σε λιγότερο χρονικό διάστημα όπως για παράδειγμα μέσα σε 7 ημέρες πρέπει το ο ρυθμός μετάδοσης που καταλαμβάνεται να αυξηθεί στο 25%.

Ολόκληρο το σύστημα υπάρχει σε μια συγκεκριμένη γεωγραφική τοποθεσία. Σε αυτή την αρχική προσέγγιση θα αγνοήσουμε σφάλματα που προέρχονται από εξωτερικά γεγονότα που μπορεί να συμβούν σε μια τοποθεσία όπως μεταβολές του περιβάλλοντος (όπως αύξηση θερμοκρασίας, υγρασίας κ.λπ.) αλλά και καταστροφικών γεγονότων όπως πλημμύρα, πυρκαγιά και σεισμός.

Το ζητούμενο είναι να υπολογίσουμε αρχικά την αξιοπιστία της διάταξης που περιγράψαμε παραπάνω. Ουσιαστικά μας ενδιαφέρει να υπολογίσουμε το μέσο χρόνο (*MTTF*) μέχρι την αστοχία της διάταξης που αντιστοιχεί στην απώλεια τουλάχιστον ενός ζεύγους δίσκων.

4.4.2 Υπολογισμός μαθηματικού τύπου για το μέσο χρόνο αστοχίας (MTTF) της αλυσίδας Markov για ένα ζεύγος δίσκων

Ο χώρος καταστάσεων της αλυσίδας Markov που περιγράψαμε στην ενότητα 4.4 είναι $\{0, 1D, 1, 2\}$. Η κατάσταση $\{F\}$ είναι απορροφητική δηλαδή η διαδικασία παραμένει σε αυτή την κατάσταση όταν εισέλθει για πρώτη φορά σε αυτή καθώς δεν προβλέπονται μεταβάσεις. Η αλυσίδα Markov είναι χρονικά ομοιογενής καθώς η πιθανότητα που περιγράφει κάθε μετάβαση κατάστασης $p_{ij}(t, t+h)$ δεν εξαρτάται από τον αρχικό χρόνο t αλλά από το χρόνο που διανύεται h . Αυτό συνεπάγεται ταυτόχρονα ότι οι ρυθμοί μετάβασης $q_{ij}(t)$ και $q_{ii}(t)$ είναι ανεξάρτητοι του t .

Υπάρχουν μια σειρά από τεχνικές που μπορεί να χρησιμοποιηθούν για τον υπολογισμό του μέσου χρόνου αστοχίας *MTTF* της αλυσίδας Markov που περιγράφει το απλό μοντέλο της διάταξης:

- Χρήση μετασχηματισμών Laplace στο σύστημα διαφορικών εξισώσεων που περιγράφουν την αλυσίδα Markov
- Λύση συστήματος γραμμικών εξισώσεων
- Αριθμητικές μέθοδοι επίλυσης. Χρησιμοποιούνται σε μεγάλες αλυσίδες Markov στις οποίες δεν μπορούν να εφαρμοστούν οι δυο πρώτες μέθοδοι λόγω της μεγάλης πολυπλοκότητας.
- Χρήση του λογισμικού SHARPE

Θα εφαρμόσουμε την δεύτερη μέθοδο για την παραγωγή ενός μαθηματικού τύπου του $MTTF$. Ένα σύστημα γραμμικών εξισώσεων θα αναπτυχθεί και θα επεξηγηθεί στην συνέχεια. Τα αποτελέσματα επιβεβαιώνονται με την βοήθεια του SHARPE.

Έστω D το σύνολο όλων των καταστάσεων αστοχίας του συστήματος (όλες οι απορροφητικές καταστάσεις ανήκουν στο σύνολο D). Το σύνολο των καταστάσεων στις οποίες το σύστημα είναι λειτουργικό περιγράφονται από το σύνολο U . Έστω Q ο πίνακας μεταβάσεων όλων των καταστάσεων και \hat{Q} ο υποπίνακας του Q που περιλαμβάνει μόνο καταστάσεις από το σύνολο U . Ομοίως θεωρούμε $\hat{\pi}(0)$ είναι το διάνυσμα του $\pi(0)$ που περιλαμβάνει μόνο τις καταστάσεις του συνόλου U . Αν θεωρήσουμε $\tau_i = \lim_{t \rightarrow \infty} L_i(t)$ ο αναμενόμενος χρόνος κατά τον οποίο παραμένει η αλυσίδα Markov στην κατάσταση i (για $i \in U$), τότε ισχύει η εξίσωση [T02]:

$$\hat{\tau} \cdot \hat{Q} = -\hat{\pi}(0)$$

Τύπος 9

Επειδή το τ_i το έχουμε ορίσει ως ο αναμενόμενος χρόνος κατά τον οποίο παραμένει η αλυσίδα Markov συνεχούς χρόνου στην κατάσταση i (κατάσταση λειτουργίας του συστήματος) μέχρι να συμβεί μια αστοχία προκύπτει ότι ο μέσος

χρόνος αστοχίας του συστήματος δίνεται ως:

$$MTTF = \sum_{i \in U} \tau_i$$

Ο πίνακας μεταβάσεων \hat{Q} για το διάγραμμα καταστάσεων της απλής διάταξης είναι:

$$\hat{Q} = \begin{bmatrix} -2\lambda & 2\lambda & 0 \\ 0 & -(\theta + \lambda) & \theta \\ \mu & 0 & -(\mu + \lambda) \end{bmatrix}$$

Οπότε το σύστημα των γραμμικών εξισώσεων που προκύπτουν με βάση το Τύπος 9 είναι:

$$\begin{aligned} -2\lambda \cdot \tau_2 + \mu \cdot \tau_1 &= -1 \\ 2\lambda \cdot \tau_2 - (\theta + \lambda) \cdot \tau_{1D} &= 0 \\ \theta \cdot \tau_{1D} - (\mu + \lambda) \cdot \tau_1 &= 0 \end{aligned}$$

Ο μέσος χρόνος αστοχίας του συστήματος δίνεται από τον τύπο:

$$MTTF = \tau_2 + \tau_1 + \tau_{1D}$$

Τύπος 10

Από την λύση του γραμμικού συστήματος προκύπτει ότι:

$$\tau_2 = \frac{(\theta + \lambda) \cdot (\mu + \lambda)}{2 \cdot \lambda^2 \cdot (\mu + \lambda + \theta)} \quad [1]$$

$$\tau_1 = \frac{\theta}{\lambda \cdot (\mu + \lambda + \theta)} \quad [2]$$

$$\tau_{1D} = \frac{\mu + \lambda}{\lambda \cdot (\mu + \lambda + \theta)} \quad [3]$$

Συνεπώς ο τύπος που μας δίνει το MTTF για την αλυσίδα Markov είναι:

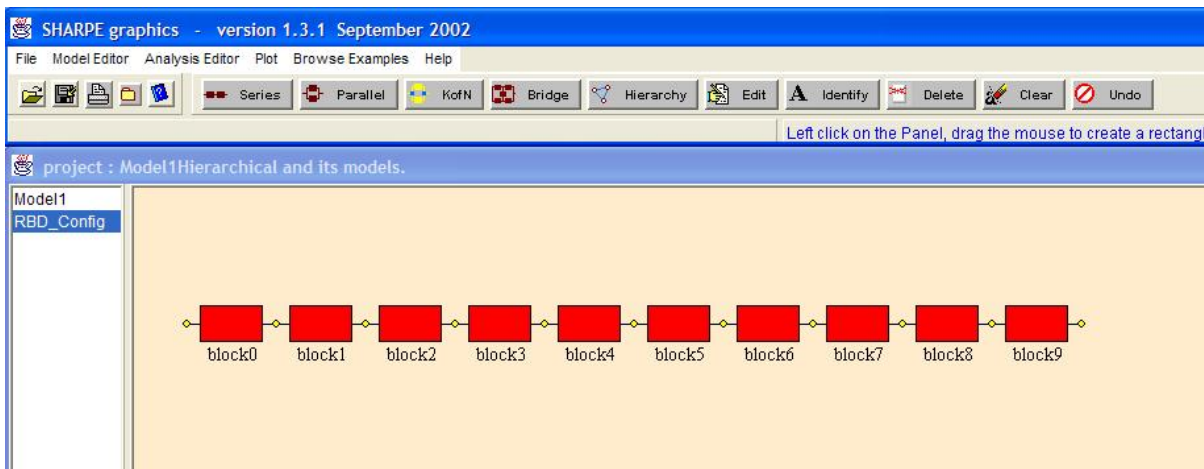
$$MTTF = \frac{(\theta + \lambda) \cdot (\mu + \lambda) + 2 \cdot \lambda \theta + 2 \cdot (\mu + \lambda)}{2\lambda^2 \cdot (\mu + \lambda + \theta)}$$

Τύπος 11

Στη συνέχεια θα χρησιμοποιήσουμε το λογισμικό SHARPE για να δείξουμε ένα ευέλικτο τρόπο ανάλυσης των μοντέλων και παραγωγής αριθμητικών αποτελεσμάτων. Τα αποτελέσματα του μαθηματικού τύπου που υπολογίσαμε σε αυτή την ενότητα ταυτίζονται απόλυτα με τα αποτελέσματα που παράγει το SHARPE για το ίδιο μοντέλο.

4.4.3 Σχεδίαση ιεραρχικού μοντέλου στο SHARPE

Η γραφική δι-επαφή του εργαλείου SHARPE επιτρέπει την σχεδίαση και

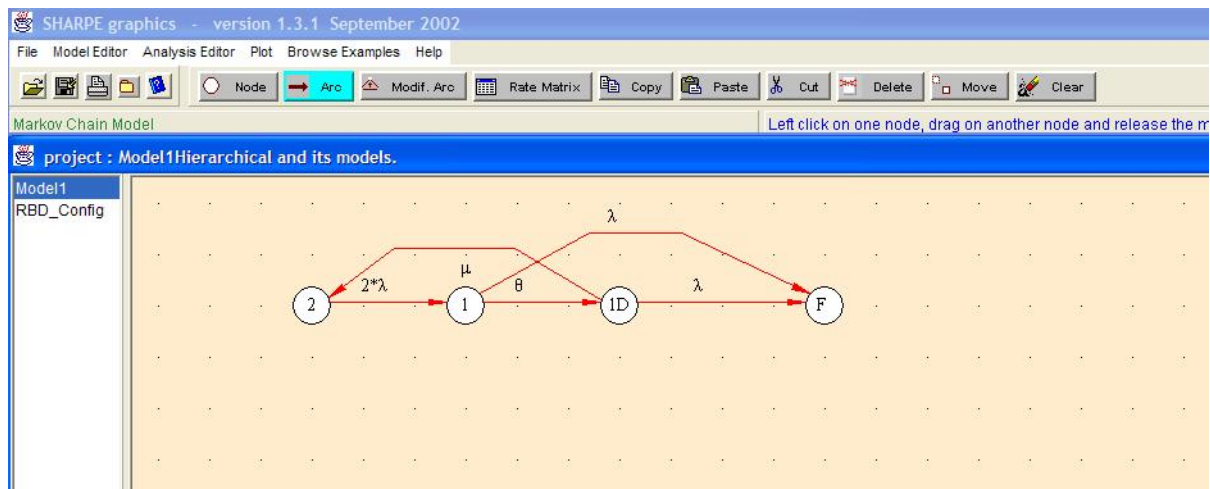


Εικόνα 10: Διάγραμμα μπλοκ αξιοπιστίας για διάταξη με N=10 ζεύγη δίσκων

Κεφάλαιο 4. Αποτίμηση αξιοπιστίας διατάξεων συστημάτων για ψηφ. διατήρηση

ανάλυση ιεραρχικών μοντέλων. Το μοντέλο που μελετάμε όπως αναφέραμε και στην ενότητα 4.4 είναι ιεραρχικό δυο επιπέδων. Όλη η διάταξη περιγράφεται με ένα διάγραμμα μπλοκ αξιοπιστίας με πλήθος μπλοκ όσα και τα ζεύγη των δίσκων της διάταξης (πρώτο επίπεδο του μοντέλου). Κάθε μπλοκ εσωτερικά (δεύτερο επίπεδο του μοντέλου) μπορεί να αναπαρασταθεί με ένα απλό μοντέλο Markov που φαίνεται στην Εικόνα 11.

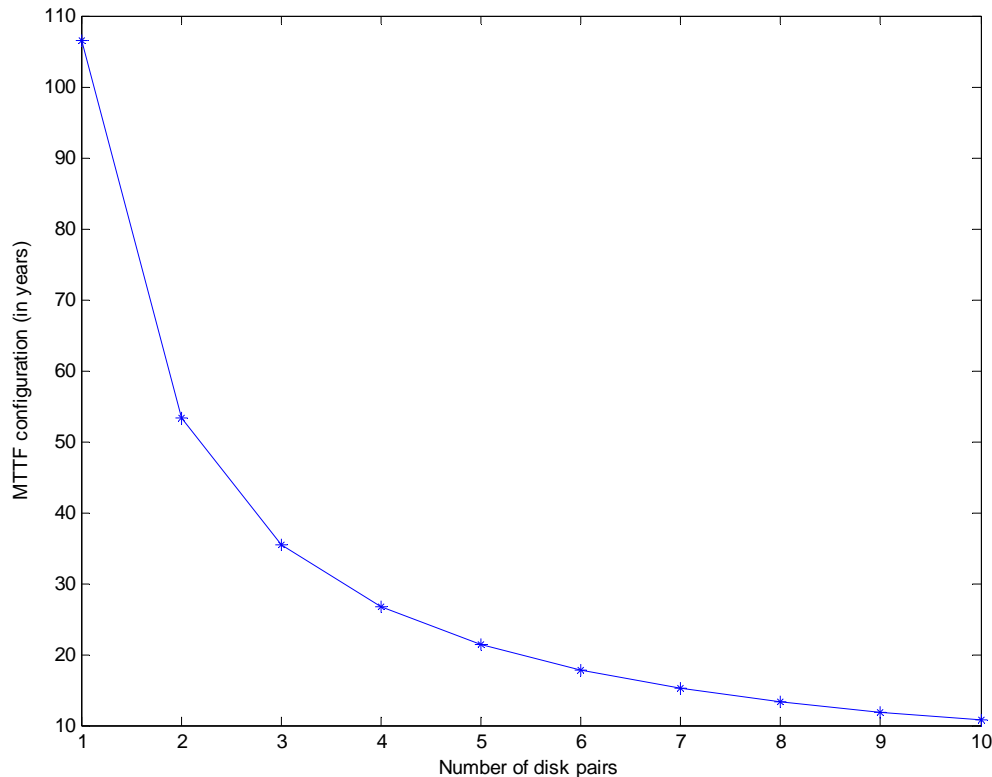
Το διάγραμμα μπλοκ αξιοπιστίας που φαίνεται στην Εικόνα 10 περιγράφει μια διάταξη με $N = 10$ ζεύγη δίσκων. Τα μπλοκ του διαγράμματος είναι συνδεδεμένα σε σειρά καθώς υποθέτουμε ότι σε περίπτωση αστοχίας έστω ενός ζεύγους δίσκων η διάταξη έχει αστοχήσεις καθώς έχει χάσει ψηφιακά έγγραφα.



Εικόνα 11. Σχεδίαση του μοντέλου στο εργαλείο SHARPE

Είναι ενδιαφέρον να μελετήσουμε τις μεταβολές του μέσου χρόνου αστοχίας της διάταξης σε συνάρτηση με το πλήθος των ζευγών των δίσκων που διαχειρίζεται. Για τους υπολογισμούς υποθέσαμε ότι ο ρυθμός αστοχίας του δίσκου είναι $\lambda = 3.80517504 \text{ E} - 005$ που αντιστοιχεί σε 3 χρόνια μέσο χρόνο αστοχίας, ο ρυθμός επισκευής του δίσκου έχει οριστεί $\mu = 0.02$ που αντιστοιχεί σε μέσο χρόνο επισκευής 50 ωρών ενώ ο ρυθμός εύρεσης σφαλμάτων των δίσκων είναι $\theta = 2.976190476 \text{ E} - 003$ που αντιστοιχεί σε μέσο χρόνο εύρεσης σφαλμάτων 14 ημερών. Οι τιμές των παραμέτρων λ, μ, θ που δίνονται έχουν υπολογιστεί με

μέσο χρόνο δοσμένο σε ώρες. Στη γραφικής παράσταση στην Εικόνα 12 απεικονίζονται οι μεταβολές του μέσου χρόνου αστοχίας της διάταξης σε συνάρτηση με το πλήθος από ζεύγη δίσκων. Είναι φανερό ότι αυτό το παράδειγμα διάταξης είναι δύσκολα επεκτάσιμο καθώς αυξάνοντας το πλήθος των δεδομένων και κατά συνέπεια το πλήθος των δίσκων που πρέπει να διαχειρίζεται η διάταξη μειώνεται η αξιοπιστία και ο μέσος χρόνος αστοχίας της διάταξης. Η συγκεκριμένη διάταξη είναι αρκετά αξιόπιστη μόνο για μικρό πλήθος δίσκων.



Εικόνα 12. Γραφική παράσταση του μέσου χρόνου αστοχίας της διάταξης σε συνάρτηση με το πλήθος των δίσκων της διάταξης

4.4.4 Ανάλυση ευαισθησίας

Η ανάλυση ευαισθησίας συνήθως συμβαίνει αφότου ολοκληρωθεί η αποτίμηση

Κεφάλαιο 4. Αποτίμηση αξιοπιστίας διατάξεων συστημάτων για ψηφ. διατήρηση

ενός συστήματος σε επίπεδο αξιοπιστίας. Στόχος σε μια ανάλυση ευαισθησίας είναι να καθορίσει με ποιο τρόπο αλλάζουν τα αποτελέσματα μια ανάλυσης όταν μεταβάλλονται αντίστοιχα μια ή περισσότεροι παράμετροι εισόδου. Για παράδειγμα: τι θα συμβεί στο σύστημα με την βελτίωση της αξιοπιστίας μιας συνιστώσας. Συνήθως η ανάλυση ευαισθησίας συνοδεύεται από μια σειρά από αναλύσεις που μπορούν να τρέξουν δίνοντας διαφορετικές τιμές στις παραμέτρους και εξετάζοντας τις αλλαγές στα κριτήρια ολικής αξιοπιστίας που έχουν ενδιαφέρον [HMT89]. Στη παρούσα ανάλυση ενδιαφέρον παρουσιάζει να εξετάσουμε τις επιρροές των παραμέτρων λ, μ, θ στο μέσο χρόνο αστοχίας του συστήματος καθώς και στην αξιοπιστία της διάταξης. Στο Πίνακας 3 έχει υπολογιστεί ο μέσος χρόνος αστοχίας της διάταξης για ένα εύρος τιμών των παραμέτρων λ, μ, θ και $N=1$ ζεύγος δίσκων. Θεωρούμε ότι η διάταξη έχει καθοριστεί ότι λειτουργεί με τιμές στις παραμέτρους όπως αναφέρθηκαν στην περιγραφή του μοντέλου (Ενότητα 4.4.1). Η αξιοπιστία της διάταξης $R(t)$ υπολογίζεται για χρόνο λειτουργίας $t=100000$ ώρες που αντιστοιχεί περίπου σε 11 χρόνια.

Αποτίμηση	
Η διάταξη με $N = 1$ έχει καθοριστεί ότι λειτουργεί με τις ακόλουθες τιμές παραμέτρων: $MTTF_{disk} = 1/\lambda = 3$ χρόνια $MTTR_{disk} = 1/\mu = 50$ ώρες $MTTFD_{disk} = 1/\theta = 14$ ημέρες	$MTTF_{config} = 106,46$ χρόνια $R(t) = 0.90, t = 100000$ ώρες
Ανάλυση ευαισθησίας - Αξιοπιστία του δίσκου	
$MTTF_{disk} = 1/\lambda = 1$ χρόνια	$R(10000) = 0.419$

Κεφάλαιο 4. Αποτίμηση αξιοπιστίας διατάξεων συστημάτων για ψηφ. διατήρηση

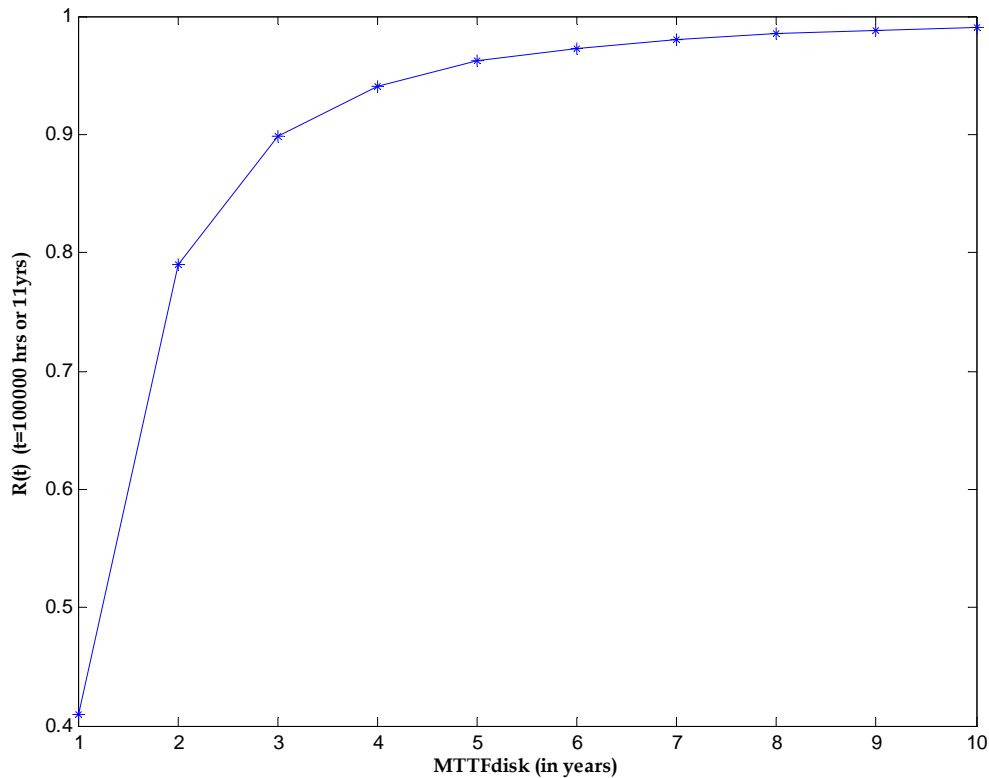
$MTTF_{disk} = 1/\lambda = 2 \text{ χρόνια}$	$R(10000) = 0.795$
$MTTF_{disk} = 1/\lambda = 3 \text{ χρόνια}$	$R(10000) = 0.901$
$MTTF_{disk} = 1/\lambda = 4 \text{ χρόνια}$	$R(10000) = 0.942$
$MTTF_{disk} = 1/\lambda = 5 \text{ χρόνια}$	$R(10000) = 0.962$
$MTTF_{disk} = 1/\lambda = 6 \text{ χρόνια}$	$R(10000) = 0.973$
$MTTF_{disk} = 1/\lambda = 7 \text{ χρόνια}$	$R(10000) = 0.980$
$MTTF_{disk} = 1/\lambda = 8 \text{ χρόνια}$	$R(10000) = 0.985$
$MTTF_{disk} = 1/\lambda = 9 \text{ χρόνια}$	$R(10000) = 0.988$
$MTTF_{disk} = 1/\lambda = 10 \text{ χρόνια}$	$R(10000) = 0.990$
Ανάλυση ευαισθησίας - Χρόνος αντικατάστασης δίσκου	
$MTTR_{disk} = 1/\mu = 8 \text{ ώρες}$	$MTTF_{config} = 119,06 \text{ χρόνια}$
$MTTR_{disk} = 1/\mu = 50 \text{ ώρες}$	$MTTF_{config} = 106,46 \text{ χρόνια}$
$MTTR_{disk} = 1/\mu = 74 \text{ ώρες}$	$MTTF_{config} = 100,42 \text{ χρόνια}$
$MTTR_{disk} = 1/\mu = 120 \text{ ώρες}$	$MTTF_{config} = 90,66 \text{ χρόνια}$
$MTTR_{disk} = 1/\mu = 240 \text{ ώρες}$	$MTTF_{config} = 72,52 \text{ χρόνια}$
$MTTR_{disk} = 1/\mu = 480 \text{ ώρες}$	$MTTF_{config} = 52,45 \text{ χρόνια}$
$MTTR_{disk} = 1/\mu = 8760 \text{ ώρες}$	$MTTF_{config} = 8,78 \text{ χρόνια}$
Ανάλυση ευαισθησίας - Χρόνος εύρεσης σφαλμάτων στους δίσκους	
$MTTFD_{disk} = 1/\theta = 7 \text{ ημέρες}$	$MTTF_{config} = 185,2 \text{ χρόνια}$

Κεφάλαιο 4. Αποτίμηση αξιοπιστίας διατάξεων συστημάτων για ψηφ. διατήρηση

$MTTFD_{disk} = 1/\theta = 14$ ημέρες	$MTTF_{config} = 106,8$ χρόνια
$MTTFD_{disk} = 1/\theta = 30$ ημέρες	$MTTF_{config} = 55,6$ χρόνια
$MTTFD_{disk} = 1/\theta = 60$ ημέρες	$MTTF_{config} = 30,9$ χρόνια
$MTTFD_{disk} = 1/\theta = 120$ ημέρες	$MTTF_{config} = 17,9$ χρόνια
$MTTFD_{disk} = 1/\theta = 360$ ημέρες	$MTTF_{config} = 9,03$ χρόνια
$MTTFD_{disk} = 1/\theta = 480$ ημέρες	$MTTF_{config} = 7,90$ χρόνια
$MTTFD_{disk} = 1/\theta = 720$ ημέρες	$MTTF_{config} = 6,77$ χρόνια

Πίνακας 3: Αποτελέσματα της ανάλυσης ευαισθησίας

Όπως φαίνεται και από την γραφική παράσταση στην Εικόνα 13 η αύξηση της αξιοπιστίας της διάταξης σε συνάρτηση με το μέσο χρόνο ζωής του δίσκου είναι

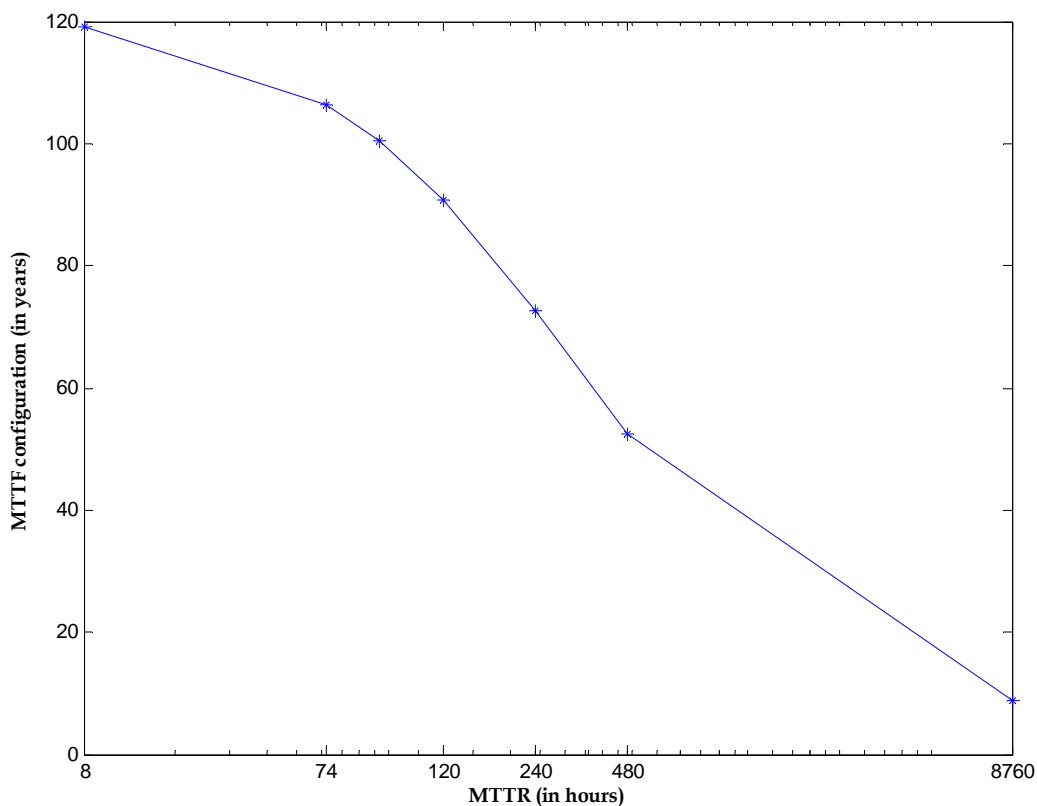


Εικόνα 13: Μεταβολές της αξιοπιστίας της διάταξης για (t=10.000 ώρες) σε σχέση με το $MTTF_{disk}$ του δίσκου

σημαντική καθώς αυξάνεται ο αναμενόμενος χρόνος ζωής του δίσκου από 1 έως 4 χρόνια. Μετά τα 4 χρόνια οι μεταβολές στην αξιοπιστία δεν είναι σημαντικές. Συνεπώς η επένδυση σε πιο αξιόπιστους δίσκους με αναμενόμενο χρόνο ζωής μεγαλύτερο των 4 ετών δεν δίνει σημαντικά μεγαλύτερη αξιοπιστία στην διάταξη.

Μελετώντας την επιρροή που έχει ο μέσος χρόνος μέχρι την επισκευή ενός δίσκου στο $MTTF$ της διάταξης όπως προκύπτει από την ανάλυση ευαισθησίας φαίνεται ότι δεν επηρεάζει σημαντικά όταν η επέμβαση επισκευής γίνεται άμεσα μέσα σε λίγες ώρες (Εικόνα 14). Ο κυριότερος λόγος που δεν έχουμε ιδιαίτερες μεταβολές

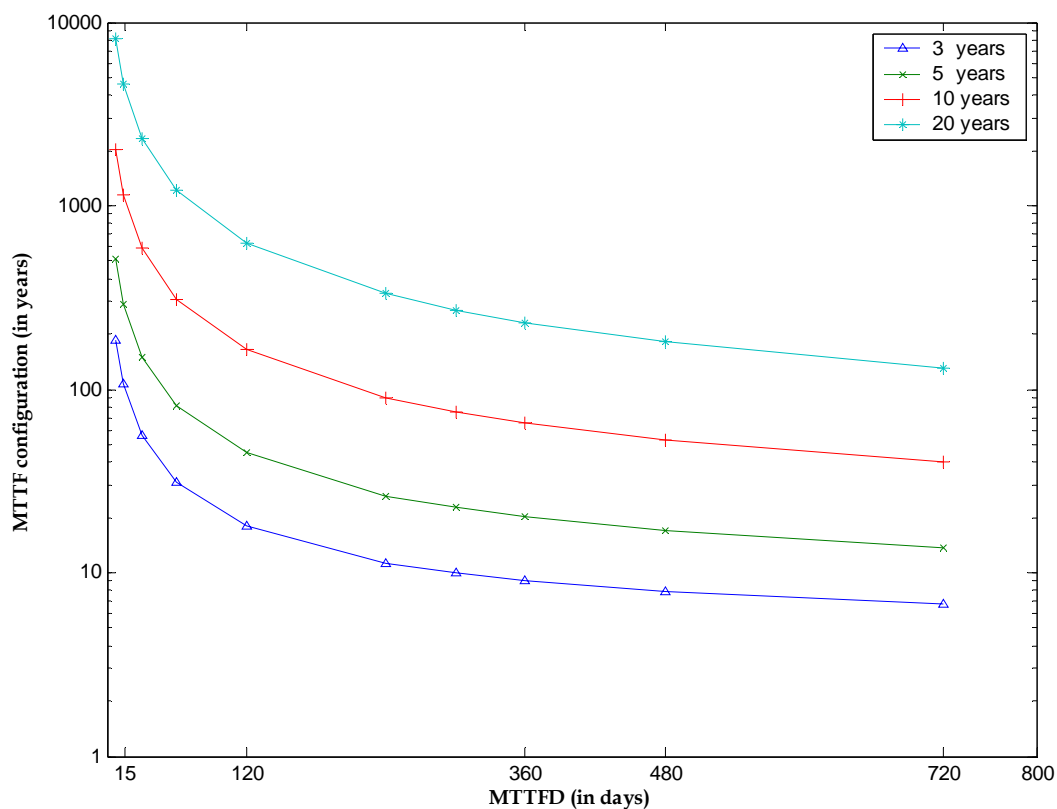
στην αξιοπιστία της διάταξης είναι ότι ο μέσος χρόνος μέχρι την αστοχία του δίσκου είναι αρκετά μεγαλύτερος όταν ο μέσος χρόνος επισκευής του δίσκου είναι μικρός (της τάξεως των 50 ωρών). Η συμπεριφορά της διάταξης ωστόσο μπορεί να χαλάσει σε σημαντικό βαθμό όταν η επισκευή καθυστερείται. Η συμπεριφορά αυτή απεικονίζεται στην γραφική παράσταση με τις απότομες πτώσεις του γραφήματος καθώς μεγαλώνει σημαντικά ο $MTTR$.



Εικόνα 14: Μεταβολές $MTTF$ για $N=1$ συνιστώσες της διάταξης σε συνάρτηση με τις μεταβολές του $MTTR$

Για την αποτίμηση της ευαισθησίας της διάταξης ως προς το χρόνο εύρεσης των σφαλμάτων στους δίσκους ($MTTFD_{disk}$) εξετάσαμε την επιρροή που μπορεί να έχει η συγκεκριμένη παράμετρος σε διαφορετικούς αναμενόμενους μέσους όρους ζωής των δίσκων. Στην Εικόνα 15 υπάρχουν τα αποτελέσματα (η γραφική

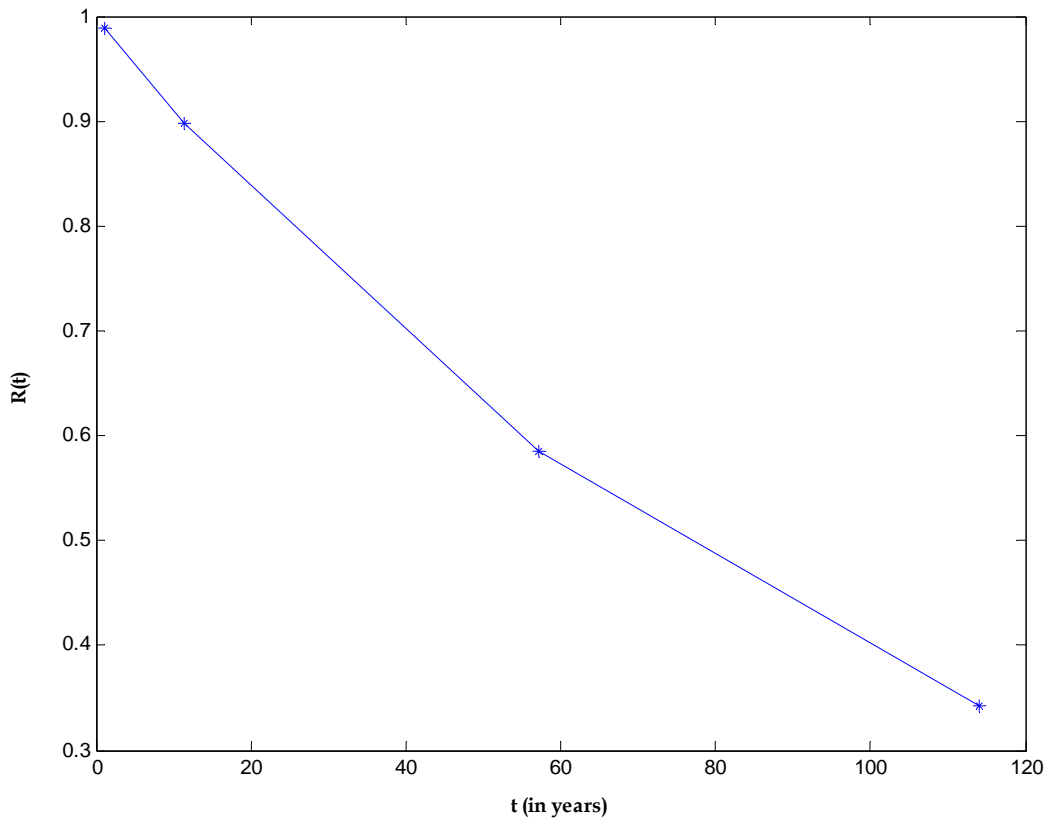
παράσταση είναι σε λογαριθμική κλίμακα). Στην καμπύλη που αντιστοιχεί σε 3 χρόνια $MTTF_{disk}$ του δίσκου είναι φανερό ότι για μικρούς χρόνους εύρεσης σφαλμάτων επηρεάζεται θετικά και σε σημαντικό βαθμό ο $MTTF$ της διάταξης ενώ καθώς αυξάνεται ο $MTTFD_{disk}$ ο $MTTF$ αντίστοιχα της διάταξης πέφτει απότομα. Ουσιαστικά για να μπορεί να έχει θετική επίδραση ο $MTTFD_{disk}$ θα πρέπει να είναι αρκετά μικρότερος από το μέσο χρόνο αστοχίας των δίσκων. Ενδιαφέρον επίσης παρουσιάζει το γεγονός ότι μπορούμε να πετύχουμε σχεδόν το ίδιο μέσο χρόνο αστοχίας της διάταξης χρησιμοποιώντας είτε υψηλά αξιόπιστα αποθηκευτικά μέσα (με μέσο χρόνο αστοχίας 20 χρόνια) και κάνοντας πολύ αραιά ελέγχους για σφάλματα (κάθε 720 ημέρες) είτε με λιγότερο αξιόπιστα μέσα (με μέσο χρόνο αστοχίας στα 3 χρόνια) και πολύ τακτικούς ελέγχους σφαλμάτων (κάθε 14 ημέρες). Συνεπώς από την ανάλυση ευαισθησίας είναι φανερό ότι ο μέσος χρόνος εύρεσης σφαλμάτων είναι «μειζων» παράγοντας για την αξιοπιστία της διάταξης.



Εικόνα 15. Γραφική παράσταση $MTTTF$ της διάταξης συναρτήσει του $MTTFD$ για δίσκους διαφορετικής αξιοπιστίας

4.4.5 Αξιοπιστία της διάταξης

Η συγκεκριμένη διάταξη παρουσιάζει απότομη πτώση της αξιοπιστίας (Εικόνα 16) με το πέρασμα του χρόνου και είναι φανερό ότι δεν μπορεί να ικανοποιήσει τις απαιτήσεις για ψηφιακή διατήρηση οργανισμών που έχουν θέσει τουλάχιστον σαν στόχο την επιβίωση 90% της ψηφιακής πληροφορίας μετά από 1000 χρόνια. Στην επόμενη ενότητα θα επεκτείνουμε το μοντέλο εισάγοντας ένα επιπλέον αντίγραφο ασφαλείας για κάθε ψηφιακό έγγραφο που διαχειρίζεται η διάταξη και θα μελετήσουμε την βελτίωση της συμπεριφορά που εισάγει ο επιπλέον πλεονασμός.



Εικόνα 16. Γραφική παράσταση αξιοπιστίας της διάταξης για μεγάλα χρονικά διαστήματα λειτουργίας

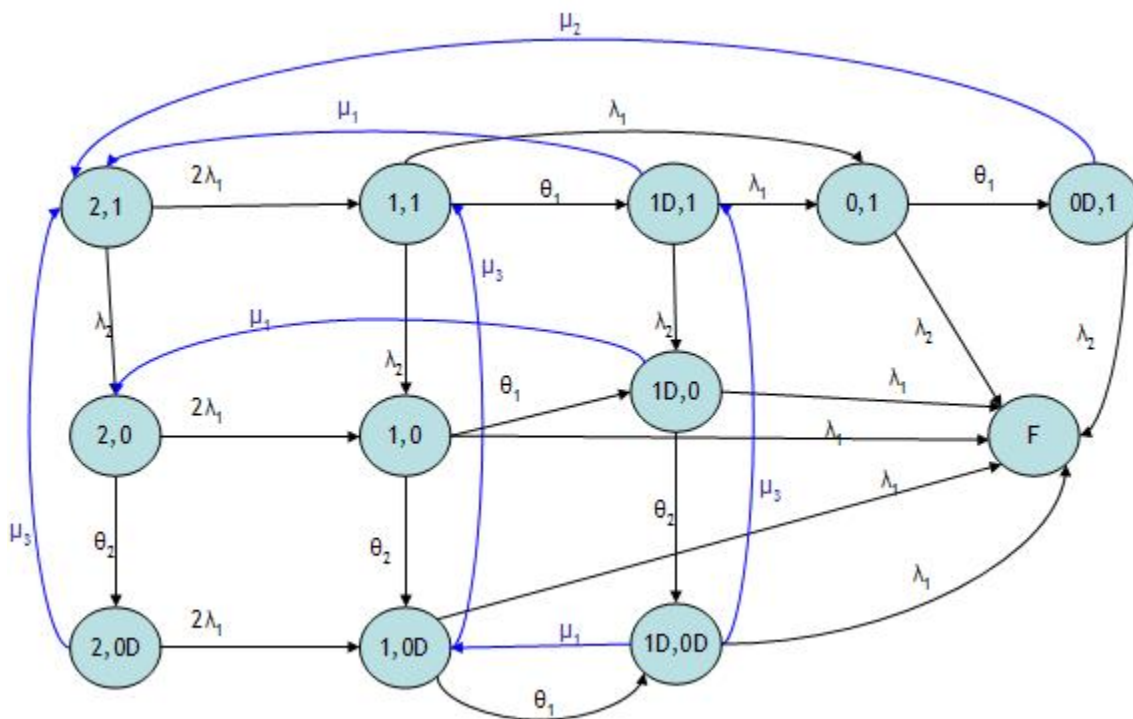
4.5 Επέκταση της διάταξη: Προσθήκη αντιγράφου ασφαλείας

4.5.1 Περιγραφή του μοντέλου

Μια σημαντική επέκταση της αρχικής απλής διάταξης είναι να θεωρήσουμε ότι κάθε ψηφιακό έγγραφο που διαχειρίζεται η διάταξη ότι έχει δυο ταυτόσημα αντίγραφα σε δυο απλούς σκληρούς δίσκους και ένα τρίτο αντίγραφο ασφαλείας σε ένα πιο αξιόπιστο αποθηκευτικό μέσο όπως για παράδειγμα μια μαγνητική ταινία ή CD-ROM. Όλη η παραπάνω διάταξη θα θεωρήσουμε ότι βρίσκεται στην ίδια τοποθεσία χωρίς ωστόσο να μελετάμε ακόμα φυσικά γεγονότα ολικής καταστροφής της διάταξης. Το μοντέλο παρουσιάζει ενδιαφέρον ως προς την

βελτίωση που ενδεχομένως να παρατηρηθεί στο μέσο χρόνο αστοχίας καθώς και στην αξιοπιστία σε σχέση με το απλό μοντέλο που μελετήσαμε στην προηγούμενη ενότητα.

Για την μοντελοποίηση της συμπεριφοράς της παραπάνω διάταξης αναπτύξαμε μια αλυσίδα Markov συνεχούς χρόνου διακριτών καταστάσεων όπως φαίνεται στην Εικόνα 17.



Εικόνα 17. Μοντέλο Markov για διάταξη με δύο σκληρούς δίσκους και μια εφεδρική μονάδα
 Στην αρχική κατάσταση $(2,1)$ θεωρούμε ότι η διάταξη ξεκινάει να λειτουργεί $(t=0)$ έχοντας δημιουργήσει για κάθε ψηφιακό έγγραφο δυο ταυτόσημα αντίγραφα σε δυο ξεχωριστούς σκληρούς δίσκους καθώς και ένα επιπλέον αντίγραφο σε ένα αποθηκευτικό μέσο υψηλότερης αξιοπιστίας (μαγνητική ταινία). Η κατάσταση $\{F\}$ είναι απορροφητική κατάσταση και υποδηλώνει την απώλεια ψηφιακών εγγράφων εξαιτίας ταυτόχρονης αστοχίας των δίσκων και της μαγνητικής ταινίας. Στο Πίνακα 4 περιγράφονται οι παράμετροι που εισάγονται στο μοντέλο.

Κεφάλαιο 4. Αποτίμηση αξιοπιστίας διατάξεων συστημάτων για ψηφ. διατήρηση

Παράμετροι	Περιγραφή
λ_1	Σταθερός ρυθμός αστοχίας δίσκων
λ_2	Σταθερός ρυθμός αστοχίας μαγνητικής ταινίας
μ_1	Σταθερός ρυθμός αντικατάστασης δίσκου που έχει αστοχήσει και ανακατασκευής του περιεχομένου του από τον δεύτερο σκληρό δίσκο
μ_2	Σταθερός ρυθμός αντικατάστασης δίσκου και ανακατασκευής των περιεχομένου του από την μαγνητική ταινία
μ_3	Σταθερός ρυθμός αντικατάσταση μαγνητικής ταινίας και ανακατασκευής περιεχομένων από ένα δίσκο
θ_1	Σταθερός ρυθμός ανίχνευσης αστοχιών των δίσκων
θ_2	Σταθερός ρυθμός ανίχνευσης αστοχιών μαγνητικής ταινίας

Πίνακας 4: Περιγραφή παραμέτρων του μοντέλου

Στο Πίνακας 5 αναλύονται όλες οι καταστάσεις, οι μεταβάσεις καθώς και τα γεγονότα που μπορεί να προκαλέσουν μεταβάσεις από κάθε κατάσταση καθώς και οι αντίστοιχοι ρυθμοί μετάβασης. Για τις επισκευές δίσκων και μαγνητικών ταινιών που έχουν αστοχήσει θα θεωρήσουμε ότι μπορούν να γίνουν ταυτόχρονα εκκινήσεις επισκευών.

Κατάσταση	Γεγονότα	Πιθανές μεταβάσεις
(2,1)	Αστοχία δίσκου	$(2,1) \xrightarrow{2\lambda_1} (1,1)$
	Αστοχία εφεδρικής μονάδας	$(2,1) \xrightarrow{\lambda_2} (2,0)$
(1,1)	Ανίχνευση αστοχίας του δίσκου	$(1,1) \xrightarrow{\theta_1} (1D,1)$
	Αστοχία εφεδρικής μονάδας	$(1,1) \xrightarrow{\lambda_2} (1,0)$
	Αστοχία δεύτερου δίσκου	$(1,1) \xrightarrow{\lambda_1} (0,1)$

Κεφάλαιο 4. Αποτίμηση αξιοπιστίας διατάξεων συστημάτων για ψηφ. διατήρηση

(2,0)	Ανίχνευση αστοχίας της εφεδρικής μονάδας	$(2,0) \xrightarrow{\theta_2} (2,0D)$
	Αστοχία δίσκου	$(2,0) \xrightarrow{2\lambda_1} (1,0)$
(1D,1)	Αστοχία εφεδρικής μονάδας	$(1D,1) \xrightarrow{\lambda_2} (1D,0)$
	Αστοχία δίσκου	$(1D,1) \xrightarrow{\lambda_1} (0,1)$
	Εκκίνηση αντικατάστασης δίσκου	$(1D,1) \xrightarrow{\mu_1} (2,1)$
(1,0)	Αστοχία δίσκου	$(1,0) \xrightarrow{\lambda_1} F$
	Ανίχνευση αστοχίας δίσκου	$(1,0) \xrightarrow{\theta_1} (1D,0)$
	Ανίχνευση αστοχίας εφεδρικής μονάδας	$(1,0) \xrightarrow{\theta_2} (1,0D)$
(0,1)	Αστοχία εφεδρικής μονάδας	$(0,1) \xrightarrow{\lambda_2} F$
	Ανίχνευση αστοχίας δίσκου	$(0,1) \xrightarrow{\theta_1} (0D,1)$
(2,0D)	Εκκίνηση αντικατάστασης δίσκου	$(2,0D) \xrightarrow{\mu_3} (2,1)$
	Αστοχία δίσκου	$(2,0D) \xrightarrow{2\lambda_1} (1,0D)$
(1D,0)	Αστοχία δίσκου	$(1D,0) \xrightarrow{\lambda_1} F$
	Εκκίνηση αντικατάστασης δίσκου	$(1D,0) \xrightarrow{\mu_1} (2,0)$
	Ανίχνευση αστοχίας εφεδρικής μονάδας	$(1D,0) \xrightarrow{\theta_2} (1D,0D)$
(1,0D)	Εκκίνηση αντικατάστασης της εφεδρικής μονάδας	$(1,0D) \xrightarrow{\mu_3} (1,1)$
	Αστοχία δίσκου	$(1,0D) \xrightarrow{\lambda_1} F$
	Ανίχνευση αστοχίας δίσκου	$(1,0D) \xrightarrow{\theta_1} (1D,0D)$
(0D,1)	Αστοχία εφεδρικής μονάδας	$(0D,1) \xrightarrow{\lambda_2} F$

	Εκκίνησης αντικατάστασης των δίσκων που έχουν αστοχήσει από την εφεδρική μονάδα. Η επισκευή των δυο δίσκων μπορεί να ξεκινήσει παράλληλα.	$(0D,1) \xrightarrow{\mu_2} (2,1)$
(1D,0D)	Αστοχία δίσκου	$(1D,0D) \xrightarrow{\lambda_1} F$
	Εκκίνηση αντικατάστασης δίσκου	$(1D,0D) \xrightarrow{\mu_1} (1,0D)$
	Εκκίνηση αντικατάστασης εφεδρικής μονάδας	$(1D,0D) \xrightarrow{\mu_3} (1D,1)$

Πίνακας 5: Οι πιθανές μεταβάσεις μεταξύ των καταστάσεων του μοντέλου

4.5.2 Σχεδίαση ιεραρχικού μοντέλου στο SHARPE

Η σχεδίαση του μοντέλου έγινε με την βοήθεια του SHARPE. Το πρώτο επίπεδο του ιεραρχικού μοντέλου αποτελείται από ένα διάγραμμα μπλοκ αξιοπιστίας με N συνιστώσες (ζεύγη δίσκων και αντίστοιχης μαγνητικής ταινίας) συνδεδεμένες σε σειρά. Κάθε μπλοκ εσωτερικά υλοποιείται από το μοντέλο Markov που περιγράψαμε στην προηγούμενη ενότητα (Εικόνα 17). Για τα αριθμητικά αποτελέσματα θεωρήσαμε ότι ισχύουν οι ίδιες τιμές στις παραμέτρους όπως και με το απλό μοντέλο της ενότητας 4.4. Οι τιμές των παραμέτρων για την ανάλυση του μοντέλου υπάρχουν στο Πίνακα 6. Ορίσαμε το μέσο χρόνο για την επισκευή ενός δίσκου από μια μαγνητική ταινία ότι είναι περίπου ο διπλάσιος (100 ώρες) από το χρόνο που απαιτείται για την επισκευή ενός δίσκου από το δεύτερο δίσκο της διάταξης. Επίσης θεωρούμε ότι ο μέσος χρόνος που απαιτείται για την εύρεση σφαλμάτων σε μαγνητικές ταινίες είναι πολύ μεγαλύτερος καθώς πρόκειται για χρονοβόρα διαδικασία ιδιαίτερα όταν οι μονάδες φυλάσσονται σε ειδικούς αρχειακούς χώρους και δεν είναι εύκολη και άμεση η πρόσβαση τους. Συνεπώς μια τέτοια διαδικασία είναι εξαιρετικά δαπανηρή σε επίπεδο κόστους όταν προγραμματίζεται σε πολύ τακτά χρονικά διαστήματα. Θεωρήσαμε ότι κάθε δυο μήνες (60 μέρες) μπορεί να προγραμματίζεται ένας τέτοιος έλεγχος [C03].

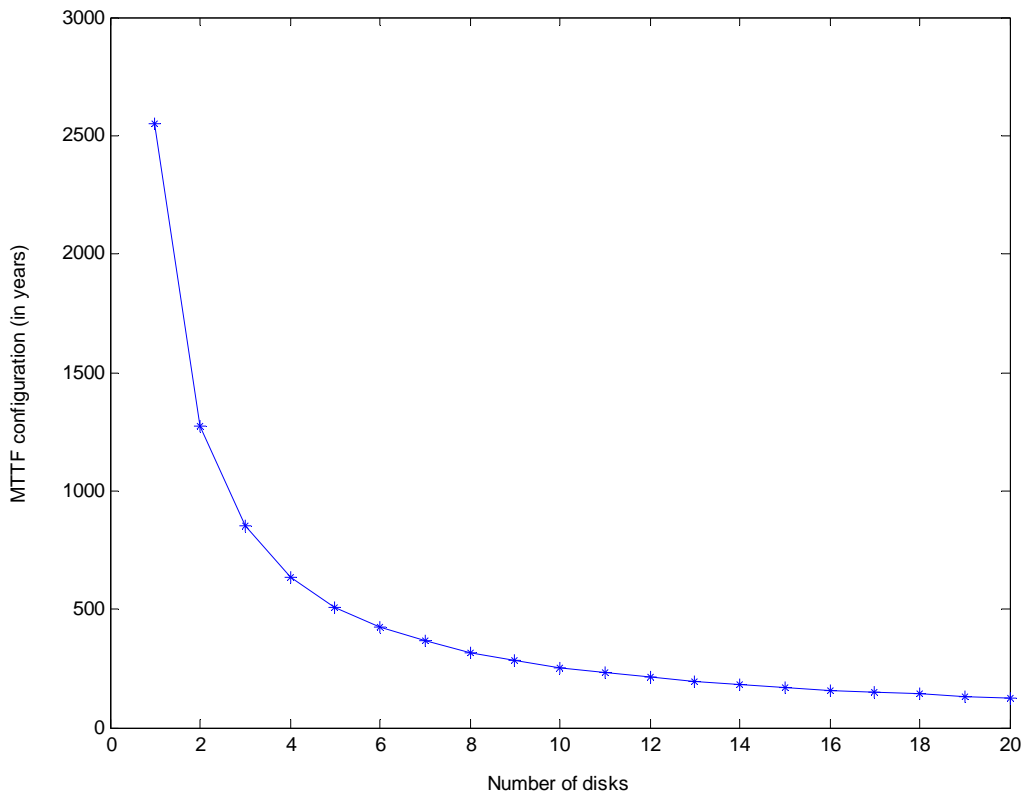
Τιμές παραμέτρων (σε ώρες)	
Μέσος χρόνος μέχρι την αστοχία του δίσκου $MTTF_{disk} = 1/\lambda_1$	3 χρόνια ($\lambda_1 = 3.80517504 \text{ E} - 005$)
Μέσος χρόνος αστοχίας της εφεδρικής μονάδας $MTTF_{backup} = 1/\lambda_2$	5 χρόνια ($\lambda_2 = 2,28310502\text{E} - 05$)
Μέσος χρόνος αντικατάστασης του δίσκου από τον δεύτερο δίσκο της διάταξης $MTTR_1 = 1/\mu_1$	50 ώρες ($\mu_1 = 0.02$)
Μέσος χρόνος επισκευής δίσκου από την εφεδρική μονάδα $MTTR_2 = 1/\mu_2$	100 ώρες ($\mu_2 = 0.01$)
Μέσος χρόνος αντικατάστασης εφεδρικής μονάδας από δίσκο $MTTR_3 = 1/\mu_3$	8 ώρες ($\mu_3 = 0.125$)
Μέσος χρόνος εύρεσης αστοχίας ενός δίσκου $MTTFD_{disk} = 1/\theta_1$	14 ημέρες ($\theta_1 = 2.976190476 \text{ E} - 003$)
Μέσος χρόνος εύρεσης αστοχίας της εφεδρικής μονάδας $MTTFD_{backup} = 1/\theta_2$	60 ημέρες ($\theta_2 = 6.944444444\text{E} - 04$)

Πίνακας 6: Τιμές παραμέτρων για την αποτίμηση του μοντέλου της διάταξης

Τα αναλυτικά αποτελέσματα που προκύπτουν από την εκτέλεση του μοντέλου στο SHARPE για το μέσο χρόνο αστοχίας της διάταξης σε συνάρτηση με το πλήθος των συνιστωσών της διάταξης απεικονίζονται στο σχεδιάγραμμα (Εικόνα 18).

Από το σχεδιάγραμμα γίνεται φανερό ότι η προσθήκη ενός αντιγράφου ασφαλείας αυξάνει το μέσο χρόνο αστοχίας της διάταξης από 106 χρόνια στα 2551 χρόνια. Η αύξηση του μέσου χρόνου αστοχίας είναι εντυπωσιακή αλλά

δικαιολογείται αν προσέξουμε ότι το τρίτο αντίγραφο φυλάσσεται σε αποθηκευτικό μέσο υψηλότερης αξιοπιστίας (μαγνητική ταινία με μέσο χρόνο ζωής στα 5 χρόνια)

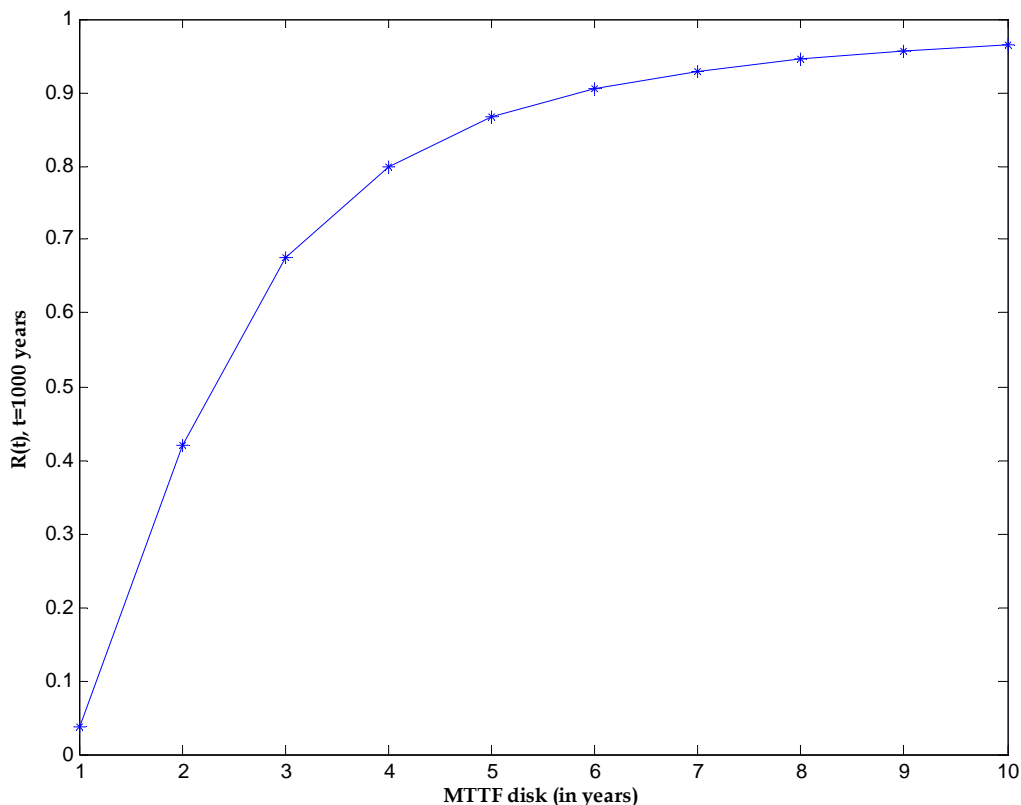


Εικόνα 18. Μεταβολές του μέσου χρόνου αστοχίας της διάταξης σε συνάρτηση με το πλήθος των δίσκων της διάταξης

4.5.3 Ανάλυση ευαισθησίας

Δεδομένης της καλής συμπεριφοράς που δείχνει η συγκεκριμένη διάταξη, αξιολογήσαμε τις μεταβολές της αξιοπιστίας στα 1000 χρόνια λειτουργίας της (ή αντίστοιχα $t = 8760000$ ώρες). Στην Εικόνα 19 υπάρχει η γραφική παράσταση με τις μεταβολές στην αξιοπιστία $R(t)$ της διάταξης σε συνάρτηση με το ρυθμό

αστοχία του δίσκου.

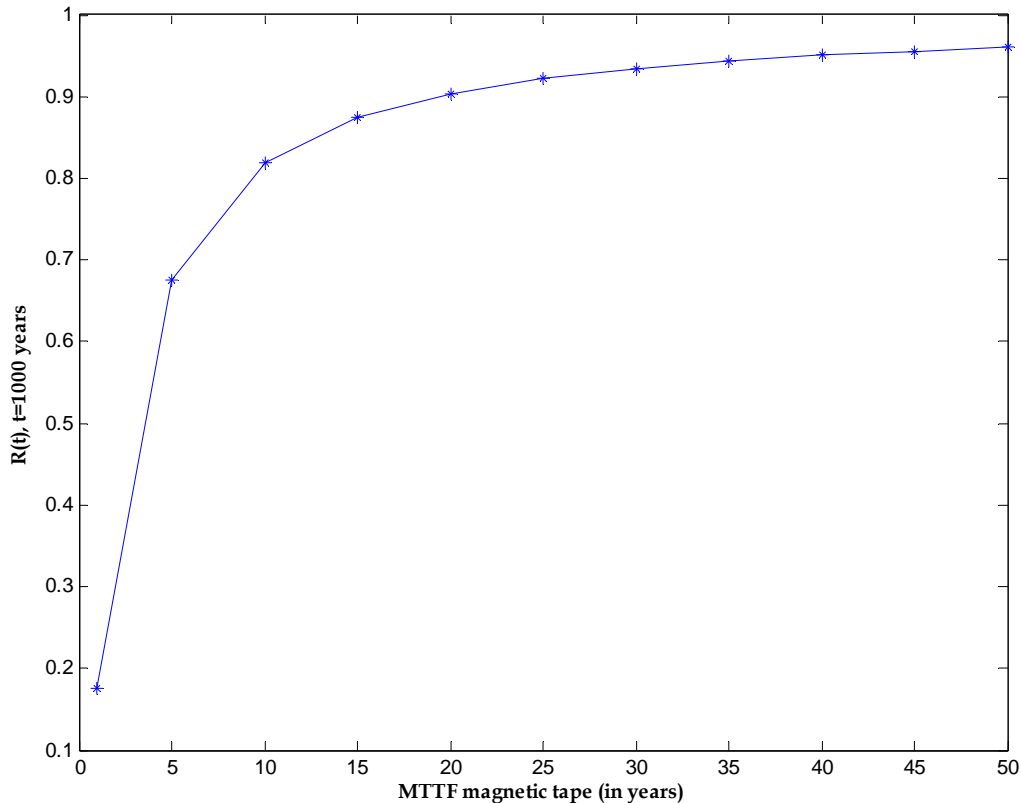


Εικόνα 19. Γραφική παράσταση αξιοπιστίας της διάταξης με $N=1$ συνιστώσες για $t=1000$ χρόνια λειτουργίας συναρτήσει του ρυθμού αστοχίας του δίσκου

Όπως προκύπτει από την γραφική παράσταση (Εικόνα 19) οι μεταβολές στην αξιοπιστία της διάταξης είναι σημαντικές όταν ο μέσος χρόνος ζωής του δίσκου αυξάνεται από 1 έως 5 έτη. Ωστόσο η διάταξη δεν παρουσιάζει σημαντικές βελτιώσεις στην αξιοπιστία για δίσκους με $MTTF_{disk}$ μεγαλύτερο των 5 ετών. Η δαπανηρή επένδυση σε υψηλά αξιόπιστους δίσκους (με μέσο χρόνο ζωής μεγαλύτερο των 5 ετών) συνεπώς δεν φαίνεται να επιφέρει θεαματικές βελτιώσεις στην αξιοπιστία της διάταξης.

Περίπου η ίδια συμπεριφορά παρατηρείται για την αξιοπιστία της διάταξης σε σχέση με της μεταβολές του μέσου χρόνου αστοχίας του δεύτερου αποθηκευτικού

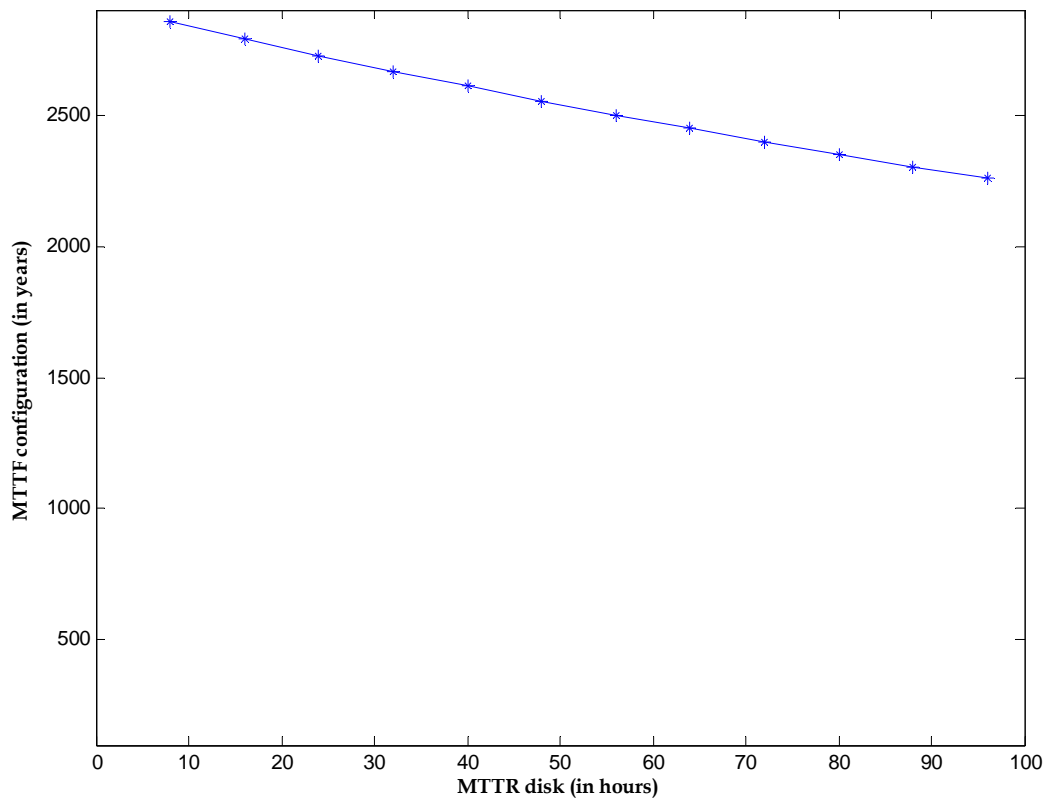
μέσου (μαγνητική ταινία) που χρησιμοποιείται στην διάταξη. Από την γραφική παράσταση γίνεται φανερό ότι η αύξηση της αξιοπιστίας της διάταξης είναι σημαντική για μέσο χρόνο αστοχίας του δεύτερου αποθηκευτικού μέσου μέχρι και 10-15 χρόνια ενώ με αύξηση πέρα από τα 10-15 χρόνια δεν παρατηρούνται σημαντικές βελτιώσεις.



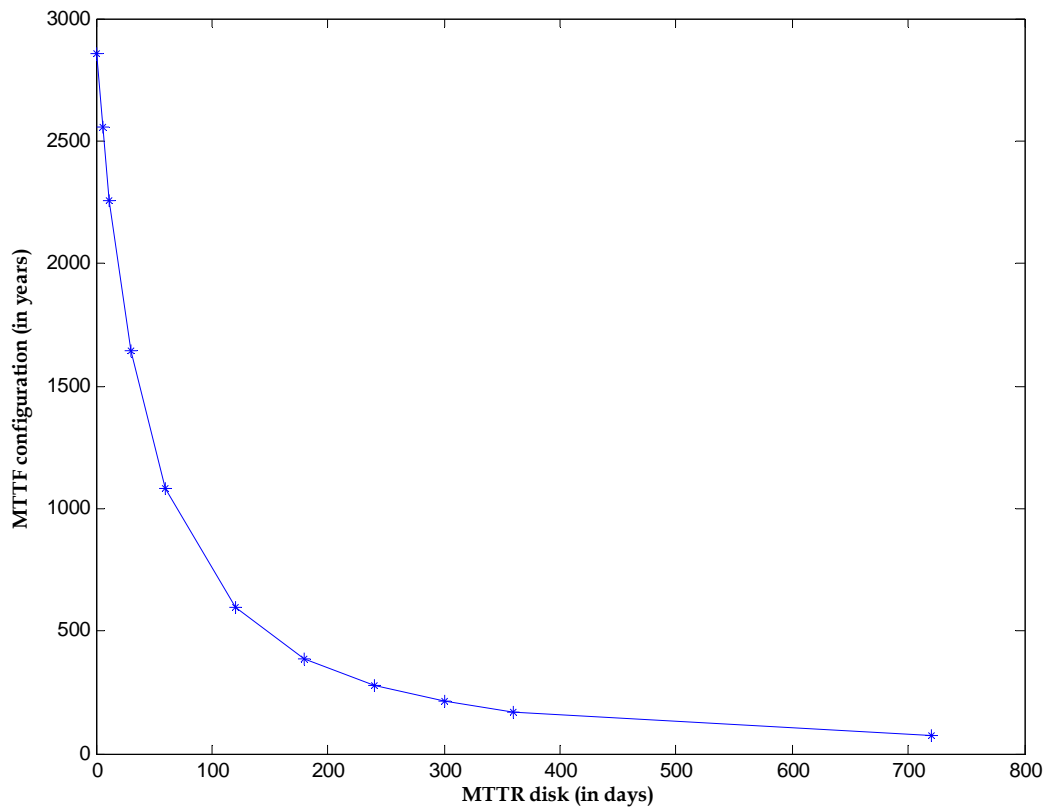
Εικόνα 20. Αποτίμηση της αξιοπιστίας της διάταξης σε t=1000 χρόνια συναρτήσει του ρυθμού αστοχίας του δεύτερου αποθηκευτικού μέσου

Σημαντικό ρόλο για την αξιοπιστία της διάταξης όπως προκύπτει από την ανάλυση ευαισθησίας παίζει ο μέσος χρόνος επισκευής των συνιστωσών της διάταξης. Ουσιαστικά για να μπορέσει η διάταξη να παραμείνει αξιόπιστη χρειάζεται να γίνεται άμεσα η επέμβαση επισκευής του δίσκου που έχει αστοχήσει. Ο μέσος χρόνος αστοχίας της διάταξης φαίνεται ότι επηρεάζεται ελάχιστα όπως προκύπτει από την γραφική παράσταση (Εικόνα 21) όταν ο

χρόνος επισκευής ενός δίσκου κυμαίνεται μέχρι και 100 ώρες (ή αντίστοιχα 12 εργάσιμες ημέρες). Σημαντικές διαφορές στο μέσο χρόνο αστοχίας παρατηρούνται όταν ο χρόνος που απαιτείται για την επισκευή ενός δίσκου ξεπεράσει τον 1 μήνα (Εικόνα 22). Έτσι για παράδειγμα με χρόνο επισκευής στα 2 χρόνια παρατηρείται πτώση του *MTTF* από 2553 χρόνια στα 72 χρόνια.



Εικόνα 21. Μεταβολές του μέσου χρόνου αστοχίας της διάταξης για μικρές αναμονές μέχρι την επισκευή ενός δίσκου (*MTTR < 100 hrs*)



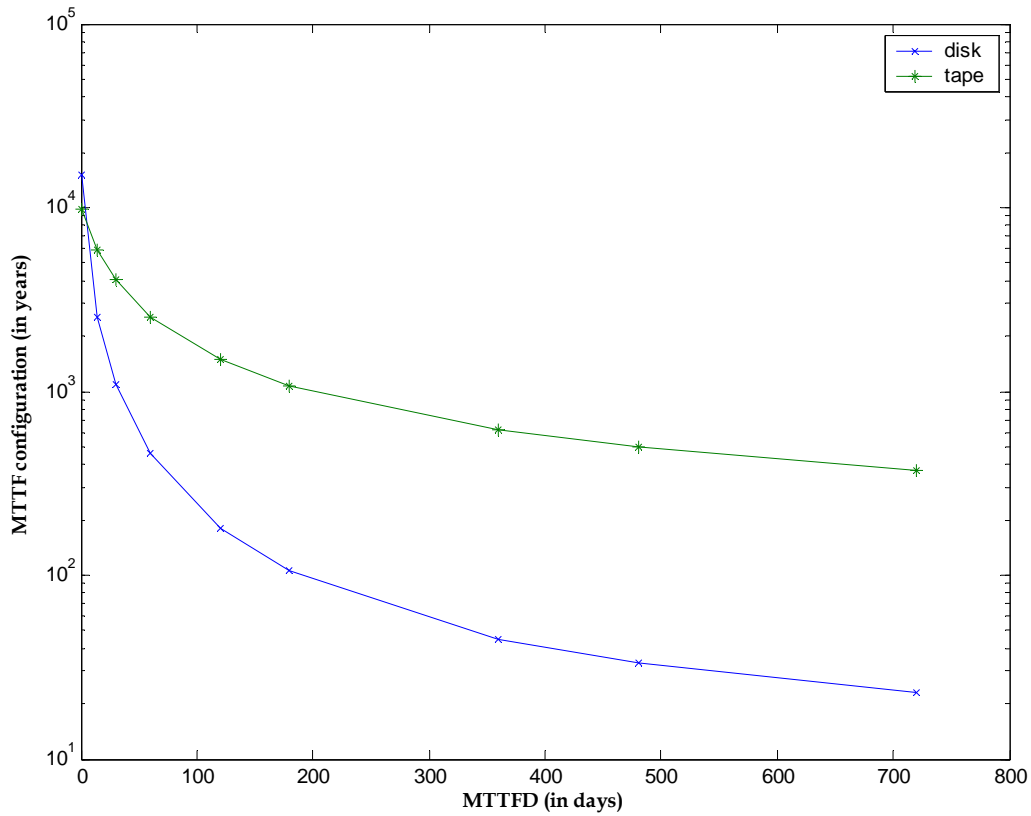
Εικόνα 22. Μεταβολές του μέσου χρόνου αστοχίας της διάταξης σε συνάρτηση το χρόνο επισκευής ενός δίσκου

Το μοντέλο παρουσιάζει επίσης μεγάλη ευαισθησία ως προς τον ρυθμό ανίχνευσης των αστοχιών στους δίσκους. Στην Εικόνα 23 φαίνονται οι μεταβολές του μέσου χρόνου αστοχίας της διάταξης σε σχέση με το μέσο χρόνο εύρεσης των σφαλμάτων στο δίσκο και στο δεύτερο αποθηκευτικό μέσο (μαγνητική ταινία). Ακόμα και μικρές μεταβολές του *MTTFD* του δίσκου όπως προκύπτει από την ανάλυση ευαισθησίας μπορεί να προκαλέσουν μεγάλες πτώσεις στο μέσο χρόνο αστοχίας της διάταξης.

Έτσι για παράδειγμα όταν ελέγχουμε κάθε μέρα τους δίσκους για σφάλματα ο μέσος χρόνος αστοχίας του συστήματος εκτοξεύεται περίπου στις 14951 χρόνια, ενώ με *MTTFD* να κυμαίνεται στις 14 ημέρες υπάρχει θεαματική πτώση του *MTTF* της διάταξης στα 2540 χρόνια. Η πτώση του *MTTF* της διάταξης συνεχίζει

να είναι απότομη, έτσι για χρόνο ανίχνευσης σφαλμάτων που κυμαίνονται στους 6 μήνες έχουμε το μέσο χρόνο αστοχίας της διάταξης να πέφτει στα 105 χρόνια.

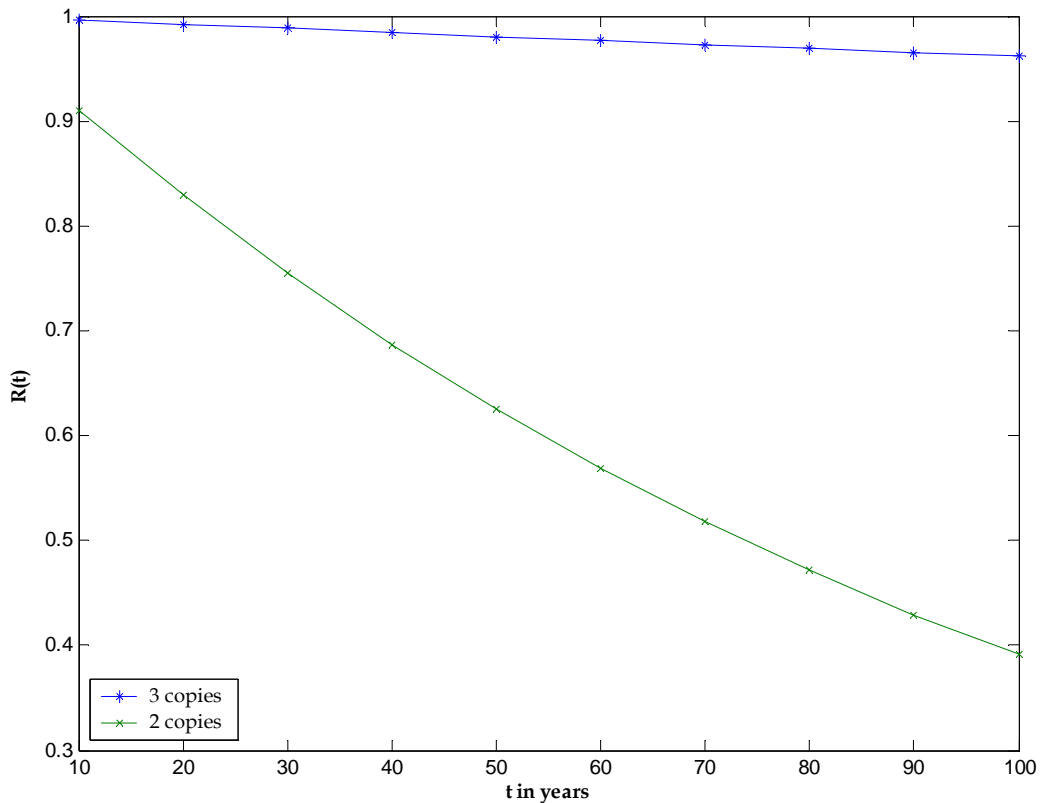
Στην Εικόνα 23 φαίνονται και οι μεταβολές του *MTTF* της διάταξης σε συνάρτηση με το χρόνο εύρεσης σφαλμάτων στο δεύτερο αποθηκευτικό μέσο της διάταξης (μαγνητική ταινία). Οι μεταβολές στις τιμές της συγκεκριμένης παραμέτρου επηρεάζει σαφώς σε μικρότερο βαθμό την αξιοπιστία της διάταξης.



Εικόνα 23. Μεταβολές του μέσου χρόνου αστοχίας της διάταξης σε συνάρτηση με το μέσο χρόνο εύρεσης σφαλμάτων στους δίσκους

4.5.4 Αξιοπιστία της διάταξης

Στην Εικόνα 24 συγκρίναμε την αξιοπιστία της απλή διάταξη με δυο αντίγραφα ασφαλείας για κάθε ψηφιακό έγγραφο με την διάταξη που κρατάει ένα επιπλέον αντίγραφο για διάστημα λειτουργίας από 10 έως 100 χρόνια. Από την γραφική παράσταση είναι φανερό ότι η προσθήκη ενός επιπλέον αντιγράφου ασφαλείας σε ένα αποθηκευτικό μέσο υψηλότερης αξιοπιστίας βελτιώνει πολύ σημαντικά την αξιοπιστία της διάταξης. Ωστόσο για οργανισμούς που έχουν θέσει σαν πολιτικό στόχο τους την διατήρηση των δεδομένων τους για πολύ μεγάλα χρονικά διαστήματα μελετήσαμε στην επόμενη ενότητα την αξιοπιστία της διάταξης στα 1000 χρόνια.



Εικόνα 24. Σύγκριση αξιοπιστίας των διατάξεων με 2 και 3 αντίγραφα

4.5.5 Ασφάλεια της διάταξης για μεγάλα χρονικά διαστήματα

Στην ενότητα 4.5.2 αποδείξαμε ότι ο μέσος χρόνος αποτυχίας της διάταξης μειώνεται με την αύξηση του πλήθους των συνιστωσών N που διαχειρίζεται η διάταξη καθώς υποθέσαμε ότι η διάταξη αποτυχεί όταν χάσει τα πρώτα ψηφιακά έγγραφα. Ωστόσο για οργανισμούς όπως μουσεία και ψηφιακές βιβλιοθήκες που ενδιαφέρονται για την διατήρηση των ψηφιακών τους εγγράφων για μεγάλα χρονικά διαστήματα (της τάξεως 1000 ετών) είναι ενδιαφέρον να μελετηθεί το ποσοστό της πληροφορίας που είναι ικανή να διασφαλίσει μια διάταξη που έχει N συνιστώσες.

Διαισθητικά η αύξηση του πλήθους των συνιστωσών της διάταξης θα πρέπει να αυξάνει την πιθανότητα σε πολύ μεγάλα χρονικά διαστήματα να επιβιώσει ένα μεγαλύτερο ποσοστό από τα ψηφιακά έγγραφα, ενώ η πιθανότητα επιβίωσης όλων των συνιστωσών (και κατά συνέπεια όλων των ψηφιακών δεδομένων) της διάταξης τείνει προς το 0. Για να αποδείξουμε αυτό τον ισχυρισμό θα χρησιμοποιήσουμε το διωνυμικό μοντέλο.

Η πιθανότητα επιβίωσης μιας συνιστώσα της υπό-μελέτη διάταξης μετά από 1000 χρόνια υπολογίζεται ότι είναι $R(t) = 0.6746$. Καθώς αυξάνεται το πλήθος των συνιστωσών της διάταξης, η πιθανότητα να έχουν επιβιώσει όλες οι συνιστώσες της μετά από 1000 χρόνια γίνεται πολύ μικρή (τείνει προς το 0). Ενδιαφέρον είναι να μελετήσουμε την πιθανότητα να επιβιώσουν για παράδειγμα 50% ή 90% των δεδομένων μετά από 1000 χρόνια λειτουργίας της διάταξη με $N=100$ ή $N=1000$ συνιστώσες.

Είναι γνωστό ότι το πλήθος Y_n των συνιστωσών που έχουν επιβιώσει από ένα πλήθος N πανομοιότυπων και ανεξάρτητων συνιστωσών ακολουθεί την διωνυμική κατανομή $B(k; N, R)$ όπου R είναι η αξιοπιστία κάθε συνιστώσας ξεχωριστά [T03]. Συνεπώς η πιθανότητα (αξιοπιστία) να έχουν επιβιώσει k από N συνιστώσες του συστήματος δίνεται από το τύπο:

$$R_{k/N} = \sum_{i=k}^n \binom{N}{i} R^i (1-R)^{N-i}$$

Τύπος 12

Για μικρό πλήθος συνιστωσών N μπορεί να γίνει απευθείας εφαρμογή του παραπάνω τύπου. Καθώς το N μεγαλώνει οι υπολογισμοί για τον τύπο της διωνυμικής κατανομής είναι αδύνατον να εκτελεστούν. Για τους υπολογισμούς προτιμήσαμε την χρήση της ενσωματωμένης συνάρτησης Binomial[n,k] του εργαλείου Mathematica [W99]. Στο Πίνακα 7 υπάρχουν τα αποτελέσματα για διαφορετικό πλήθος N . Όπως δείχνουν τα αποτελέσματα, η αύξηση του πλήθους των συνιστωσών της διάταξης αυξάνει την πιθανότητα επιβίωσης 50% των ψηφιακών δεδομένων μετά από 1000 χρόνια. Ωστόσο αν ένας οργανισμός έχει σαν στόχο την διατήρηση 90% των δεδομένων του σε 1000 χρόνια η συγκεκριμένη διάταξη είναι ανεπαρκής.

N	K/N (50%)	$R_{k/N}$	K/N (90%)	$R_{k/N}$
2	1/2	0.8597	2/2	0.3911
10	5/10	0.8731	9/10	0.0639796
100	50/100	0.9960	90/100	$5.17553 \cdot 10^{-10}$
500	250/500	1	450/500	$2.52509 \cdot 10^{-44}$
1000	500/1000	1	900/1000	$2.00336 \cdot 10^{-63}$

Πίνακας 7: Αποτελέσματα διωνυμικού μοντέλου για διαφορετικό πλήθος συνιστωσών N της διάταξης

4.5.6 Επιρροή εξωτερικών γεγονότων καταστροφής στην αξιοπιστία διατάξεων συστημάτων για ψηφιακή διατήρηση

Στη σχεδίαση διατάξεων που έχουν σαν στόχο την μακροχρόνια διατήρηση των ψηφιακών δεδομένων που διαχειρίζονται, είναι σημαντικό να μελετηθούν

πιθανές επιρροές στην αξιοπιστία που μπορεί να προκαλέσουν εξωτερικά γεγονότα καταστροφής όπως πυρκαγιά, σεισμός, πλημμύρα. Τέτοια γεγονότα μπορεί να προκαλέσουν ταυτόχρονη αστοχία των ξεχωριστών συνιστωσών.

Θα τροποποιήσουμε το μοντέλο που παρουσιάσαμε στην ενότητα 4.5.1 για την μελέτη της επιρροής τέτοιων εξωτερικών γεγονότων καταστροφής. Οι αλλαγές στο μοντέλο θα γίνουν με βάση τις παρακάτω υποθέσεις:

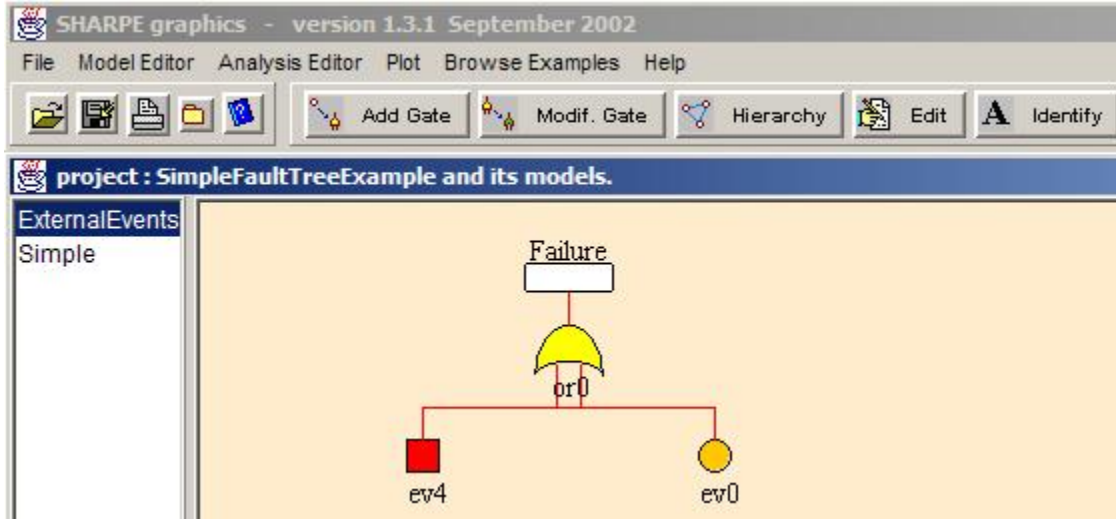
- Οι φορείς πληροφορίας (δίσκοι και μαγνητικές ταινίες) της διάταξης βρίσκονται στον ίδιο φυσικό χώρο.
- Οι φορείς πληροφορίας υπάρχουν σε δυο διαφορετικούς φυσικούς χώρους. Θεωρούμε ότι η φύλαξη των δύο δίσκων και των μαγνητικών ταινιών που κρατάμε το τρίτο αντίγραφο κάθε ψηφιακού εγγράφου γίνεται σε διαφορετικούς φυσικούς χώρους. Αυτό αυτόματα συνεπάγεται ότι το ένα εξωτερικό γεγονός καταστροφής με τοπική εμβέλεια δεν μπορεί να καταστρέψει ταυτόχρονα όλα τα αντίγραφα της διάταξης.

Για τους αριθμητικούς υπολογισμούς θα πάρουμε ως παράδειγμα την εκδήλωση πυρκαγιάς με εμβέλεια ενός φυσικού χώρου. Από την μελέτη των [FT00] προκύπτει ότι η εκδήλωση πυρκαγιάς με εμβέλεια ενός φυσικού χώρου εμφανίζεται κάθε 10 χρόνια ($\lambda = \frac{1}{10}$) με πιθανότητα 0.9% ($c = 0.009$).

Για την πρώτη υπόθεση, επεκτείνουμε το μοντέλο της ενότητας 4.5.2 με ένα επιπλέον επίπεδο. Θεωρούμε ότι το ανώτερο επίπεδο στο ιεραρχικό μοντέλο είναι ένα δέντρο σφαλμάτων που αναπαριστά το λογικό συνδυασμό με τον οποίο αστοχεί η διάταξη (Εικόνα 25). Η είσοδος εν4 της λογικής πόλη OR, εσωτερικά μοντελοποιείται με το μοντέλο Markov που περιγράψαμε στην ενότητα 4.5.1 για την περίπτωση $N=1$ συνιστωσών της διάταξης, ενώ η είσοδος εν0 μοντελοποιείται με τον ρυθμό εμφάνισης μιας πυρκαγιάς με εμβέλεια ενός φυσικού χώρου που όπως αναφέραμε είναι λc .

Κεφάλαιο 4. Αποτίμηση αξιοπιστίας διατάξεων συστημάτων για ψηφ. διατήρηση

Το δέντρο σφαλμάτων ουσιαστικά δηλώνει ότι η διάταξη αποτυγχάνει είτε όταν οι φορείς πληροφορίας χάσουν ψηφιακά έγγραφα είτε αν εκδηλωθεί φωτιά στην τοποθεσία της διάταξης.



Εικόνα 25 Δέντρο σφαλμάτων για την μελέτη φυσικών γεγονότων καταστροφής της διάταξης

Η δεύτερη υπόθεση συνεπάγεται αλλαγές στο αρχικό μοντέλο Markov (Εικόνα 17). Μια σειρά από νέες μεταβάσεις έχουν εισαχθεί στον μοντέλο για την αναπαράσταση πυρκαγιάς (Εικόνα 26) που εκδηλώνεται με ρυθμό μετάβασης λ_c .

Κεφάλαιο 4. Αποτίμηση αξιοπιστίας διατάξεων συστημάτων για ψηφ. διατήρηση

Η επιρροή που μπορεί να έχει ένα εξωτερικό φυσικό γεγονός καταστροφής στην αξιοπιστία της διάταξης είναι φανερή από την πτώση του *MTTF* ιδιαίτερα όταν η φύλαξη των δεδομένων γίνεται στον ίδιο φυσικό χώρο. Συνεπώς στην σχεδίαση και υλοποίηση διατάξεων για ψηφιακή διατήρηση η μαζική καταστροφή δεδομένων από φυσικά γεγονότα όπως το παράδειγμα της πυρκαγιάς με εμπέλεια ενός φυσικού χώρου είναι σημαντικό να ληφθούν υπόψη. Τα αποτελέσματα δείχνουν ότι η φύλαξη διαφορετικών φορέων που κρατάνε ταυτόσημα δεδομένα σε διαφορετικούς φυσικούς χώρους δίνει μεγαλύτερα ασφάλεια στην διατήρησή τους για μεγάλα χρονικά διαστήματα.

Διάταξη χωρίς εξωτερικά γεγονότα καταστροφής ($N = 1$)	Διάταξη με ένα εξωτερικό γεγονός καταστροφής και όλους τους φορείς δεδομένων στον ίδιο φυσικό χώρο ($N = 1$).	Διάταξη με ένα εξωτερικό γεγονός καταστροφής και φορείς δεδομένων σε διαφορετικούς χώρους ($N = 1$)
<i>MTTF = 2551,29 χρόνια</i>	<i>MTTF = 773 χρόνια</i>	<i>MTTF = 2375 χρόνια</i>

Πίνακας 8: Συγκριτικά αποτελέσματα

4.6 Επικύρωση αποτελεσμάτων με αντίστοιχα παραδείγματα στο ArchSim

Όπως αναφέραμε στην εισαγωγή του κεφαλαίου, στα πλαίσια της διδακτορικής διατριβής του Crespo [C03] αναπτύχθηκε το εργαλείο ArchSim που βασίζεται στη μέθοδο προσομοίωση Monte-Carlo και χρησιμοποιείται για την αποτίμηση μοντέλων που περιγράφουν αρχειακές αποθήκες. Είναι ενδιαφέρον να δούμε συγκριτικά αποτελέσματα που παράγει το ArchSim για μελέτες περιπτώσεων που μοιράζονται κοινές υποθέσεις με τα αναλυτικά παραδείγματα που έχουμε μελετήσει έως τώρα. Στο Πίνακα 9 περιγράφονται οι παράμετροι και τα συγκριτικά αποτελέσματα.

Εργαλείο προσομοίωσης: ArchSim	Αναλυτικά μοντέλα παρούσας μελέτης
<p>Παράδειγμα διάταξης που κρατάει δυο αντίγραφα ασφαλείας για κάθε ψηφιακό έγγραφο.</p> <p>Παράμετροι εισόδου:</p> <ul style="list-style-type: none"> - Μέσος χρόνος αστοχίας του δίσκου: 3 χρόνια - Μέσος χρόνος εύρεσης και επισκευής σφαλμάτων στους δίσκους: 60 ημέρες 	<p>Παράδειγμα διάταξης που κρατάει δυο αντίγραφα ασφαλείας για κάθε ψηφιακό έγγραφο.</p> <p>Παράμετροι εισόδου:</p> <ul style="list-style-type: none"> - Μέσος χρόνος αστοχίας δίσκου: 3 χρόνια - Μέσος χρόνος εύρεσης σφαλμάτων στους δίσκους: 60 μέρες - Μέσος χρόνος επισκευής που έχει αστοχήσει: 50 ώρες
<p>Μέσος χρόνος αστοχίας διάταξης: 34 χρόνια</p>	<p>Μέσος χρόνος αστοχίας διάταξης: 30,91 χρόνια</p>
<p>Παράδειγμα διάταξης που κρατάει τρία αντίγραφα ασφαλείας για κάθε ψηφιακό έγγραφο.</p> <p>Μοντελοποιούνται οι παράμετροι:</p> <ul style="list-style-type: none"> - Μέσος χρόνος αστοχίας του δίσκου: 3 χρόνια - Μέσος χρόνος εύρεσης και επισκευής σφαλμάτων στους δίσκους: 60 ημέρες 	<p>Παράδειγμα διάταξης που κρατάει τρία αντίγραφα ασφαλείας για κάθε ψηφιακό έγγραφο.</p> <p>Μοντελοποιούνται οι παράμετροι:</p> <ul style="list-style-type: none"> - Μέσος χρόνος αστοχίας του δίσκου: 3 χρόνια - Μέσος χρόνος αστοχίας δεύτερης αποθηκευτικής μονάδας: 5 χρόνια

	<ul style="list-style-type: none"> - Μέσος χρόνος επισκευής δίσκου/δεύτερης αποθηκευτικής μονάδας: 50 ώρες - Μέσος χρόνος εύρεσης σφαλμάτων δίσκους: 14 ημέρες - Μέσος χρόνος εύρεσης σφαλμάτων δεύτερο αποθηκευτικό μέσο: 60 ημέρες
Μέσος χρόνος αποτυχίας διάταξης: 2101 χρόνια	Μέσος χρόνος αποτυχίας διάταξης: 2540 χρόνια

Πίνακας 9: Συγκριτικά αποτελέσματα με το ArchSim

Η καλύτερη συμπεριφορά που παρατηρείται στα αποτελέσματα του αναλυτικού μοντέλου για το παράδειγμα της διάταξης με τρία αντίγραφα οφείλεται στις διαφορετικές τιμές των παραμέτρων, καθώς θεωρούμαι ότι το ένα από τα τρία αντίγραφα ασφαλείας αποθηκεύεται σε ένα πιο αξιόπιστο μέσο. Επίσης υπάρχει διαφορά στους χρόνους εύρεσης σφαλμάτων.

4.7 Επέκταση διάταξης: Μελέτη διάταξης με τέσσερα αντίγραφα ασφαλείας

4.7.1 Περιγραφή του μοντέλου

Ένα επιπλέον βήμα στην μελέτη των διατάξεων για ψηφιακή διατήρηση με ορίζοντα μεγάλα χρονικά διαστήματα αποτελεί η προσθήκη ενός επιπλέον αντιγράφου ασφαλείας στην προηγούμενη διάταξη. Ουσιαστικά μελετάμε μια διάταξη που δημιουργεί δυο αντίγραφα σε δυο διαφορετικούς σκληρούς δίσκους και επιπλέον δυο αντίγραφα σε ένα διαφορετικό αποθηκευτικό μέσο (μαγνητική ταινία). Η αλυσίδα Markov που περιγράφει την συγκεκριμένη διάταξη υπάρχει στην Εικόνα 27. Είναι φανερό η αύξηση της πολυπλοκότητας με την προσθήκη μιας επιπλέον συνιστώσας στην διάταξη. Αυτό αποτελεί και ένα βασικό μειονέκτημα αυτού του τρόπου μοντελοποίησης.

Η εκτέλεση του μοντέλου έγινε στο SHARPE και οι παράμετροι και οι τιμές που

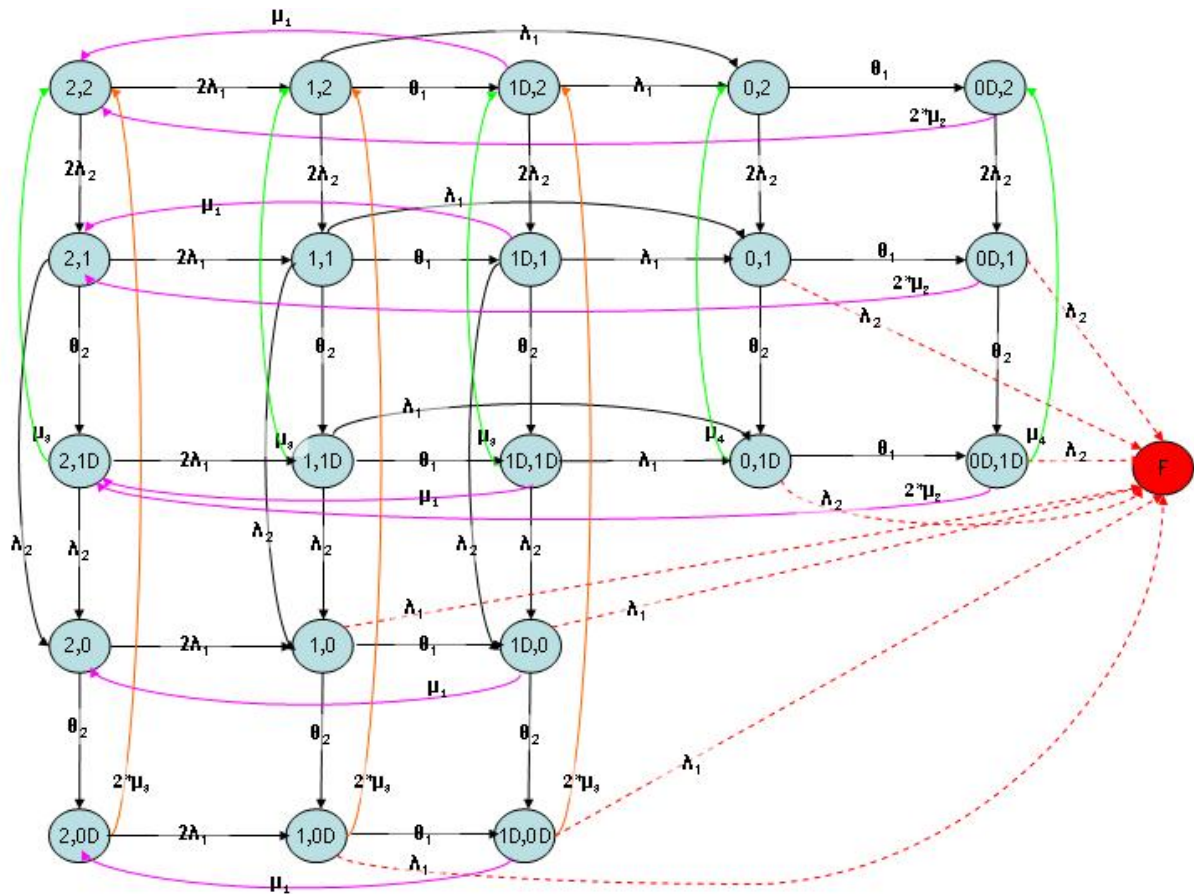
Κεφάλαιο 4. Αποτίμηση αξιοπιστίας διατάξεων συστημάτων για ψηφ. διατήρηση

χρησιμοποιήθηκαν για την αποτίμηση του μέσου χρόνου αστοχίας και της αξιοπιστίας της διάταξης περιγράφονται στο Πίνακα 10.

Παράμετροι	Περιγραφή	Τιμές (οι τιμές των παραμέτρων έχουν υπολογιστεί σε ώρες)
λ_1	Σταθερός ρυθμός αστοχίας δίσκων	$\lambda_1 = 3.80517504 \text{ E} - 005$ (Μέσος χρόνος αστοχίας του δίσκου στα 3 χρόνια)
λ_2	Σταθερός ρυθμός αστοχίας μαγνητικής ταινίας	$\lambda_2 = 2.28310502 \text{ E} - 05$ (Μέσος χρόνος αστοχίας της μαγνητικής ταινίας στα 5 χρόνια)
μ_1	Σταθερός ρυθμός αντικατάστασης δίσκου που έχει αστοχήσει και ανακατασκευής του περιεχομένου του από τον δεύτερο σκληρό δίσκο	$\mu_1 = 0.02$ (Μέσος χρόνος επισκευής δίσκου από δίσκο στις 50 ώρες)
μ_2	Σταθερός ρυθμός αντικατάστασης δίσκου και ανακατασκευής των περιεχομένου του από την μαγνητική ταινία	$\mu_2 = 0.01$ (Μέσος χρόνος επισκευής δίσκου από τον δεύτερο δίσκο είναι 100 ώρες)
μ_3	Σταθερός ρυθμός αντικατάσταση μαγνητικής ταινίας και ανακατασκευής περιεχομένων από ένα δίσκο	$\mu_3 = 0.125$ (Μέσος χρόνος επισκευής μαγνητικής ταινίας από δίσκο είναι 8 ώρες)
μ_4	Σταθερός ρυθμός αντικατάσταση μαγνητικής ταινίας και ανακατασκευής περιεχομένων από δεύτερη μαγνητική ταινία	$\mu_3 = 0.125$ (Μέσος χρόνος επισκευής μαγνητικής ταινίας από μαγνητική ταινία είναι 8 ώρες)
θ_1	Σταθερός ρυθμός ανίχνευσης αστοχιών των δίσκων	$\theta_1 = 2.976190476 \text{ E} - 003$ (Μέσος χρόνος εύρεσης σφαλμάτων στο δίσκο είναι 14 ημέρες)
θ_2	Σταθερός ρυθμός ανίχνευσης αστοχιών μαγνητικής ταινίας	$\theta_2 = 6.94444444 \text{ E} - 04$ (Μέσος χρόνος εύρεσης σφαλμάτων σε μαγνητική ταινία είναι 60 ημέρες)

Αριθμητικά αποτελέσματα	
Μέσος χρόνος αστοχίας της διάταξης για $N = 1$	$MTTF_{config} = 20082.91$
Αξιοπιστίας της διάταξης $R(t)$, $t = 1000$ χρόνια για $N = 1$	$R(t) = 0.9514$

Πίνακας 10: Παράμετροι μοντέλου Markov με τέσσερα αντίγραφα ασφαλείας για κάθε ψηφιακό έγγραφο



Εικόνα 27. Αλυσίδα Markov για την μελέτη διάταξης με τέσσερα αντίγραφα ασφαλείας

Τα συγκριτικά αποτελέσματα μεταξύ της διάταξης με τρία αντίγραφα ασφαλείας που μελετήσαμε στην προηγούμενη ενότητα και της παρούσας διάταξης με τέσσερα αντίγραφα είναι εντυπωσιακά. Ο μέσος χρόνος αστοχίας εκτοξεύεται στα 20.000 χρόνια με την προσθήκη ενός επιπλέον αντιγράφου εν αντιθέσει με τα 2553 χρόνια που είχαμε στη διάταξη με τρία αντίγραφα ασφαλείας. Επίσης

έχουμε σημαντική βελτίωση στην αξιοπιστία που αξιολογήσαμε στα 1000 χρόνια λειτουργίας της διάταξης που αυξάνεται με την προσθήκη ενός αντιγράφου ασφαλείας από $R(t) = 0.6746, t = 1000\text{yrs}$ σε $R(t) = 0.9514, t = 1000\text{yrs}$.

4.7.2 Ασφάλεια της διάταξης για μεγάλα χρονικά διαστήματα

Ενδιαφέρον παρουσιάζει η μελέτη της διάταξης ως προς την ασφάλεια που παρέχει στην διατήρηση των ψηφιακών εγγράφων στο χρονικό ορίζοντα των 1000 ετών. Όπως αναφέραμε στην ενότητα 4.5.5 η εφαρμογή του διωνυμικού μοντέλου θα μπορέσει να μας δώσει την πιθανότητα να επιβιώσουν για παράδειγμα 90% των ψηφιακών εγγράφων δεδομένου έχοντας N πλήθος συνιστωσών. Δεδομένης της πιθανότητας να επιβιώσει μια συνιστώσα σε 1000 χρόνια ($R = 0.9514$) εφαρμόσαμε την ενσωματωμένη συνάρτησης Binomial[n,k] του εργαλείου Mathematica [W99]. Τα αποτελέσματα υπάρχουν στο Πίνακας 11.

N	K/N (90%)	$R_{k/N}$
10	9 στα 10	0.918137
100	90 στα 100	0.990645
500	450 στα 500	0.999999
1000	900 στα 1000	1

Πίνακας 11: Αποτελέσματα διωνυμικού μοντέλου

4.8 Επέκταση διάταξης: Μελέτη αξιοπιστίας αρχιτεκτονικών παρατάξεων δίσκων (RAID)

Μια ενδιαφέρουσα προσέγγιση στην μελέτη αποθηκευτικών μέσων που παρέχουν υψηλή αξιοπιστία είναι μια σειρά από αρχιτεκτονικές παρατάξεων δίσκων. Ο Patterson [PGK88] εισήγαγε τον όρο RAID (Redundant Arrays of Inexpensive Disks) για συστήματα παρατάξεων δίσκων με πλεονασμό. Στην μελέτη του Patterson οι διάφορες υπάρχουσες αρχιτεκτονικές παρατάξεων

δίσκων έχουν ενοποιηθεί ως διαφορετικά επίπεδα RAID (επίπεδο 1,2,3,4) και επίσης γίνεται εισαγωγή μιας νέας υψηλής απόδοσης αρχιτεκτονική (RAID επιπέδου 5). Στην μελέτη [MT93] αναπτύχθηκαν μια σειρά από ιεραρχικά μοντέλα αξιοπιστίας για RAID - 1,2,3,4,5.

Σκοπός αυτής της ενότητας είναι η αποτίμηση της αξιοπιστίας αυτών των αρχιτεκτονικών παρατάξεων δίσκων ως μια εναλλακτική προσέγγιση για την φύλαξη ψηφιακών δεδομένων σε διατάξεις συστημάτων για ψηφιακή διατήρηση.

Οι παρατάξεις δίσκων συνήθως αποτελούνται από N ομάδες δίσκων και κάθε ομάδα αποτελείται από D δίσκους δεδομένων (data disks) και C δίσκους ελέγχου (check disks). Ο χρόνος αστοχίας κάθε δίσκου είναι εκθετικά κατανομημένος με μέσο χρόνο μέχρι την αστοχία του δίσκου ($MTTF$) να ισούται με $1/\lambda$. Κάθε ομάδα ανέχεται μια μοναδική αστοχία δίσκου αφού είναι δυνατή η ανασκευή των δεδομένων του καταστρεμμένου δίσκου από την πλεονάζουσα πληροφορία. Στην διάρκεια ανακατασκευής της πληροφορίας γίνεται αντικατάσταση του δίσκου που έχει αστοχήσει από εφεδρικό δίσκο που διαθέτει το RAID και τα δεδομένα ανακατασκευάζονται από τους υπόλοιπους δίσκους που λειτουργούν σωστά και την πληροφορία ισοτιμίας που διαθέτει κάθε ομάδα που αποτελεί την παράταξη των δίσκων. Ωστόσο κατά την διάρκεια ανακατασκευής ενός δίσκου αν συμβεί αστοχία σε δεύτερο δίσκο της ίδιας ομάδας σημαίνει απώλεια δεδομένων καθώς δεν μπορεί να γίνει πλέον ανακατασκευή δεδομένων και συνεπώς η ομάδα δίσκων θεωρείται ότι έχει αστοχήσει. Η απώλεια δεδομένων σε οποιαδήποτε ομάδα δίσκων συνεπάγεται ταυτόχρονα την αστοχία ολόκληρης της παράταξης δίσκων. Αρχικά θα υποθέσουμε ότι κάθε ομάδα έχει το δικό της μηχανισμό ανακατασκευής που είναι ανεξάρτητος των υπόλοιπων δίσκων και επίσης θα θεωρήσουμε ότι υπάρχει απεριόριστο πλήθος εφεδρικών δίσκων. Οι δίσκοι που αποτελούν την παράταξη είναι ακριβώς ίδιοι (θεωρούμε ότι προέρχονται από τον ίδιο κατασκευαστή).

Ο χρόνος επισκευής ενός δίσκου που έχει αστοχήσει υποθέτουμε ότι είναι

εκθετικά κατανεμημένος με μέσο χρόνο μέχρι την ανακατασκευή (*MTTR*) να είναι $1/\mu$. Οι αστοχίες καλύπτονται από το σύστημα με πιθανότητα p ενώ με πιθανότητα $1-p$ παραμένουν ακάλυπτες. Ένα ακάλυπτο σφάλμα οδηγεί σε απώλεια δεδομένων τις ομάδες των δίσκων. Εκδηλώσεις ακάλυπτων σφαλμάτων θεωρούνται λάθη σε δυαδικά ψηφία που δεν ανιχνεύονται, δεν διορθώνονται ή διορθώνονται λαθεμένα. Ακάλυπτα σφάλματα προκαλούνται επίσης λόγω σφαλμάτων στο κύκλωμα που υλοποιεί το κώδικα διόρθωσης λαθών (Error Correcting Code - ECC) ή σε περιπτώσεις μη σωστής ενεργοποίησης του ECC. Αστοχίες του υποστηρικτικού υλικού, καταστροφικές αστοχίες από ακραίες περιβαλλοντικές συνθήκες καθώς και πολλαπλά λάθη στα δυαδικά ψηφία (που δεν αντιμετωπίζονται από το ECC) ερμηνεύονται επίσης ως ατελής καλύψεις. Πριν προχωρήσουμε στην ανάπτυξη των μοντέλων Markov για την μελέτη της αξιοπιστίας των RAID και την σύγκριση τους με τις ήδη προτεινόμενες διατάξεις θα εισάγουμε σύντομα τα επίπεδα RAID. Εκτεταμένες μελέτες για RAID υπάρχουν στην βιβλιογραφία [CLG+93], [MT93], [PGK88], [GP92].

4.8.1 RAID επιπέδου 1

Ο κατοπτρισμός είναι μια παραδοσιακή προσέγγιση για την βελτίωση της αξιοπιστίας παρατάξεων δίσκων. Ουσιαστικά για ένα σύστημα που απαιτεί N πλήθος δίσκων για την αποθήκευση δεδομένων απαιτεί $2N$ πλήθος δίσκων για την υλοποίηση ενός κατοπτρικού συστήματος. Η συγκεκριμένη RAID αρχιτεκτονική είναι η πιο υψηλή σε επίπεδο κόστους. Κάθε ζεύγος δίσκων που αντικατοπτρίζουν ο ένας το περιεχόμενο του άλλου σχηματίζουν μια ομάδα δίσκων. Σε περίπτωση αστοχίας ενός δίσκου σε μια ομάδα η ανακατασκευή των δεδομένων γίνεται σε ένα εφεδρικό δίσκο (spare disk). Η ανακατασκευή ουσιαστικά περιλαμβάνει την αντιγραφή των δεδομένων από τον λειτουργικό δίσκο στον εφεδρικό.

RAID επιπέδου 2

Σε αυτό το σχήμα κάθε ομάδα αποτελείται από D δίσκους δεδομένων και C δίσκους ελέγχου (όπου ισχύει $C \geq \log_2(D+C+1)$). Ουσιαστικά στην αρχιτεκτονική RAID επιπέδου 2 γίνεται χρήση του κώδικα Hamming [SS98] για την δημιουργία πληροφορίας ισοτιμίας. Στην συγκεκριμένη έκδοση το σχήμα απαιτεί για τέσσερις δίσκους δεδομένων τρεις δίσκους για την πλεονάζουσα πληροφορία δηλαδή ένα δίσκο λιγότερο σε σχέση με το RAID-1. Σε περίπτωση αστοχίας μιας μοναδικής συνιστώσας, η πληροφορία ισοτιμίας έχει ασυνεπείς τιμές και η συνιστώσα που θεωρείται ότι έχει αστοχήσει είναι εκείνη που είναι κοινή μεταξύ των λαθεμένων υποσυνόλων. Η πληροφορία που έχει χαθεί ανακτάται διαβάζοντας τις υπόλοιπες συνιστώσες του υποσυνόλου μαζί με την πληροφορία ισοτιμίας και θέτοντας το δυαδικό ψηφίο που λείπει σε 0 ή 1 για να δημιουργηθεί η κατάλληλη τιμή ισοτιμίας για το υποσύνολο. Στην ουσία οι C δίσκοι ελέγχου απαιτούνται για την ανίχνευση της θέσης του σφάλματος, ενώ μετά την ανίχνευση ένα μοναδικό δυαδικό ψηφίο ισοτιμίας είναι αρκετό για την ανακατασκευή των δεδομένων που έχουν χαθεί.

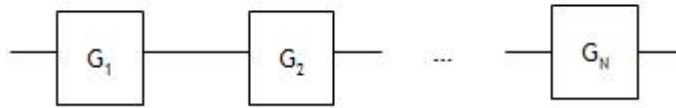
4.8.2 RAID επιπέδου 3, 4, 5

Στο RAID επιπέδου 3, 4, 5 ο ελεγκτής δίσκου μπορεί να ανιχνεύσει το δίσκο που έχει αστοχήσει. Συνεπώς ένας δίσκος ελέγχου για κάθε ομάδα δίσκων είναι αρκετός για την ανακατασκευή της πληροφορίας. Η αρχιτεκτονική RAID-3 επιπέδου προτάθηκε από τους Parker και Balasubramaniam ενώ η αρχιτεκτονική RAID-4 προτάθηκε από τους Salem και Garcia Mollina. Η αρχιτεκτονική RAID-5 προτάθηκε από τους Patterson et al. και σε αυτό το σχήμα η πληροφορία ισοτιμίας είναι διασκορπισμένη σε όλους τους δίσκους που ανήκουν σε μια ομάδα (εναλλασσόμενη ισοτιμία). Το σχήμα αυτό είναι πιο αποτελεσματικό καθώς επιτρέπει βελτιωμένες αποδόσεις κατά την ανάγνωση και εγγραφή στο δίσκο. Σε επίπεδο αξιοπιστίας οι αρχιτεκτονικές RAID-3, RAID-4, RAID-5 είναι ισότιμες καθώς απαιτούν το ίδιο πλήθος δίσκων ανά ομάδα [MT93].

Οι παρατάξεις δίσκων RAID -3,4,5 βασίζονται στην δυνατότητα του ελεγκτή του δίσκου να προβλέπει σωστά αστοχίες δίσκων πριν συμβούν. Σε ορισμένες υλοποιήσεις γίνεται χρήση αυτής της ιδιότητας ώστε να προλαμβάνονται απώλειες δεδομένων και για την μείωση του χρόνου ανακατασκευής των δεδομένων. Υποθέτουμε ότι δεν υπάρχουν απώλειες δεδομένων σε περιπτώσεις σωστή πρόβλεψης των αστοχιών. Επιπλέον υποθέτουμε ότι υπάρχει ηλεκτρονική ενεργοποίηση του εφεδρικού δίσκου και τα δεδομένα αντιγράφονται στον εφεδρικό δίσκο πριν απενεργοποιηθεί ο δίσκος που πρόκειται να αστοχήσει. Ωστόσο ο ελεγκτής δίσκων μπορεί να μην προβλέπει πάντα σωστά μια αστοχία. Για παράδειγμα αστοχίες που προέρχονται από ακάλυπτα σφάλματα δεν είναι προβλέψιμες. Με πιθανότητα $1 - a$ μια επικείμενη αστοχία που οφείλεται σε ένα σφάλμα που έχει καλυφθεί δεν είναι προβλέψιμη. Επίσης υπάρχει η πιθανότητα λαθεμένης πρόβλεψης από τον ελεγκτή δίσκων. Η περίπτωση αυτή αντιμετωπίζεται σαν ορθή πρόβλεψη αστοχίας από το σύστημα καθώς όπως αναφέραμε θεωρούμε ότι υπάρχει απεριόριστο πλήθος από εφεδρικούς δίσκους. Ωστόσο σε περίπτωση που οι διαθέσιμοι εφεδρικοί δίσκοι είναι πεπερασμένοι η επιρροή λαθεμένων προβλέψεων είναι σημαντική και έχει επίδραση στην αξιοπιστία της παράταξης των δίσκων. Θεωρούμε ότι ο χρόνος μέχρι την επόμενη λαθεμένη πρόβλεψη είναι εκθετικά κατανομημένος με ρυθμό γ .

4.8.3 Γενικό μοντέλο αξιοπιστίας

Με βάση της παραπάνω υποθέσεις το μοντέλο αξιοπιστίας που θα κατασκευάσουμε για τις αρχιτεκτονικές RAID-3,4,5 είναι ιεραρχικό δυο επιπέδων. Η γενική αξιοπιστία των παρατάξεων των δίσκων μοντελοποιείται από ένα διάγραμμα μπλοκ αξιοπιστίας (RBD) που φαίνεται στην Εικόνα 28.

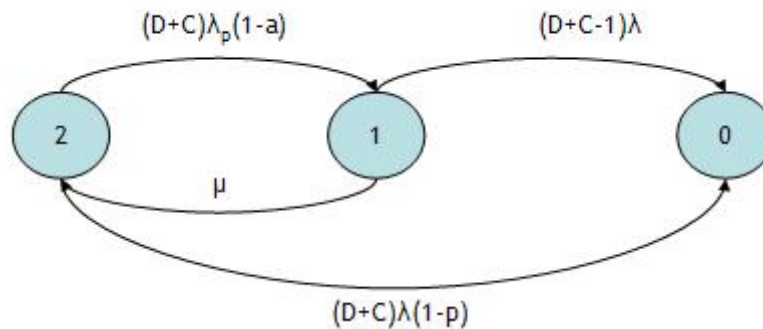


Εικόνα 28 Διάγραμμα μπλοκ αξιοπιστίας για RAID

Κάθε μπλοκ αναπαριστά μια ομάδα δίσκων. Υποθέτουμε ότι οι ομάδες δίσκων που συμμετέχουν στην παράταξη των δίσκων λειτουργούν ανεξάρτητα μεταξύ τους. Αν $R_i(t)$ είναι η αξιοπιστία μιας ομάδας δίσκων η αξιοπιστία ολόκληρης της παράτασης δίσκων δίνεται από την σχέση:

$$R_{da}(t) = \prod_{i=1}^N R_i(t)$$

Για τον υπολογισμό της αξιοπιστίας μια ομάδας δίσκων θα χρησιμοποιηθεί το απλό μοντέλο Markov που φαίνεται στην Εικόνα 29.



Εικόνα 29. Μοντέλο αξιοπιστίας Markov για μια ομάδα δίσκων που περιλαμβάνει πρόβλεψη αστοχιών (RAID -3,4,5) [MT93]

Στην κατάσταση 2 όλοι οι δίσκοι της ομάδας λειτουργούν κανονικά. Μετά που θα συμβεί μια αστοχία δίσκου μεταβαίνουμε στην κατάσταση 1 όπου αρχικοποιείται η ανακατασκευή των δεδομένων. Αν πριν την ολοκλήρωση της ανακατασκευής των δεδομένων συμβεί μια δεύτερη αστοχία στην ομάδα έχουμε απώλεια των δεδομένων και η παράταξη δίσκων θεωρείται ότι έχει αστοχήσει. Η κατάσταση 0 αντιστοιχεί στην αστοχία της ομάδας των δίσκων. Από την κατάσταση 2 μεταβαίνουμε απευθείας στην κατάσταση 0 σε περίπτωση που συμβεί ένα

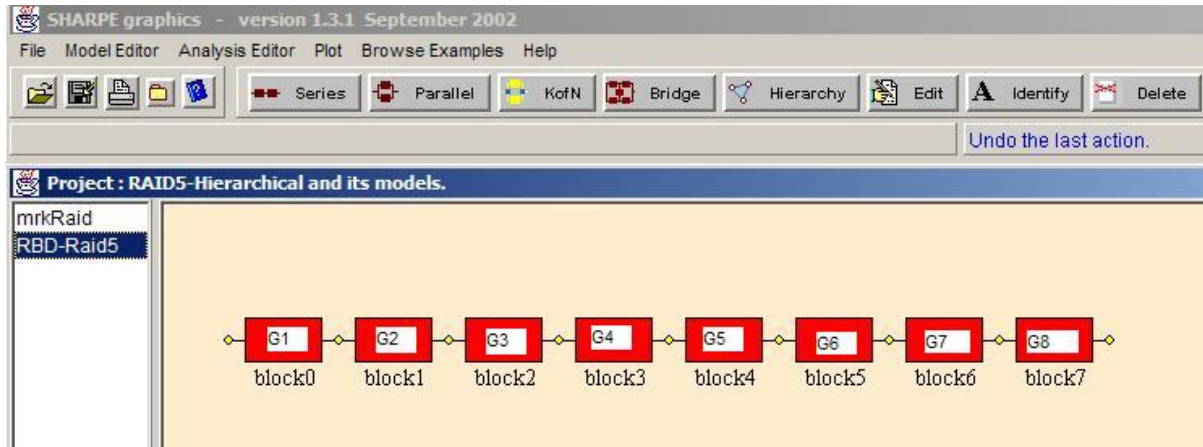
σφάλμα που δεν έχει καλυφθεί με πιθανότητα $1 - p$ (υπενθυμίζουμε ότι p είναι η πιθανότητα κάλυψης ενός σφάλματος)

Η αξιοπιστία και ο μέσος χρόνος μέχρι την απώλεια δεδομένων για τις διαφορετικές RAID αρχιτεκτονικές λαμβάνονται με αντικαταστάσεις στις ακόλουθες τιμές: για RAID-1 $a = 0, D = C = 1$, για RAID-2 $a = 0, C \geq \log_2(C + D + 1)$, για RAID-3,4,5 $C = 1$.

4.8.4 Σχεδίαση ιεραρχικού μοντέλου αξιοπιστίας RAID 3,4,5 με περιορισμένο πλήθος εφεδρικών δίσκων (cold & hot spares)

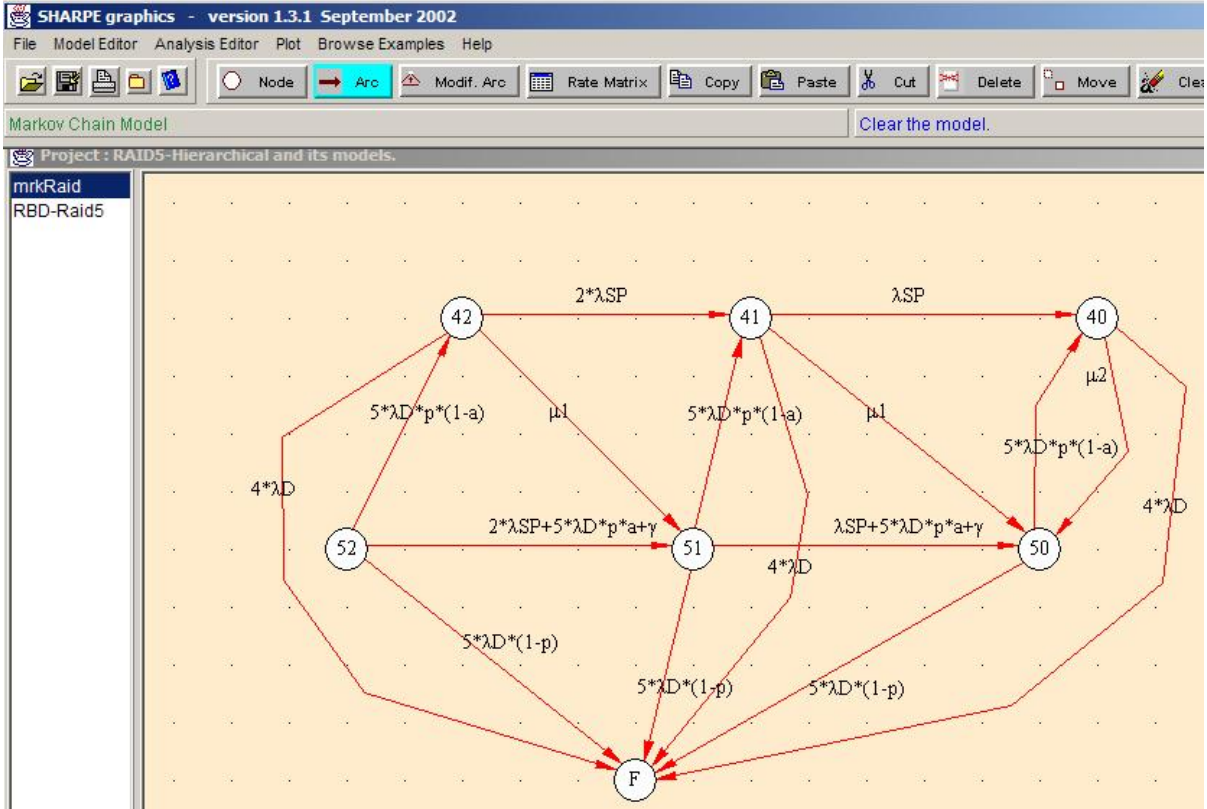
Στην αρχική προσέγγιση θεωρήσαμε ότι το πλήθος των εφεδρικών δίσκων των RAID αρχιτεκτονικών είναι απεριόριστος. Στη πραγματικότητα υπάρχει ένα πεπερασμένο πλήθος από εφεδρικούς δίσκους που διατηρεί το σύστημα. Οι εφεδρικοί δίσκοι μπορεί να είναι “cold” ή “hot”. Οι “hot” εφεδρικοί δίσκοι είναι δυνατόν να αστοχήσουν ακόμα και όταν δεν είναι σε ενεργή χρήση. Για τους “cold” εφεδρικούς δίσκους ισχύει ότι δεν αστοχούν μέχρι να ενεργοποιηθούν κατά την αντικατάσταση ενός δίσκου που έχει αστοχήσει. Ωστόσο οι “hot” εφεδρικοί δίσκοι ενεργοποιούνται ηλεκτρονικά μετά την αστοχία ενός δίσκου και ο χρόνος για την ενεργοποίησή τους είναι αμελητέος σε αντίθεση με του “cold” εφεδρικούς δίσκους που πρέπει να εγκατασταθούν από το προσωπικό που είναι υπεύθυνο για τις επισκευές με αποτέλεσμα να αυξάνεται ο ολικός χρόνος επισκευής.

Για την μελέτη της αξιοπιστίας RAID αρχιτεκτονικών επιπέδου 3,4,5 θα κατασκευάσουμε ένα βασικό μοντέλο που αποτελείται από 8 ομάδες δίσκων που καθεμία αποτελείται από 4 δίσκους δεδομένων και 1 δίσκο ελέγχου. Θα επιλέξουμε αρχικά $M = 2$ “hot” εφεδρικούς δίσκους για κάθε ομάδα δίσκων. Όπως προκύπτει από την μελέτη των [MT93] η αύξηση του μέσου χρόνου μέχρι την αστοχία του RAID δεν είναι σημαντική για πλήθος εφεδρικών δίσκων $M > 2$ ανά ομάδα δίσκων.



Εικόνα 30. Διάγραμμα μπλοκ αξιοπιστίας για τις 8 ομάδες δίσκων της RAID αρχιτεκτονικής

Το ιεραρχικό μοντέλο που αναπτύχθηκε στο SHARPE για την αρχιτεκτονική που μόλις περιγράψαμε υπάρχει στην Εικόνα 30 και στην Εικόνα 31. Στο πρώτο επίπεδο μοντελοποιείται με ένα διάγραμμα μπλοκ αξιοπιστίας όπου κάθε μπλοκ αναπαριστά μια ομάδα δίσκων του RAID που είναι συνδεδεμένες σε σειρά καθώς όπως αναφέραμε η αστοχία μιας ομάδας δίσκων συνεπάγεται ταυτόχρονα την αστοχία όλου του RAID καθώς έχουμε χάσει δεδομένα. Το δεύτερο επίπεδο του μοντέλου περιγράφεται από ένα γενικότερο μοντέλο Markov που περιλαμβάνει και τους εφεδρικούς δίσκους (Εικόνα 31).



Εικόνα 31. Μοντέλο αξιοπιστίας Markov για αρχιτεκτονική RAID-3,4,5 με M=2 “hot” εφεδρικούς δίσκους

Κάθε κατάσταση του μοντέλου Markov για την αξιοπιστία μιας ομάδας δίσκων της RAID αρχιτεκτονικής, είναι ένα ζεύγος (i,j) όπου i είναι ο πλήθος των ενεργών δίσκων (με λειτουργικά δεδομένα και οι δίσκοι ελέγχου) και j είναι το πλήθος των υπολειπόμενων εφεδρικών δίσκων. Η κατάσταση F αντιστοιχεί στην κατάσταση αστοχίας της ομάδας δίσκων. Στο γενικό μοντέλο έχουμε $G = D + C$ που αντιστοιχεί στο πλήθος των ενεργών δίσκων. Οι μεταβάσεις αντιστοιχούν σε αστοχίες των ενεργών δίσκων που καλύπτονται (με πιθανότητα p) και δεν προβλέπονται (με πιθανότητα $1-a$) και δίνονται από το γενικό τύπο $\lambda_i = (D + C)\lambda_d p(1-a)$ όπου λ_d είναι ο ρυθμός αστοχίας ενός δίσκου που είναι σε ενεργή χρήση. Τέτοιες μεταβάσεις υπάρχουν στο μοντέλο μεταξύ των εξής καταστάσεων $\{(5,2) \rightarrow (4,2)\} \{(5,1) \rightarrow (4,1)\} \{(5,0) \rightarrow (4,0)\}$.

Στις καταστάσεις όπου έχει ήδη αστοχήσει ένας δίσκος υπάρχει περίπτωση πριν

ολοκληρωθεί η ανακατασκευή των δεδομένων να συμβεί μια δεύτερη αστοχία. Οι μεταβάσεις αυτές δίνονται από το γενικό τύπο $\lambda_d = (D + C - 1)\lambda_d$ και οδηγούν στην αστοχία της ομάδας δίσκων. Τέτοιες μεταβάσεις υπάρχουν στο μοντέλο μεταξύ των εξής καταστάσεων $\{(4,2) \rightarrow F\}$, $\{(4,1) \rightarrow F\}$, $\{(4,0) \rightarrow F\}$.

Αστοχίες μπορεί να συμβούν και στους “hot” εφεδρικούς δίσκους με ρυθμό λ_{sp} που πολλαπλασιάζεται αντίστοιχα με το πλήθος των εφεδρικών δίσκων. Τέτοιες μεταβάσεις υπάρχουν στο μοντέλο μεταξύ των εξής καταστάσεων $\{(4,2) \rightarrow (4,1)\}$, $\{(4,1) \rightarrow (4,0)\}$.

Τέλος στο μοντέλο υπάρχουν μεταβάσεις μεταξύ καταστάσεων σε περιπτώσεις κατά τις οποίες είτε αστοχεί ένα εφεδρικός δίσκος, είτε προβλέπεται ορθώς μια αστοχία (με πιθανότητα a) ή σε περιπτώσεις που γίνεται μια λαθεμένη πρόβλεψη (με ρυθμό γ). Στις περιπτώσεις ορθής ή λαθεμένης πρόβλεψης για αστοχία, ο χρόνος ανακατασκευής των δεδομένων είναι αμελητέος καθώς οι εφεδρικές μονάδες είναι εγκατεστημένες ήδη και τα δεδομένα ανακατασκευάζονται από το δίσκο που πρόκειται να αστοχήσει. Οι περιπτώσεις αυτές αντιστοιχούν σε μεταβάσεις στο μοντέλο που οδηγούν απλά σε μείωση του αριθμού των υπολειπόμενων εφεδρικών μονάδων. Ο ρυθμός μεταξύ αυτών των μεταβάσεων δίνονται από το γενικό τύπο $\lambda_{s,i} = i\lambda_{sp} + (D + C)\lambda_d pa + \gamma$. Τέτοιες μεταβάσεις υπάρχουν στο μοντέλο στην Εικόνα 31 μεταξύ των καταστάσεων $\{(5,2) \rightarrow (5,1)\}$, $\{(5,1) \rightarrow (5,0)\}$.

Ο ρυθμός επισκευής ενός δίσκου με την βοήθεια “hot” εφεδρικού δίσκου είναι μ_1 , ενώ στην κατάσταση (5,0) ο ρυθμός επισκευής είναι μ_2 και ισχύει $\mu_2 < \mu_1$, καθώς η επισκευή γίνεται σε εφεδρικό δίσκο που πρέπει να εγκατασταθεί πριν ξεκινήσει η ανακατασκευή των δεδομένων. Το γενικό μοντέλο αξιοπιστίας για μια ομάδα δίσκων με M εφεδρικούς δίσκους υπάρχει στο [MT93].

4.8.5 Ενδεικτικά αριθμητικά αποτελέσματα

Για την μελέτη της αξιοπιστίας της RAID αρχιτεκτονικής θα χρησιμοποιήσουμε μια σειρά από αριθμητικές τιμές για τις παραμέτρους του μοντέλου που βασίζονται στην μελέτη [MT93] και υπάρχουν στο Πίνακας 12.

Τιμές παραμέτρων (σε ώρες)	
Μέσος χρόνος μέχρι την αστοχία του δίσκου $MTTF_{disk} = 1/\lambda_d$	40.000 ώρες ($\lambda_d = 0.000025$)
Μέσος χρόνος ανακατασκευής δεδομένων σε "hot" εφεδρικό δίσκο $MTTR_1 = 1/\mu_1$	2 ώρες ($\mu_1 = 0.5$)
Μέσος χρόνος ανακατασκευής δεδομένων ενός δίσκου σε "cold" εφεδρικό δίσκο $MTTR_2 = 1/\mu_2$	50 ώρες ($\mu_2 = 0.02$)
Μέσος χρόνος μέχρι την αστοχία ενός "hot" εφεδρικού δίσκου $MTTF_{sp} = 1/\lambda_{sp}$	50.000 ώρες ($\lambda_{sp} = 0.00002$)
Πιθανότητα κάλυψης σφαλμάτων c	0.9
Ρυθμός λαθεμένων προβλέψεων αστοχίας δίσκου	$\gamma = 1/100000$
Πιθανότητα ορθής πρόβλεψης μια επικείμενης αστοχίας ενός ενεργού δίσκου a	0.9
Αριθμητικά αποτελέσματα	

Μέσος χρόνος αστοχίας RAID	$MTTF = 1,14$ χρόνια
----------------------------	----------------------

Πίνακας 12: Τιμές παραμέτρων για το μοντέλο αξιοπιστίας RAID

Να σημειώσουμε ότι το αριθμητικό αποτέλεσμα για το μέσο χρόνο αστοχίας του RAID μεταβάλλεται σημαντικά συναρτήσει των μεταβολών στην πιθανότητα κάλυψης του σφάλματος.

ΚΕΦΑΛΑΙΟ 5

Επίλογος και μελλοντική εργασία

5.1 Επίλογος

Η ψηφιακή πληροφορία σχηματίζει όλο και περισσότερο ένα μεγάλο μέρος της πολιτιστικής και πνευματικής μας κληρονομιάς και προσφέρει σημαντικά πλεονεκτήματα στους χρήστες. Η χρήση των υπολογιστών αλλάζει για πάντα τον τρόπο με τον οποίο η πληροφορία δημιουργείται, διαχειρίζεται και είναι προσβάσιμη. Η δυνατότητα δημιουργίας, εύκολης τροποποίησης και αντιγραφής πληροφορίας σε ψηφιακή μορφή, αναζήτησης κειμένων και βάσεων δεδομένων, μετάδοσης πληροφορίας παγκοσμίως μέσω των δικτύων, έχει οδηγήσει σε δραματική αύξηση την εφαρμογή ψηφιακών τεχνολογιών. Παρόλα τα σπουδαία αυτά πλεονεκτήματα, η ψηφιακή πληροφορία είναι συνυφασμένη με την τεράστια ευθραυστότητα αυτού του μέσου στην διάρκεια του χρόνου σε σύγκριση με παραδοσιακά μέσα όπως το χαρτί. Η απώλεια δεδομένων λόγω φτωχής διαχείρισης των ψηφιακών δεδομένων αποτελεί σήμερα μια σημαντική πρόκληση για οργανισμούς όπως ψηφιακές βιβλιοθήκες και μουσεία που έχουν ως βασική αποστολή τους την διατήρηση της πολιτιστικής και πνευματικής κληρονομιάς που υπάρχει σε ψηφιακή μορφή για μεγάλα χρονικά διαστήματα [BG01].

Μια σειρά από αποφάσεις εμπλέκονται στον τρόπο αποθήκευσης των ψηφιακών δεδομένων. Η παρούσα μεταπτυχιακή εργασία αναφέρθηκε στο πρόβλημα αποθήκευσης των ψηφιακών δεδομένων εξετάζοντας μια σειρά από διατάξεις συστημάτων ως προς την αξιοπιστία και την ασφάλεια που μπορεί να

προσφέρουν από αστοχίες και απώλειες. Χρησιμοποιήθηκαν μια σειρά από αναλυτικές τεχνικές μοντελοποίησης τέτοιων διατάξεων με σκοπό την υποστήριξη αποφάσεων όπως το πλήθος των αντιγράφων που είναι απαραίτητο να υπάρχουν για κάθε ψηφιακό έγγραφο, το είδος και την αξιοπιστία των αποθηκευτικών μέσων, την συχνότητα με την οποία απαιτείται να ελέγχονται οι διατάξεις για τυχόν σφάλματα, την επιρροή που μπορεί να έχουν σε τέτοιες διατάξεις γεγονότα που μπορεί να καταστρέψουν μαζικά ψηφιακή πληροφορία (όπως για παράδειγμα εκδήλωση πυρκαγιάς στους χώρους φύλαξης ψηφιακών δεδομένων). Η επιλογή αναλυτικών μοντέλων επέτρεψε την εκτέλεση αναλύσεων ευαισθησίας για την εξέταση των επιρροών που μπορεί να έχουν οι παράμετροι εισόδου των μοντέλων στην αξιοπιστία τέτοιων διατάξεων. Οι αναλύσεις αυτές βοήθησαν στην ανάδειξη σημαντικών παραγόντων που επηρεάζουν σε μεγάλο βαθμό την αξιοπιστία και λειτουργούν καθοδηγητικά στην λήψη πολιτικών αποφάσεων από οργανισμούς όπως για παράδειγμα φύλαξη των φορέων πληροφορίας σε διαφορετικούς φυσικούς χώρους ή ακόμα και διαφορετικές γεωγραφικές τοποθεσίες.

5.2 Μελλοντική εργασία

Μια σημαντική επέκταση της παρούσας εργασίας αποτελεί η μελέτη του κόστους που εμπλέκεται στην σχεδίαση και διαχείριση των προτεινόμενων διατάξεων συστημάτων για ψηφιακή διατήρηση [RW00, A00]. Ο παράγοντας κόστος σε συνδυασμό με την αξιοπιστία αποτελούν τους βασικούς άξονες τόσο στην σχεδίαση στρατηγικών όσο και στην λήψη πολιτικών αποφάσεων σε οργανισμούς που ενδιαφέρονται για την μακροχρόνια διατήρηση των δεδομένων τους. Ένα δεύτερο σκέλος επέκτασης της παρούσας μελέτης αποτελεί η μελέτη του προβλήματος περιοδικής αντικατάστασης των μονάδων αποθήκευσης [CT02, AF03] που αποτελεί μια σημαντική δραστηριότητα στα πλαίσια υποστήριξης των διατάξεων για την αποφυγή σφαλμάτων και απώλειας ψηφιακών δεδομένων. Το πρόβλημα εδώ επικεντρώνεται στην εύρεση βέλτιστων

στρατηγικών για τον καθορισμό της ηλικίας αντικατάστασης των μονάδων αποθήκευσης με σκοπό ταυτόχρονα μεγιστοποίησης της αξιοπιστίας και ελαχιστοποίησης του μέσου κόστους για κάθε κύκλο αντικατάστασης.

Παρακάτω παραθέτουμε μια σύντομη ανασκόπηση των πηγών κόστους που εμπλέκονται στην σχεδίαση διατάξεων για ψηφιακή διατήρηση και πρέπει να ληφθούν υπόψη στην ανάπτυξη μαθηματικών μοντέλων για την οικονομική αποτίμηση κάθε προτεινόμενης σχεδίασης [CM01].

Υλικό και λογισμικό: Η κατηγορία αυτή περιλαμβάνει δαπάνες για την αγορά υπολογιστών, δίσκων, περιφερειακών μονάδων, δικτύου και απαραίτητο λογισμικό. Ένα παράγοντα δυσκολίας στον υπολογισμό των δαπανών που απαιτούνται για την αγορά εξοπλισμού αποτελεί η ανάγκη πρόβλεψης μελλοντικών τιμών για αντικατάσταση υλικού και λογισμικού. Προβλέψεις τέτοιας μορφής μπορεί να γίνουν με την βοήθεια κατανομών πιθανοτήτων που βασίζονται στις τρέχουσες τάσεις της αγοράς. Έτσι για παράδειγμα μπορεί να προβλεφθεί ότι σε 10 χρόνια από τώρα οι τιμές των δίσκων θα στοιχίζουν 10€ (ή 15€) φθηνότερα ανά terabyte με πιθανότητα 60% 15€ φθηνότερα ανά terabyte με πιθανότητα 80%, και 50€ φθηνότερα ανά terabyte με πιθανότητα 99%. Από τα παραπάνω γίνεται φανερό ότι μπορούμε να ορίσουμε ένα μέγιστο και ένα ελάχιστο όριο στις προβλεπόμενες τιμές με βάση τρέχουσα τεχνολογία και τις επικρατούσες τάσεις τις αγοράς.

Δαπάνες εργασίας: Οι δαπάνες εργασίες αποτελούν τα μεγαλύτερα έξοδα στην διατήρηση των υπό μελέτη συστημάτων. Οι δαπάνες εργασίες κυμαίνονται ανάλογα με το μέσο χρόνο μεταξύ των αστοχιών ενός συστήματος, το μέσο χρόνο διόρθωσης ή αντικατάστασης εξοπλισμού, τα διαστήματα προληπτικής διατήρησης που προβλέπονται για τον εξοπλισμό, το μέσο χρόνο που απαιτείται για την εκτέλεση της προληπτική διατήρηση, χρόνο μετακίνησης συνεργείων, το μέσο κόστος εργασιών. Επίσης στις δαπάνες εργασίες συγκαταλέγονται αναβαθμίσεις του συστήματος σε πιο σύγχρονες τεχνολογίες, που μπορεί να

οδηγήσουν και σε μείωση του ετησίου κόστους καθώς για παράδειγμα η χρήση πιο σύγχρονων δίσκων μπορεί να συνεπάγεται μείωση του κόστους διαχείρισης, λιγότερες απαιτήσεις σε φυσικό χώρο και ηλεκτρικό ρεύμα κ.λ.π. Το ύψος των δαπανών εργασίας εξαρτάται από τον τρόπο λειτουργίας του οργανισμού καθώς η υποστήριξη του συστήματος μπορεί να γίνεται είτε με μόνιμο προσωπικό είτε να εκτελείται από εξωτερικά συνεργεία με μίσθωση υπηρεσιών ανά ώρα.

Ένας πολύ απλός και γενικός τύπος υπολογισμού των ετησίων δαπανών για εργασίες σε ένα υπολογιστικό σύστημα είναι [SS98]:

$$ALE = (CPH)(8760)\left(\frac{MTTR + TTR}{MTBF} + \frac{MTPM + TTPM}{MTBP}\right)$$

όπου **ALE** = ετήσια δαπάνη σε εργασίες, **CPH** = κόστος εργασιών ανά ώρα, **8760** = πλήθος ωρών ανά έτος, **MTTR** = μέσος χρόνος επισκευής, **TTR**= χρόνος μετακίνησης ανά εργασίες επισκευής, **MTBF**= μέσος χρόνος μεταξύ αστοχιών, **MTPM**= μέσος χρόνος για την εκτέλεση εργασιών διατήρησης, **TTPM**= χρόνος μετακίνησης εργασιών προληπτικής διατήρησης, **MTBP**=μέσος χρόνος μεταξύ εργασιών προληπτικής διατήρησης. Ο όρος μέσος χρόνος μεταξύ αστοχιών (MTBF) συχνά συγχέεται με τον όρο μέσος χρόνος μέχρι την αστοχία μας συνιστώσας (MTTF). Ουσιαστικά ο MTBF αναφέρεται στο μέσο χρόνο ανάμεσα σε δυο διαδοχικές αστοχίες ενός συστήματος που επιδέχεται επισκευή. Η πιο απλή προσέγγιση για το MTBF είναι: $MTBF = MTTF + MTTR$

Δαπάνες λειτουργίας υπολογιστικού συστήματος: Στην κατηγορία αυτή συγκαταλέγονται έξοδα για την υποστήριξη του συστήματος διάταξης. Για παράδειγμα στα έξοδα συμπεριλαμβάνεται το ηλεκτρικό ρεύμα που απαιτείται για την λειτουργία του συστήματος, το κλιματισμό του χώρου καθώς και ενοικίαση φυσικού χώρου αν αυτό απαιτείται.

Μη-διαθεσιμότητα του συστήματος: Οικονομικές επιπτώσεις μπορεί να προκληθούν από την μη διαθεσιμότητα του συστήματος είτε λόγω εργασιών

επισκευής είτε λόγω προληπτικής διατήρησης. Έτσι για παράδειγμα αν ο οργανισμός έχει άμεσα οικονομικά κέρδη από την λειτουργία του συστήματος, η μη διαθεσιμότητα του συστήματος μπορεί να μεταφραστεί σε κόστος.

Ασφάλιση: Κόστος ασφάλισης μπορεί να προκύψει σε περιπτώσεις σύλληψης συμβάσεων με τρίτα πρόσωπα που αναλαμβάνουν συγκεκριμένες υποχρεώσεις όπως για παράδειγμα τυχόν επισκευές αστοχιών σε δίσκους ή εργασίες διατήρησης που μπορεί να προκύψουν στην διάταξη με αντίτιμο σταθερής αμοιβής ετησίως.

Κόστος απώλειας εγγράφων: Σε αρκετές περιπτώσεις η αναπόφευκτη απώλεια ψηφιακών εγγράφων που μπορεί να συμβεί σε μια διάταξη για ψηφιακή διατήρηση μπορεί να συνοδεύεται από οικονομικές επιπτώσεις. Για παράδειγμα η απώλεια ενός σπάνιου ψηφιακού εγγράφου.

Βιβλιογραφία

- [A00] Satoshi Asami, Reducing the Cost of System Administration of a Disk Storage System from Commodity Components, Report No. UCB/CSD-00-1100, University of California, Berkley, May 2000
- [AES28-1997] AES Standard for audio preservation and restoration-Method for estimating life expectancy of compact discs (CD-ROM), based on effects of temperature and relative humidity
- [AF03] Suprasad Amari, Wes Fuldon, Bounds of Optimal Replacement Time of Age Replacement Policy, 2003 IEEE.
- [BG01] Neil Beagrie and Daniel Greenstein. A strategic policy framework for creating and preserving digital collections. Arts and Humanities Data Service Executive, King's College London, Version 5.0, July 2001
- [B95] John Van Bogart, Magnetic Tape Storage and Handling, A Guide for Libraries and Archives, National Media Laboratory, June 1995
- [CL02] P.L.Clemens, Fault Tree Analysis, February 2000, 4th Edition
- [CPA-RLG96] Preserving Digital Information: Report on the Task Force on Archiving of Digital Information (1996)
- [CLG+93] Peter M.Chen, Edward K.Lee, Garth A.Gibson, Randy H.Katz, David A.Patterson. *RAID: High-Performance, Reliable Secondary Storage*. Submitted to ACM Computing Surveys, October 1993
- [C03] Arturo Crespo, *Archival Repositories for Digital Libraries*, PhD Dissertation, University of Stanford, March 2003
- [CM01] Arturo Crespo and Hector Garcia Mollina. Cost-Driven Design for Archival Repositories. Computer Science Department Stanford University, CA 94305-2140, USA
- [CT02] Dongyan Chen and Kishor S.Trivedi, Analysis of Periodic Preventive Maintenance with General System Failure Distribution, Duke University, Durham, NC27708-0294, USA
- [DPC] Digital Preservation Coalition, HANDBOOK,
<http://www.dpconline.org>

- [DPGN03] Adrian Brown, Digital Preservation Guidance Note 3: Care, handling, and storage of removable media, June 2003
- [GP92] Gibson, G.A and Patterson, D.A. Designing disk arrays for high data reliability. Tech.Rep CMU-CS-92-130, Carnie Mellon University, April 1992.
- [H01] Den Haag. Testbed Digital Bewaring Migration: Context and Current Status (2001)
- [H02] Den Haag. Digital Preservation Testbed. White Paper, XML and Digital Preservation (2002)
- [HFM+02] G.F Hughes, Fellow, J.F. Murray, Kreutz-Delgado *Senior Member*, and C. Elkan, Improved Disk Drive Failure Warnings, IEEE Transactions on Reliability, September 2002
- [HMT89] David I.Heimann, Nitin Mittal and Kishor S.Trivedi. Availability and Reliability Modeling for Computer Systems. In M.Yotis, editor, *Advances in Computer Systems*, volume 31, pages 176-233. Academic Press, San Diego, CA, 1990
- [HSZ+00] C.Hirel, R.Sahner, X.Zhang, K.Trivedi, Reliability and Performability Modeling using SHARPE 2000. Center for Advances Computing and Communication Department of Electrical and Computer Engineering Duke University, Durham.
- [L85] J.C.Laprie. Dependable computing and fault-tolerance: Concepts and Terminology. In *Proceedings of the Fifteen International Symposium on Fault-Tolerant Computing*, pages 2-7, Los Alamitos, CA, July 1985. IEEE Computer Society Press.
- [LKR+00] Gregory W.Lawrence, William R.Kehoe, Oya Y.Rieger, William H. Walters, Anne R. Kenney. Risk Management of Digital Information: A File Format Investigation (2000)
- [L01] Raymond A. Lorie. Long Term Preservation of Digital Information. *Joint Conference on Digital Libraries*, ACM/IEEE, June 2001
- [MT93] Manish Malhotra, Kishor S.Trivedi. Reliability Analysis of Redundant Arrays of Inexpensive Disks. *Journal of Parallel and Distributed Computing* 17, 146-151, Academic Press, 1993.
- [MFT00] Jogesh K.Muppala, Ricardo M.Fricks and Kishor S.Trivedi. Techniques for System Dependability Evaluation. *Computational Probability*, pp.445-480, Kluwer Academic Publisher, The

Netherlands, 2000

- [NML03] Koichi Sadashige, National Media Laboratory, Host to the National Technology Alliance. Data Storage Assessment – 2002 Projections through 2010. March 2003.
- [NPO] National Preservation Office Web Site,
<http://www.bl.uk/services/npo/npo.html>
- [NSF+] It's About Time: Research Challenges in Digital Archiving and Long-term Preservation, Final Report, Workshop on Research Challenges in Digital Archiving and Long-term Preservation, August 2003
- [PGK88] Patterson D.A, Gibson G and Katz R. A case for redundant array of inexpensive disks (RAID). *Proc of ACM SIGMOD*. Chicago, IL, June 1988.
- [RW00] Kelly Russell, Ellis Weinberger, Cost elements of digital preservation, draft on 31 May 2000.
- [ST92] Robin A.Sahner, Kishor S.Trivedi. SHARPE: Symbolic Hierarchical Automated Reliability and Performance Evaluator. Introduction and Guide for Users, February 1992.
- [T02] Kishor S.Trivedi. Probability and Statistics with Reliability, Queuing and Computer Science Applications, Wiley-Interscience Publication, 2002
- [T99] SHARPE Interface. User's Manual, Version 1.01, August 1999
- [STP93] Robin A. Sahner, Kishor S.Trivedi, Antonio Puliafito. Performance and Reliability Analysis of Computer Systems: *An Example-Based Approach Using the SHARPE Software Package*. Kluwer Academic Publisher, 1996
- [SS98] Siewierok Daniel, Robert Swarz, *Reliable Computer Systems: Design and Evaluation*. Third Edition, 1998
- [W99] S.Wolfram, *The Mathematica Book*, 4th ed., Wolfram Media/Cambridge Univ.Press, 1999
- Estimating Drive Reliability in Desktop Computers Consumer Electronic Systems, By Seagate Technology, <http://www.digit-life.com/articles/storagereliability/>