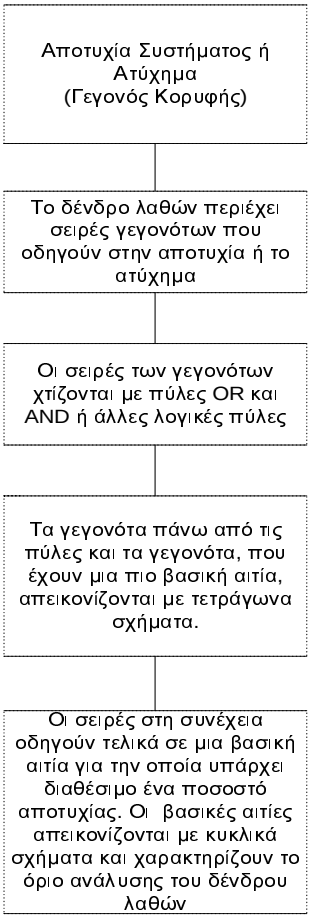
ΠΕΡΙΕΧΟΜΕΝΑ

1. Εισαγωγή

Τα δέντρα λαθών κατασκευάζονται και αναλύονται με σκοπό να μειωθεί η πιθανότητα αποτυχίας και οι επακόλουθες ανθρώπινες (π.χ. θάνατος, αρρώστια), οικονομικές (π.χ. απώλεια κεφαλαίου) και περιβαλλοντικές (π.χ. μόλυνση του αέρα,της θάλασσας) απώλειες της. Οι απώλειες αυτές προκύπτουν όταν ένα ή περισσότερα βασικά γεγονότα αποτυχίας δημιουργούν ένα σύστημα κινδύνου. Τέτοια βασικά γεγονότα είναι γεγονότα σχετικά με ανθρώπους (π.χ. λάθη στο χειρισμό,στη σχεδίαση, στη συντήρηση) γεγονότα σχετικά με το υλικό (π.χ. διαροή τοξικών από βαλβίδα) και γεγονότα σχετικά με το περιβάλλον (π.χ. σεισμοί, καταιγίδες, καθιζήσεις). Τα συστήματα κινδύνων συχνά προκαλούνται από ένα συνδυασμό τέτοιων γεγονότων. Η κατασκευή των δέντρων λαθών και η ανάλυσή τους, ποσοτική και ποιοτική βοηθάει στην αναγνώριση των σχέσεων μεταξύ των βασικών γεγονότων, που οδηγούν στην αποτυχία του συστήματος. Έτσι το σύστημα στη συνέχεια μπορεί να βελτιωθεί, να ξανασχεδιαστεί αν αυτό είναι απαραίτητο και να μειωθούν οι κίνδυνοι.

1.1 Η δομή των δέντρων λαθών

Η δομή ενός δέντρου λαθών φαίνεται στο Σχήμα 1.1:



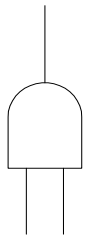
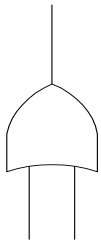
Σχήμα 1.1

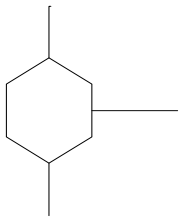
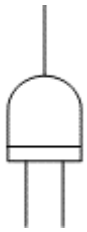
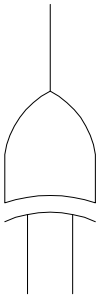
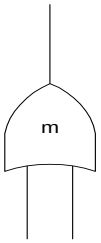
Το ανεπιθύμητο γεγονός εμφανίζεται στην κορυφή του δέντρου. Αμέσως παρακάτω υπάρχουν τα γεγονότα, που συνδυάζονται με λογικές πύλες AND, OR και άλλες, και οδηγούν στην αποτυχία του συστήματος,

Το μεγαλύτερο πλεονέκτημα των δέντρων λαθών έναντι άλλων τεχνικών είναι ότι η ανάλυση περιορίζεται μόνο στον προσδιορισμό των στοιχείων και των γεγονότων του συστήματος που οδηγούν στην ανεπιθύμητη αποτυχία ή στο ατύχημα. Απ' ότι όλα δείχνουν όμως στο μέλλον τα δέντρα λαθών θα αντικατασταθούν από τους πίνακες απόφασης, γιατί είναι περισσότερο ευπροσάρμοστοι. Τα δέντρα λαθών είναι λογικά Boolean διαγράμματα τα οποία δείχνουν μόνο μία κατάσταση επιτυχίας ή αποτυχίας (π.χ. σπάσιμο μιας βαλβίδας), ενώ οι πίνακες απόφασης μπορούν να δείχνουν περισσότερα από ένα συστατικά αποτυχίας. Επιπλέον τα δέντρα λαθών περιγράφουν τα συστήματα σε μια ορισμένη χρονική στιγμή και η ακολουθία των γεγονότων φαίνεται με δυσκολία, αντίθετα με τους πίνακες απόφασης, όπου η ακολουθία των γεγονότων αποτυχίας παρουσιάζεται με ακρίβεια. Τέλος, όσο μεγαλύτερα γίνονται τα δέντρα λαθών, τόσο δυσκολότερο είναι να βρεθούν τα λάθη και να ακολουθήσουμε τη λογική τους.

1.2 Σύμβολα πυλών

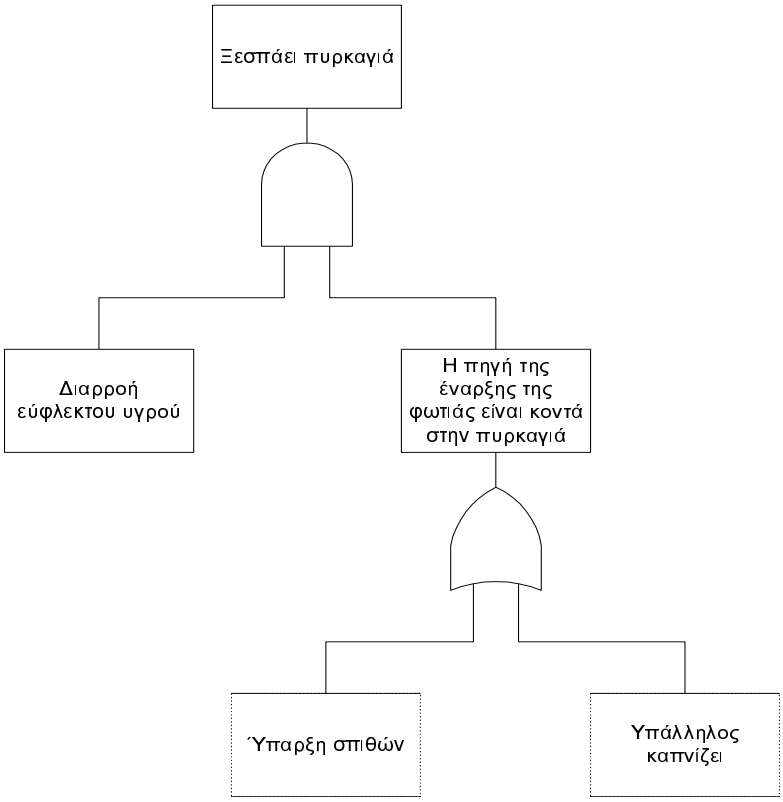
Όπως αναφέραμε παραπάνω τα γεγονότα συνδυάζονται με λογικές πύλες AND, OR και άλλες, και οδηγούν στην αποτυχία του συστήματος. Τα σύμβολα των πυλών αυτών φαίνονται στον Πίνακα 1.1:

	Σύμβολο Πύλης	Όνομα Πύλης	Περιγραφή Πύλης
1		Πύλη AND	Το αποτέλεσμα της πύλης συμβαίνει αν συμβούν όλα τα γεγονότα ταυτόχρονα
2		Πύλη OR	Το αποτέλεσμα της πύλης συμβαίνει αν συμβεί τουλάχιστον ένα γεγονός
3		Πύλη INHIBIT	Η είσοδος παράγει την έξοδο όταν ισχύει η συνθήκη

			
4		Πύλη Priority AND	Το αποτέλεσμα συμβαίνει όταν συμβούν στη σειρά που είναι τα γεγονότα της εισόδου από τα αριστερά προς τα δεξιά
5		Πύλη Exclusive OR	Το αποτέλεσμα της πύλης συμβαίνει όταν συμβαίνει ένα από τα γεγονότα εισόδου αλλά όχι και τα δύο
6		Πύλη m out of n	Το αποτέλεσμα της πύλης συμβαίνει όταν συμβούν τα m από τα n γεγονότα της εισόδου

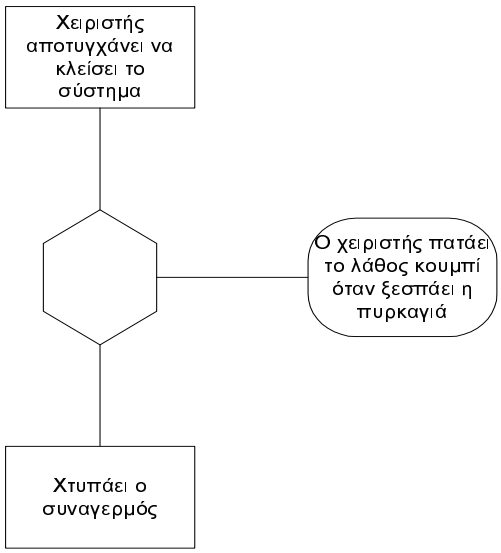
Πίνακας 1.1

Κάθε πύλη μπορεί να έχει μία οι περισσότερες εισόδους, αλλά μία μόνο έξοδο. Ένα γεγονός εξόδου σε μία πύλη **AND** προκύπτει όταν όλα τα γεγονότα εισόδου συμβαίνουν ταυτόχρονα. Ενώ ένα γεγονός εξόδου σε μία πύλη **OR** προκύπτει όταν ένα οποιοδήποτε γεγονός εισόδου συμβαίνει. Ένα παράδειγμα με πύλες **AND** και **OR** φαίνεται στο Σχήμα 1.2:



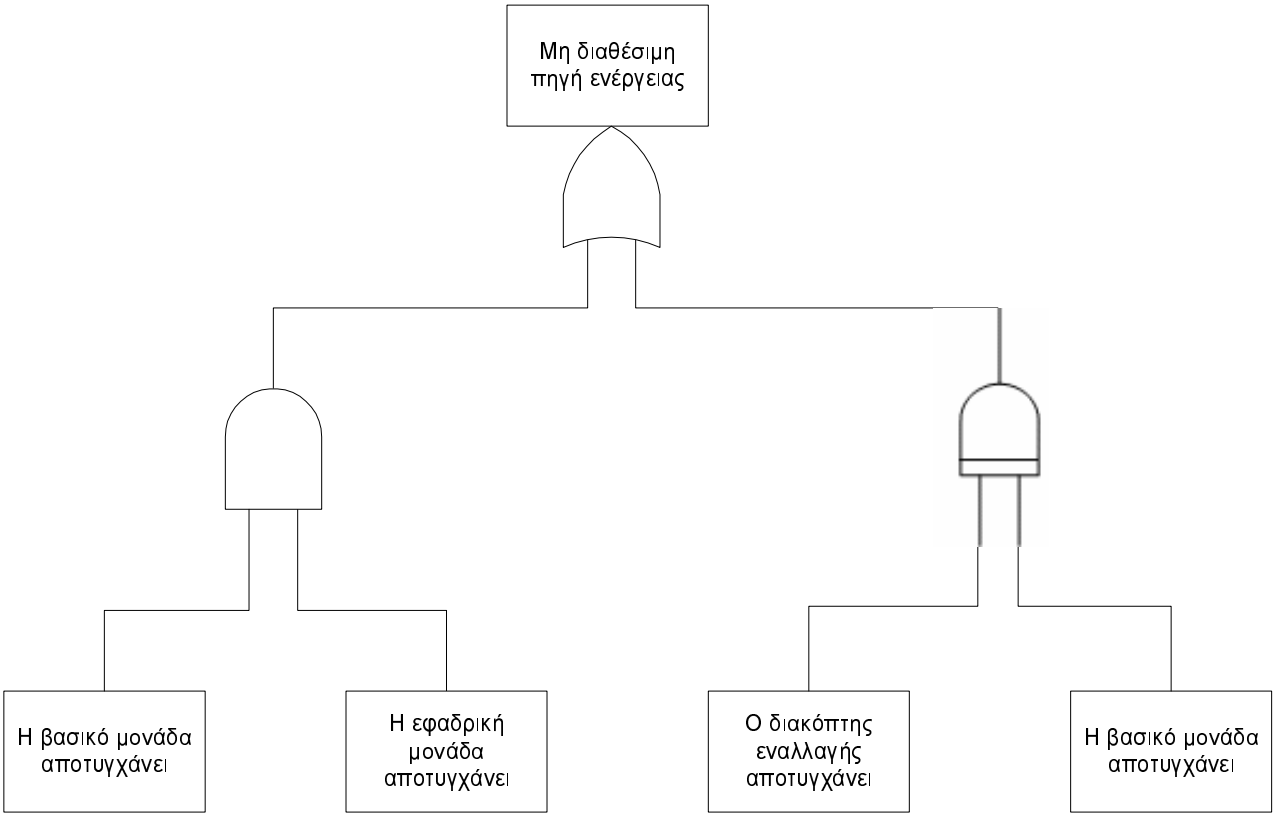
Σχήμα 1.2

Η **πύλη Inhibit**, ή αλλιώς εξάγωνο, χρησιμοποιείται για να αναπαραστήσει μία σχέση αιτίας-αποτελέσματος με πιθανότητα. Το γεγονός στον πάτο της πύλης ονομάζεται γεγονός εισόδου και το γεγονός στο πλάγιο μέρος της πύλης είναι το γεγονός υπό όρους. Το γεγονός εξόδου προκύπτει αν και το γεγονός εισόδου και το γεγονός υπό όρους συμβαίνουν ταυτόχρονα. Ένα παράδειγμα **πύλης Inhibit** φαίνεται στο Σχήμα 1.3:



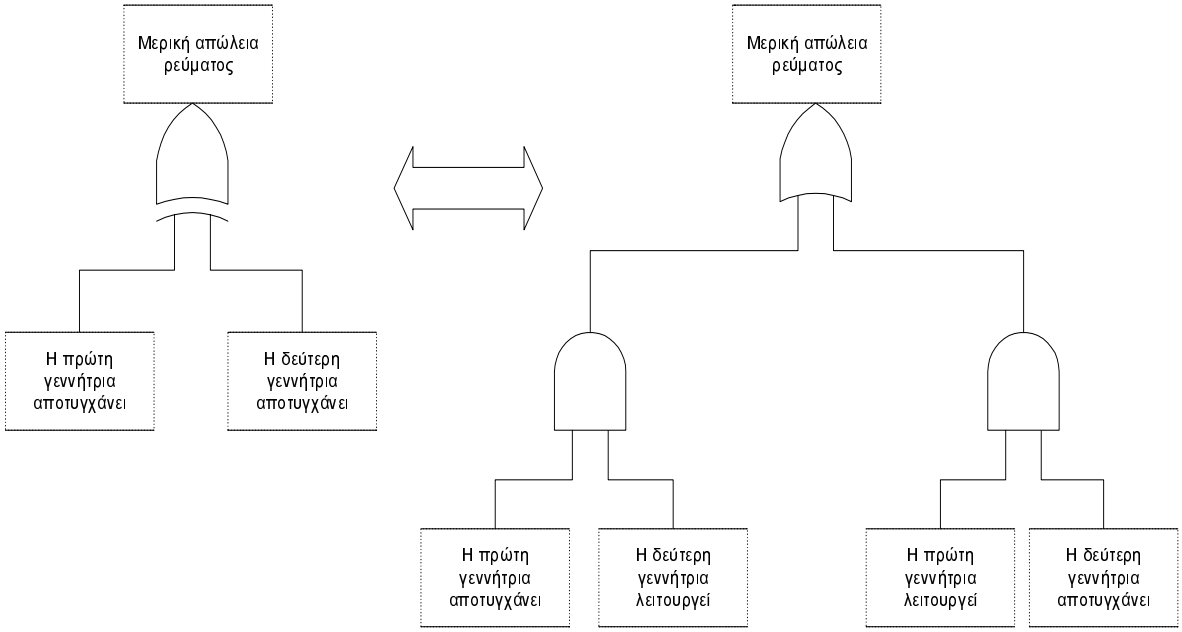
Σχήμα 1.3

Η πύλη **priority AND** είναι λογικά ισοδύναμη με την πύλη **AND** με επιπλέον απαίτηση τα γεγονότα εισόδου να συμβαίνουν με καθορισμένη σειρά. Το γεγονός εξόδου προκύπτει αν τα γεγονότα εισόδου συμβαίνουν με τη σειρά που εμφανίζονται από αριστερά προς τα δεξιά. Ένα παράδειγμα με χρήση της πύλης **priority AND** δείχνεται στο Σχήμα 1.4:



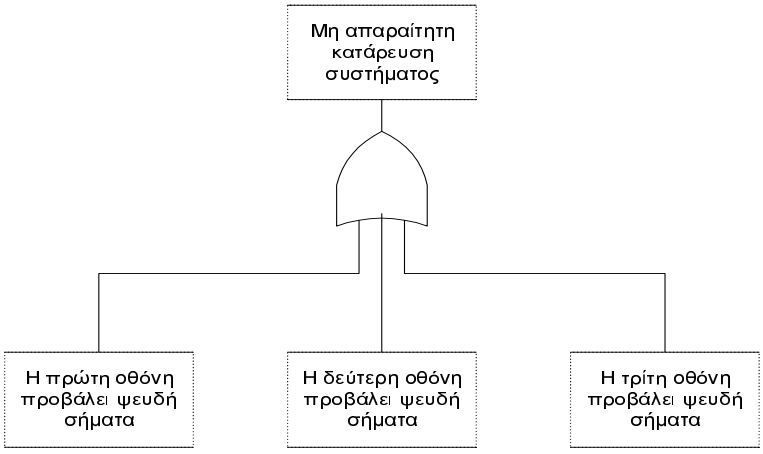
Σχήμα 1.4

Η πύλη **exclusive OR** περιγράφει μια κατάσταση όπου το γεγονός εξόδου προκύπτει όταν ένα, όχι και τα δύο, από τα γεγονότα εισόδου συμβαίνουν. Η πύλη **exclusive OR** μπορεί να αναπαρασταθεί ισοδύναμα με πύλες **AND** και **OR.** Ένα παράδειγμα φαίνεται στο Σχήμα 1.5:



Σχήμα 1.5

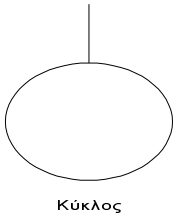
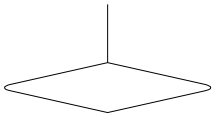
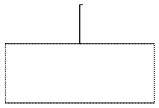
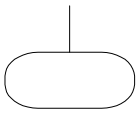
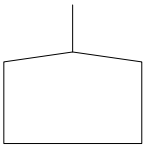
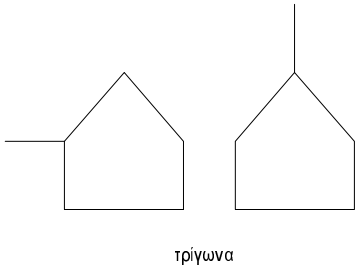
Η πύλη **m-out-of-n voting** έχει n γεγονότα εισόδου και το γεγονός εξόδου προκύπτει αν τουλάχιστον m από τα n γεγονότα εισόδου συμβαίνουν. Ένα παράδειγμα 2-out-of-3 πύλης μπορείτε να δείτε στο Σχήμα 1.6:



Σχήμα 1.6

1.3 Σύμβολα γεγονότων

Τα σύμβολα γεγονότων παρουσιάζονται στον πίνακα 1.2:

	Σύμβολο γεγονότος	Σημασία συμβόλων
1		Βασικό γεγονός με επαρκή στοιχεία
2		Μη αναπτύξιμο γεγονός
3		Γεγονός παρουσιασμένο από μια πύλη
4		Υπό συνθήκη γεγονός χρησιμοποιώντας μια πύλη INHIBIT
5		House γεγονός, που είτε συμβαίνει είτε δεν συμβαίνει
6		Σύμβολο μεταφοράς

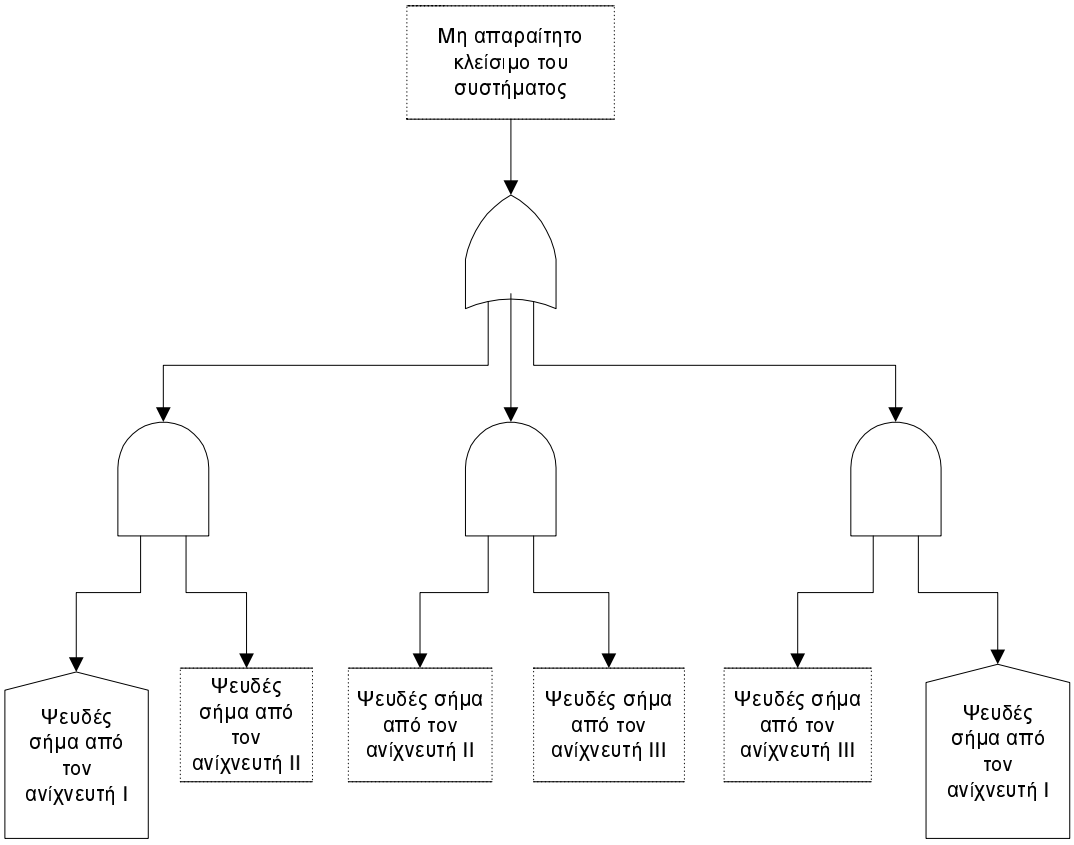
Πίνακας 1.2

Ο **κύκλος (circle)** χρησιμοποιείται για να αναπαραστήσει βασικά γεγονότα, με επαρκή δεδομένα, για τα οποία η αξιοπιστία των πληροφοριών είναι διαθέσιμη. Ο κύκλος ορίζει ένα βασικό συστατικό αποτυχίας, που οφείλεται σε λάθος σχεδιασμό ή σε φαινόμενα του περιβάλλοντος. Γενικά με τον κύκλο αναπαριστάται ένα γεγονός για το οποίο το συστατικό από μόνο του είναι υπεύθυνο, και κάθε φορά που συμβαίνει το συστατικό πρέπει να επισκευαστεί ή να αντικατασταθεί.

Το **διαμάντι (diamond)** χρησιμοποιείται για να δείξει ένα μη αναπτύξιμο γεγονός, διότι δεν μπορεί να γίνει λεπτομερή ανάλυση για όλα τα βασικά γεγονότα, λόγω έλλειψης χρόνου ή χρήματος.

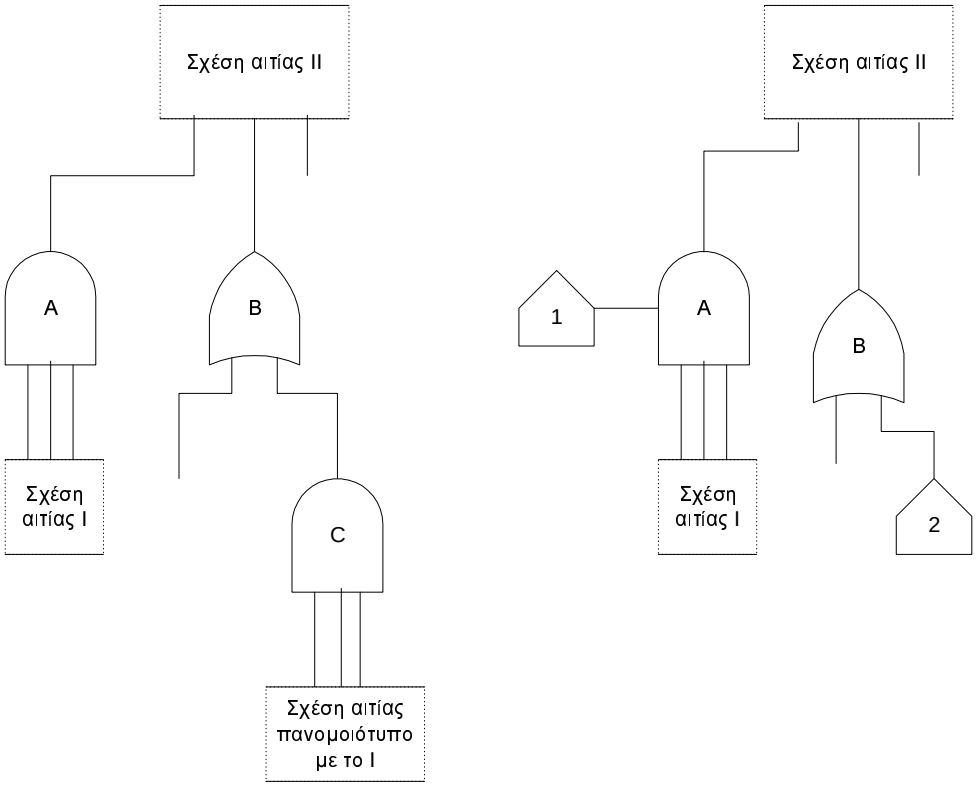
Το **τετράγωνο (rectangle)** αναπαριστά ένα γεγονός αποτυχίας το οποίο προέκυψε από περισσότερα βασικά γεγονότα, που συνδυάζονται μεταξύ τους με λογικές πύλες.

Μερικές φορές θέλουμε να μελετήσουμε δέντρα λαθών στα οποία κάποια γεγονότα συμβαίνουν και κάποια άλλα δεν συμβαίνουν. Σε τέτοιες περιπτώσεις θα χρησιμοποιούμε το **House γεγονός.** Όταν ανοίγουμε το **House γεγονός** το δέντρο προϋποθέτει την εμφάνιση του γεγονότος, ενώ το αντίθετο συμβαίνει όταν κλείνουμε το **House γεγονός**. Ένα παράδειγμα με **House γεγονός** μπορείτε να δείτε στο Σχήμα 1.7:



Σχήμα 1.7

Τα δύο **τρίγωνα (triangles)** έχουν τον ίδιο προσδιοριστικό αριθμό. Το **τρίγωνο από μεταφορά** εισάγεται δίπλα στην πύλη, ενώ το **τρίγωνο μεταφορά στο** εισάγεται κάτω από μία άλλη πύλη. Τα τρίγωνα χρησιμοποιούνται για να απλοποιήσουν την αναπαράσταση των δέντρων λαθών και αυτό φαίνεται στο Σχήμα 1.8:



Σχήμα 1.8

1.4 Κατασκευή δέντρων λαθών

Σε αυτή την παράγραφο παρουσιάζονται τα αρχικά βήματα και οι τεχνικές που ακολουθούμε για την κατασκευή των δέντρων λαθών.

1.4.1 Εμπρόσθια και Οπίσθια ανάλυση

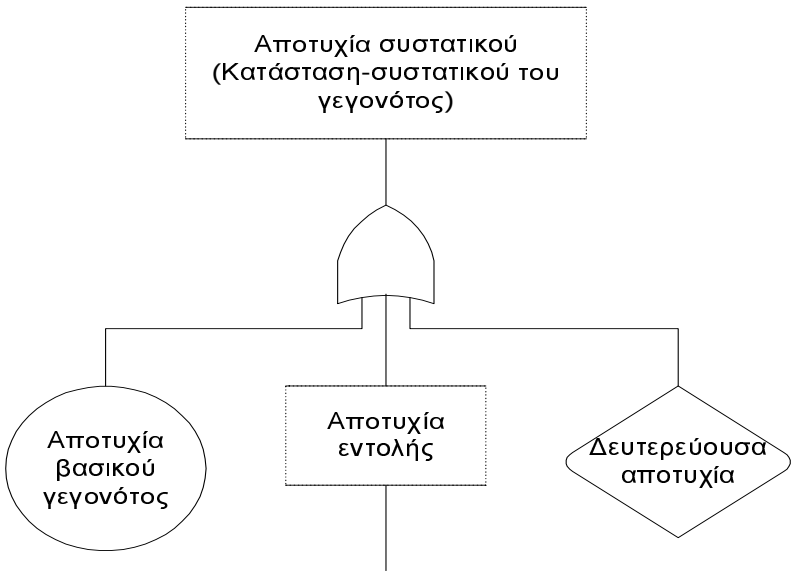
Υπάρχουν δύο προσεγγίσεις για την ανάλυση των σχέσεων αιτίου-αποτελέσματος: η **εμπρόσθια ανάλυση** και **οπίσθια ανάλυση**. Η **εμπρόσθια ανάλυση** ξεκινάει με ένα σύνολο από γεγονότα αποτυχίας και προχωράει προς τα εμπρός, αναζητώντας πιθανές καταστάσεις που προκύπτουν από αυτά τα γεγονότα. Η **οπίσθια ανάλυση** αρχίζει με ένα σύστημα κινδύνου και προχωράει προς τα πίσω, ψάχνοντας πιθανές αιτίες του κινδύνου. Για την κατασκευή των δέντρων λαθών ακολουθείται η **οπίσθια ανάλυση,** γατί το δέντρο λαθών είναι μία γραφική αναπαράσταση των σχέσεων αιτίου-αποτελέσματος που επιτυγχάνεται όταν ένα σύστημα κινδύνου αναζητά τις πιθανές αιτίες του. Το σύστημα κινδύνου στη συνέχεια περνάει στην κορυφή του δέντρου (**γεγονός κορυφής**).

1.4.2 Χαρακτηριστικά των συστατικών αποτυχίας

Οι αποτυχίες των συστατικών θεωρούνται θεμελιώδεις για την ανάλυση των σχέσεων αιτίου-αποτελέσματος. Χωρίζονται σε τρεις κατηγορίες: στις **στοιχειώδεις αποτυχίες**, στις **δευτερεύουσες αποτυχίες** και στα **σφάλματα εντολής**. Η κατηγοριοποίηση αυτή είναι χρήσιμη για την κατασκευή των δέντρων λαθών. Σε μια

στοιχειώδη αποτυχία το συστατικό είναι από μόνο του υπεύθυνο για την αποτυχία, λόγω κάποιων λαθών σχεδιασμού ή λόγω της φυσικής του ηλικίας. Σε μια δευτερεύουσα αποτυχία δεν ευθύνεται το ίδιο το συστατικό για την αποτυχία, αλλά άλλα γειτονικά χαρακτηριστικά ή το περιβάλλον. Όταν συμβεί μια από τις προηγούμενες δύο αποτυχίες, το συστατικό πρέπει να αντικατασταθεί, γιατί είναι άχρηστο πλέον. Αντιθέτως, σε ένα σφάλμα εντολής δεν πρέπει να αντικατασταθεί το συστατικό απαραίτητα, διότι η αποτυχία οφείλεται σε λανθασμένο σήμα ελέγχου ή σε θόρυβο.

Η στοιχειώδης αποτυχία αναπαρίσταται από ένα κύκλο, γιατί είναι βασικό γεγονός για το οποίο τα δεδομένα της αποτυχίας είναι όλα διαθέσιμα. Η δευτερεύουσα αποτυχία είναι ένα μη αναπτύξιμο γεγονός γι' αυτό και συμβολίζεται με διαμάντι. Το σφάλμα εντολής συμβολίζεται με τετράγωνο και αναλύεται περαιτέρω. Αυτά φαίνονται στο Σχήμα 1.9.



Σχήμα 1.9

1.5 Μέθοδοι ανάλυσης αξιοπιστίας λογισμικού με δένδρα λαθών

Υπάρχουν ποικίλες μέθοδοι για την ανάλυση της αξιοπιστίας του λογισμικού, αλλά εμείς θα μελετήσουμε αυτές που βασίζονται στα δένδρα λαθών. Τέτοιου τύπου αναλύσεις είναι η ποιοτική ανάλυση (qualitative analysis), η ποσοτική ανάλυση (quantitative analysis) και η Monte Carlo προσομοίωση. Παρακάτω δίνεται μια σύντομη περιγραφή αυτών των μεθόδων, με τις οποίες θα ασχοληθούμε αναλυτικά στο επόμενο κεφάλαιο.

1.5.1 Ποιοτική ανάλυση

Η αποτυχία του συστήματος μπορεί να προκύψει με πολλούς διαφορετικούς τρόπους, οι οποίοι ονομάζονται δομές αποτυχίας. Για να μειώσουμε την πιθανότητα της αποτυχίας, πρέπει να αναγνωρίσουμε τους τρόπους αυτούς και μετά να εξαλείψουμε αυτούς που εμφανίζονται πιο συχνά και έχουν μεγαλύτερη πιθανότητα να συμβούν. Τα δένδρα λαθών μας διευκολύνουν στον εντοπισμό των διαφορετικών αυτών τρόπων, που οδηγούν στην αποτυχία του συστήματος.

Η ποιοτική ανάλυση γίνεται με σκοπό την απλοποίηση της διαδικασίας της ανάλυσης αξιοπιστίας λογισμικού. Το σύστημά μας αναλύεται στην αρχή ποιοτικά και στη συνέχεια μπορεί να αναλυθεί χρησιμοποιώντας είτε την ποσοτική ανάλυση, είτε τη Monte Carlo προσομοίωση. Μέθοδοι ποιοτικής ανάλυσης είναι τα **σύνολα ελάχιστης τομής** και τα **σύνολα ελάχιστων μονοπατιών,** τα οποία θα μελετήσουμε διεξοδικά στο επόμενο κεφάλαιο**.**

1.5.2 Ποσοτική ανάλυση

Μόλις ολοκληρωθεί η διαδικασία της ποιοτικής ανάλυσης, το σύστημά μας είναι πλέον έτοιμο να αναλυθεί ποσοτικά. Το πρώτο βήμα στη ποσοτική ανάλυση είναι η ποσοτικοποίηση των βασικών γεγονότων. Στη συνέχεια μπορούμε να προχωρήσουμε στην ποσοτική ανάλυση ολόκληρου του συστήματος που είναι και αυτή που μας ενδιαφέρει.

Όλα τα συστήματα τελικά αποτυγχάνουν, τίποτα δεν είναι τελείως αξιόπιστο και τίποτα δεν κρατάει για πάντα. Αυτό που πρέπει να κάνουμε εμείς είναι να αποδεχθούμε ότι το σύστημα θα αποτύχει και στη συνέχεια να βρούμε τρόπους για τη μείωση της συχνότητας της αποτυχίας σε ένα οικονομικά και κοινωνικά αποδεκτό επίπεδο.

Οι πιθανολογικές καταστάσεις δεν είναι άγνωστες στο κοινό. Για παράδειγμα, όταν πιάσει καταιγίδα μπορεί να εκτιμηθεί η πιθανότητα να βραχεί ένα άτομο, αν η ομπρέλα του έχει προβλήματα στη λειτουργία της. Αυτή η πιθανότητα βέβαια εξαρτάται από το χρόνο. Η **αξιοπιστία (reliability)** της ομπρέλας μειώνεται όσο περνάει ο καιρός, μια ομπρέλα δύο ετών είναι πιθανότερο να αποτύχει, από μια ομπρέλα ενός έτους. Η αξιοπιστία δεν είναι το μοναδικό χαρακτηριστικό που μπορεί να χαρακτηρίσει την ομπρέλα, αλλά και κάθε συστατικό. Αν η ομπρέλα σπάσει ή δε λειτουργεί καλά, τότε μπορεί να επισκευαστεί. Άρα πρέπει να εκτιμηθεί και η **διαθεσιμότητα (availability)**, δηλαδή το κομμάτι του χρόνου που η ομπρέλα είναι διαθέσιμη για χρήση και λειτουργεί φυσιολογικά. Αλλά η επισκευή κοστίζει χρήματα, έτσι πρέπει επίσης να γνωρίζουμε τον **αναμενόμενο αριθμό αποτυχιών** κατά τη διάρκεια οποιοδήποτε δοσμένου χρόνου.

Είναι εμφανές ότι υπάρχουν αναλυτικές σχέσεις μεταξύ της **αξιοπιστίας,** της **διαθεσιμότητας** και του **αναμενόμενου αριθμού αποτυχιών.** Μια ακριβής περιγραφή των συστατικών αποτυχίας και των δομών αποτυχίας είναι απαραίτητη για την αναγνώριση των κινδύνων του συστήματος, από τη στιγμή που αυτοί προκαλούνται από συνδυασμούς των αποτυχίων των συστατικών.

1.5.3 Monte Carlo προσομοίωση

Αφού γίνει ποιοτική ανάλυση στο σύστημά μας, μπορούμε να προχωρήσουμε στην ποσοτική ανάλυσή του, αλλά και στη προσομοίωση του με μεθόδους Monte Carlo. Η πόλη Monte Carlo είναι γνωστή για το Casino της στο οποίο οι παίχτες βασίζονται στη τύχη. Το όνομα της Monte Carlo προσομοίωσης προέκυψε από την πόλη, καθώς σε μια προσομοίωση γίνεται παραγωγή και χρήση τυχαίων μεταβλητών. Η Monte Carlo προσομοίωση υλοποιείται χρησιμοποιώντας ένα προσεγγιστικό στοχαστικό μοντέλο προσομοίωσης ενός ντετερμινιστικού συστήματος .

Πριν την ανάπτυξη της μεθόδου KITT (θεωρία δένδρου κίνησης) που εντάσσεται στην ποσοτική ανάλυση, οι μέθοδοι Monte Carlo χρησιμοποιούνταν ευρέως για την ανάλυση των δέντρων λαθών.

2. Παρουσίαση μεθόδων ανάλυσης αξιοπιστίας λογισμικού

Σε αυτό το κεφάλαιο παρουσιάζονται αναλυτικά οι μέθοδοι ανάλυσης αξιοπιστίας λογισμικού, που βασίζονται στα δένδρα λαθών, και περιγράφηκαν πολύ σύντομα στο τέλος του πρώτου κεφαλαίου. Σκοπός μας είναι να κατανοήσει ο αναγνώστης πως λειτουργούν οι διάφορες αυτές τεχνικές και να ανακαλύψει τον τρόπο που αυτές μπορούν να βοηθήσουν στην ανάλυση ενός συστήματος.

2.1 Ποιοτική ανάλυση

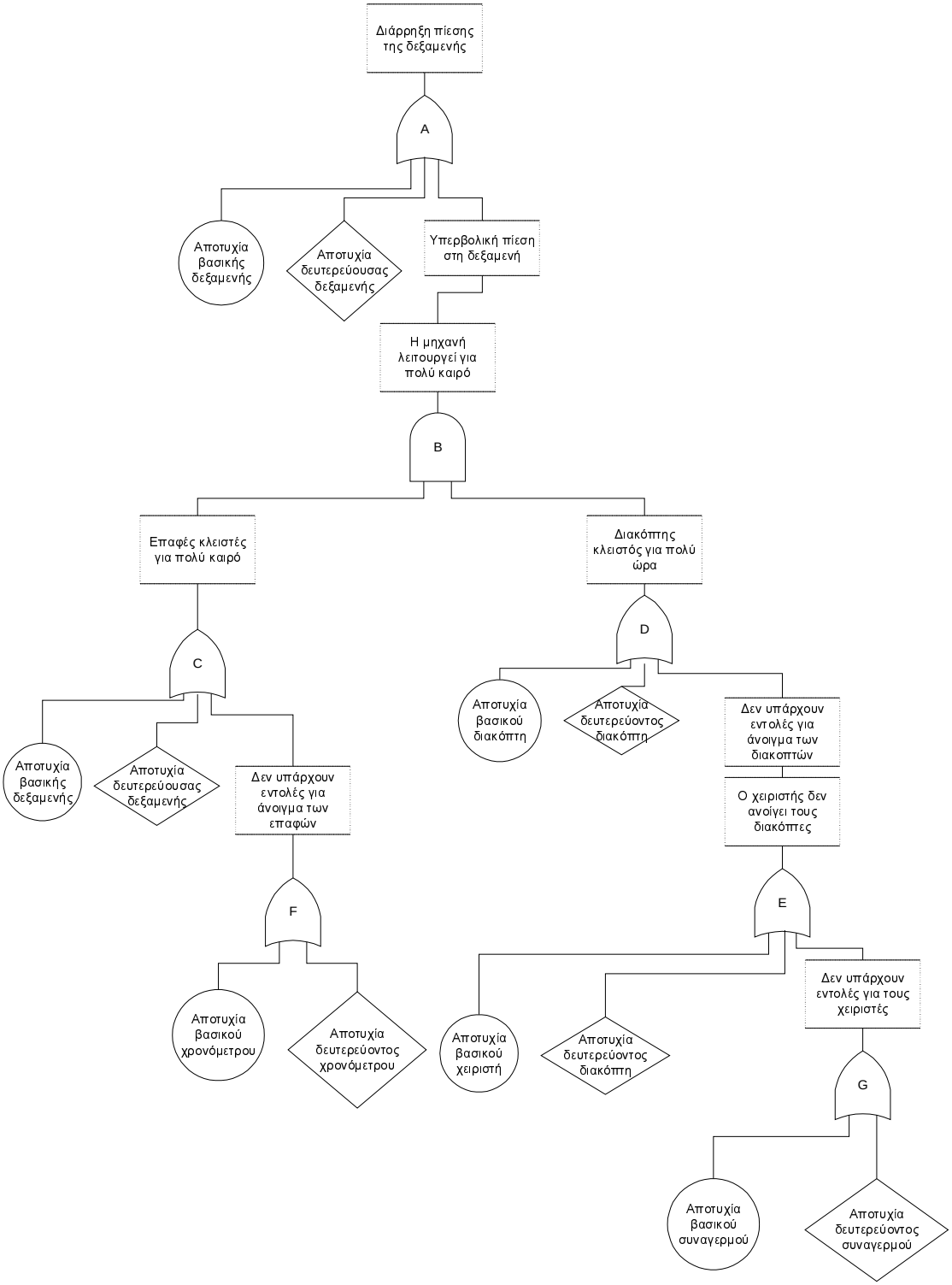
Όπως αναφέραμε στο προηγούμενο κεφάλαιο η ποιοτική ανάλυση γίνεται πάντα στα πρώτα στάδια της ανάλυσης αξιοπιστίας λογισμικού και βοηθάει στην απλοποίηση της διαδικασίας. Οι μέθοδοι που χρησιμοποιούνται για τέτοιου είδους ανάλυση είναι τα **σύνολα ελάχιστης τομής** και τα **σύνολα ελάχιστων μονοπατιών.**

Όταν έχουμε ένα δένδρο λαθών οι δομές αποτυχίας ορίζονται καθαρά από την ιδέα ενός **συνόλου τομής.** Σύνολο τομής είναι μια συλλογή από βασικά γεγονότα και αν όλα αυτά τα βασικά γεγονότα συμβαίνουν το γεγονός κορυφής προκύπτει σίγουρα, δηλαδή το σύστημα αποτυγχάνει εγγυημένα. Για παράδειγμα στο Σχήμα 2.1 το σύνολο {1,2} είναι ένα σύνολο τομής**,** όπως επίσης το σύνολο {1} και το σύνολο {3,5} είναι σύνολα τομής**.**

Τα **σύνολα μονοπατιών** τώρα είναι η άλλη όψη του ίδιου νομίσματος. Είναι μια συλλογή από βασικά γεγονότα και αν κανένα από αυτά δε συμβαίνει, το γεγονότος κορυφής δε συμβαίνει σίγουρα, δηλαδή το σύστημα λειτουργεί με επιτυχία. Στο Σχήμα 2.1 ως σύνολα μονοπατιών μπορούν να θεωρηθούν τα σύνολα {1,2,3} και {1,4,5,6}.

Όταν σε ένα σύστημα υπάρχουν πολλά συστατικά (components) , τότε υπάρχουν και πολλά σύνολα τομής. Είναι απαραίτητο λοιπόν, να μειωθεί ο αριθμός των δομών αποτυχίας για να απλοποιηθεί η ανάλυση. Αυτό επιτυγχάνεται χρησιμοποιώντας τα **σύνολα ελάχιστης τομής**. Ένα σύνολο ελάχιστης τομής δηλώνει πως αν μετακινηθεί ένα οποιοδήποτε βασικό γεγονός από το σύνολο, τα εναπομείναντα γεγονότα δεν αποτελούν πλέον ένα σύνολο ελάχιστης τομής. Το σύνολο τομής που περιέχει μερικά άλλα σύνολα δεν είναι σύνολο ελάχιστης τομής. Το σύνολο ελάχιστης τομής μας δίνει τη δυνατότητα να μειώσουμε τον αριθμό των συνόλων τομής και των αριθμό των βασικών γεγονότων που περιλαμβάνονται σε κάθε σύνολο τομής. Έτσι απλοποιείται η διαδικασία της ανάλυσης.

Το δέντρο λαθών του Σχήματος 2.1 έχει εφτά σύνολα ελάχιστης τομής {1} , {2,4} , {2,5} , {2,6} , {3,4} , {3,5} , {3,6}.Το σύνολο τομής {1,2,4} δεν είναι ελάχιστο γιατί περιλαμβάνει το {1} ή το {2,4}.



Σχήμα 2.1

Το **σύνολο ελάχιστου μονοπατιού** είναι ένα σύνολο μονοπατιού που δηλώνει ότι αν οποιοδήποτε βασικό γεγονός μετακινηθεί από το σύνολο τα εναπομείναντα γεγονότα δεν αποτελούν πλέον ένα σύνολο μονοπατιού. Το δέντρο λαθών του σχήματός μας έχει δύο σύνολα ελαχίστων μονοπατιών, {1,2,3} και {1,4,5,6}. Αν είτε το πρώτο, είτε το δεύτερο δεν αποτύχει, τότε το σύστημα λειτουργεί επιτυχώς.

2.1.1 Ανάλυση αποτυχίας κοινής-κατάστασης

Σε αυτό το κεφάλαιο θα σας παρουσιάσουμε την έννοια «*Κοινή-Κατάσταση*» που προσφέρει μια άλλη ερμηνεία στους όρους που αποτελούν το δένδρο λαθών. Για να είναι ευκολότερα κατανοητό θα σας την παρουσιάσουμε μέσω ενός παραδείγματος. Θεωρείστε ένα σύστημα που αποτελείται από δύο βαλβίδες την Α και τη Β. Αυτές οι βαλβίδες έχουν μια σχέση «*Με εφεδρικά τμήματα*» μεταξύ τους και η αποτυχία μιας μόνο βαλβίδας δεν αρκεί για την απότυχία του γεγονότος της κορυφής. Το δένδρο λαθών που δημιουργείται έχει ένα σύνολο ελάχιστης τομής το

{ δυσλειτουργία στη βαλβίδα Α, δυσλειτουργία στη βαλβίδα Β }

Αυτό το σύστημα βαλβίδων είναι αρκετά πιο αξιόπιστο από ένα σύστημα που έχει μια μόνο βαλβίδα. Ωστόσο, αν η μια από τις βαλβίδες είναι επιρρεπής στην αποτυχία κάτω από τις ίδιες συνθήκες με το άλλο, τότε το σύστημα δύο-βαλβίδων είναι ελάχιστα καλύτερο από το σύστημα μονής-βαλβίδας. Οι δύο βαλβίδες αποτυχαίνουν ταυτόχρονα, αν και οι δύο περιέχουν σφάλματα δυσλειτουργίας. Κάτω από αυτές τις συνθήκες η δύο είναι το ίδιο αξιόπιστες όσο η μονή. Μια συνθήκη ή ένα γεγονός που είναι η αιτία για να συμβούν πολλαπλά βασικά γεγονότα ονομάζεται «*Κοινή Κατάσταση*». Ένα παράδειγμα μιας «*Κοινής Κατάστασης*» είναι μια πλημμύρα που προκαλεί όλα τα «με εφεδρικά τμήματα» στοιχεία να αποτύχουν ταυτόχρονα.

Η εύρεση των συνόλων-ελαχίστων αναλύθηκε στα προήγουμενα κεφάλαια και αποδείχθηκε ότι βγαίνουν σύνολα-ελαχίστων ποικίλου μεγέθους. Ένα σύνολο τομής, που αποτελείται από ένα σύνολο με βασικά γεγονότα, ονομάζεται n- γεγονότα σύνολο τομής. Τα σύνολα τομής των γεγονότων συμβάλλουν σημαντικά στην επιτυχία του γεγονότος της κορυφής, εκτός αν έχουν μικρή πιθανότητα να συμβούν. Συνήθως, τα σφάλματα υλικού εμφανίζουν μικρή συχνότητα, δηλαδή δύο ή περισσότερα γεγονότα μπορεί να παραλειφθούν, αν είναι παρόν μονό-γεγονός γιατί η ταυτόχρονη ύπαρξη δύο σφαλμάτων έχει σημαντικά μικρότερες πιθανότητες. Παρόλα αυτά, όταν μια Κοινή Κατάσταση εμπεριέχεται, τότε μπορεί να προκαλέσει πολλαπλά σφάλματα βασικού γεγονότος. Έτσι δεν μπορούμε συνέχεια να αποκλείουμε υψηλότερης σειράς σύνολα τομής μόνο και μόνο επειδή υπάρχουν δύο ή περισσότερα γεγονότα που συμπεριφέρονται όπως μονά- γεγονότα συνόλων τομής. Ένα σύνολο τομής ονομάζεται «Κοινή Κατάσταση συνόλου τομής», όταν μια Κοινή Κατάσταση οδηγεί στη ταυτόχρονη ύπαρξη όλων των γεγονότων στο σύνολο τομής.

Όπως φαινόταν στην παρακάτω λίστα, οι αιτίες που προκαλούν σφάλματα στα συστατικά προέρχονται από μια ή περισσότερες από τις ακόλουθες πηγές:

1. Γήρανση (ηλικίας)
2. Προσωπικό
3. Περιβάλλον του συστήματος
4. Συστατικά του συστήματος

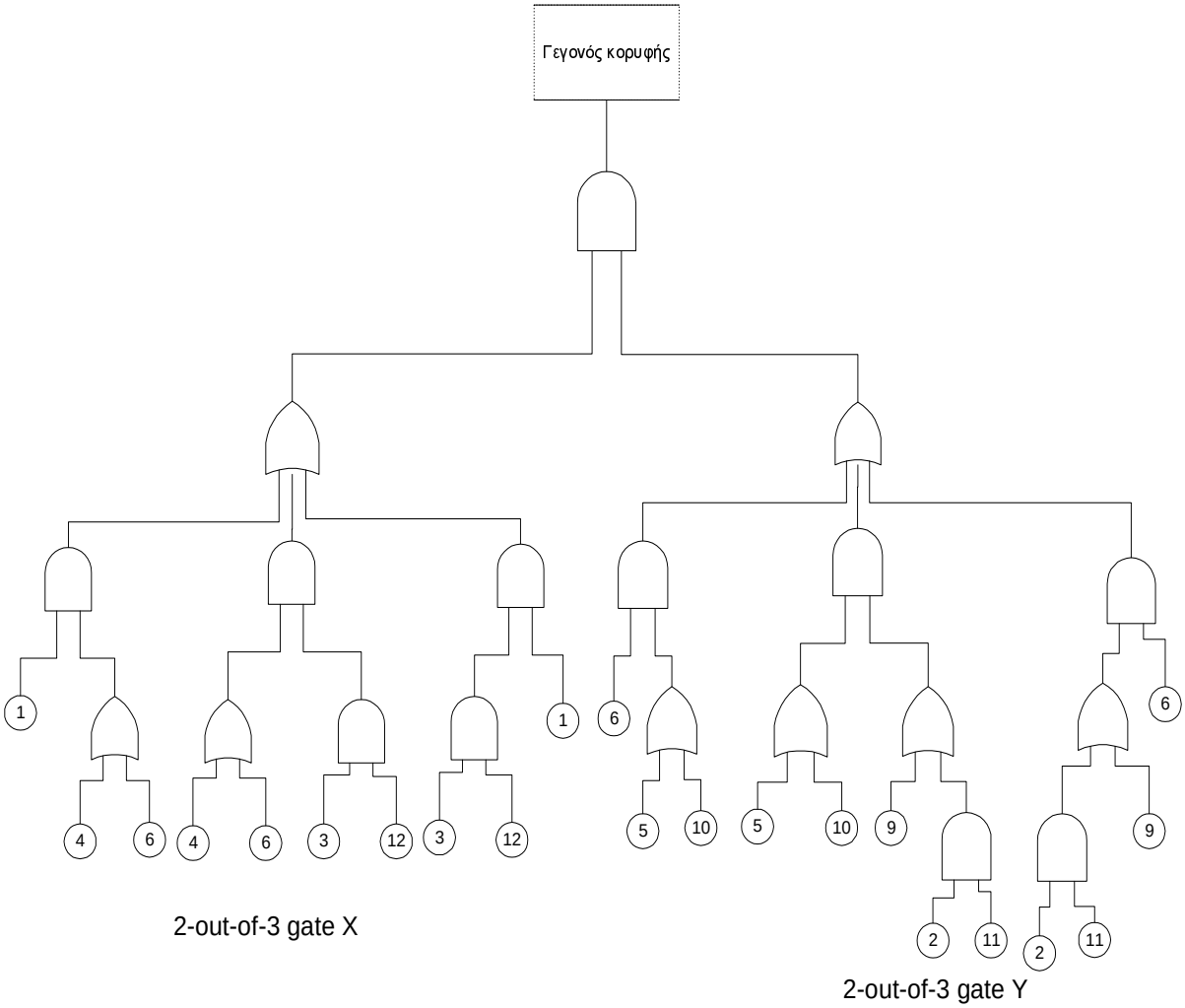
Υπάρχει σε κάθε κατηγορία ένας μεγάλος αριθμός Κοινών Καταστάσεων, τα οποία μπορούν να κατηγοριοποιηθούν σε υποκατηγορίες. Μερικές κατηγορίες και παραδείγματα φάινονται στο Πίνακα 2.1

Πινακας 2.1 Κατηγορίες και παραδείγματα Common Cause

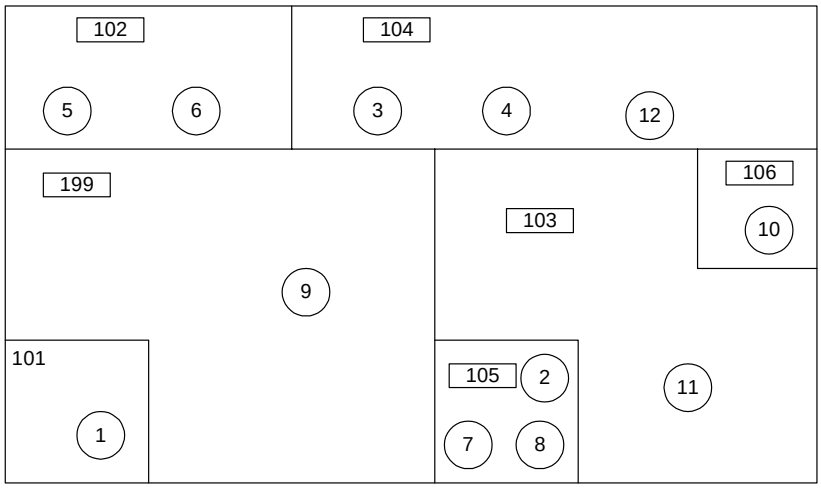
Πηγή	Σύμβολο	Κατηγορία	Παραδείγματα
Περιβάλλον, Συστατικά Συστήματων ή Υποσυστημάτων	I	Επίδραση	Κάβουρας βάνας, θόρυβος υδροσωλήνα, πύραυλοι, σεισμός, κατασκευαστικό λάθος
	V	Δόνηση	Μηχανήματα σε λειτουργία, σεισμός
	P	Πίεση	Έκρηξη, εκτός ορίων ανοχής αλλαγών του συστήματος (υπερπίεση αντλίας, εμπόδιση της ροής)
	G	Άμμος	Σκόνη του αέρα, μεταλλικά κομμάτια που δημιουργήθηκαν από κινούμενα μέρη με ανεπαρκείς
	S	Πίεση	Θερμική πίεση στις ενώσεις των διαφορετικών μετάλλων, θερμικές πιέσεις thermal stresses και στιγμές ευκαιψίας
	T	Θερμοκρασία	Φωτιά, κεραυνός, ενώσεις εξαρτημάτων, αποτυχίες ψυκτικού συστήματος
	E	Απώλεια της πηγής ενέργειας	Κοινή πηγή ρεύματος
	C	Βαθμονόμηση	Κακογραμμένες οδηγίες βαθμονόμησης
	F	Κατασκευαστής	Επαναλαμβανόμενο λάθος κατασκευής.
Προσωπικό Εργοστασίο	IN	Εργολάβος εγκατάστασης	Παρόμοιος υποεργολάβος ή εργατικό δυναμικό
	M	Συντήρηση	Μη σωστή διαδικασία, ανεπαρκώς εκπαιδευμένο εργατικό δυναμικό
	O	Χειριστής της εφαρμογής	Ο χειριστής αδυνατεί ή υπερφορτωμένος με δουλειά, ελλατωματικές διαδικασίες χειρισμού
	TS	Διαδικασία ελέγχου	Ελλατωματικές διαδικασίες ελέγχου που μπορεί να επηρεάσουν τα υπόλοιπα μέρη των συστατικών
Παλαιότητα	A	Παλαιότητα	Συστατικά παρόμοιων υλικών

Για κάθε Κοινή Κατάσταση έχουμε να αναγνωρίσουμε τα βασικά γεγονότα που επηρρεάζονται. Κάνοντας το αυτό, μια περιοχή για κάθε Κοινή Κατάσταση, γνωστή επίσης και ως «Physical Location» των συστατικών και των βασικών γεγονότων αναγνωρίζεται. Μερικές Συνήθεις Αποτυχίες έχουν περιορισμένο αριθμό περιοχών επιρροής, και τα βασικά γεγονότα που υπάρχουν έξω από αυτή την περιοχή δεν επηρρεάζονται από τις Αποτυχίες. Τα βασικά γεγονότα που προκαλούνται από μια συνήθης αιτία ονομάζονται γεγονότα κοινής-κατάστασης μιας αποτυχίας.

Θεωρείστε το δένδρο λαθών του Σχήματος 2.2. Το σχέδιο του δωματίου είναι στο Σχήμα 2.3. Αυτό το σχήμα περιλαμβάνει επίσης και την τοποθεσία των βασικών γεγονότων. Θεωρούμε 20 συνήθεις αποτυχίες. Κάθε συνήθης αιτία έχει ένα σύνολο γεγονότων κοινής-κατάστασης, που φαίνονται στον Πίνακα 2.2.



Σχήμα 2.2



Σχήμα 2.3

Πίνακας 2.2 Παραδείγματα Συνήθων Αποτυχίων, Περιοχών, και Γεγονότων Κοινής-Κατάστασης

Κατηγορία	Συνήθης αιτία	Περιοχή	Γεγονότα Κοινής-Κατάστασης
Επίδραση	I1 I2 I3	102,104 101,103,105 106	6,3 1,2,7,8 10
Ένταση	S1 S2 S3	103,105,106 199 101,102,104	11,2,7,10 9 1,4
Θερμοκρασία	T1 T2	106 101,102,103, 104, 105, 199	10 5,11,8,12,3,4
Δόνηση	V1 V2	102,104,106 101,103,105, 199	5,6,10 7,8
Χειριστής	O1 O2	All All	1,3, 12 5,7,10
Πηγή Ενέργειας	E1 E2	All All	2,9 1,12
Κατασκευαστής	F1	All	2,11
Ανάδοχος Εγκατάστασης	IN1 1N2 1N3	All All All	1,12 6,7,10 3,4,5,8,9,11
Διαδικασία Ελέγχου	TS1 TS2	All All	2,11 4,8

Μόνο δύο βασικά γεγονότα, 6 και 3, προκαλούνται από το Impact I1, ενώ τα βασικά γεγονότα προκαλούνται από το Impact I2. Η διαφορά γεννιέται επειδή κάθε Impact έχει την δική του περιοχή επιρροής, και κάθε βασικό γεγονός έχει την δική του τοποθεσία εμφάνισης. Ούτε το γεγονός 4 ούτε το γεγονός 12 προκαλούνται από το Impact I1, παρόλου που ανιχνεύτηκαν στην περιοχή 104 του I1. Αυτό συμβαίνει επειδή αυτά τα γεγονότα συμβαίνουν ανεξάρτητα από το Impact, παρόλο που μοιράζονται την ίδια φυσική τοποθεσία του γεγονότος 3.

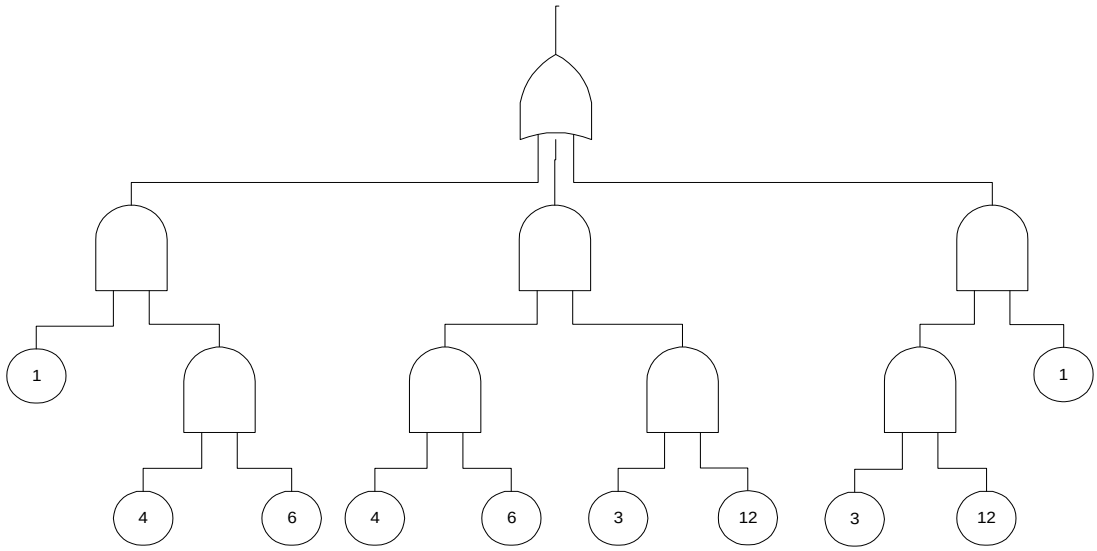
2.1.2 Εύρεση συνόλων τομής κοινής-κατάστασης

Φανταστείτε μια λίστα από συνήθεις αιτίες, γεγονότα κοινής-κατάστασης και βασικά γεγονότα. Μπορούμε μελετώντας να βρούμε τα σύνολα τομής κοινής-κατάστασης, αν έχουμε όλα τα σύνολα ελάχιστης τομής ενός δένδρου λαθών. Εξαιτίας του τεράστιου αριθμού των σύνολων ελάχιστης τομής των μεγάλων δένδρων λαθών, η

διαδικασία να βρούμε τα σύνολα ελάχιστης τομής είναι χρονοβόρα. Για ενα τέτοιο δένδρο λαθών, οι μέθοδοι εύρεσης, που συζητήθηκαν στις προηγούμενες ενότητες, είναι έτσι ρυθμισμένες ώστε να βρίσκουν τα διπλά-ή-λιγότερα-γεγονότα σύνολα τομής. Όπως αναφέρθηκε στην προηγούμενη ενότητα μπορεί τρία-ή-περισσότερα- γεγονότα σύνολα τομής να είναι όπως και τα μονό-γεγονότα σύνολα τομής. Γι αυτό το λόγο δεν πρέπει να χρησιμοποιείται πάντα αυτή ρύθμιση για να βρίσκουμε μόνο τα διπλά-ή-λιγότερα- γεγονότα σύνολα τομής.

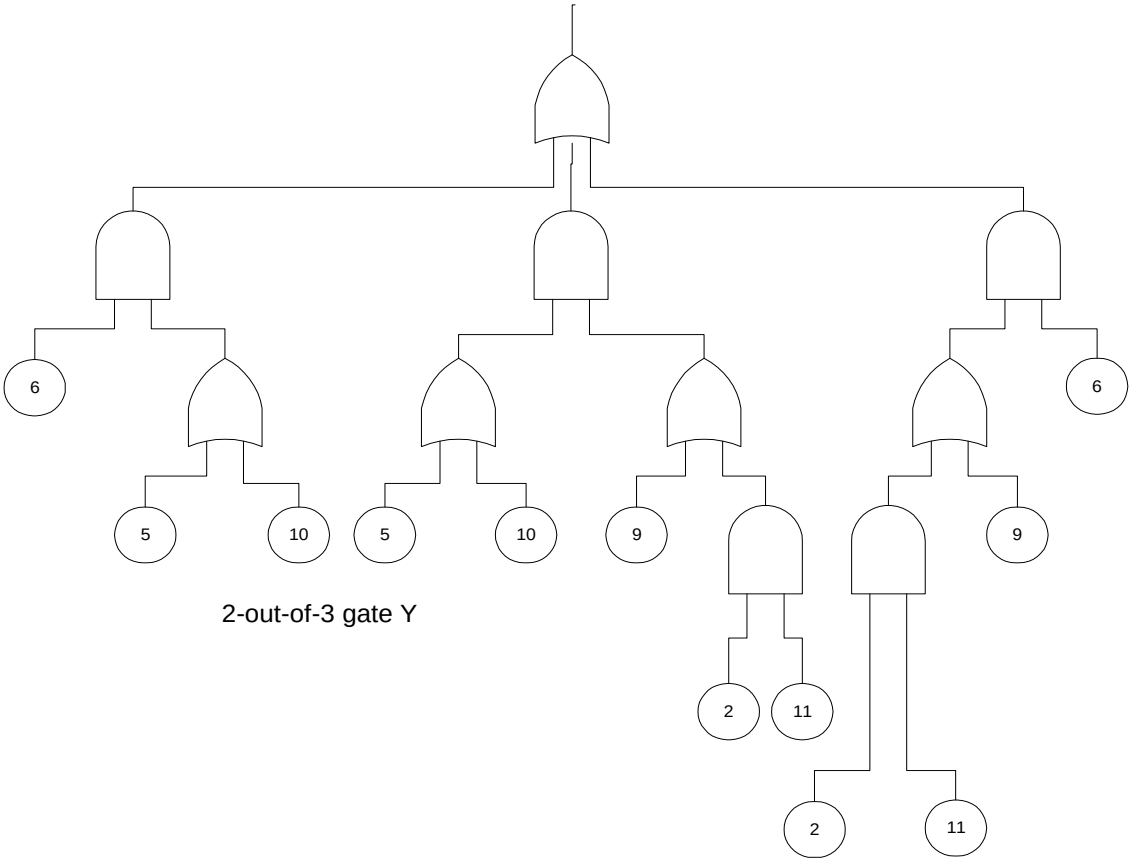
Στη συνέχεια θα αναπτύξουμε μια καινούρια προσέγγιση του προβλήματος Κοινής Κατάστασης, χρησιμοποιώντας ένα απλοποιημένο δένδρο λαθών. Μια άλλη προσέγγιση, από στους Fussle και Wagner, υπάρχει στο βιβλίο «Reliability Enginneering and Risk Assessment» των Ernest J. Henley και Hiromitsu Kumamoto βασισμένη στην ανατομή των δένδρων λαθών υπάρχει στην παραπομπή του Σχήματος 2.2 στη σελίδα 121. Ένα βασικό γεγονός ονομάζεται «ουδέτερο γεγονός» όμοια με τη συνήθη αιτία, αν είναι ανεξάρτητο από την αιτία. Για μια συγκεκριμένη συνήθη αιτία, βασικό γεγονός είναι είτε ένα «ουδέτερο γεγονός» είτε ένα «γεγονός κοινής-κατάστασης». Αυτή η προσέγγιση υποθέτει μια πιθανή κατάσταση για κάθε συνήθη αιτία. Αυτή η υπόθεση υποστηρίζεται από την άποψη: «Έστω μια συνήθης αιτία. Από τη στιγμή που τα περισσότερα ουδέτερα γεγονότα έχουν πολύ πιο μικρές πιθανότητες να συμβούν από τα γεγονότα κοινής-κατάστασης, αυτά τα ουδέτερα γεγονότα θεωρείται ότι δεν συμβαίνουν ποτέ στο συγκεκριμένο δένδρο λαθών.» Άλλες καταστάσεις που προσπαθούν να παραβιάσουν αυτή την άποψη μπορούν να παραβλεφθούν, επειδή συνεπάγονται να συμβούν ένα ή περισσότερα σπάνια γεγονότα.

Την κατηγοριοποίηση των πιθανών-κατάστασεων απλοποιεί το δένδρο λαθών. Όσον αφορά τα απλοποιημένα δένδρα λαθών, μπορούμε να αποκτήσουμε πολύ εύκολα τα σύνολα ελάχιστης τομής. Αυτά τα σύνολα ελάχιστης τομής γίνονται τα σύνολα τομής κοινής-κατάστασης. Ως παράδειγμα θεωρείστε το δένδρο λαθών του Σχήματος 2.2. Υποθέστε ότι δεν υπάρχουν αποκλειστικά βασικά γεγονότα. Παρατηρείστε ότι οι πύλες X και Y, two-out-of-three, μπορούν να ξαναγραφούν όπως στα Σχήματα 2.4 και 2.5 αντίστοιχα.



2-out-of-3 gate X

Σχήμα 2.4

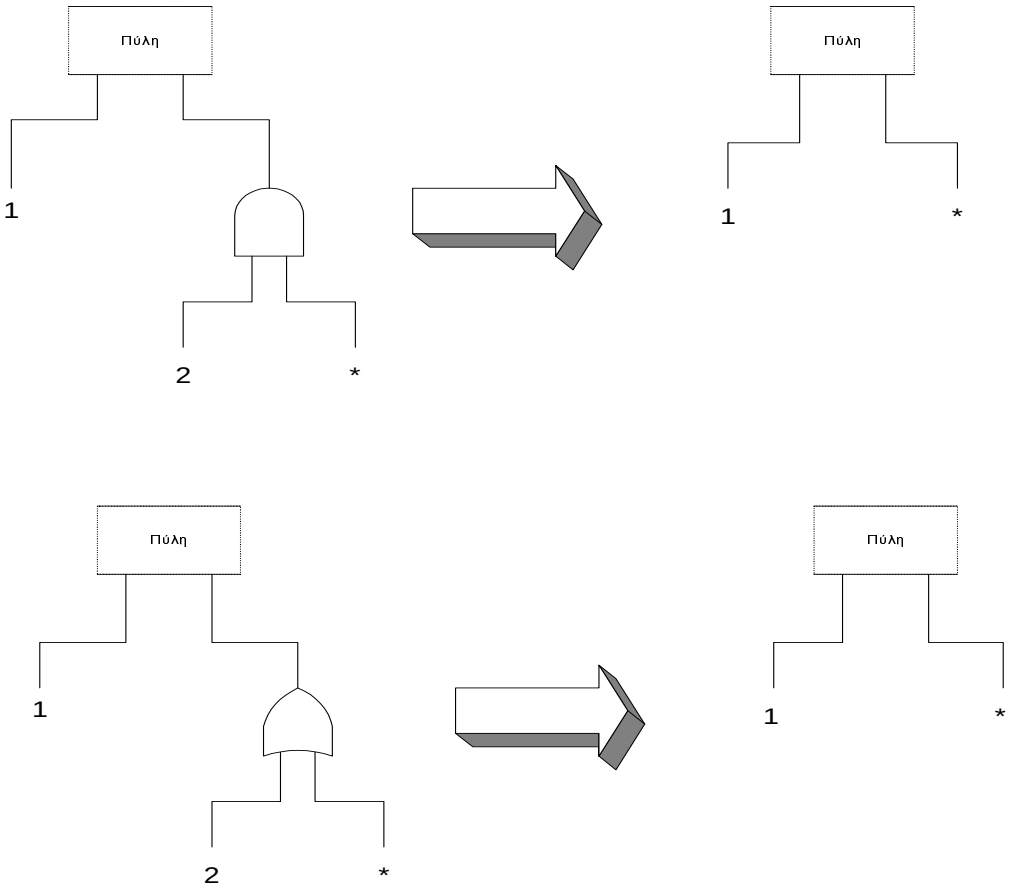


Σχήμα 2.5

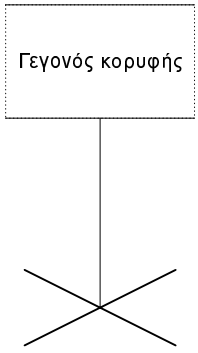
Ας αναλύσουμε πρώτα τη συνήθη αιτία 1. Τα γεγονότα κοινής κατάστασης της αιτίας είναι 1, 3 και 12. Για αυτό το λόγο, τα ουδέτερα γεγονότα είναι 2, 4, 5, 6, 7, 8, 9, 10 και 11. Υποθέστε αυτά τα ουδέτερα γεγονότα έχουν κατα πολύ πιο μικρές πιθανότητες απο τα γεγονότα κοινής-κατάστασης, όταν συμβαίνει η συνήθη αιτία 1. Η βασική απλοποίηση του δένδρου λαθών του Σχήματος 2.6 δίνει το απλοποιημένο δένδρο λαθών του Σχήματος 2.8. Χρησιμοποιείται το MOCUS, το οποίο είναι πρόγραμμα στον υπολογιστή για να αποκτήσουμε τα σύνολα ελάχιστης τομής, για να απλοποιηθεί το δένδρο λαθών του Σχήματος 2.8 με τον ακόλουθο τρόπο:

A	
B,C	
1, 3, 12, 3	1, 3, 12
1, 3, 12, 1	1, 3, 12

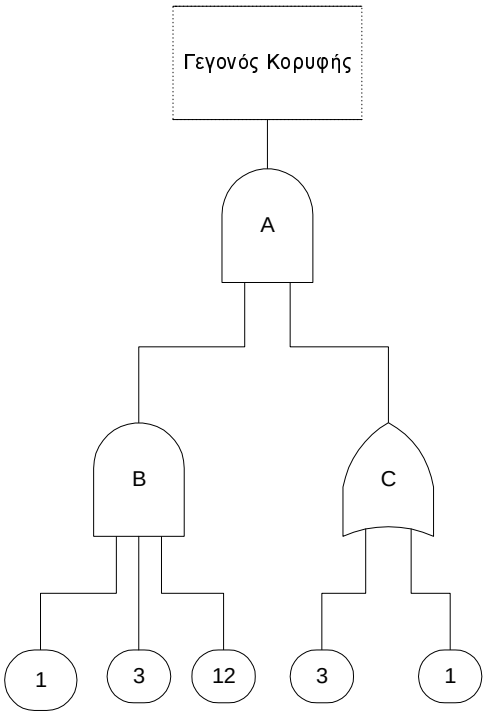
Υπάρχει ένα και μονάδικό σύνολο τομής κοινής-κατάστασης {1, 3, 12} για τη συνήθης αιτία 1. Στη συνέχεια θεωρείστε τη συνήθης αιτία Ι3 του Πίνακα 2.2. Τα ουδέτερα βασικά γεγονότα είναι 1, 2, 3, 4, 5, 6, 7, 8, 9, 11 και 12. Οι βασικές απλοποιήσεις παράγουν το μειωμένο δένδρο λαθών του Σχήματος 2.7. Βλέπουμε ότι δεν υπάρχουν σύνολα τομής κοινής-κατάστασης για τη συνήθη αιτία Ι3.



Σχήμα 2.6



Σχήμα 2.7: Απλοποιημένο δένδρο
λαθών για τη συνήθη αιτία Ι3



Σχήμα 2.8: Απλοποιημένο δένδρο
λαθών για τη συνήθη αιτία 1

Επαναλαμβάνουμε την ίδια διαδικασία και για τις υπόλοιπες συνήθεις αιτίες ώστε να αποκτήσουμε τα σύνολα τομής κοινής-κατάστασης που υπάρχουν στον Πίνακα 2.3.

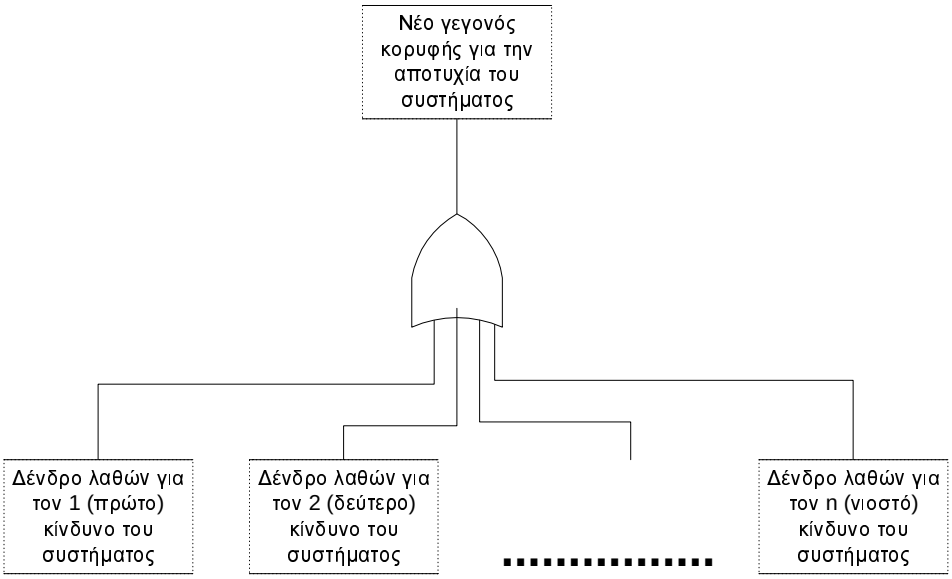
Πίνακας 2.3: Συνήθεις αιτίες και σύνολα τομής κοινής-κατάστασης

Συνήθεις αιτίες	Σύνολα τομής κοινής-κατάστασης
12	{1,2}
12	{1,7,8}
S3	{1,4}
S1	{2,10,11}
T2	{3,4,12}
1	{1,3,12}

2.2 Ποσοτική ανάλυση του συστήματος

Η αποτυχία ή η επιτυχία του συστήματος μπορεί να περιγραφεί από ένα συνδυασμό από γεγονότα κορυφής που ορίζονται με τη σειρά τους από έναν συνδυασμό OR πυλών για όλα τα συστήματα κινδύνου σε ένα σύνθετο δέντρο λαθών. Αν κανένα από τα συστήματα κινδύνου δεν συμβαίνει τότε το σύστημα επιτυγχάνει. Σε

οποιαδήποτε άλλη περίπτωση το σύστημα αποτυγχάνει, όπως εύκολα μπορούμε να διακρίνουμε στο Σχήμα 2.9.



Σχήμα 2.9 Ορισμός ενός νέου δέντρου λαθών από το συνδυασμό με OR πύλες όλων των δέντρων λαθών για τα συστήματα κινδύνου

Οι παρακάτω πιθανολογικές παράμετροι μπορούν να οριστούν για ολόκληρο το σύστημα.

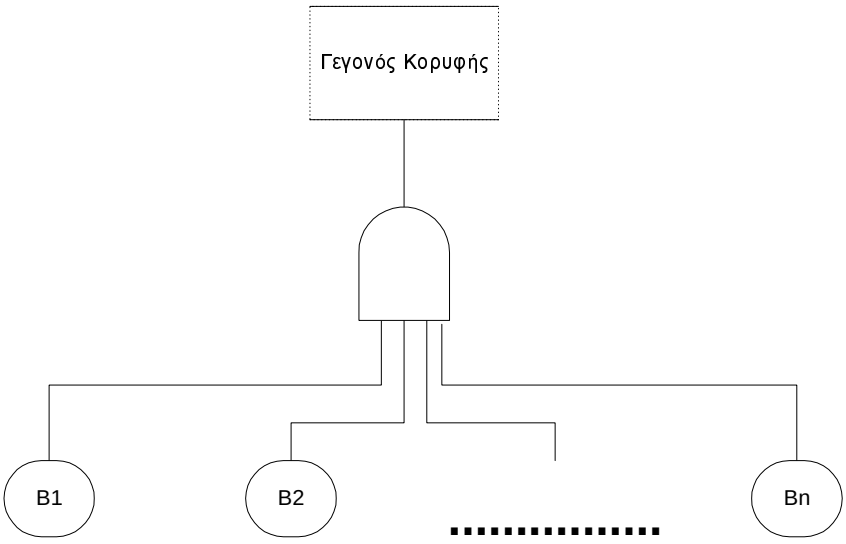
- **Διαθεσιμότητα του συστήματος** (System availability), $A_s(t)$ = Η πιθανότητα ότι το γεγονός κορυφής δεν υπάρχει στο χρόνο t. Το σύστημα δηλαδή είναι διαθέσιμο στο χρόνο t, λειτουργεί κανονικά αν δεν συμβαίνει το γεγονός κορυφής.
- **Μη διαθεσιμότητα του συστήματος** (System unavailability), $Q_s(t)$ = Η πιθανότητα ότι το γεγονός κορυφής υπάρχει στο χρόνο t. Το σύστημα δηλαδή δεν είναι διαθέσιμο στο χρόνο t και αποτυγχάνει. Η μη διαθεσιμότητα του συστήματος είναι συμπληρωματική με την διαθεσιμότητα του συστήματος και ισχύει: $A_s(t) + Q_s(t) = 1$.
- **Αξιοπιστία του συστήματος** (System reliability), $R_s(t)$ = Η πιθανότητα ότι το γεγονός κορυφής δεν συμβαίνει πάνω από ένα διάστημα χρόνου (0,t]. Η αξιοπιστία του συστήματος απαιτεί συνέχεια της μη ύπαρξης του γεγονότος κορυφής και διαφέρει από την διαθεσιμότητα του συστήματος. Η αξιοπιστία συχνά χρησιμοποιείται για να χαρακτηρίσει καταστροφικές αποτυχίες του συστήματος, αλλά και αποτυχίες που δεν μπορούν να επιδιορθωθούν. Ισχύει: $R_s(t) <= A_s(t)$.
- **Μη αξιοπιστία του συστήματος** (System unreliability), $F_s(t)$ = Η πιθανότητα ότι το γεγονός κορυφής συμβαίνει πριν από χρόνο t. Είναι συμπληρωματική με την αξιοπιστία και ισχύει: $R_s(t) + F_s(t) = 1$.Επιπλέον $F_s(t) >= Q_s(t)$.

2.2.1 Διαθεσιμότητα και μη διαθεσιμότητα για απλά συστήματα με ανεξάρτητα βασικά γεγονότα

Η συνήθης παραδοχή για τα βασικά γεγονότα $B_1,\ldots,B_n$ είναι ότι είναι ανεξάρτητα, πράγμα που σημαίνει ότι η εμφάνιση ενός βασικού γεγονότος δεν επηρεάζεται με κανέναν τρόπο από την εμφάνιση οποιουδήποτε άλλου βασικού γεγονότος.Για ανεξάρτητα βασικά γεγονότα, η ταυτόχρονη πιθανότητα ύπαρξης είναι πλέον

$$\Pr(B_1 \cap B_2 \cap \ldots \cap B_n) = \Pr(B_1)\Pr(B_2)\ldots\Pr(B_n)$$

Σύστημα με μία AND πύλη: Ένα σύστημα με μία πύλη AND φαίνεται στο Σχήμα 2.10



Σχήμα 2.10

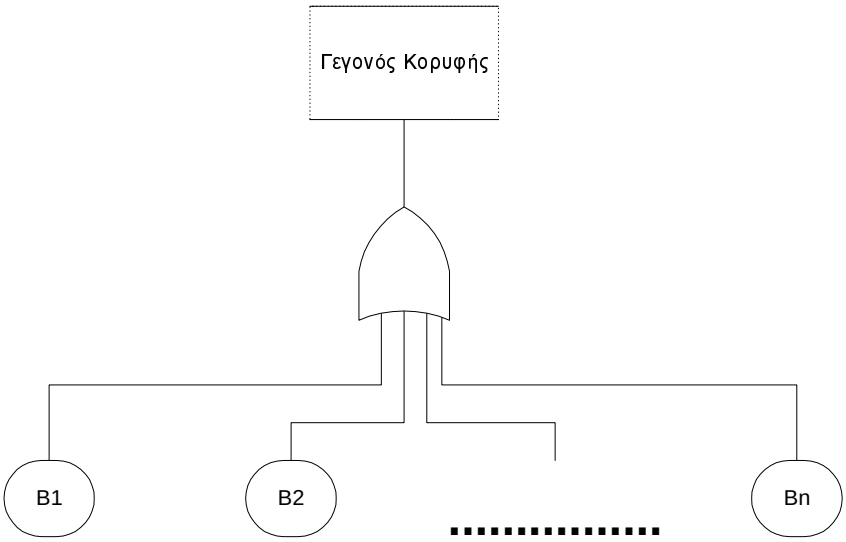
Η ταυτόχρονη ύπαρξη των βασικών γεγονότων $B_1,\ldots,B_n$ έχει ως αποτέλεσμα το γεγονός κορυφής. Έτσι η μη διαθεσιμότητα του συστήματος $Q_s(t)$ δίνεται από την πιθανότητα ότι όλα τα βασικά γεγονότα υπάρχουν στο χρόνο t:

$$Q_s(t) = \Pr(B_1 \cap B_2 \cap \ldots \cap B_n) = \Pr(B_1)\Pr(B_2)\ldots\Pr(B_n)$$

Για ένα σύστημα με μία πύλη AND, που έχει δύο εισόδους το $Q_s(t)$ είναι:

$$Q(t)=\Pr(B_1)\Pr(B_2)$$

Σύστημα με μία OR πύλη: Ένα σύστημα με μία πύλη OR φαίνεται στο Σχήμα 2.11



Σχήμα 2.11

Το γεγονός κορυφής υπάρχει στο χρόνο t, αν συμβαίνει τουλάχιστον ένα από τα βασικά γεγονότα σε αυτό το χρόνο. Η διαθεσιμότητα $A_s(t)$ και η μη διαθεσιμότητα $Q_s(t)$ του συστήματος δίνονται από:

$$A_s(t)= \Pr(\overline{B}_1 \cap \overline{B}_2 \cap \ldots \cap \overline{B}_n)$$

$$Q_s(t)= \Pr(B_1 \cup B_2 \cup \ldots \cup B_n)$$

Παρατηρούμε ότι η διαθεσιμότητα δίνεται από την τομή των συμπληρωματικών στοιχείων του Β. Το συμπληρωματικό στοιχείο του Β σημαίνει ότι δεν συμβαίνει το γεγονός Β στο χρόνο t. Η ανεξαρτησία των βασικών γεγονότων $B_1,\ldots,B_n$ οδηγεί και στην ανεξαρτησία των συμπληρωματικών τους. Έτσι η διαθεσιμότητα μπορεί να γραφτεί:

$$\begin{aligned} A_s(t) &= \Pr(\overline{B}_1)\Pr(\overline{B}_2)\ldots\Pr(\overline{B}_n) \\ &= \left[1-\Pr(B_1)\right]\left[1-\Pr(B_2)\right]\ldots\left[1-\Pr(B_n)\right] \end{aligned}$$

Και αφού ξέρουμε ότι ισχύει $A_s(t) + Q_s(t) = 1$, η μη διαθεσιμότητα μπορεί να υπολογιστεί ως εξής:

$$\begin{aligned} Q_s(t) &= \Pr(B_1 \cup B_2 \cup \ldots \cup B_n) \\ &= 1 - A_s(t) \\ &= 1 - \left[1-\Pr(B_1)\right]\left[1-\Pr(B_2)\right]\ldots\left[1-\Pr(B_n)\right] \end{aligned}$$

Όταν έχουμε δύο εισόδους ισχύει

$$\begin{aligned} Q_s(t) &= \Pr(B_1 \cup B_2) \\ &= \Pr(B_1) + \Pr(B_2) - \Pr(B_1)\Pr(B_2) \end{aligned}$$

Με άλλα λόγια, η πιθανότητα $Q_s(t)$ ότι τουλάχιστον ένα από τα γεγονότα B_1 και B_2 υπάρχει είναι ίση με το άθροισμα της πιθανότητας του κάθε γεγονότος ξεχωριστά αφαιρώντας την πιθανότητα της ταυτόχρονης ύπαρξης και των δύο γεγονότων.

Όταν έχουμε τρείς εισόδους ισχύει:

$$\begin{aligned} Q_s(t) &= \Pr(B_1 \cup B_2 \cup B_3) \\ &= \Pr(B_1) + \Pr(B_2) + \Pr(B_n) \\ &\quad - \Pr(B_1)\Pr(B_2) - \Pr(B_2)\Pr(B_3) - \Pr(B_3)\Pr(B_1) \\ &\quad + \Pr(B_1)\Pr(B_2)\Pr(B_3) \end{aligned}$$

2.2.2 Truth Tables

Ένας «Πίνακας Αληθείας» είναι η λίστα όλων των συνδυασμών των καταστάσεων των βασικών γεγονότων, η επακόλουθη πράξη να συμβεί το γεγονός της κορυφής και οι αντίστοιχες πιθανότητες για αυτούς τους συνδυασμούς. Μια πρόσθεση ενός συνόλου πιθανοτήτων από τον πίνακα αποφέρει την μη διαθεσιμότητα του συστήματος $Q_s(t)$ και μια πρόσθεση των συμπληρωματικών πιθανοτήτων τους δίνει την διαθεσιμότητα του συστήματος $A_s(t)$.

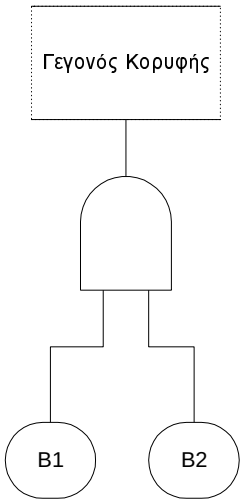
2.2.2.1 Σύστημα με μια πύλη AND

Ο Πίνακας 2.4 είναι ο Πίνακας Αληθείας (Truth Table) για το σύστημα του Σχήματος 2.12. Η μη διαθεσιμότητα του συστήματος $Q_s(t)$ δίνεται από από την παρακάτω συνάρτηση:

$$Q_s(t) = Pr(B_1) * Pr(B_2)$$

Πίνακας 2.4: Πίνακας Αληθείας για το δένδρο λαθών του Σχήματος 2.12

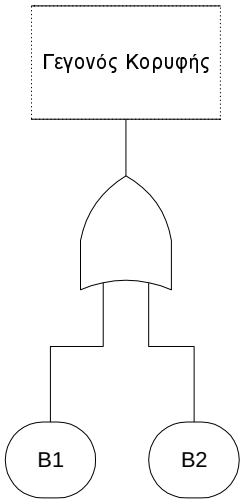
	Βασικό Γεγονός B_1	Βασικό Γεγονός B_2	Γεγονός Κορυφής	Πιθανότητα
1	Exists	Exists	Exists	$Pt(B_1)Pt(B_2)$
2	Exists	Not Exist	Not Exist	$Pr(B_1)Pr(B_2)$
3	Not Exist	Exists	Not Exist	$Pr(B_1)Pr(B_2)$
4	Not Exist	Not Exist	Not Exist	$Pr(B_1)Pr(B_2)$



Σχήμα 2.12

2.2.2.2 Σύστημα με μια πύλη OR

Το σύστημα του Σχήματος 2.13 αναπαριστάται από τον Πίνακα Αληθείας του Πίνακα 2.5. Η μη διαθεσιμότητα $Q_s(t)$ αποκτάται από την πρόσθεση των πιθανοτήτων των αμοιβαία αποκλειόμενων γραμμών 1, 2 και 3.



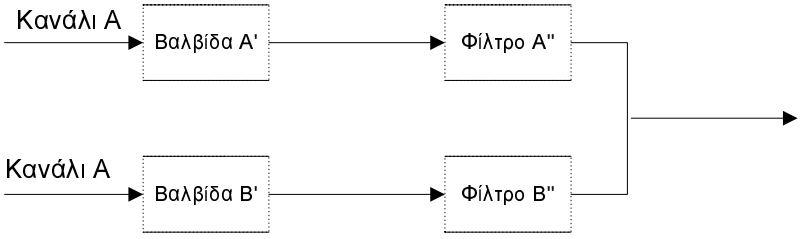
Σχήμα 2.13

$Q_s(t) = Pr(B_1)*Pr(B_2) + Pr(B_1)*Pr(B_2) + Pr(B_1)*Pr(B_2) =$
$= Pr(B_1)*[\ 1- Pr(B_2)] + [1-Pr(B_1)]*Pr(B_2) + Pr(B_1)*Pr(B_2)$
$= Pr(B_1) + Pr(B_2) - Pr(B_1)*Pr(B_2)$

Πίνακας 2.5: Πίνακας Αληθείας για το δένδρο λαθών του Σχήματος 2.13

	Basic Event B_1	Basic Event B_2	Top Event	Probability
1	Exists	Exists	Exists	$Pr(B_1)Pr(B_2)$
2	Exists	Not Exist	Exists	$Pr(B_1)Pr(B_2)$
3	Not Exist	Exists	Exists	$Pr(B_1)Pr(B_2)$
4	Not Exist	Not Exist	Not Exist	$Pr(B_1)Pr(B_2)$

Στη συνέχεια θα παρουσιαστεί ένα πρόβλημα για να κατανοήσετε την χρήση των Πινάκων Αληθείας. Ο πίνακας αληθείας παρέχει μια χρονοβόρα αλλά και αξιόπιστη τεχνική για υπολογισμούς της διαθεσιμότητας και της μη διαθεσιμότητας για μέσα πολύπλοκα συστήματα, όπως δείχνει το παρακάτω παράδειγμα. Ένα εργοστάσιο έχει δύο παράλληλα Κανάλια Α και Β, και περιέχει μια αντλία και ένα φίλτρο όπως στο Σχήμα 2.14. Η πιθανότητα αποτυχίας των αντλιών και των φίλτρων είναι αντίστοιχα 0,04 και 0,08 αποτυχίας κάθε μέρα, είτε ο εξοπλισμός είναι σε λειτουργία είτε σε αναμονή. Υποθέστε ότι ο απαραίτητος χρόνος για τους σωλήνες και τα φίλτρα αντίστοιχα είναι των 5 και 10 ωρών. Το σχήμα αυτού του προβλήματος είναι στο Σχήμα 2.14:

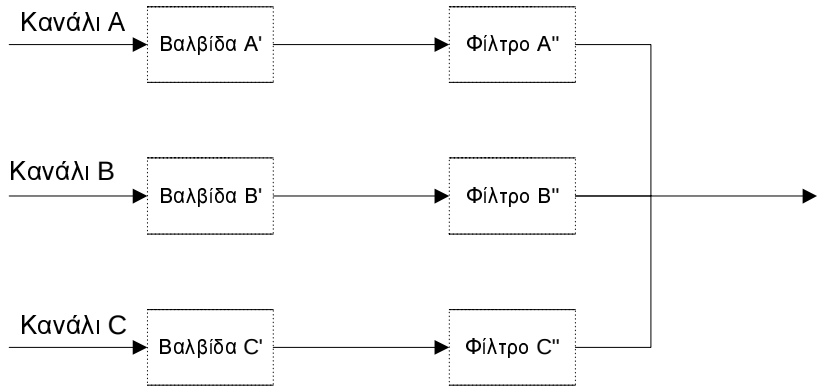


Σχήμα 2.14

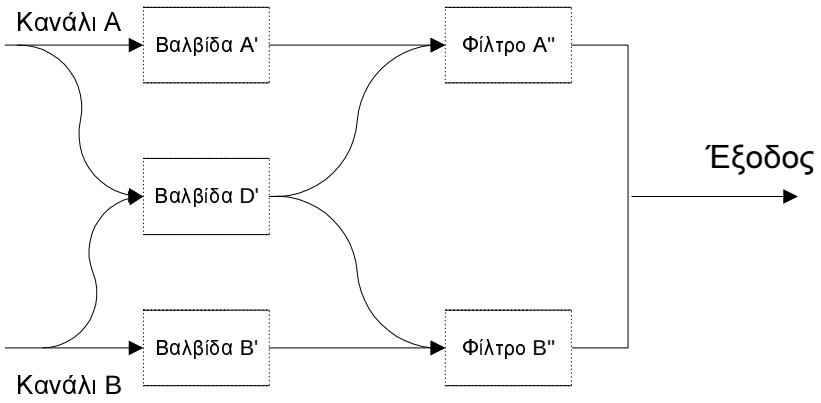
Δυό ενναλακτικές περιπτώσεις για να αυξήσουμε την διαθεσιμότητα του εργοστασίου είναι στο Σχήμα 2.15 και Σχήμα 2.16:

1. Προσθέστε ένα τρίτο πανομοιότυπο, C
2. Εγκατέστησε ένα τρίτο σωλήνα μεταφοράς ικανό για την μεταφορά υλικού σε κάθε φίλτρο

Σύγκρινε τα αποτελέσματα των δύο παραπάνω σχεδίων στην ικανότητα του εργαστασίου να διατηρεί: (a) πλήρες αποτέλεσμα και (b) όχι λιγότερο από το μισό αποτέλεσμα



Σχήμα 2.15



Σχήμα 2.16

Η λύση των εξισώσεων αυτού του προβλήματος, επειδή είναι πολύ πολύπλοκες δεν θα αναλυθούν σε αυτό το κεφάλαιο. Αλλά μπορείτε να ανατρέξετε στη σελίδα 305-309 του βιβλίου «Reliability Enginneering and Risk Assessment» των Ernest J. Henley και Hiromitsu Kumamoto.

2.2.3 Υπολογισμοί της διαθεσιμότητας και της μη διαθεσιμότητας χρησιμοποιώντας structure functions (συναρτήσεις δομής)

2.2.3.1 Structure functions

Είναι πιθανό να περιγράψουμε την κατάσταση του βασικού γεγονότος ή ολόκληρου του συστήματος με μία δυαδική μεταβλητή. Έστω ότι αυτή είναι Y_i για το βασικό γεγονός i, τότε

$Y_i = 1$, όταν το βασικό γεγονός συμβαίνει
$Y_i = 0$, όταν το βασικό γεγονός δεν συμβαίνει.

Ομοίως το γεγονός κορυφής σχετίζεται με μία δυαδική μεταβλητή ψ(Y) που αναφέρεται στην κατάσταση του συστήματος και έχουμε

ψ(Y) = 1, όταν το γεγονός κορυφής συμβαίνει,
ψ(Y) = 0, όταν το γεγονός κορυφής δεν συμβαίνει.

Η συνάρτηση ψ(Y) είναι γνωστή σαν συναρτήσεις δομής για το γεγονός κορυφής. Οι ενώσεις και οι τομές, ∪ και ∩, χρησιμοποιούνται για να εκφράσουν τις σχέσεις μεταξύ των γεγονότων, και αντιστοιχούν στους Boolean τελεστές ∨(OR) και ∧(AND), και στους συνηθισμένους αλγεβρικούς τελεστές + και *. Επίσης πρέπει να σημειωθεί ότι $Pr(B_i) = E(Y_i)$, έτσι E( ) είναι ένας αναμενόμενος αριθμός, ή πιθανότητα.Οι τελεστές ∨ και ∧ μπορούν να χειριστούν σύμφωνα με τους κανόνες της άλγεβρας Boole.

2.2.3.2 Αναπαράσταση του συστήματος με όρους από συναρτήσεις δομής

Το σύστημά μας μπορεί να αναπαρασταθεί με όρους από συναρτήσεις δομής. Το γεγονός κορυφής του δένδρου με πύλη AND του Σχήματος 2.10 υπάρχει, αν και μόνο αν υπάρχουν τα βασικά γεγονότα $B_1,\ldots,B_n$. Με όρους από συναρτήσεις δομής έχουμε,

$$\psi(Y) = \psi(Y_1, Y_2,..., Y_n) = \bigwedge_{i=1}^{n} Y_i = Y_1 \wedge Y_2 \wedge ... \wedge Y_n$$

Η συναρτήση δομής μπορεί να εκφραστεί με όρους αλγεβρικών τελεστών, έτσι

$$\psi(Y)=\prod_{i=1}^{n} Y_i = Y_1 Y_2,..., Y_n$$

Αντίστοιχα, το γεγονός κορυφής του δέντρου με πύλη OR του Σχήματος 2.11 εμφανίζεται αν συμβαίνει οποιοδήποτε από τα γεγονότα $B_1,\ldots,B_n$. Η συνάρτηση δομής αυτή τη φορά είναι

$$\psi(Y) = \psi(Y_1, Y_2,..., Y_n) = \bigvee_{i=1}^{n} Y_i = Y_1 \vee Y_2 \vee ... \vee Y_n$$

και η αλγεβρική της μορφή είναι

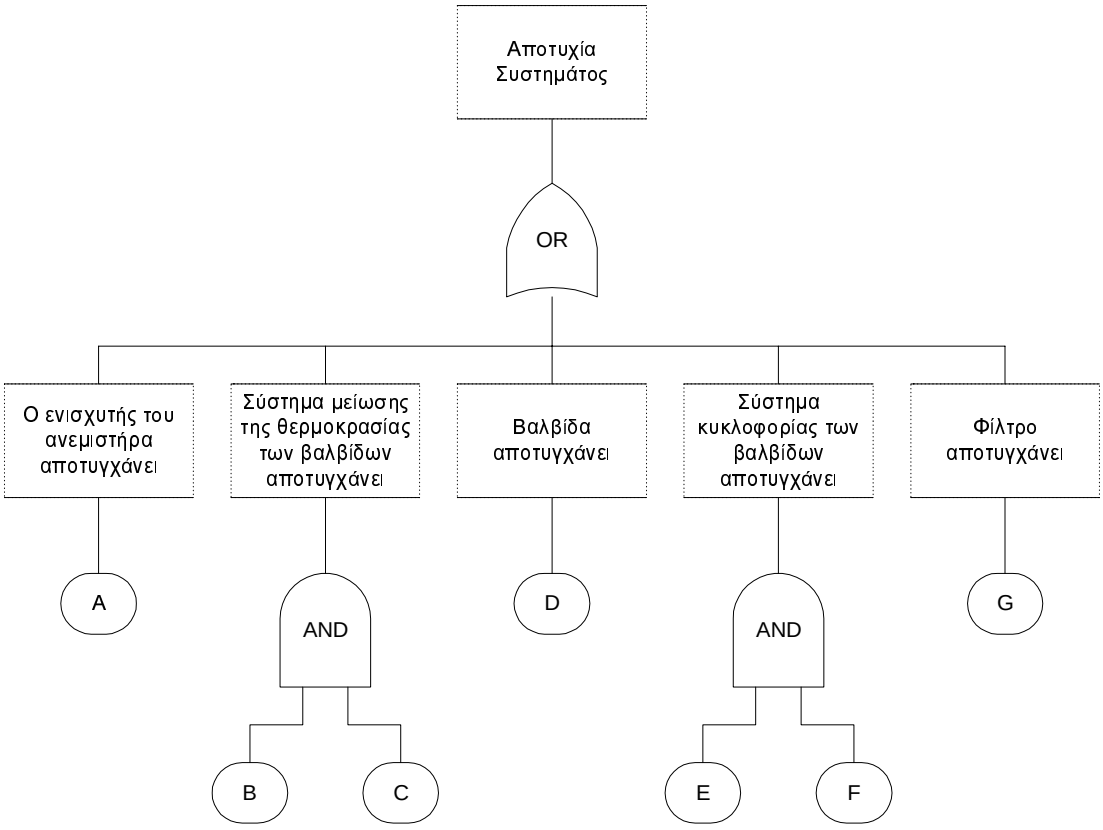
$$\begin{aligned}\psi(Y) &= 1 - \prod_{i=1}^{n} [1 - Y_i] \\ &= 1 - [1 - Y_1][1 - Y_2]\ldots[1 - Y_n]\end{aligned}$$

Αν το δένδρο στο σχήμα 2.4 έχει δύο εισόδους η συνάρτηση δομής γίνεται

$$\psi(Y)= Y_1 \vee Y_2 = 1-[1-Y_1][1-Y_2]$$
$$= Y_1+Y_2-Y_1Y_2$$

αυτό το αποτέλεσμα είναι ανάλογο με τον υπολογισμό της μη διαθεσιμότητας, όπου τότε το Y_1Y_2 είναι η πιθανότητα να συμβαίνουν τα γεγονότα B_1 και B_2 ταυτόχρονα.

Οι συναρτήσεις δομής μπορούν να επιτευκτούν με διαδοχικά βήματα. Για παράδειγμα, για το παρακάτω δέντρο του Σχήματος 2.17



Σχήμα 2.17

η συνάρτηση δομής δίνεται με τον ακόλουθο τρόπο:

$$\psi_1(Y)=Y_B \wedge Y_C=Y_BY_C, \quad \psi_2(Y)=Y_E \wedge Y_F=Y_EY_F$$

όπου $\psi_1(Y)$ είναι η συνάρτηση δομής για την πρώτη AND πύλη
$\psi_2(Y)$ είναι η συνάρτηση δομής για την δεύτερη AND πύλη.

Εδώ, το Y_B είναι μια δυαδική μεταβλητή για το βασικό γεγονός B, κ.τ.λ. Η συνάρτηση δομής για όλο το δένδρο λαθών είναι

$$\Psi(Y)=Y_A \vee \psi_1(Y) \vee Y_D \vee \psi_2(Y) \vee Y_G$$
$$=1-[1-Y_A][1-\psi_1(Y)][1-Y_D][1-\psi_2(Y)][1-Y_G]$$
$$=1-[1-Y_A][1-Y_BY_C][1-Y_D][1-Y_EY_F][1-Y_G]$$

2.2.3.3 Υπολογισμοί της μη διαθεσιμότητας χρησιμοποιώντας συναρτήσεις δομής

Έχει μεγάλη σημασία να αναγνωρίσουμε την πιθανολογική φύση των εκφράσεων που χρησιμοποιήσαμε στην προηγούμενη παράγραφο. Αν εξετάσουμε το σύστημα σε κάποιο χρόνο και η κατάσταση του βασικού γεγονότος Y_i θεωρηθεί να είναι μια τυχαία μεταβλητή Bernoulli, τότε η $\psi(Y)$ είναι επίσης μια τυχαία μεταβλητή Bernoulli. Η πιθανότητα εμφάνισης της κατάστασης $Y_i = 1$ είναι ίση με την αναμενόμενη τιμή της Y_i και με την πιθανότητα του γεγονότος B_i.

$$Pr(Y_i=1) = Pr(B_i) = E(Y_i)$$

Να σημειωθεί ότι αυτή η πιθανότητα είναι η μη διαθεσιμότητα $Q_s(t)$. Η πιθανότητα του γεγονότος κορυφής, η μη διαθεσιμότητα $Q_s(t)$, είναι η πιθανότητα $Pr(\psi(Y)=1)$, ή η ελπίδα $E(\psi(Y))$. Ένας εναλλακτικός τρόπος για να φανεί αυτό είναι ο ακόλουθος:

$$Q_s(t) = Pr(\text{top event}) = Pr(\psi(Y)=1) = E(\psi(Y))$$

2.2.4 Υπολογισμοί μη διαθεσιμότητας χρησιμοποιώντας αναπαραστάσεις ελάχιστης τομής

Στην ενότητα που προηγήθηκε παρουσιάστηκε μια μέθοδος για την κατασκευή συναρτήσεων δομής για τον υπολογισμό της μη διαθεσιμότητας του συστήματος. Σε αυτήν την ενότητα, θα παρουσιαστεί μια άλλη προσέγγιση βασισμένη στα σύνολα ελάχιστης τομής ή σύνολα ελάχιστων μονοπατιών.

Θεωρείστε ένα δένδρο λαθών που έχει τα ακόλουθα σύνολα ελάχιστης τομής.

$\{ B_{1,1}, B_{2,1}, \ldots, B_{n1,1} \}$: σύνολο τομής 1
……
$\{ B_{1,j}, B_{2,j}, \ldots, B_{nj,j} \}$: σύνολο τομής j
……
$\{ B_{1,m}, B_{2,m}, \ldots, B_{nm,m} \}$: σύνολο τομής m

Σημειώστε ως $Y_{i,j}$ την μεταβλητή για το γεγονός $B_{i,j}$. Το γεγονός της κορυφής συμβαίνει μόνο και μόνο αν όλα τα βασικά γεγονότα συμβαίνουν ταυτόχρονα. Για αυτό το λόγο το δένδρο λαθών του Σχήματος 2.18 είναι ισοδύναμο στο δένδρο λαθών. Η συνάρτηση δομής του δένδρου λαθών είναι

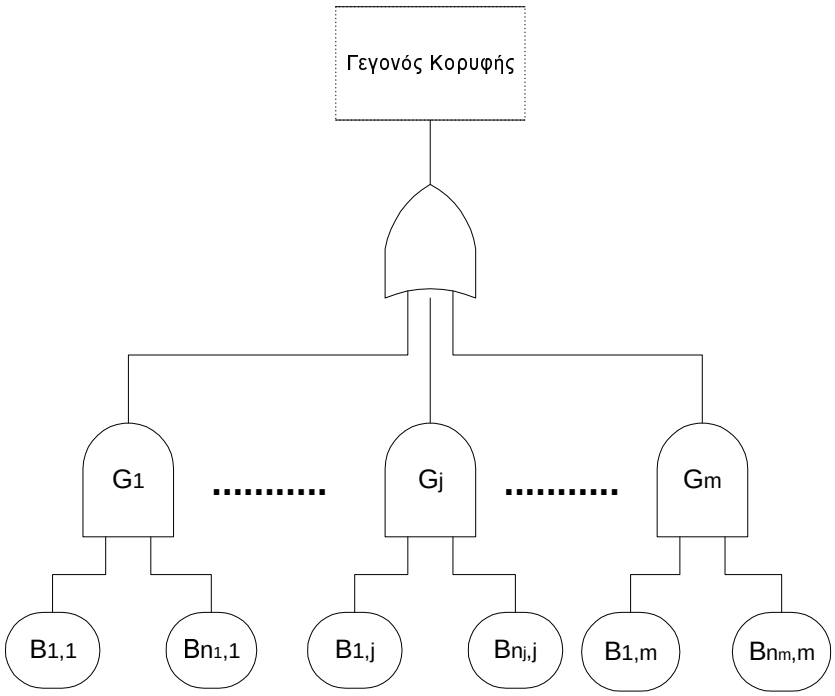
$$\psi(Y) = \bigvee_{j=1}^{m} \left[\bigwedge_{i=1}^{nj} Y_{i,j} \right]$$

και η αλγεβρική του μορφή δίνεται από την παρακάτω σχέση

$$\psi(\mathrm{Y}) = \bigvee_{j=1}^{m}\left[\prod_{i=1}^{n_j} \mathrm{Y}_{i,\,j}\right] = 1 - \prod_{j=1}^{m}\left[1 - \prod_{i=1}^{n_j} \mathrm{Y}_{i,\,j}\right]$$

Θεωρείστε το $\kappa_j(Y)$ ότι είναι μια συνάρτηση δομής για την πύλη AND G_j του Σχήματος 2.18:

$$\kappa_j(\mathrm{Y}) = \prod_{i=1}^{n_j} \mathrm{Y}_{i,\,j}$$



Πρώτη ελάχιστη τομή jστη ελάχιστη τομή mστη ελάχιστη τομή

Σχήμα 2.18

Η συνάρτηση $\kappa_j(Y)$ είναι το j*στη* δομή ελάχιστης τομής. Η ισότητα με την αλγεβρική μορφή μπορεί να γραφεί ως

$$\psi(\mathrm{Y}) = 1 - \prod_{j=1}^{m}\left[1 - \kappa_j(\mathrm{Y})\right]$$

2.2.5 Υπολογισμοί μη διαθεσιμότητας χρησιμοποιώντας αναπαραστάσεις ελάχιστου μονοπατιού

Θεωρείστε ένα δένδρο λαθών με *m* σύνολα ελάχιστου μονοπατιού:

$\{ B_{1,1}, B_{2,1}, \ldots, B_{n1,1} \}$: σύνολο μονοπατιού 1

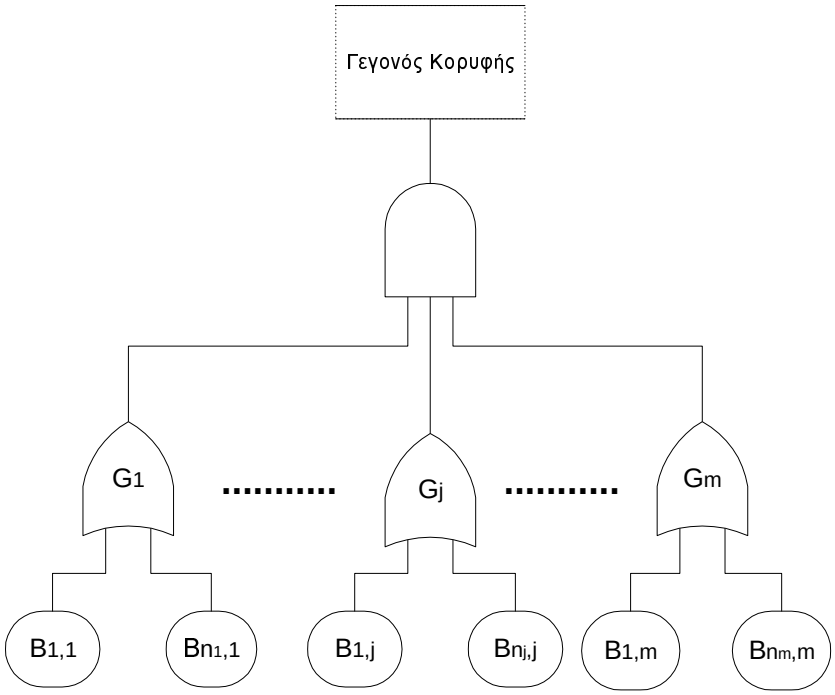
…….....

$\{ B_{1,j}, B_{2,j}, \ldots, B_{nj,j} \}$: σύνολο μονοπατιού j

……

$\{ B_{1,m}, B_{2,m}, \ldots, B_{nm,m} \}$: σύνολο μονοπατιού m

Σημειώστε ως $Y_{i,j}$ την μεταβλητή για το γεγονός $B_{i,j}$. Το γεγονός της κορυφής συμβαίνει μόνο και μόνο αν όλα τα βασικά γεγονότα συμβαίνουν ταυτόχρονα. Για αυτό το λόγο το δένδρο λαθών του Σχήματος 2.19 είναι ισοδύναμο στο δένδρο λαθών.



Πρώτη ελάχιστη τομή jστη ελάχιστη τομή mστη ελάχιστη τομή

Σχήμα 2.19

Η συνάρτηση δομής για το δένδρο είναι

$$\psi(Y) = \bigwedge_{j=1}^{m} \left[\bigvee_{i=1}^{nj} Y_{i,j} \right]$$

Η αλγεβρική του μορφή ειναι

$$\psi(Y) = \bigwedge_{j=1}^{m} \left[1 - \prod_{i=1}^{nj} [1 - Y_{i,j}] \right] = \prod_{j=1}^{m} \left[1 - \prod_{i=1}^{nj} [1 - Y_{i,j}] \right]$$

Το $\rho_j(Y)$ είναι η συνάρτηση δομής για την πύλη OR G_j του Σχήματος 2.19

$$\rho_j(Y) = 1 - \prod_{i=1}^{nj} \left[1 - Y_{i,j} \right]$$

Η συνάρτηση δομής της αλγεβρικής μορφής μπορεί να γραφεί ως

$$\psi(Y) = \prod_{j=1}^{m} \rho_j(Y)$$

2.2.6 Υπολογισμοί μη διαθεσιμότητας χρησιμοποιώντας την αρχή της Inclusion-Exclusion

Έστω ένα γεγονός d_t ως

> d_t = όλα τα βασικά γεγονότα που συμβαίνουνστο *ίστο* cut set την χρονική στιγμή t

Το γεγονός κορυφής S μπορεί να εκφραστεί με όρους του d_t ως

$$S = \bigcup_{i=1}^{N_c} d_i \quad (N_c = \text{συνολικός αριθμός των συνόλων ελάχιστης τομής})$$

το οποίο καταλήγει στο

$$\begin{aligned} Q_s(t) &= \Pr\left(\bigcup_{i=1}^{N_c} d_i\right) \\ &= \sum_{i=1}^{N_c} \Pr(d_i) - \sum_{i=2}^{N_c} \sum_{j=1}^{i-1} \Pr(d_i \cap d_j) + \\ &= \ldots + (-1)^{Nc-1} \Pr(d_1 \cap d_2 \cap \ldots \cap d_{N_c}) \end{aligned}$$

Η δεύτερη συνάρτηση είναι επέκταση της πρώτης και απορέει από την αρχή της *Inclusion-Exclusion*. Ο *m στος* όρος στο δεξί μέλος της δεύτερης συνάρτησης δηλώνει την συμβολή της $Q_s(t)$ των *m* σύνολων ελάχιστης τομής από τα N_c που αποτυγχάνουν ταυτόχρονα στη χρονική στιγμή *t*. π.χ. όλα τα βασικά γεγονότα σε αυτά τα *m* σύνολα ελάχιστης τομής συμβαίνουν. Μια πολύ χρήσιμη ιδιότητα της δεύτερης συνάρτησης είναι ότι η πιθανότητα του γεγονότος κορυφής δίνεται με όρους παραγοντοποίησης, που είναι ευκολότερο για να υπολογίσεις αυτά τα τμήματα. Για μικρά συστήματα είναι σχετικά εύκολο να ληφθούν ακριβείς τιμές για το $Q_s(t)$. Αυτό φαίνεται από το παράδειγμα που υπάρχει στη Σελίδα 321 του βιβλίου «Reliability Enginneering and Risk Assessment» των Ernest J. Henley και Hiromitsu Kumamoto.

2.2.7 Χρήση των άνω και κάτω ορίων για την ποσοτική ανάλυση

Για μεγάλα και πολύπλοκα δένδρα, οι υπολογισμοί για την εύρεση της ακριβής τιμής της μη διαθεσιμότητας του συστήματος είναι χρονοβόρες. Όταν ο χρόνος γίνεται παράγοντας για τους υπολογισμούς, τότε χρησιμοποιούμε τα άνω και κάτω όρια της μη

διαθεσιμότητας που χρησιμοοιούνται και από το πρόγραμμα που αναπτύσσουμε στην επόμενη ενότητα.

Για τον υπολογισμό χρησιμοποιούμε μια μέθοδο ευθείας υπολογισμού από τις πιθανότητες που είναι ανεξάρτητες. Αυτή η μέθοδος βασίζεται πάνω στο μειωμένο δένδρο λαθών. Αλλά η ακρίβεια του αποτελέσματος εξαρτάται και από το πλήθος των όρων που υπάρχουν στην έκφραση για την πιθανότητα του γεγονότος της κορυφής. Η πολυπλόκοτητα μιας τέτοιας απορρέει από το γεγονός ότι το ίδιο στοιχειώδες γεγονός μπορεί να υπάρχει και σε άλλα μέρη του δένδρου λαθών, δηλαδή σημαίνει ότι τα συστατικά του δένδρου λαθών δεν είναι ανεξάρτητα.

Αν τα σύνολα ελάχιστης τομής είναι αυτά (M1, M2, ..., Mn), το δένδρο λαθών είναι ισοδύναμο με την έκφραση (M1 OR M2 OR ...OR Mn). Θυμηθείτε ότι τα σύνολα ελάχιστης τομής είναι είτε αμοιβαίως αποκλειόμενα, είτε ανεξάρτητα. Η γενική έκφραση για την πιθανότητα του OR των n γεγονότων είναι:

$$P(M_1 \cup M_2 \cup \ldots \cup M_n) = \sum_{i=1}^{n} P(M_i) - \sum_{i=2}^{n}\sum_{j=1}^{i-1} P(M_i \cup M_j) + \sum_{i=3}^{n}\sum_{j=2}^{i-1}\sum_{k=1}^{j-1} (M_i \cap M_j \cap M_k) - \ldots + (-1)^{n-1} P(M_1 \cup M_2 \cup \ldots \cup M_n)$$

Αυτό είναι το άθροισμα όρων που ο καθένας είναι η πιθανότητα των συνόλων ελάχιστης τομής που συνδεόνται με τις πύλες AND. Η πιθανότητα των AND των συνόλων ελάχιστης τομής δεν είναι απλώς το προιόν των ατομικών τους πιθανοτήτων, καθώς μπορεί να μοιράζονται τα ίδια στοιχειώδη γεγονότα. Υποθέστε ότι όλα τα στοιχειώδη γεγονότα είναι ανεξάρτητα, τότε η πιθανότητα των AND των συνόλων ελάχιστης τομής είναι το προιόν των πιθανοτητων όλων των στοιχειωδών γεγονότων σε κάθε σύνολο τομής, υπολογίζοντας τα ένα ένα κάθε φορά.

Αυτή η σειρά έχει 2^N όρους, όπου N είναι ο αρθμός των συνόλων ελάχιστης τομής. Γενικά θα έπαιρνε ένα αρκετά μεγάλο χρονικό διάστημα για να υπολογιστούν οι όροι αυτής της σειράς. Επειδή στη πραγματικότητα δεν χρειάζεται να υπολογιστούν όλοι οι όροι, χρησιμοποιείται η παρακάτω απλοποιημένη έκφραση.

$$P_1 = \sum_{i=1}^{n} P(M_i)$$

$$P_1 = P_1 - \sum_{i=2}^{n}\sum_{j=1}^{i-1} P(M_i \cup M_j)$$

$$P_1 = P_2 - \sum_{i=3}^{n}\sum_{j=2}^{i-1}\sum_{k=1}^{j-1} (M_i \cap M_j \cap M_k)$$

…

Η σειρά έχει N όρους ο καθένας από τους οποίους έχει υποόρους και συνολικά υπάρχουν 2*N όροι. Ο πρώτος όρος είναι απλώς το άθροισμα των πιθανοτήτων των συνόλων ελάχιστης τομής. Οι μεταβολές στη σειρά εναλάσσονται (αύξηση ή μείωση) και μπορεί να δειχθεί ότι οι όροι πάντα αποτελούν διαστήματα της απάντησης, π.χ. ο πρώτος όρος είναι ένα ανώτερο όριο, ο δεύτερος όρος είναι ένα κάτω όριο, ο τρίτος όρος είναι ένα καλύτερο πάνω όριο, κλπ. Γι αυτό το αποτέλεσμα μπορεί να φτιαχτεί ακριβές παίρνοντας ένα επαρκές πλήθος όρων π.χ.

$$\forall x \exists n : | P_i - P | < x \quad \forall i > n$$

όπου

$P = P(M_1 \cup M_2 \cup \ldots \cup M_n)$

Στην πραγματικότητα οι όροι μικραίνουν με γοργό ρυθμό και είναι σχεδόν περιττό να προχωρήσουμε μετά το τρίτο όρο. Για 100 σύνολα ελάχιστης τομής, ο πρώτος όρος έχει 100 υποόρους, ο δεύτερος όρος έχει 4950 υποόρους, ο τρίτος 161,700 και ο τέταρτος 3,921,225. Η καλύτερη μέθοδος είναι να υπολογίζουμε τους πρώτους δύο όρους και να προχωρούμε στον τρίτο ή παραπάνω, μόνο αν είναι απαραίτητο.

2.2.8 Ποσοτική ανάλυση του συστήματος με τη μέθοδο KITT

Η λέξη KITT είναι συντομογραφία της έκφρασης θεωρία δένδρου κίνησης (kinetic tree theory). Η μέθοδος KITT χρησιμοποιείται για την ποσοτικοποίηση ποικίλων παραμέτρων του συστήματος για μεγάλα και πολύπλοκα δέντρα λαθών. Πιο συγκεκριμένα ξεκινάμε βρίσκοντας τα **σύνολα ελάχιστης τομής** ή τα **σύνολα ελάχιστων μονοπατιών**, με τη διαδικασία που περιγράψαμε στη παράγραφο 2.1. Στη συνέχεια μπορούμε να εκτιμήσουμε ποσοτικά την μη διαθεσιμότητα (unavailability) του συστήματος, τη διαθεσιμότητα (availability), τον αναμενόμενο αριθμό αποτυχιών (expected number of failures) και επισκευών (expected number of repairs) που θα χρειαστούν, την αποτυχία υπο όρους (conditional failure) και την ένταση επισκευών (repair intensity).

Η μέθοδος KITT χειρίζεται ανεξάρτητα βασικά γεγονότα, τα οποία είτε είναι επισκευάσιμα είτε όχι, αρκεί να έχουν σταθερά ποσά αποτυχίας λ και σταθερά ποσά επισκευής μ. Επίσης απαιτεί να δέχεται σαν είσοδο τα σύνολα ελάχιστης τομής ή τα σύνολα ελάχιστων μονοπατιών και επιτρέπει τη χρήση των πυλών inhibit.

Οι παράμετροι αξιοπιστίας, που εξαρτώνται από το χρόνο, είναι καθορισμένες για κάθε βασικό γεγονός και για κάθε συνόλο τομής, όμως για όλο το σύστημα οι παράμετροι υπολογίζονται με τη βοήθεια των πάνω και κάτω ορίων (upper and lower bounds), ή με τη τεχνική braketing. Τα πάνω και κάτω όρια είναι γενικά εξαιρετικές προσεγγίσεις στις ακριβείς παραμέτρους, ενώ με τη τεχνική braketing οι ακριβείς τιμές για τις παραμέτρους του συστήματος επιτυγχάνονται μόνο αν το επιθυμεί ο χρήστης.

Το w(t) και το u(t) υπολογίζονται πριν από το Q(t) με τους παρακάτω τύπους:

$$w(t) = f(t) + \int_0^t f(t-u)v(u)du$$

$$v(t) = \int_0^t g(t-u)w(u)du$$

Το w(t) είναι η χωρίς όρους ένταση της αποτυχίας, το u(t) η ένταση της επισκευής και υπολογίζονται με αριθμητική ολοκλήρωση, όταν τα f(t) και g(t) είναι γνωστά. Στην περίπτωση που απαιτείται μια αυστηρή και αναλυτική λύση, μπορούν να χρησιμοποιηθούν οι μετασχηματισμοί Laplace.

Παράμετροι συνόλων ελάχιστης τομής: Ένα σύνολο τομής συμβαίνει αν όλα τα βασικά γεγονότα στο σύνολο τομής συμβαίνουν. Η πιθανότητα να συμβαίνει το σύνολο τομής σε χρόνο t, Q*(t) είναι:

$$Q^*(t) = \Pr(B_1 \cap B_2 \cap \ldots \cap B_n) = \prod_{j=1}^{n} Q_j(t)$$

όπου n είναι ο αριθμός των μελών που βρίσκονται στο σύνολο τομής και το $Q_j(t)$ η πιθανότητα της ύπαρξης του joστου βασικού γεγονότος στο χρόνο t. Έτσι όταν έχουμε ένα δέντρο λαθών μπορούμε να εντοπίσουμε τα σύνολα τομής και γνωρίζοντας τα λ και μ μπορούμε να υπολογίσουμε τις παραμέτρους που θέλουμε.

Η μέθοδος KITT δέχεται σαν είσοδο και σύνολα μονοπατιών και οι υπολογισμοί γίνονται με τον ίδιο ακριβώς τρόπο όπως με τα σύνολα τομής.

Η μη διαθεσιμότητα του συστήματος $Q_s(t)$: Το γεγονός d_i ορίζεται σαν όλα τα βασικά γεγονότα στο ioστό σύνολο ελάχιστης τομής που υπάρχουν στο χρόνο t. Η παρακάτω σχέση:

$$\begin{aligned} Q_s(t) &= \Pr\left(\bigcup_{i=1}^{N_c} d_i\right) \\ &= \sum_{i=1}^{N_c} \Pr(d_i) - \sum_{i=2}^{N_c}\sum_{j=1}^{i-1} \Pr(d_i \cap d_j) + \\ &= \ldots + (-1)^{Nc-1} \Pr(d_1 \cap d_2 \cap \ldots \cap d_{N_c}) \end{aligned}$$

που παραθέσαμε σε προηγούμενη παράγραφο του κεφαλαίου μπορεί να γραφτεί και ως εξής:

$$\begin{aligned} Q_s(t) = &\sum_{i=1}^{N_c} \Pr(d_i) - \sum_{i=2}^{N_c}\sum_{j=1}^{i-1} \Pr(d_i \cap d_j) + \\ &\ldots + (-1)^{m-1} \sum_{1 \le i_1 < i_2 < \ldots < i_m < N_c} \Pr(d_{i1} \cap d_{i2} \cap \ldots \cap d_{im}) + \\ &\ldots + (-1)^{Nc-1} \Pr(d_1 \cap d_2 \cap \ldots \cap d_{N_c}) \end{aligned}$$

Ο μοστός όρος στο δεξιό μέλος της εξίσωσης είναι οι m αποτυχίες του σύνολου ελάχιστης τομής που υπάρχουν ταυτόχρονα στο χρόνο t. Έτσι η εξίσωση μπορεί να γραφτεί σαν:

$$Q_s(t) = \sum_{i=1}^{Nc} Q_1*(t) - \sum_{i=2}^{Nc}\sum_{j=1}^{i-1}\prod_{i,j} Q(t) +$$

$$\ldots+(-1)^{m-1} \sum_{1\le i_1<i_2<\ldots<i_m<N_c} \prod_{i_1\ldots i_m} Q(t) +$$

$$\ldots+(-1)^{Nc-1} \prod_{i_1\ldots i_{Nc}} Q(t)$$

όπου $\prod_{i_1\ldots i_m}$ είναι το αποτέλεσμα του Q(t) για τα βασικά γεγονότα στο σύνολο τομής i_1,or i_2,…, or i_m. Τα πάνω και τα κάτω όρια μπορούν να υπολογιστούν ως εξής:

$$\sum_{i=1}^{Nc} Q_i*(t) - \sum_{i=2}^{Nc}\sum_{j=1}^{i-1}\prod_{i,j} Q(t) \le Q_s(t) \le \sum_{i=1}^{Nc} Q_i*(t)$$

όπου $\prod_{i,j}$ είναι το αποτέλεσμα του Q(t) για το βασικό γεγονός το οποίο είναι μέλος είτε του συνόλου τομής i, είτε του j.

Η παράμετρος του συστήματος $w_s(t)$: Η παράμετρος $w_s(t)$ είναι ο αναμενόμενος αριθμός των φορών που το γεγονός κορυφής συμβαίνει σε χρόνο t, στη μονάδα του χρόνου. Με κάποιους πολύπλοκους υπολογισμούς μπορούμε να εκτιμήσουμε την παράμετρο αυτή. Από τη στιγμή που έχουμε υπολογίσει τα $w_s(t)$ και $Q_s(t)$ είναι εξαιρετικά εύκολο να υπολογίσουμε και τις άλλες παραμέτρους λ_s και Ws, από το τύπο:

$$w_s(t)dt = \left[1 - Q_s(t)\right]\lambda_s(t)dt$$

2.2.9 Ποσοτικοποίηση της αξιοπιστίας (reliability) του συστήματος

Το W, ο αναμενόμενος αριθμός των αποτυχιών και το Q, η μη διαθεσιμότητα του συστήματος, αναφέρονται σε μια υπάρχουσα πιθανότητα για μια αποτυχία του συστήματος και είναι χρήσιμα για προβλεπόμενα και όχι καταστροφικά λάθη, όπως τα λάθη κατασκευής. Αυτού του είδους η αποτυχία του συστήματος δεν έχει αποτέλεσμα ολοκληρωτική καταστροφή του συστήματος και θα συμβαίνει πολλές φορές κατά τη διάρκεια της ζωής (λειτουργίας) του. Ένα λάθος το οποίο συμβαίνει και επισκευάζεται πριν από χρόνο t μπορεί να συμβεί ξανά στο χρόνο t.

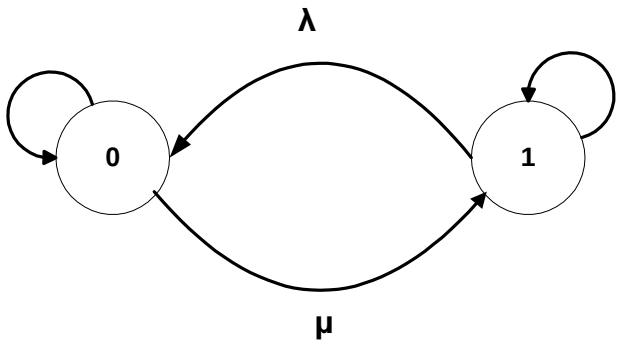
Από την άλλη πλευρά, η αξιοπιστία του συστήματος είναι πιο χρήσιμη για περιγραφή καταστροφικών, μη-επισκευάσιμων διακοπών του συστήματος, όπως είναι

εκρήξεις κ.τ.λ. Αυτού του είδους τα λάθη καταστρέφουν το σύστημα, έτσι η πιθανότητα να εμφανιστεί ξανά στο ίδιο σύστημα είναι ασήμαντη. Η αξιοπιστία (reliability) του συστήματος $R_s(t)$, είναι η πιθανότητα ότι το σύστημα υποφέρει από κινδύνους που δεν υπάρχουν στο χρόνο t, και είναι ισοδύναμη με την πιθανότητα επιβίωσης του συστήματος. Το συμπλήρωμά του είναι η αναξιοπιστία (unrealibility) του συστήματος $F_s(t)$, η οποία ορίζεται ως η πιθανότητα ότι το σύστημα υποφέρει από ένα κίνδυνο στο χρόνο t.

Με τη μέθοδο KITT, που περιγράψαμε στην προηγούμενη παράγραφο, δεν είναι δυνατή η ποσοτικοποίηση της παραμέτρου της αξιοπιστίας. Γι' αυτό και στη συνέχεια θα παρουσιάσουμε ενδεικτικά κάποιες μεθόδους, με τις οποίες μπορούμε να επιτύχουμε ακριβείς τιμές.

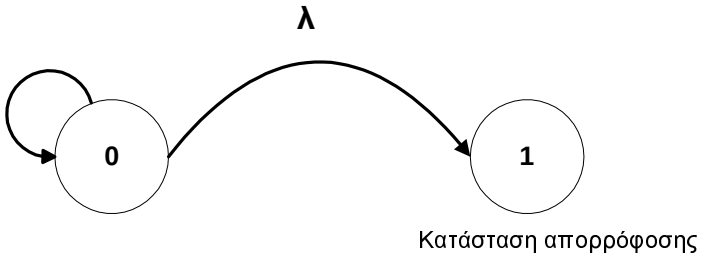
2.2.9.1 Σύστημα με ένα συστατικό

Θεωρούμε ένα σύστημα με ένα συστατικό, το οποίο έχει ποσό αποτυχίας λ και ποσό επισκευής μ. Ένα διάγραμμα μετάβασης Markov φαίνεται στο Σχήμα 2.20:



Σχήμα 2.20 Διάγραμμα μετάβασης για σύστημα με ένα συστατικό

Το βέλος από την κατάσταση 1 στην κατάσταση 0 δηλώνει την επισκευή του συστήματος. Στην εκτίμηση της αξιοπιστίας, όμως, θεωρούμε ότι η περίοδος ξεκινάει με αρχικό χρόνο 0 και τελειώνει με την πρώτη αποτυχία του συστήματος. Έτσι το διάγραμμα μετάβασης μετατρέπεται στο παρακάτω, Σχήμα 2.21:



Σχήμα 2.21 Διάγραμμα μετάβασης για υπολογισμό της αξιοπιστίας

Η διαφορική εξίσωση που περιγράφει την κατάσταση πιθανότητας $P_0(t)$ του συστατικού είναι

$$\dot{P}_0 = -\lambda P_0, P_0(0) = 1$$

Αυτή έχει τη λύση,

$$P_0(t) = e^{-\lambda t}$$

$P_0(t)$ είναι η πιθανότητα συνέχισης της λειτουργίας του συστήματος στο χρόνο t, όσο δεν υπάρχει ροή από την κατάσταση 1 στην κατάσταση 0. Έτσι η αξιοπιστία του συστήματος $R_s(t)$ είναι:

$$R_s(t) = P_0(t) = e^{-\lambda t t}$$

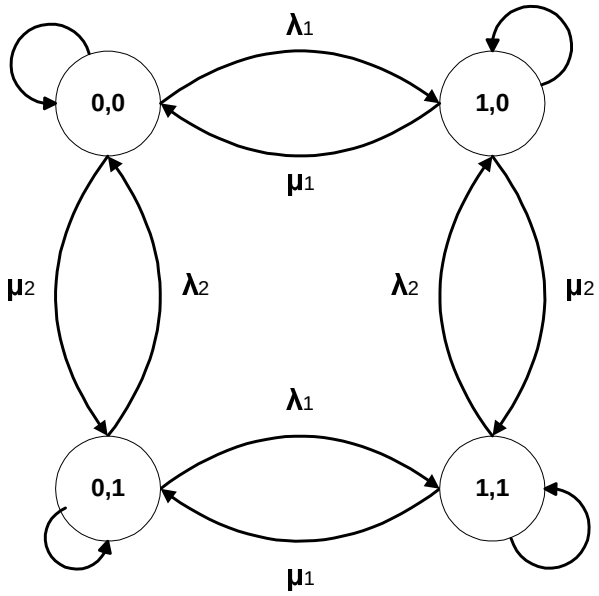
Η αναξιοπιστία (unreliability) του συστήματος $F_s(t)$, όπως έχουμε αναφέρει σε προηγούμενη παράγραφο, είναι συμπληρωματική με την αξιοπιστία. Άρα,

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

Μπορούμε να παρατηρήσουμε ότι η αναξιοπιστία πλησιάζει τη μονάδα, όσο το t γίνεται μεγαλύτερο. Με άλλα λόγια, το σύστημα αποτυγχάνει μετά από ένα αρκετά μεγάλο χρονικό διάστημα.

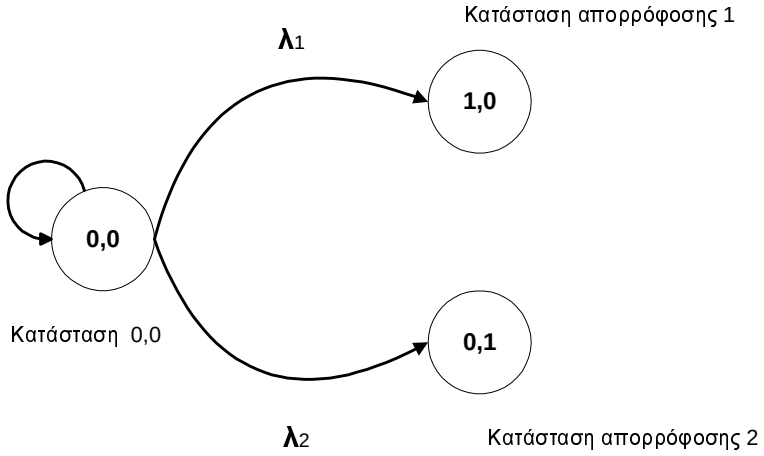
2.2.9.2 Σειριακό σύστημα με δύο συστατικά

Θεωρούμε ένα σειριακό σύστημα που περιέχει τα συστατικά 1 και 2. Το διάγραμμα μετάβασης Markov φαίνεται στο Σχήμα 2.22. Το σύστημα αποτυγχάνει όταν εισέρχεται στην κατάσταση (1,0) ή στην (0,1).



Σχήμα 2.22 Διάγραμμα μετάβασης για σύστημα με δύο συστατικά

Από τη στιγμή που θεωρούμε μία διαδικασία, η οποία τελειώνει με την πρώτη αποτυχία του συστήματος, το διάγραμμα μπορεί να απλοποιηθεί, όπως φαίνεται στο Σχήμα 2.23.



Σχήμα 2.23 Διάγραμμα μετάβασης για υπολογισμό της αξιοπιστίας

Η διαφορική εξίσωση για την πιθανότητα $P_0(t)$ είναι

$$P_0 = -(\lambda_1 + \lambda_2)P_0, P_0(0) = 1$$

Η οποία έχει τη λύση,

$$P_0(t) = e^{-(\lambda_1+\lambda_2)t}$$

Η αξιοπιστία του συστήματος $R_s(t)$ είναι ίση με το $P_0(t)$,άρα:

$$R_s(t) = e^{-(\lambda_1+\lambda_2)t}$$

Παρατηρούμε ότι η αξιοπιστία του συστήματος είναι αποτέλεσμα των αξιοπιστιών $e^{-\lambda_1 t}$ και $e^{-\lambda_2 t}$ των συστατικών. Αυτό γενικά ισχύει και για σειριακό σύστημα με n συστατικά. Η αναξιοπιστία του συστήματος $F_s(t)$ είναι

$$F_s(t) = 1 - R_s(t) = 1 - e^{-(\lambda_1+\lambda_2)t}$$

2.2.9.3 Σειριακό σύστημα με n συστατικά

Τα σειριακά συστήματα που αποτελούνται από n συστατικά περιγράφονται από το διάγραμμα μετάβασης του Σχήματος 2.24. Η διαφορική εξίσωση για την κατάσταση 0 είναι

$$P_0 = -(\lambda_1 + ... + \lambda_n)P_0, P_0(0) = 1$$

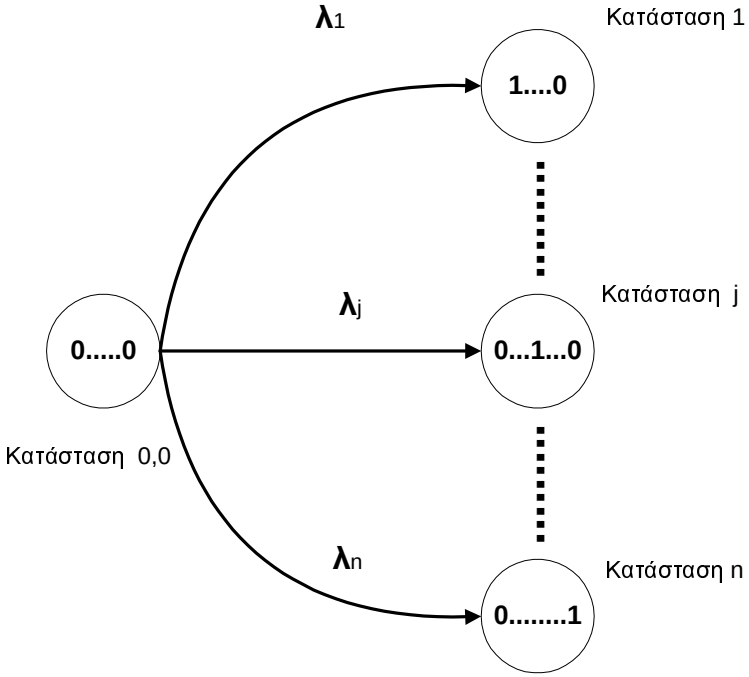
Η αξιοπιστία του συστήματος $R_s(t)$ είναι ίση με την $P_0(t)$,

$$R_s(t) = e^{-(\lambda_1+\ldots+\lambda_n)t}$$

Βλέπουμε δηλαδή ότι η αξιοπιστία στα σειριακά συστήματα είναι αποτέλεσμα όλων των αξιοπιστιών $e^{-\lambda_i t}$, i=1,…,n. Η αναξιοπιστία του συστήματος είναι

$$F_s(t) = 1 - e^{-(\lambda_1+\ldots+\lambda_n)t}$$

Δηλαδή η αναξιοπιστία είναι ίση με το άθροισμα των πιθανοτήτων όλων των μη αναστρέψιμων καταστάσεων.



Σχήμα 2.24 Διάγραμμα μεταβάσεων για υπολογισμό της αξιοπιστίας σε ένα σειριακό σύστημα με n συστατικά

2.2.9.4 Παράλληλο σύστημα με δύο συστατικά

Τα παράλληλα συστήματα με δύο συστατικά περιγράφονται από το διάγραμμα μετάβασης του Σχήματος 2.22. Από τη στιγμή που θεωρούμε μια περίοδο που τελειώνει με την πρώτη αποτυχία του συστήματος, η μετάβαση των επισκευών από την κατάσταση (1,1) μπορεί να μην υπάρχει και το διάγραμμα απλοποιείται σε αυτό του Σχήματος 2.25. Οι διαφορικές εξισώσεις είναι:

$$\dot{P}_{0,0} = -(\lambda_1+\lambda_2)P_{0,0} + \mu_1 P_{1,0} + \mu_2 P_{0,1}$$

$$\dot{P}_{1,0} = \lambda_1 P_{0,0} - (\mu_1+\lambda_2)P_{1,0}$$

$$\dot{P}_{0,1} = \lambda_2 P_{0,0} - (\mu_2+\lambda_1)P_{0,1}$$

$$\dot{P}_{1,1} = \lambda_2 P_{1,0} + \lambda_1 P_{0,1}$$

με αρχικές συνθήκες,

$$P_{0,0}(0) = 1, P_{1,0}(0) = P_{0,1}(0) = P_{1,1}(0) = 0$$

Το σύστημα λειτουργεί όσο βρίσκεται στις καταστάσεις (0,0), (1,0), (0,1). Δηλαδή, σε αυτές τις περιπτώσεις το σύστημα είναι αξιόπιστο, γιατί μπορεί να επισκευάζεται και μπορεί να συνεχίζει να λειτουργεί κανονικά. Έτσι η αξιοπιστία του συστήματος $R_s(t)$ δίνεται από το άθροισμα των πιθανοτήτων των παραπάνω καταστάσεων,

$$R_s(t) = P_{0,0}(t) + P_{1,0}(t) + P_{0,1}(t)$$

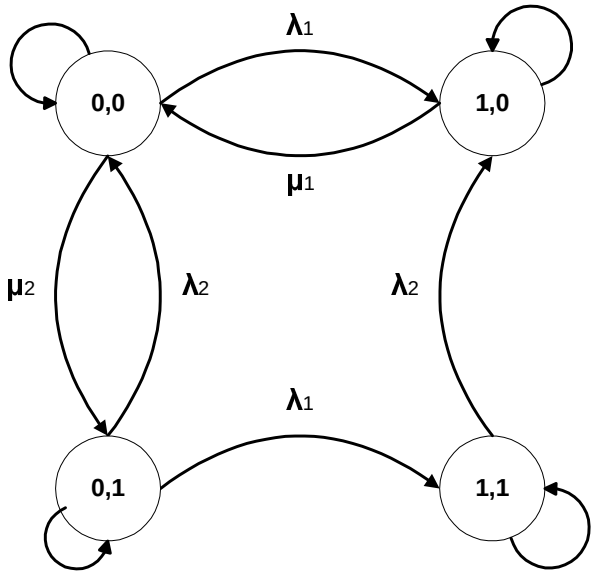
Η αναξιοπιστία του συστήματος $F_s(t)$ είναι

$$F_s(t) = 1 - P_{0,0}(t) - P_{1,0}(t) - P_{0,1}(t)$$

Η αναξιοπιστία, όμως είναι ίση και με $P_{1,1}(t)$, που είναι η πιθανότητα να βρεθεί το σύστημα στην κατάσταση (1,1).

$$F_s(t) = P_{1,1}(t)$$

Σε αυτή την περίπτωση το σύστημα θεωρείται αναξιόπιστο, αφού δεν μπορεί να επισκευαστεί. Δηλαδή επέρχεται η καταστροφή και δεν υπάρχει επιστροφή και επαναλειτουργία για το σύστημα.



Σχήμα 2.25 Διάγραμμα μετάβασης για υπολογισμό της αξιοπιστίας σε ένα παράλληλο σύστημα με δυο συστατικά

Στη συνέχεια θα παρουσιάσουμε ένα παράδειγμα υπολογισμού της αξιοπιστίας και της αναξιοπιστίας για ένα παράλληλο σύστημα με δύο συστατικά.

Παράδειγμα. Παράλληλο σύστημα με δύο συστατικά

Θεωρούμε τα παρακάτω ποσά αποτυχίας και επισκευής (ανά ώρα) για τα συστατικά 1 και 2.

Συστατικό 1	**Συστατικό 2**
λ_1=1/1000	λ_2=2/1000
μ_1=1/10	μ_2=1/40

Θα υπολογίσουμε τα $R_s(t)$ και $F_s(t)$ για t=100, 500, 1000 ώρες, και θα συγκρίνουμε τις τιμές με αυτές της $Q_s(t)$ και της $A_s(t)$.
Λύση: Οι τρεις πρώτες διαφορικές εξισώσεις

$$\dot{P}_{0,0} = -(\lambda_1 + \lambda_2)P_{0,0} + \mu_1 P_{1,0} + \mu_2 P_{0,1}$$

$$\dot{P}_{1,0} = \lambda_1 P_{0,0} - (\mu_1 + \lambda_2)P_{1,0}$$

$$\dot{P}_{0,1} = \lambda_2 P_{0,0} - (\mu_2 + \lambda_1)P_{0,1}$$

γίνονται,

$$\dot{P}_{0,0} = -0{,}003P_{0,0} + 0{,}1P_{1,0} + 0{,}025P_{0,1}$$

$$\dot{P}_{1,0} = 0{,}001P_{0,0} - 0{,}102P_{1,0}$$

$$\dot{P}_{0,1} = 0{,}002P_{0,0} - 0{,}026P_{0,1}$$

Με αριθμητική ολοκλήρωση, οι εξισώσεις

$$R_s(t) = P_{0,0}(t) + P_{1,0}(t) + P_{0,1}(t)$$

και

$$F_s(t) = 1 - P_{0,0}(t) - P_{1,0}(t) - P_{0,1}(t)$$

αποφέρουν τα αποτελέσματα που φαίνονται στον παρακάτω πίνακα

T	**$R_s(t)$**	**$F_s(t)$**	**$A_s(t)$**	**$Q_s(t)$**
100	0,993630	0,006370	0,999316	0,000684
500	0,959001	0,040999	0,999267	0,000733
1000	0,917232	0,082768	0,999267	0,000733

Η διαθεσιμότητες $A_s(t)$ και η μη διαθεσιμότητες $Q_s(t)$ υπολογίστηκαν με τη μέθοδο KITT, με την οποία ασχοληθήκαμε σε προηγούμενη παράγραφο. Παρατηρούμε ότι η αξιοπιστία είναι μικρότερη από τη διαθεσιμότητα, και η αναξιοπιστία είναι μεγαλύτερη από τη μη διαθεσιμότητα. Επίσης, η αναξιοπιστία συνεχώς αυξάνει, ενώ η μη διαθεσιμότητα παραμένει σταθερή.

Για μεγάλα συστήματα είναι δύσκολο να εκτιμήσουμε την αναξιοπιστία (ή την αξιοπιστία), διότι τα διαγράμματα μετάβασης έχουν μεγάλο αριθμό καταστάσεων. Έτσι σε τέτοιες περιπτώσεις, μπορούμε να ορίσουμε όρια για την αναξιοπιστία ώστε να απλοποιήσουμε τους υπολογισμούς.

2.3 Monte Carlo προσομοίωση

Η τεχνική συνίσταται στην κατασκευή, συνήθως με ένα πρόγραμμα υπολογιστή, ενός πιθανολογικού μοντέλου του συστήματος, ύστερα από έρευνα και μελέτη του συστήματος. Μια δοκιμή του μοντέλου επαναλαμβάνεται πολλές φορές, και κάθε φορά καταγράφονται τα στοιχεία που προέκυψαν. Για παράδειγμα, ας υποθέσουμε ότι ενδιαφερόμαστε για την αξιοπιστία ενός συστήματος με πολλά συστατικά σε 5000 ώρες. Ένα μοντέλο προσομοίωσης του συστήματος μπορεί να αναπτυχθεί και να τρέχει 100 φορές. Κάθε τρέξιμο είναι ανεξάρτητο και έτσι μοντελοποιεί το σύστημα ξανά. Αν 75 από τα μοντελοποιημένα συστήματα κρατάνε περισσότερο 5000 ώρες, αλλά 25 αποτυγχάνουν πριν από το χρόνο αυτό,τότε μπορούμε να πούμε ότι η αξιοπιστία του συστήματος στις 5000 ώρες είναι 0,75.

Γενικά οι προσομοιώσεις Monte Carlo είναι εύκολο να πραγματοποιηθούν και είναι κατάλληλες για πολύ πολύπλοκα ή πολύ μεγάλα συστήματα, που χρειάζεται να επιλυθούν με ντετερμινιστικές μεθόδους.

3. Το λογισμικό OpenFTA

Οι μέθοδοι που χρησιμοποιούνται για την ανάλυση δένδρων λαθών είναι πολύπλοκοι και χρονοβόροι εξαιτίας του πλήθους των απαραίτητων υπολογισμών. Υπήρχε μια γενικότερη ανάγκη να βρεθεί ένας τρόπος για να επιταχυνθεί αυτή η διαδικασία. Ψάχνοντας στο Internet για κάποιο αντιπροσωπευτικό λογισμικό που να υποστηρίζει αυτή την διαδικασία, βρήκαμε διάφορα λογισμικά (προγράμματα). Το λογισμικό **OpenFTA** δημιουργήθηκε για να καλύψει το κενό της υλοποίησης και δημιουργίας δένδρων λαθών, τα οποία όπως αναφέραμε προηγουμένως χρησιμοποιούνται στην ανάλυση της αξιοπιστίας συστημάτων.

3.1 Γενικά

Το λογισμικό **OpenFTA** βοηθάει να γίνονται γρηγορότερα και με μεγαλύτερη αξιοπιστία οι υπολογισμοί των μεθόδων, που χρησιμοποιούνται στην ανάλυση των δένδρων λαθών. Αυτό που στην ουσία κάνει το λογισμικό είναι να υπολογίζει την πιθανότητα να αποτύχει το σύστημα (το οποίο περιγράφεται στον κόμβο-ρίζα) αναλύοντας το δένδρο που κατασκευάσαμε. Όπως σε κάθε υπολογιστικό σύστημα, έτσι και στο λογισμικό υπάρχει κάποια αλλοίωση στα αποτελέσματα σε σχέση με τα πραγματικά. Οι αριθμοί υπολογίζονται με στρογγυλοποίηση αρκετών δεκαδικών ψηφίων. Συνεπώς η απόκλιση από τις πραγματικές τιμές των αποτελεσμάτων θεωρείται αμελητέα και δε δημιουργεί προβλήματα. Υπάρχουν και άλλα λογισμικά στην αγορά που χρησιμοποιούνται για αυτό το σκοπό, αλλά εμείς προτιμήσαμε το συγκεκριμένο εργαλείο επειδή η διανομή του από την κατασκευάστρια εταιρεία ήταν δωρεάν. Ένα ακόμα στοιχείο που ήταν κρίσιμο για την επιλογή του συγκεκριμένου λογισμικού είναι η απλότητα του προγράμματος ως προς τον τρόπο χρήσης του και η ευκολία στην κατανόηση των βασικών εννοιών των Δένδρο Λαθών. Τα στοιχεία της κατασκευάστριας εταιρείας είναι:

Formal Software Construction Limited
CBTC Senghenydd Road,
Cardiff CF24 4AY
Wales, UK
Tel: + 44 (0)29 2064 6080
Fax: + 44 (0)29 2064 7009
Web: www.fsc.co.uk
E-mail: fta@fsc.co.uk

3.2 Κατασκευή δένδρου λαθών με το OpenFTA

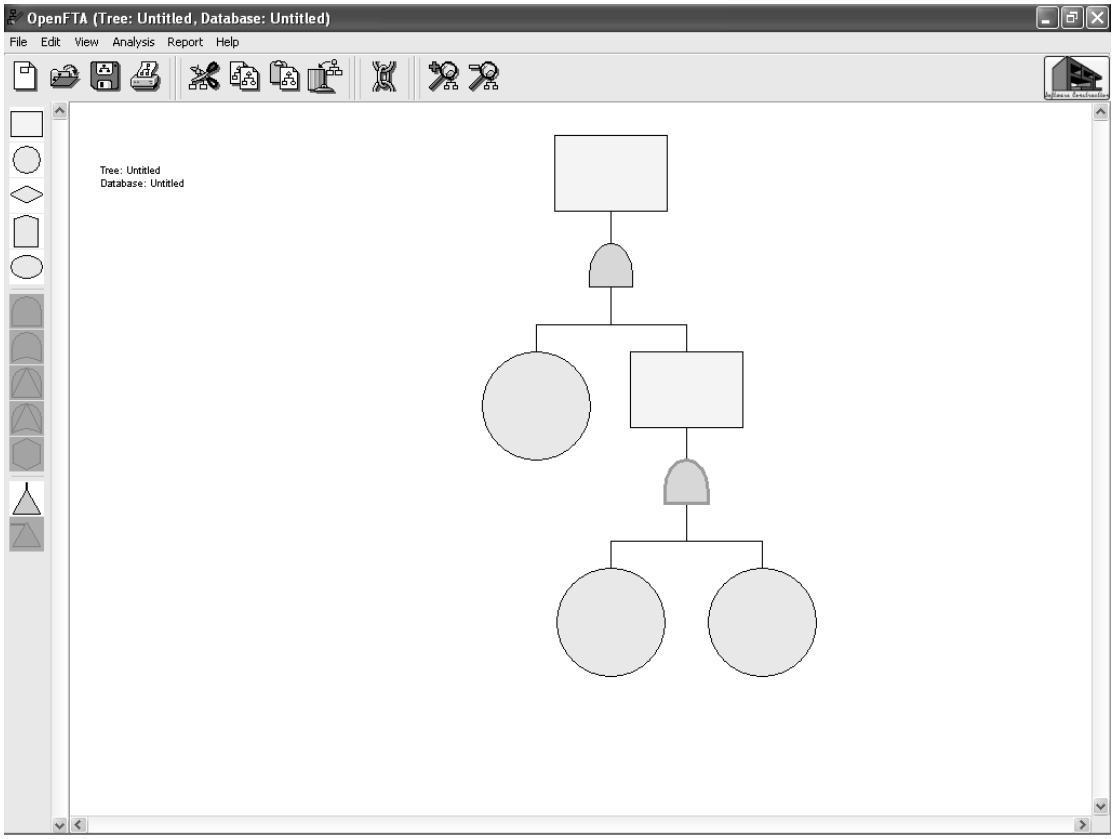
Το πρώτο βήμα είναι να εγκαταστήσουμε το πρόγραμμα, που είναι μια απλή διαδικασία. Όταν τελειώσουμε με την εγκατάσταση, τότε στη λίστα των προγραμμάτων υπάρχει ο φάκελος **OpenFTA** που περιέχει το πρόγραμμα και το Εγχειρίδιο Χρήσης. Το Εγχειρίδιο Χρήσης περιγράφει το πρόγραμμα και τις δυνατότητες που έχει. Όταν πατήσουμε να ανοίξει το πρόγραμμα θα εμφανιστούν δύο παράθυρα. Το πρώτο παράθυρο, που ονομάζεται OpenFTA, απεικονίζει τα σύμβολα και τα εργαλεία που χρησιμοποιούμε για να κατασκευάσουμε τα δένδρα λαθών. Το δεύτερο παράθυρο, που ονομάζεται OpenPED, είναι μια βάση δεδομένων που χρησιμοποιείται για να αποθηκεύονται στοιχεία για τους κόμβους-φύλλα, που είναι απαραίτητα για τον υπολογισμό της πιθανότητας να αποτύχει το σύστημα. Στη συνέχεια θα εξεταστεί με τη σειρά το καθένα από τα δύο παράθυρα χρησιμοποιώντας ταυτόχρονα ως παράδειγμα ένα από αυτά, που υπάρχουν στην εγκατάσταση του προγράμματος. Πιο συγκεκριμένα αυτό που ονομάζεται transTest.fta.

3.2.1 Παράθυρο OpenFTA

Στα αριστερά του παραθύρου OpenFTA υπάρχουν οι πύλες, τα γεγονότα και τα μεταφορές. Οι κόμβοι χωρίζονται σε ενδιάμεσους (intermediate), στοιχειώδης (basic initiating), μη αναπτύξιμους (undeveloped), εξωγενής (external) και υπό συνθήκη (υπό συνθήκη). Οι κόμβοι στοιχειώδη, μη αναπτύξιμοι και εξωγενής λέγονται στοιχειώδη γεγονότα. Οι πύλες διακρίνονται σε AND, OR, PRIORITY AND, EXCLUSIVE OR και INHIBIT. Υπάρχουν δυο κατηγορίες transfer το IN και το OUT. Όλες οι ιδιότητες από τις παραπάνω κατηγορίες και τις υποκατηγορίες τους περιγράφονται λεπτομερώς στο πρώτο κεφάλαιο. Η κατασκευή του δένδρου αρχίζει από τον ενδιάμεσο κόμβο που υπάρχει ήδη στην οθόνη εισάγοντας μια πύλη.

Για να εισάγετε μια πύλη πρέπει να επιλέξετε τον προηγούμενο κόμβο και να κάνετε click στην πύλη (μπορούμε να εισάγουμε μια και μοναδική πύλη). Για να εισάγετε έναν κόμβο πρέπει να διαλέξετε μια πύλη και να κάνετε κλικ στον κόμβο (σε κάθε πύλη μπορεί να υπάρχουν περισσότεροι από έναν κόμβοι). Το υπό συνθήκη γεγονός χρησιμοποιείται κυρίως με τις *PRIORITY AND* και *INHIBIT* πύλες. Τα transfer έχουν συγκεκριμένη χρήση, οπότε θα αναλυθούν με λεπτομέρεια στη συνέχεια. Το μεταφορά στο (transfer IN) εισάγεται σε μια πύλη και δηλώνει, ότι εξαιτίας του μεγάλου μεγέθους του δένδρου, το κομμάτι που υπήρχε εδώ έχει μεταφερθεί αλλού σαν ένα ξεχωριστό δέντρο. Το από μεταφορά (transfer OUT) εισάγεται στο ενδιάμεσο γεγονός της κορυφής και δηλώνει ότι το δένδρο που ακολουθεί είναι κομμάτι δένδρου που έχει μεταφερθεί εδώ. Η μόνη εξαίρεση στην εισαγωγή κόμβων είναι στον ενδιάμεσο, όπου μπορεί να εισάγει κάποιος έναν και μοναδικό κόμβο.

Ουσιαστικά η εισαγωγή των κόμβων και των πυλών γίνεται εναλλάξ στα επίπεδα του δένδρου π.χ. στο πρώτο επίπεδο κόμβοι, στο δεύτερο πύλες, στο τρίτο κόμβοι κ.τ.λ. Στο Σχήμα 3.1 απεικονίζεται αυτή η δομή.



Σχήμα 3.1

Το δένδρο που απεικονίζεται στην παραπάνω εικόνα είναι συντακτικά σωστό (valid). Αν υπήρχε ένα λάθος στη δομή του δένδρου, θα μας είχε προειδοποιήσει από την αρχή το λογισμικό π.χ. εισαγωγή ενδιάμεσου κόμβου κάτω από μη αναπτύξιμο κόμβο. Πατώντας την επιλογή *Validate* από το *Analysis*, αφού έχουμε σώσει προηγουμένως το δένδρο, το λογισμικό αρχίζει ένα έλεγχο του δένδρου λαθών. Αυτό που προσέχει είναι για την συντακτική ορθότητα του δένδρου και αν όλα τα στοιχειώδη γεγονότα έχουν όλες τις απαραίτητες ιδιότητες, που χρειάζονται για να γίνει η ανάλυση. Μετά το τέλος του ελέγχου εμφανίζεται μια αναφορά, που ονομάζεται FTA αναφορά (Formal-FTA: Report), που περιέχει λάθος (error) και προειδοποίηση (warning). Τα στοιχεία που περιέχει η αναφορά είναι:

- το όνομα του δένδρου λαθών που αντιστοιχεί στην αναφορά
- τα λάθος και τα προειδοποίηση που υπάρχουν στο δένδρο λαθών με τη σειρά που ανιχνεύτηκαν, επισημαίνοντας ακριβώς το λόγο που είναι λάθος ή προειδοποίηση
- η εκτίμηση για το εάν το δένδρο λαθών είναι σωστό (valid) ή λάθος (invalid). Τα λάθος είναι λάθη που πρέπει να διορθωθούν για να είναι λειτουργικό και αναλύσιμο το δένδρο λαθών. Ενώ τα προειδοποίηση είναι προτάσεις του λογισμικού για να βελτιωθεί το δένδρο λαθών χωρίς να αποτελεί δέσμευση η υλοποίηση τους από τον χρήστη. Συνεπώς αν μια αναφορά περιέχει λάθος (και/ ή προειδοποίηση), τότε η εκτίμηση είναι λάθος. Αν όμως δεν υπάρχει κανένα λάθος, αλλά μόνο προειδοποίηση, τότε η εκτίμηση είναι σωστό.

Το παρακάτω κείμενο είναι το report του παραδείγματος που εξετάζουμε:

VALIDATION REPORT ON transTest.fta

Formal-FTA : Warning : ID> : Item without id located
Formal-FTA : Warning : ID> : Item without id located
Formal-FTA : Warning : ID> : Item without id located
Formal-FTA : Warning : ID> : Item without id located

TREE VALID

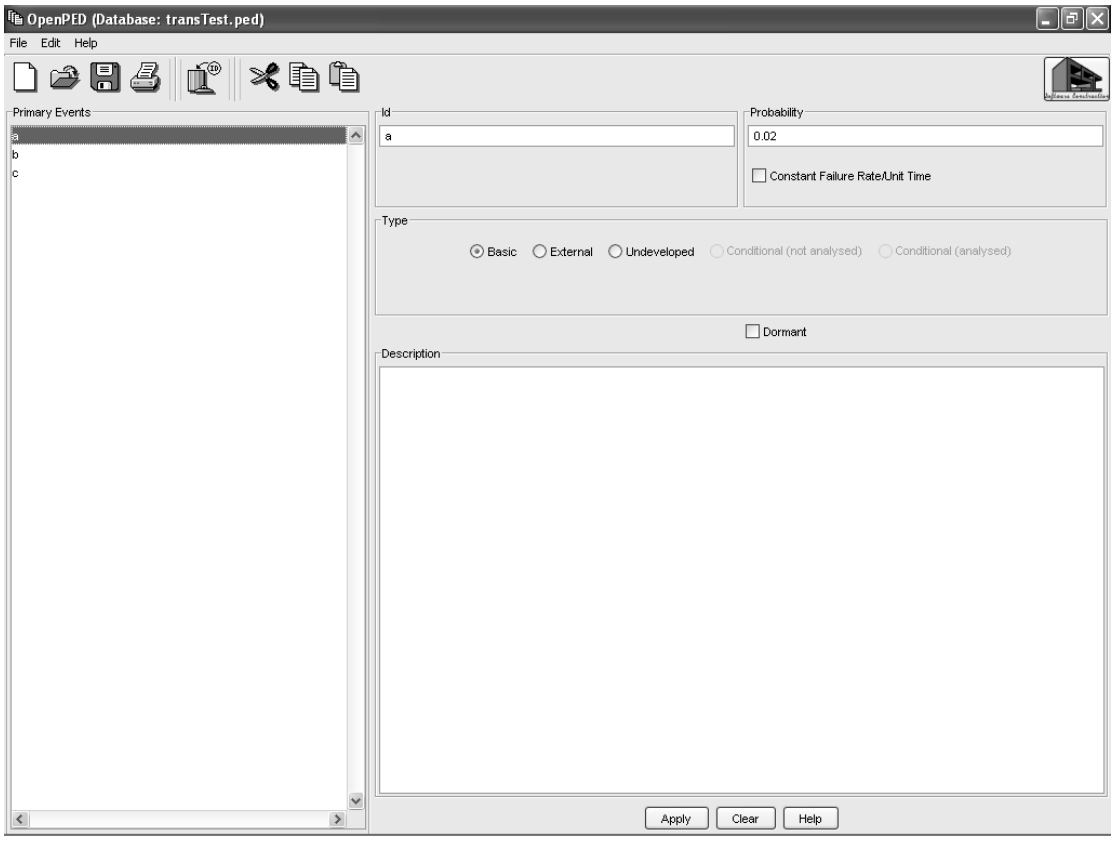
3.2.2 Παράθυρο OpenPED

Στο παράθυρο αυτό γίνεται η ανάθεση τιμών και ιδιοτήτων στους κόμβους που θεωρούνται φύλλα του δένδρου, όπως στοιχειώδη, μη αναπτύξιμοι, εξωγενής και υπό συνθήκη που αναφέρονται ως Βασικό, Εξωγενές, Μη αναπτύξιμο, Υπό συνθήκη (μη αναλυμένο) και Υπό συνθήκη (αναλυμένο) στο παράθυρο αντίστοιχα. Στο υπό συνθήκη γεγονός αντιστοιχούν οι τελευταίες δύο επιλογές. Ποια επιλογή θα αντιστοιχηθεί στο υπό συνθήκη γεγονός εξαρτάται από τον τρόπο που χρησιμοποιείται στο δένδρο λαθών. Αν ο ρόλος του είναι η ανάθεση πιθανότητας στο γεγονός και αποτελεί μέρος της ανάλυσης του δένδρου, τότε δηλώνεται ως αναλυμένο. Αν όμως ο σκοπός του είναι να προσθέσει μερικά σχετικά σχόλια στο γεγονός, τότε δηλώνεται ως μη αναλυμένο. Θα δηλώνουμε τον κάθε κόμβο στην βάση δεδομένων ξεχωριστά.

Θα ακολουθήσουμε ορισμένα βήματα για να καθορίσουμε τις ιδιότητες των στοιχειώδη γεγονότων. Κατ' αρχήν πρέπει να θέσουμε ένα *ID* στον κόμβο και την πιθανότητα να συμβεί το γεγονός που περιγράφει ο κόμβος. Η επιλογή *Ρυθμός αποτυχίας (Constant Failure Rate/Unit Time)* δηλώνει ότι η πιθανότητα να συμβεί το γεγονός θα υπολογιστεί συνάρτηση του χρόνου. Στη συνέχεια στο πλαίσιο του παραθύρου που λέγεται *Type* επιλέγουμε τον τύπο για τον κόμβο που περιγράφουμε π.χ. αν ο κόμβος είναι στοιχειώδης, τότε επιλέγουμε Βασικό. Αν επιλέξουμε λάθος τύπο για έναν κόμβο, θα μας εμφανίσει προειδοποιητικό μήνυμα όταν θα

επιχειρήσουμε να συνδέσουμε τον κόμβο από τη βάση δεδομένων με τον αντίστοιχο στο δένδρο λαθών. Αν ένα στοιχειώδες γεγονός αποτύχει χωρίς να μπορέσει να γίνει αντιληπτό από το περιβάλλον, τότε δηλώνεται ως *Μη ανιχνευθέν (Dormant)* στην OpenPED. Στο πλαίσιο *Περιγραφή (Description)* μπορείτε να κάνετε μια σύντομη περιγραφή του γεγονότος και να γράψετε οτιδήποτε στοιχεία θεωρείται απαραίτητα. Αυτά που υπάρχουν στο πλαίσιο αυτό εμφανίζονται μέσα στο αντίστοιχο γεγονός του δένδρου, οπότε είναι καλό να είναι λίγα και περιεκτικά αυτά που θα γράψετε. Για να δηλωθεί στη βάση το γεγονός πρέπει να πατήσετε το κουμπί *Apply (Εφαρμογή)*.

Η ίδια διαδικασία θα επαναληφθεί τόσες φορές όσα είναι τα στοιχειώδη και υπό συνθήκη γεγονότα στο δένδρο. Για να είναι πλήρως λειτουργικό ένα δένδρο πρέπει να δηλωθούν όλα τα στοιχειώδη γεγονότα του. Στο Σχήμα 3.2 φαίνονται όλα αυτά που περιγράψαμε προηγουμένως.



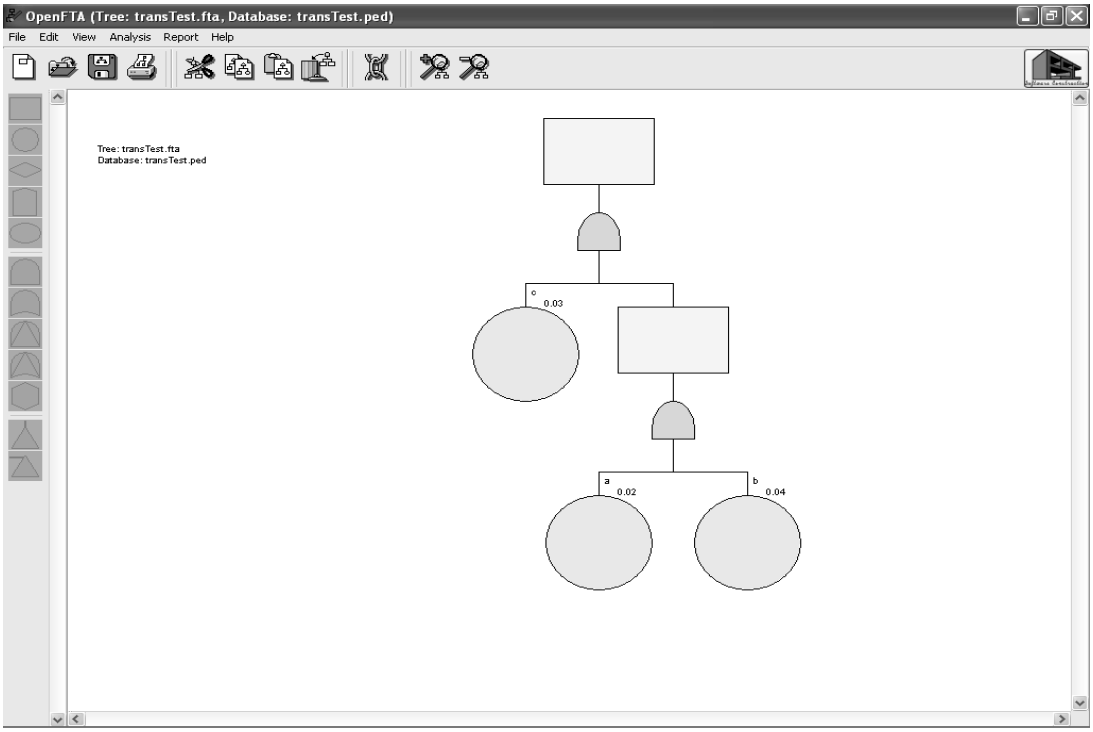
Σχήμα 3.2

3.2.3 Σύνδεση Δένδρου Λαθών με τη Βάση Δεδομένων

Αφού έχουμε τελειώσει και με τα δύο παράθυρα και τα έχουμε σώσει με το ίδιο όνομα κατά προτίμηση για δική μας ευκολία, στο παράθυρο OpenFTA πατάμε το *Database (Βάση Δεδομένων)* από το *File (Αρχείο)*. Έτσι γίνεται ο συσχετισμός των γεγονότων της Database που απεικονίζονται στο OpenPED με αυτά που υπάρχουν στο OpenFTA. Πρέπει όμως να συνδέσουμε ξεχωριστά το κάθε γεγονός του OpenFTA με το αντίστοιχο του OpenPED για να δώσουμε τις ιδιότητες που θέλουμε σε κάθε κόμβο. Αυτό γίνεται σε τρία βήματα:

- στο OpenPED παράθυρο επιλέγουμε το γεγονός που θέλουμε από το πλαίσιο στοιχειώδες γεγονός
- στο OpenFTA παράθυρο επιλέγουμε το αντίστοιχο γεγονός
- στο OpenFTA παράθυρο πατάμε το κουμπί που έχει τη μορφή αλυσίδας ή *Ctrl+I* ή την επιλογή *Link* από το *Edit*

Η ίδια διαδικασία ακολουθείται για κάθε γεγονός ξεχωριστά. Αν ξεχαστεί να συσχετισθεί κάποιο γεγονός με τις αντίστοιχες ιδιότητες του στη βάση δεδομένων, τότε θα εμφανιστεί ως λάθος στην αναφορά που δημιουργείται όταν κάνουμε *Validate (Έλεγχος Ορθότητας)* το δένδρο. Θα μας υπενθυμίζει ότι ξεχάσαμε να κάνουμε αυτή την κίνηση. Στο Σχήμα 3.3 απεικονίζεται το δένδρο του Σχήματος 3.1, αφού έχουμε κάνει όλη την προηγούμενη διαδικασία.



Σχήμα 3.3

3.3 Ανάλυση του δένδρου λαθών με το OpenFTA

Το λογισμικό **OpenFTA** είναι πολύ απλό σε σχέση με τις δυνατότητες ανάλυσης που υπάρχουν, δηλαδή προσφέρει λίγες μεθόδους ανάλυσης σε σύγκριση με το μεγάλο πλήθος που υπάρχει. Αυτό είναι ένα μειονέκτημα, γιατί δεν μας δίνεται η δυνατότητα να συγκρίνουμέ τα αποτελέσματα από τις διάφορες μεθόδους. Ωστόσο για κάποιον που είναι αρχάριος με το συγκεκριμένο πεδίο (ανάλυση αξιοπιστίας λογισμικού με δένδρα λαθών) είναι κατανοητό και εύκολα αξιοποιήσιμο για περισσότερη μελέτη και πρακτική με το αντικείμενο. Συγκεκριμένα το εργαλείο

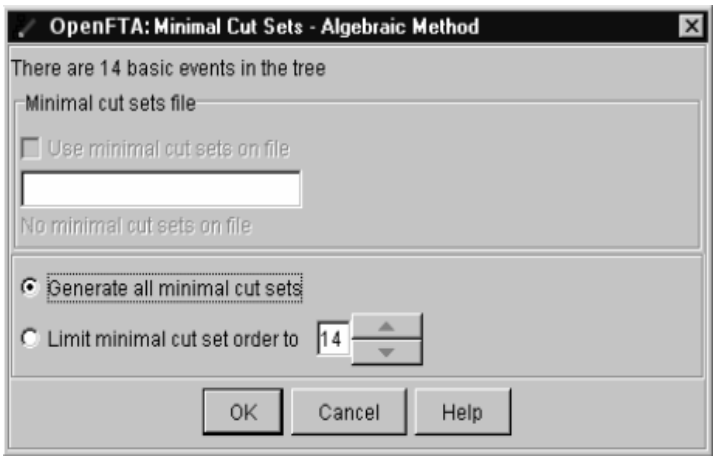
προσφέρει δυο μεθόδους ανάλυσης μια Ποσοτική Ανάλυση με χρήση των συνόλων ελάχιστης τομής και Monte Carlo προσομοίωση. Πριν κάνουμε οποιαδήποτε από τις δύο αναλύσεις, θα ήταν πολύ χρήσιμο αν κάνουμε Έλεγχο Ορθότητας το δένδρο λαθών. Αν δεν κάνουμε Έλεγχο Ορθότητας και υπάρχει κάποιο λάθος, τότε θα μας το επισημάνει και το ίδιο το πρόγραμμα με ένα μήνυμα.

3.3.1 Ποσοτική Ανάλυση με χρήση συνόλων ελάχιστης τομής

Στην αρχή επειδή το δένδρο πιθανότατα θα είναι πολύπλοκο και θα χρειαστούν τεράστιοι και δύσκολοι υπολογισμοί, θα χρησιμοποιήσουμε την επιλογή των συνόλων ελάχιστης τομής που προσφέρει το λογισμικό. Με αυτόν τον τρόπο, όπως έχει αναφερθεί σε προηγούμενο κεφάλαιο για τα σύνολα ελάχιστης τομής, ελαχιστοποιείται το δένδρο και απλοποιούνται οι υπολογισμοί. Όταν πατήσουμε από το *Analysis (Ανάλυση)* το *Minimal Cut Sets… (Σύνολα Ελάχιστης Τομής)*, τότε εμφανίζεται το παράθυρο καθορισμού των ιδιοτήτων της Minimal Cut Sets Method (Μέθοδος Συνόλου Ελάχιστης Τομής). Το παράθυρο περιέχει τα εξής στοιχεία:

- ο αριθμός των στοιχειώδων γεγονότων που υπάρχουν στο δένδρο λαθών
- αν το αρχείο συνόλων ελάχιστης τομής υπάρχει ήδη, τότε εμφανίζεται ο φάκελος που είναι αποθηκευμένο καθώς και ο αριθμός και σειρά των διαθέσιμων συνόλων ελάχιστης τομής
- αν επιλέξουμε το κουμπί *Generate all minimal cut sets*, τότε θα υπολογιστούν όλες οι σειρές των minimal cut sets που υπάρχουν στο δένδρο λαθών. Αν όμως δεν επιθυμούμε να υπολογιστούν όλες οι σειρές των συνόλων ελάχιστης τομής, τότε επιλέγουμε το κουμπί *Limit minimal cut set order to* και καθορίζουμε τον αριθμό των σειρών των συνόλων ελάχιστης τομής που θέλουμε να υπολογιστούν

Το παράθυρο καθορισμού των ιδιοτήτων της Minimal Cut Sets Method (Μέθοδος Συνόλου Ελάχιστης Τομής) φαίνεται στο Σχήμα 3.4.



Σχήμα 3.4

Όταν πατήσουμε το OK, εμφανίζεται ένα αρχείο κειμένου, που ονομάζεται FTA αναφορά και περιέχει τα αποτελέσματα της Minimal Cut Sets Method (Μεθόδου Σύνολα Ελάχιστης Τομής).

- το φάκελο όπου αποθηκεύεται το δένδρο λαθών που αναλύεται εδώ
- την ημερομηνία και ώρα δημιουργίας της αναφοράς
- η μέθοδος που χρησιμοποιείται για να υπολογιστούν τα σύνολα ελάχιστης τομής
- τον αριθμό των ξεχωριστών στοιχειώδων γεγονότων που αναπαρίστανται στο δένδρο λαθών
- το εύρος των σειρών των συνόλων ελάχιστης τομής που πιθανόν υπάρχουν στο δένδρο
- μια λίστα των συνόλων ελάχιστης τομής κατηγοριοποιημένα ανάλογα με τη σειρά που ανιχνεύτηκαν
- ένας πίνακας, που ονομάζεται Qualitative Importance Analysis. Ο πίνακας απεικονίζει την κατανομή του αριθμού των συνόλων ελάχιστης τομής, που βρέθηκαν σε κάθε σειρά των συνόλων τομής που υπάρχουν

Στο κείμενο παρακάτω φαίνεται η αναφορά του παραδείγματος που εξετάζουμε.

Minimal Cut Sets
==========
Tree : transTest.fta
Time : Tue Jul 26 18:52:09 2005

Method : Algebraic

No. of primary events = 3
Minimal cut set order = 1 to 3

Order 1:

Order 2:

Order 3:
1) a b c

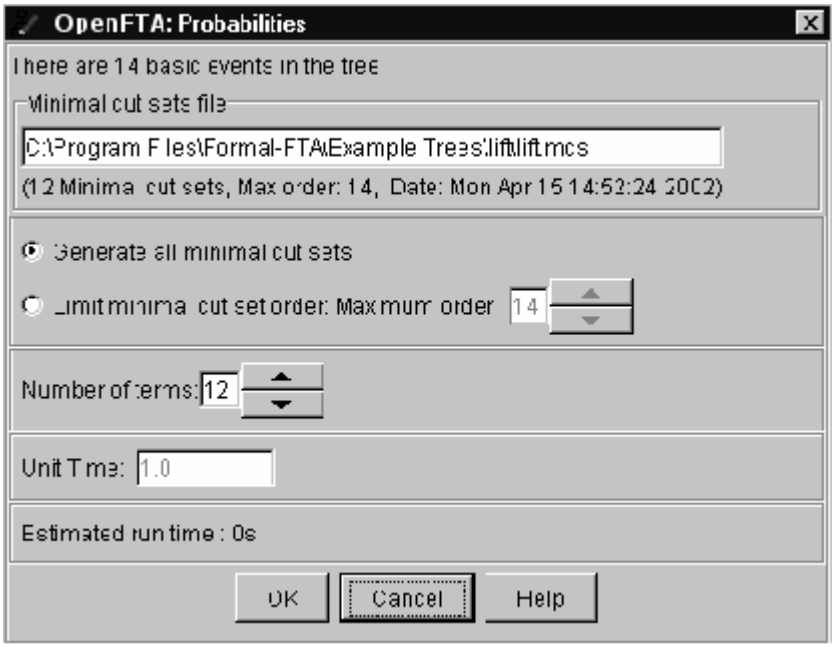
Qualitative Importance Analysis:

Order	Number
1	0
2	0

3	1
ALL	1

Στη συνέχεια θα κάνουμε την Ποσοτική Ανάλυση για να βγάλουμε ορισμένα αριθμητικά αποτελέσματα που θα βοηθήσουν στην εξαγωγή συμπερασμάτων. Λέγοντας << *Ποσοτική Ανάλυση*>> εννοούμε την χρήση σειρών Ν όρων για να υπολογιστούν οι διάφορες πιθανότητες, όπως του γεγονότος της κορυφής, των συνόλων ελάχιστης τομής, κ.α. Αυτό είχε περιγραφεί λεπτομερώς σε προηγούμενο κεφάλαιο. Η σειρές Ν όρων δημιουργούνται εξετάζοντας τη δομή των κόμβων του δένδρου λαθών. Όταν τις κατασκευάσουμε, τότε υπολογίζουμε τόσους όρους όσους έχουν καθοριστεί από τις ιδιότητες. Ο τελευταίος όρος θα θεωρήσουμε ότι αποτελεί μια καλή προσέγγιση του πραγματικού αποτελέσματος.

Όταν πατήσουμε το *Numerical Probability…* από το *Analysis (Ανάλυση)*, θα εμφανιστεί το παράθυρο καθορισμού των ιδιοτήτων της *Numerical Probability Method (Ποσοτική Μέθοδος Ανάλυσης)*. Στο Σχήμα 3.5 φαίνεται το συγκεκριμένο παράθυρο.



Σχήμα 3.5

Το παράθυρο ιδιοτήτων περιέχει:

- Στην αρχή δηλώνεται ο αριθμός των ξεχωριστών στοιχειώδων γεγονότων στο εξεταζόμενο δένδρο λαθών
- Στο πλαίσιο Minimal cut sets file καθορίζεται ο φάκελος που σώζεται το Formal-FTA

- Στο επόμενο πλαίσιο καθορίζεται ο αριθμός των σειρών των συνόλων ελάχιστης τομής που θα ληφθούν υπόψη στον ποσοτική ανάλυση
- Επίσης μπορούμε να ρυθμίσουμε τον αριθμό των όρων που θα χρησιμοποιηθούν. Αυτή η επιλογή υπάρχει ως όριο στον αριθμό των όρων που χρησιμοποιούνται στους υπολογισμούς των πιθανοτήτων. Αυτό χρησιμοποιεί μια επέκταση όρων στην οποία κάθε όρος έχει ${}^{n}C_{r}$ υποόρους μεγαλώνοντας το σύνολο των όρων στους 2^{n}. Περιορίζοντας τον αριθμό των όρων επιταχύνεται η διαδικασία εξαγωγής των αποτελεσμάτων, αλλά μειώνεται η ακρίβειά τους
- Το *Unit Time* ορίζει το χρονικό διάστημα που αναφέρεται σε στοιχειώδες γεγονός που οι πιθανότητες τους έχουν δηλωθεί στη βάση δεδομένων OpenPED συναρτήσει του χρόνου
- Τέλος το estimated time δηλώνει το χρόνο που χρειάζεται για να ολοκληρωθεί η Ποσοτική Ανάλυση

Όταν πατήσουμε το κουμπί OK, θα εμφανιστεί ένα αρχείο κειμένου, που ονομάζεται FTA αναφορά και περιέχει τα αποτελέσματα της ποιοτικής ανάλυσης.

- το φάκελο όπου αποθηκεύεται το δένδρο λαθών που αναλύεται εδώ
- την ημερομηνία και ώρα δημιουργίας της αναφοράς
- τον αριθμό των ξεχωριστών στοιχειώδων γεγονότων που αναπαρίστανται στο δένδρο λαθών
- τον αριθμό των διαθέσιμων συνόλων ελάχιστης τομής για το δένδρο λαθών
- τη μέγιστη σειρά των διαθέσιμων συνόλων ελάχιστης τομής για χρήση στους υπολογισμούς των πιθανοτήτων του δένδρου λαθών
- δήλωση της σειράς των συνόλων ελάχιστης τομής που χρησιμοποιήθηκαν στους υπολογισμούς των πιθανοτήτων, αν είναι μικρότερος από τον προηγούμενο
- καταγραφή του unit time span που χρειάσθηκε για τους υπολογισμούς
- ένας πίνακας, που ονομάζεται Minimal cut set probabilities (Πιθανότητες συνόλων ελάχιστης τομής): Περιέχει μια λίστα των συνόλων ελάχιστης τομής και οι πιθανότητες για κάθε γεγονός σε κάθε σύνολο ελάχιστης τομής που συμβάλει στο να γίνει το γεγονός της κορυφής (αποτυχία του συστήματος)
- η πιθανότητα αποτυχίας του γεγονότος της κορυφής. Όταν έχουν υπολογισθεί όλοι οι όροι, που ο αριθμός έχει καθορισθεί στις ιδιότητες του προηγούμενου παραθύρου, ο τελευταίος όρος ισούται με την ζητούμενη πιθανότητα
- ένας πίνακας, που ονομάζεται Basic Event Analysis (Ανάλυση Βασικού Γεγονότος). Περιέχει μια λίστα όλων των στοιχειώδων γεγονότων του δένδρου λαθών και την αντίστοιχη συμβολή της αποτυχίας τους στην πραγματοποίηση του γεγονότος της κορυφής. Η συμβολή αυτή εκφράζεται και ως ποσοστό σημαντικότητας του κάθε στοιχειώδους γεγονότος

Στο παρακάτω κείμενο καταγράφονται τα στοιχεία της Ποιοτικής Ανάλυσης του παραδείγματος που εξετάζουμε.

Probabilities Analysis
==========

Tree : transTest.fta
Time : Tue Jul 26 20:04:18 2005

Number of primary events = 3
Number of minimal cut sets = 1
Order of minimal cut sets = 3

Unit time span = 1.000000

Minimal cut set probabilities :

1 a b c 2.400000E-005

Probability of top level event (minimal cut sets up to order 3 used):

1 term +2.400000E-005 = 2.400000E-005 (upper bound)

Exact value : 2.400000E-005

Primary Event Analysis:

Event	Failure contrib.	Importance
a	2.400000E-005	100.00%
b	2.400000E-005	100.00%
c	2.400000E-005	100.00%

3.3.2 Προσομοίωση Monte Carlo

Σε αυτό το κεφάλαιο θα εξετάσουμε τη δεύτερη μέθοδο ανάλυσης δένδρων λαθών που υπάρχει στο λογισμικό και ονομάζεται *Προσομοίωση Monte Carlo*. Ο αλγόριθμος που χρησιμοποιείται σε αυτήν την μέθοδο είναι διαφορετικός σε σχέση με τις υπόλοιπες μεθόδους ανάλυσης. Όπως έχει προαναφερθεί σε προηγούμενο κεφάλαιο τα αποτελέσματα βγαίνουν μετά από μια σειρά διαδοχικών εκτελέσεων του δένδρου λαθών συγκεκριμένης χρονικής διάρκειας η καθεμία. Υπολογίζοντας τα ποσοστά των εκτελέσεων που αποτυγχάνουν και που ολοκληρώνονται επιτυχώς αντίστοιχα βγαίνουν τα αριθμητικά αποτελέσματα για το γεγονός της κορυφής, τα σύνολα τομής και τα σύνολα ελάχιστης τομής. Πιο λεπτομερής περιγραφή του

αλγορίθμου θα γίνει στο επόμενο κεφάλαιο που θα εξετασθεί αναλυτικά με τη βοήθεια ενός προβλήματος.

Όταν πατήσουμε *Monte Carlo Simulation…* από το *Analysis (Ανάλυση)*, θα εμφανιστεί το παράθυρο καθορισμού των ιδιοτήτων της μεθόδου. Τα στοιχεία που υπάρχουν στο παράθυρο είναι

- ο αριθμός των ξεχωριστών στοιχειώδων γεγονότων στο εξεταζόμενο δένδρο λαθών
- ο αριθμός των εκτελέσεων του δένδρου λαθών. Όσο περισσότερες είναι οι εκτελέσεις, τόσο πιο χρονοβόρα γίνεται η διαδικασία, επειδή απαιτείται να γίνουν επιπρόσθετοι υπολογισμοί. Ωστόσο η ακρίβεια των αποτελεσμάτων είναι μεγαλύτερη
- η χρονική διάρκεια της κάθε εκτέλεσης. Η χρονική διάρκεια της κάθε εκτέλεσης είναι το *Unit Time*, που χρειάζεται μόνο αν υπάρχουν στοιχειώδη γεγονότα στο δένδρο λαθών που οι πιθανότητες τους στη βάση δεδομένων έχουν οριστεί συναρτήσει του χρόνου
- ο εκτιμώμενος χρόνος μέχρι να βγουν τα αποτελέσματα

Στο Σχήμα 3.6 φαίνεται το συγκεκριμένο παράθυρο.

Σχήμα 3.6

Όταν δηλώσουμε τις ιδιότητες που θέλουμε και πατήσουμε OK, τότε εμφανίζεται μια αναφορά για την Monte Carlo Simulation. Η ανάφορα περιέχει τις παρακάτω πληροφορίες:

- το φάκελο όπου αποθηκεύεται το δένδρο λαθών που αναλύεται εδώ
- την ημερομηνία και ώρα δημιουργίας της αναφοράς
- τον αριθμό των ξεχωριστών στοιχειώδων γεγονότων που αναπαρίστανται στο δένδρο λαθών
- τον αριθμό των διαδοχικών εκτελέσεων του δένδρου λαθών
- το unit time που χρησιμοποιήθηκε για κάθε εκτέλεση
- πόσες φορές απέτυχε το σύστημα εξαιτίας αποτυχίας κάποιου στοιχειώδους γεγονότος
- η πιθανότητα να αποτύχει τουλάχιστον ένα συστατικό σε μια εκτέλεση

- η πιθανότητα να συμβεί το γεγονός της κορυφής (αποτυχία του συστήματος)
- ένα πίνακα με όλα τα σύνολα ελάχιστης τομής που βρέθηκαν στο δένδρο λαθών. Κάθε γραμμή του πίνακα περιέχει: το σύνολο ελάχιστης τομής, τον αριθμό των αποτυχιών που οφείλονται σε αυτό, την πιθανότητα ένα από τα γεγονότα του σύνολο τομής να συμβεί και το ποσοστό σημαντικότητας του συνόλου τομής σε σχέση με τα υπόλοιπα που βρέθηκαν
- ένας πίνακας που ονομάζεται Compressed: Είναι ίδιο με τον προηγούμενο, αλλά τα σύνολα τομής που είναι λιγότερο μινιμαλιστικά από τα υπόλοιπα τα μετατρέπει σε περισσότερο μινιμαλιστικά. Τα υπόλοιπα πεδία προσαρμόζονται σύμφωνα με τα καινούρια στοιχεία
- ένας πίνακας που ονομάζεται Basic Event Analysis: Περιέχει μια λίστα με όλα τα στοιχειώδη γεγονότα και την η συμβολή της αποτυχίας όταν συμβαίνει το γεγονός της κορυφής. Αυτή η συμβολή εκφράζεται και ως ποσοστό σημαντικότητας του κάθε στοιχειώδους γεγονότος

Η ανάφορα για το συγκεκριμένο παράδειγμα με προκαθορισμένες ιδιότητες απεικονίζεται παρακάτω:

Monte Carlo Simulation
==========

Tree : transTest.fta
Time : Wed Jul 27 13:06:14 2005
Note: Only runs with at least one component failure are simulated

Number of primary events = 3
Number of tests =10000
Unit Time span used = 1.000000

Number of system failures = 1

Probability of at least = 8.742400E-002 (exact)
one component failure

Probability of top event = 8.742400E-006 (+/- 8.742400E-006)

Rank	Failure mode	Failures	Estimated Probability	Importance
1	a b c	1	8.742400E-006 (+/- 8.742400E-006)	100.00%

Compressed:

Rank	Failure mode	Failures	Estimated Probability	Importance
1	a b c	1	842400E-006 (+/- 8.742400E-006)	100.00%

Primary Event Analysis:

Event	Failure contrib.	Importance
a	8.742400E-006	100.00%
b	8.742400E-006	100.00%
c	8.742400E-006	100.00%

4. Εφαρμογή στην Ανάλυση Αξιοπιστίας μιας Διαδικτυακής Υπηρεσίας

Σε αυτό το κεφάλαιο θα παρουσιασθεί και θα εξεταστεί μια *Διαδικτυακή Υπηρεσία* για να κατανοήσουμε καλύτερα τον τρόπο σκέψης και τη μέθοδο για την κατασκευή δένδρων λαθών καθώς και πως λειτουργούν οι διάφορες μέθοδοι ανάλυσης αξιοπιστίας σε ένα λογισμικό. Επίσης θα εφαρμόσουμε όσα παρουσιάστηκαν στο προηγούμενο κεφάλαιο για να υλοποιήσουμε το δένδρο λαθών της προηγούμενης *Διαδικτυακής Υπηρεσίας*.

4.1 Γενικά

Η *Διαδικτυακή Υπηρεσία* με την οποία θα ασχοληθούμε είναι μια υπηρεσία δημοπρασίας on-line και λέγεται Υπηρεσία Δημοπρασιών. Η υπηρεσία δέχεται πληροφορίες από πωλητές (Sellers) και αγοραστές (Buyers) μιας συγκεκριμένης δημοπρασίας, στέλνει τα κατάλληλα στοιχεία σε μια Υπηρεσία Καταγραφής Δημοπρασίας και μετά απαντάει στους αγοραστές και πωλητές ανάλογα με τα αποτελέσματα που δέχεται από την Υπηρεσία Καταγραφής Δημοπρασίας. Μια διαδικασία αρχίζει με δύο δραστηριότητες η μια είναι για να δέχεται πληροφορίες από τους πωλητές και η άλλη για να δέχεται πληροφορίες από τους αγοραστές. Κάθε Οίκος Δημοπρασίας (Auction House) έχει έναν και μοναδικό *Κωδικό Δημοπρασίας*, έτσι κάθε πωλητή και αγοραστή πρέπει να στέλνει το δικό *Κωδικό Δημοπρασίας* του μαζί με τις προτάσεις του. Η σειρά με την οποία φτάνουν οι προτάσεις από τους πωλητές και τους αγοραστές στην Υπηρεσία Δημοπρασιών είναι τυχαίος. Όταν φτάνει στην Διαδικτυακή Υπηρεσία μια καινούρια πρόταση, τότε ελέγχεται αν υπάρχει μια διαδικάσία ή όχι. Αν όχι, τότε δημιουργείται μια καινούρια. Όταν φτάσουν και οι δύο προτάσεις, ενεργοποιείται η Υπηρεσία Καταγραφής Δημοπρασίας. Επειδή η ενεργοποίηση είναι ασύγχρονη, ο οίκος δημοπρασίας στέλνει τον Κωδικό Δημοπρασίας του στην Υπηρεσία Καταγραφής Δημοπρασίας. Η Υπηρεσία Καταγραφής Δημοπρασίας στέλνει μαζί με την απάντησή του και τον αντίστοιχο Κωδικό Δημοπρασίας, έτσι ώστε να μπορεί να βρει ο οίκος δημοπρασίας την κατάλληλη Υπηρεσία Δημοπρασιών. Εξαιτίας του μεγάλου πλήθους των πωλητών και αγοραστών, ο καθένας από αυτούς οφείλει να στείλει τη δική του διεύθυνση για να μπορεί να απαντήσει η Υπηρεσία Δημοπρασιών. Τέλος ο οίκος δημοπρασίας πρέπει να στείλει τη δική του διεύθυνση στην Υπηρεσία Καταγραφής Δημοπρασίας, έτσι ώστε η Υπηρεσία Καταγραφής Δημοπρασίας να μπορεί να απαντήσει στο σωστό οίκο δημοπρασίας.

Το παράδειγμα που παρουσιάστηκε προηγουμένως πάρθηκε από ένα BPEL (Business Process Execution Language) for Web Services Specification. Το BPEL είναι μια γλώσσα για να παρουσιαστούν οι ιστοσελίδες των Διαδικτυακών Υπηρεσιών σε μορφή που μπορεί να είναι κατανοητός από τους χρήστες που χρειάζεται να γνωρίζουν την δομή των Διαδικτυακών Υπηρεσιών. Οι Διαδικτυακές Υπηρεσίες είναι γραμμένες σε XML γλώσσα. Τα έγγραφα BPEL είναι οι

«μεταφράσεις» των XML αρχείων. Τα BPEL έγγραφα απεικονίζουν την δομή, τις υπηρεσίες, και τον τρόπο επικοινωνίας μεταξύ τους των σύνθετων Διαδικτυακών Υπηρεσιών. Περιέχουν όλα τα απαραίτητα στοιχεία, που στην περίπτωση μας είναι η δομή, τα συστατικά, οι σχέσεις μεταξύ των συστατικών και η ροή δεδομένων. Η ιστοσελίδα που μπορεί κάποιος να κατεβάσει το συγκεκριμένο έγγραφο είναι:

http://dev2dev.bea.com/technologies/webservices/BPEL4WS.jsp

http://www-106.ibm.com/developerworks/webservices/library/ws-bpel/

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnbiz2k2/html/bpel1-1.asp

http://ifr.sap.com/bpel4ws/

http://www.siebel.com/bpel

Για να κατασκευαστεί από το BPEL έγγραφο το δένδρο λαθών ακολουθείται μια συγκεκριμένη διαδικασία. Αυτή τη διαδικασία την βρήκαμε σε ένα έγγραφο το ***Model-Driven Dependability Analysis of WebServices***. Τα βήματα που ακολουθεί είναι:

1. Το BPEL έγγραφο μετατρέπεται με βάση κάποιους κανόνες που αναφέρονται μέσα στο *Model-Driven Dependability Analysis of WebServices* σε ένα UML διάγραμμα. Το UML διάγραμμα δείχνει τα συστατικά, τη ροή δεδομένων και τις σχέσεις μεταξύ των συστατικών.
2. Μετά το UML διάγραμμα μετατρέπεται σε *Διάγραμμα Block (Block Diagram)* που περιέχει μόνο τα συστατικά και τη δομή που υπάρχει μεταξύ των συστατικών.
3. Τώρα μπορεί με βάση το *Διάγραμμα Block* και τη δομή που υπάρχει μεταξύ των συστατικών να κατασκευαστεί το δένδρο λαθών. Το ενδιάμεσο στάδιο της κατασκευής είναι η δημιουργία συναρτήσεων πιθανοτήτων αποτυχίας του συστήματος. Οι συναρτήσεις δείχνουν πως το κάθε συστατικό και σε ποιο βαθμό οδηγεί στην αποτυχία.
4. Η εναλλακτική επιλογή του $2^{ου}$ βήματος είναι να προχωρήσει η ανάλυση αξιοπιστίας του συστήματος με τη βοήθεια των Markov Models. Η ανάλυση αξιοπιστίας με τα Markov Models δίνει τη δυνατότητα για μεγαλύτερη ακρίβεια στα αριθμητικά αποτελέσματα.

Το συγκεκριμένο έγγραφο μπορείτε να το κατεβάσετε από τη παρακάτω σελίδα:

http://www.cs.uoi.gr/~zarras/papers/doa04-long.pdf

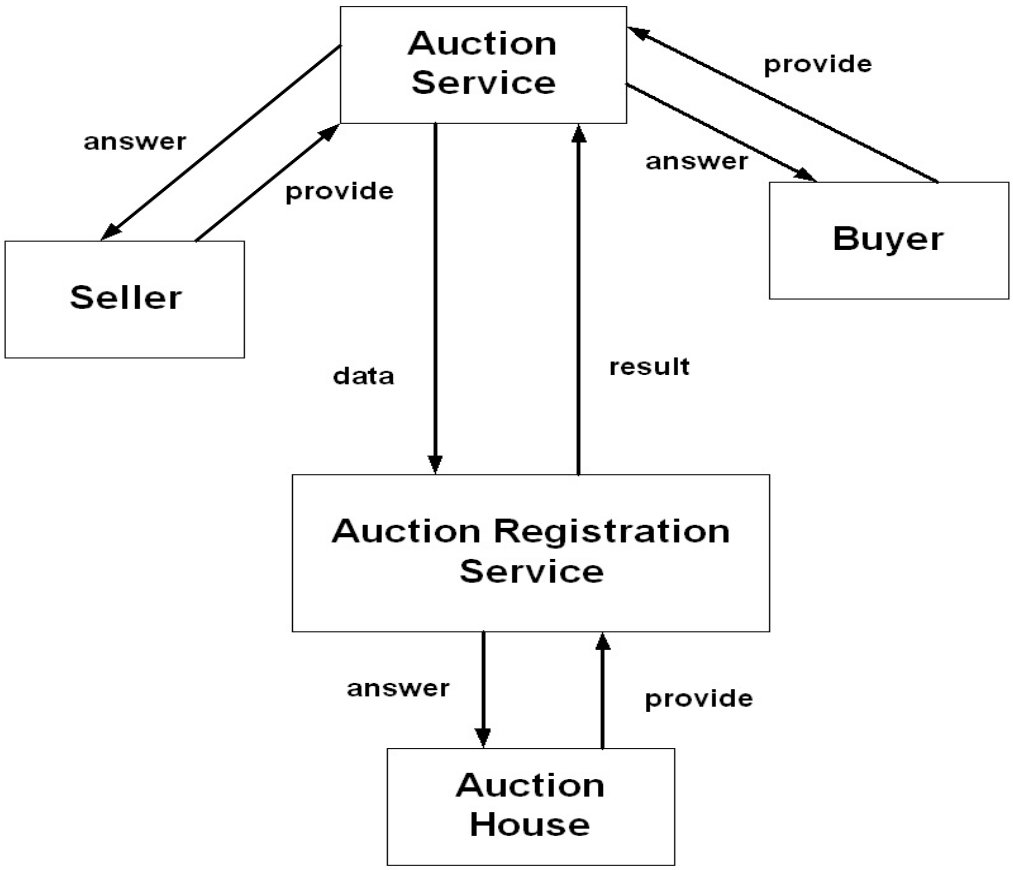
Στα δύο επόμενα κεφάλαιο θα παρουσιάσουμε δύο δένδρα λαθών. Το πρώτο δένδρο λαθών θα το δημιουργήσουμε όπως είναι στο παράδειγμα (χωρίς εφεδρικά τμήματα). Το δεύτερο δένδρο λαθών θα περιέχει και εφεδρικά τμήματα. Με εφεδρικά τμήματα είναι όταν υπάρχει εναλλακτικό συστατικό για κάποιο βασικό. Επιλέξαμε να υπάρχει με εφεδρικά τμήματα στην Υπηρεσία Καταγραφής Δημοπρασίας, γιατί είναι το μοναδικό συστατικό στο οποίο μπορεί να υλοποιηθεί η επιλογή αυτή. Έτσι αν αποτύχει η πρώτη Υπηρεσία Καταγραφής Δημοπρασίας θα υπάρχει ως ενναλακτικό η δεύτερη.

4.2 Δένδρο λαθών χωρίς εφεδρικά τμήματα

Η παραγωγή του δένδρου λαθών από το BPEL έγγραφο είναι μια δύσκολη διαδικασία, γιατί δεν ξέραμε ποια είναι τα συστατικά και ποιες οι σχέσεις μεταξύ τους. Έτσι αυτό που κάναμε ήταν να καταγράψουμε στην αρχή αυτά τα συστατικά που θεωρούσαμε σίγουρα ότι αποτελούν συστατικά του συστήματος (της Υπηρεσίας Δημοπρασιών). Στην αρχή βρήκαμε τα συστατικά που είναι την Υπηρεσία Καταγραφής Δημοπρασίας, το Πωλητή, τον Αγοραστή και τον Οίκο Δημοπρασίας.

Το Auction House είναι ο οίκος δημοπρασίας που ανήκουν ο Πωλητής και ο Αγοραστής. Απαραίτητο στοιχείο είναι και οι δύο να προέρχονται απο τον ίδιο οίκο δημοπρασίας. Αυτο μπορούμε να το ελέγξουμε δίνοντας σε κάθε Πωλητή και Αγοραστή έναν Κωδικό Δημοπρασίας που αντιστοιχει στον Οίκο Δημοπρασίας. Αυτό τον Κωδικό Δημοπρασίας οι Πωλητές και Αγοραστές το παιρνούν ως δεδομένο μαζί με τις προσφορές που καταθέτουν στην Υπηρεσία Δημοπρασιών. Συνεπώς με βάση όλα τα προηγούμενα αποσαφηνίζεται ο ακριβής ρόλος του επιπρόσθετου βασικού συστατικού, ο οποίος δεν επηρεάζει τους υπόλοιπους και τις σχέσεις μεταξύ τους όπως έχουν οριστεί μέχρι τώρα.

Θεωρήσαμε ως γεγονός της κορυφής την Υπηρεσία Δημοπρασιών και κατασκευάσαμε το UML διάγραμμα (Σχήμα 4.1) που αντιστοιχούσε με βάση τα παραπάνω στοιχεία.



Σχήμα 4.1

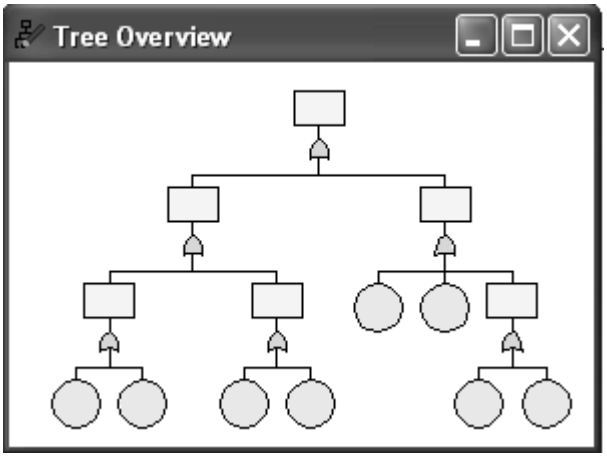
4.2.1 Κατασκευή δένδρου λαθών χωρίς εφεδρικά τμήματα

Αρχικά κατασκευάσαμε το δένδρο λαθών σε χαρτί και στη συνέχεια το μεταφέραμε στο λογισμικό OpenFTA. Στον αρχικό ενδιάμεσο κόμβο, που υπάρχει όταν ανοίγουμε το λογισμικό, τοποθετήσαμε ως γεγονός της κορυφής την Υπηρεσία Δημοπρασιών. Ακολουθεί μια πύλη OR, γιατί οποιαδήποτε από τα βασικά συστατικά (Υπηρεσία Καταγραφής Δημοπρασίας, Πωλητές, Αγοραστές, Οίκος Δημοπρασίας) αποτύχει, τότε αποτυγχάνει το γεγονός της κορυφής. Οι δραστηριότητες που κάνουν τα τέσσερα συστατικά είναι:

- για τον Πωλητή να στέλνει τις προτάσεις στην Υπηρεσία Δημοπρασιών (provide) και να λαμβάνει απαντήσεις από την Υπηρεσία Δημοπρασιών (answer)
- για τον Αγοραστή να στέλνει τις προτάσεις στην Υπηρεσία Δημοπρασιών (provide) και να λαμβάνει απαντήσεις από την Υπηρεσία Δημοπρασιών (answer) και

- για την Υπηρεσία Καταγραφής Δημοπρασίας να παίρνει τα δεδομένα από την Υπηρεσία Δημοπρασιών των Πωλητών και Αγοραστών (data) και να στέλνει τα αποτελέσματα στην Υπηρεσία Δημοπρασιών
- για τον Οίκο Δημοπρασίας είναι να δίνει τον Κωδικό Δημοπρασίας του στην Υπηρεσία Καταγραφής Δημοπρασίας όταν δημιουργείται μια καινούρια διαδικασία. Διαδικασία είναι το σύνολο των προτάσεων των Πωλητών και Αγοραστών και περιλαμβάνει όλες τις δραστηριότητες σχετικές με αυτές. Η Υπηρεσία Καταγραφής Δημοπρασίας στέλνει μαζί με τις απαντήσεις και τον Κωδικό Δημοπρασίας για να μπορεί ο Οίκος Δημοπρασίας να αναγνωρίσει την αντίστοιχη διαδικασία.

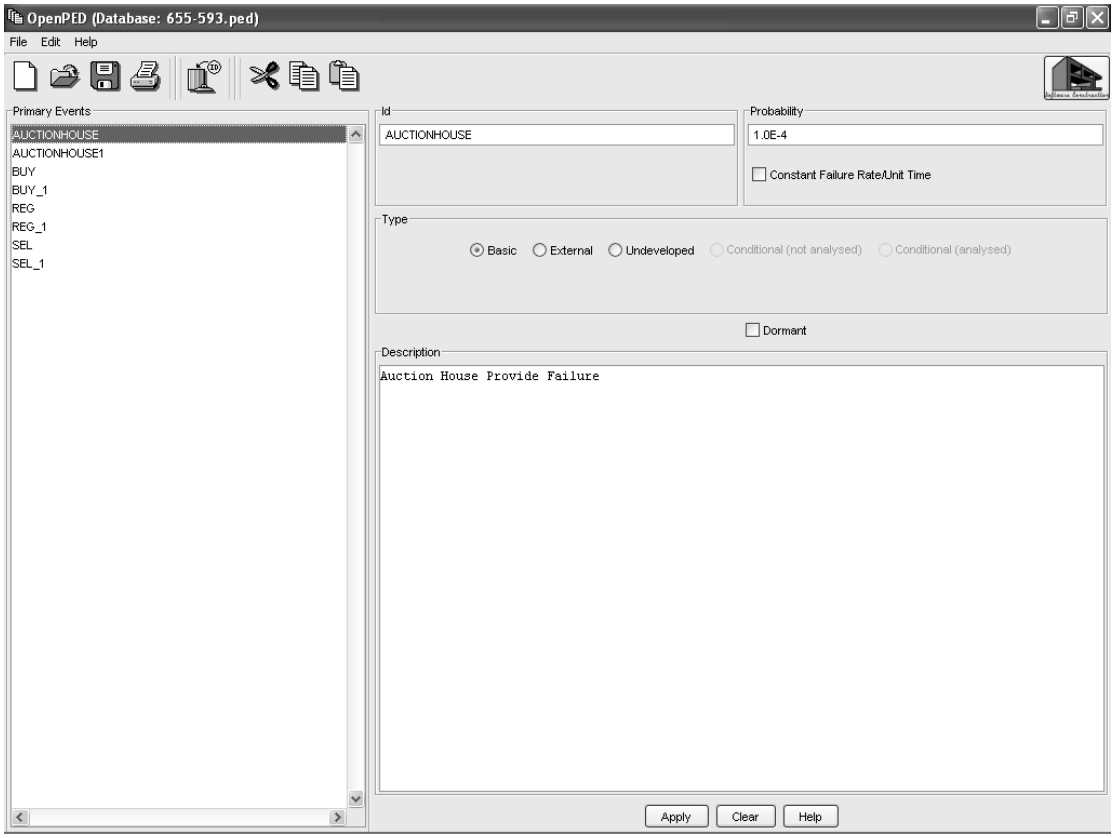
Υπάρχουν συνολικά οκτώ στοιχειώδη γεγονότα, αφού ανάλογες είναι και οι δραστηριότητες των βασικών συστατικών που μπορεί να αποτύχουν. Στην πύλη OR θα βάλουμε δύο ενδιάμεσα γεγονότα ένα θα το ονομάσουμε «Buyer and Seller Failure» και το άλλο «Auction Registration Service Failure». Σε κάθε ενδιάμεσο γεγονός εισάγουμε μια πύλη OR και στην πύλη δύο ενδιάμεσα γεγονότα (ένα για τον Αγοραστή και ένα για τον Πωλητή). Σε κάθε ενδιάμεσο γεγονός εισάγουμε μια πύλη OR και στην πύλη δύο στοιχειώδεις κόμβους. Στο ενδιάμεσο γεγονός Seller τα στοιχειώδη γεγονότα ονομάζονται «Seller Provide Failure» και «Seller Answer Failure». Στο ενδιάμεσο γεγονός Buyer τα στοιχειώδη γεγονότα ονομάζονται «Buyer Provide Failure» και «Buyer Answer Failure». Οποιαδήποτε από τις τέσσερις δραστηριότητες αποτύχει, το βασικό συστατικό, στο οποίο ανήκει, αποτυγχάνει. Αυτό έχει ως αποτέλεσμα να αποτύχει το γεγονός της κορυφής (Υπηρεσία Δημοπρασιών), αφού προηγουμένως αναφέραμε ότι οποιοδήποτε από τα τέσσερα βασικά συστατικά προκαλεί την πραγματοποίηση του. Στο ενδιάμεσο γεγονός Auction Registration Service Failure τοποθετούμε μια πύλη OR, στην οποία εισάγουμε ένα ενδιάμεσο γεγονός με όνομα Auction Registration Service Answer Failure και δύο στοιχειώδη γεγονότα. Στα στοιχειώδη γεγονότα περιγράφονται τα «Auction House Provide Failure» και «Auction Registration Service Data Failure» αντίστοιχα. Στο ενδιάμεσο γεγονός Auction Registration Service Answer Failure τοποθετούμε μια πύλη OR, στην οποία εισάγουμε δύο στοιχειώδη γεγονότα. Στα δύο στοιχειώδη γεγονότα περιγράφονται «Auction Registration Service Answer Failure» και «Auction House Answer Failure». Συνολικά δημιουργηθηκαν οκτώ στοιχειώδη γεγονότα. Το σφάλμα σε οποιοδήποτε από τα οκτώ στοιχειώδη γεγονότα θα προκαλέσει την πραγματοποίηση του γεγονότος της κορυφής (αποτυχία της Υπηρεσίας Δημοπρασιών). Στο Σχήμα 4.2 φαίνεται το δένδρο λαθών που δημιουργήθηκε με τα παραπάνω βήματα.



Σχήμα 4.2

Στο παραπάνω σχήμα στο δένδρο λαθών τα στοιχειώδη γεγονότα δεν έχουν πάρει τιμές. Το επόμενο βήμα είναι να δημιουργήσουμε στη βάση δεδομένων μας τα στοιχειώδη γεγονότα με τις ιδιότητες τους. Θα δημιουργήσουμε τόσες εγγραφές στη βάση δεδομένων όσες είναι και οι δραστηριότητες στο δένδρο λαθών. Θα δημιουργήσουμε τα στοιχεία για μια εγγραφή και η συνέχεια για τις υπόλοιπες θα είναι ανάλογη. Όλες οι εγγραφές είναι ίδιες στα χαρακτηριστικά τους, αλλά διαφέρουν στις ονομασίες και στις περιγραφές τους.

Θα δημιουργήσουμε ως παράδειγμα για τις υπόλοιπες εγγραφές την δραστηριότητα του Πωλητή για αποστολή των προτάσεων στην Υπηρεσία Δημοπρασιών (provide). Στο πλαίσιο ID γράφουμε κάτι που είναι χαρακτηριστικό για την δραστηριότητα αυτή, δηλαδή SEL. Στο probability (πιθανότητα) δίνουμε ως τυχαία τιμή για να συμβεί το γεγονός 0,0004 ή 1.0E-4. Το κουμπί Constant Failure Rate/Unit Time (Ρυθμός Αποτυχίας) δεν το επιλέγουμε, γιατί η πιθανότητα να συμβει το γεγονός δεν είναι συνάρτηση του χρόνου. Στο πλαίσιο Type επιλέγουμε το κουμπί, που γράφει basic (βασικό), το γεγονός που περιγράφει είναι στοιχειώδη γεγονότα. Αν το γεγονός αποτύχει, θα γίνει αντιληπτό από το περιβάλλον. Συνεπώς δεν επιλέγουμε το κουμπί Dormant (Μη ανιχνευθέν). Στο πλαίσιο description γράφουμε Seller Provide Failure δηλώνοντας ότι το στοιχειώδες γεγονός SEL είναι η αποτυχία του Πωλητή να στείλει την πρόταση στην Υπηρεσία Δημοπρασιών. Τέλος πατάμε το apply για να δημιουργηθεί η εγγραφή στη βάση δεδομένων με αυτά τα στοιχεία για το στοιχειώδες γεγονός SEL. Συνεχίζουμε ανάλογα με τα υπόλοιπα στοιχειώδη γεγονότα αλλάζοντας μόνο τα πλαίσια description και ID. Η τελική βάση δεδομένων φαίνεται στην Εικόνα 4.1.



Εικόνα 4.1

4.2.2 Ανάλυση του δένδρου λαθών χωρίς εφεδρικά τμήματα

Το επόμενο βήμα είναι να κάνουμε «πλήρες» το δένδρο λαθών, δηλαδή να διαμορφώσουμε το δένδρο λαθών ώστε να είναι έτοιμο για την περαιτέρω ανάλυση. Αρχικά θα συνδέσουμε το δένδρο λαθών του OpenFTA με τη βάση δεδομένων και τα γεγονότα του δένδρου με τις αντίστοιχες ιδιότητες τους απο τη βάση.

Μετά θα σώσουμε το δένδρο λαθών και τη βάση δεδομένων με το ίδιο όνομα στον ίδιο φάκελο. Τέλος θα κάνουμε *Validate (Έλεγχος Ορθότητας)* από το *Analysis (Ανάλυση)* για να ελέγξουμε την ορθότητα του δένδρου λαθών. Η αναφορά του επόμενου κειμένου, που παράγει το λογισμικό, δείχνει ότι το δένδρο λαθών είναι σωστό.

VALIDATION REPORT ON 655-593.fta

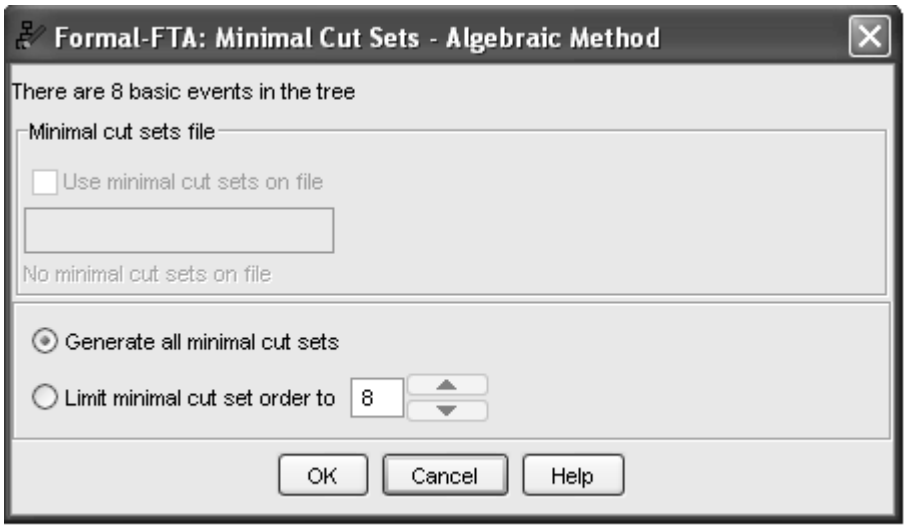
TREE VALID

Τώρα μπορούμε να προχωρήσουμε στην ανάλυση του δένδρου λαθών με τις μεθόδους *Minimal Cut Sets... (Σύνολα Ελάχιστης Τομής...), Numerical Probability…*

(Ποσοτική Ανάλυση...) και *Monte Carlo Simulation… (Προσομοίωση Monte Carlo)* κατά σειρά από το *Analysis (Ανάλυση).*

4.2.2.1 Ανάλυση δένδρου με τη μέθοδο Σύνολα Ελάχιστης Τομής

Η ανάλυση με τη μέθοδο «*Ποιοτική Ανάλυση*» (Σύνολα Ελάχιστης Τομής) αρχίζει προσδιορίζοντας τις ιδιότητές της. Θα επιλέξουμε τις προκαθορισμένες επιλογές, που έχει η ανάλυση, και φαίνονται στην Εικόνα 4.2.



Εικόνα 4.2

Όταν πατήσουμε το OK, τότε εμφανίζεται μια αναφορά με τα αποτελέσματα της ανάλυσης. Στο παρακάτω κείμενο είναι γραμμένα τα αποτελέσματα που παρουσιάζονται στην αναφορά.

Minimal Cut Sets
==========

Tree : 655-593.fta
Time : Mon Aug 01 13:01:05 2005

Method : Algebraic

No. of primary events = 8
Minimal cut set order = 1 to 8

Order 1:

1) AUCTIONHOUSE
2) AUCTIONHOUSE1
3) BUY
4) BUY_1
5) REG
6) REG_1
7) SEL
8) SEL_1

Order 2:

Order 3:

Order 4:

Order 5:

Order 6:

Order 7:

Order 8:

Qualitative Importance Analysis:

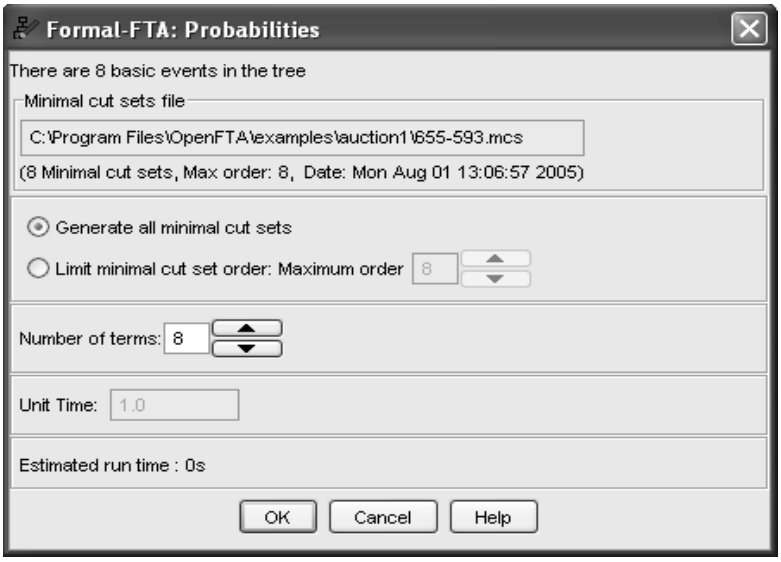
Order	Number
1	8
2	0
3	0
4	0
5	0
6	0
7	0
8	0
ALL	8

Τα αποτελέσματα αναφέρουν ότι υπάρχουν οκτώ στοιχειώδη γεγονότα και οι σειρές εύρεσης στις οποίες θα αναλυθούν τα σύνολα ελάχιστης τομής είναι επίσης οκτώ. Όλα τα σύνολα ελάχιστης τομής ανήκουν στην πρώτη σειρά εύρεσης. Αυτό σημαίνει ότι τα σύνολα ελάχιστης τομής ανακαλύφθηκαν στο ίδιο επίπεδο και είναι ίδιας σημαντικότητας για την πραγματοποιήση του γεγονότος της κορυφής (αποτυχία της Υπηρεσίας Δημοπρασιών). Αυτό διακρίνεται και από την ανάλυση που γίνεται στον πίνακα «Σημαντικότητα των συνόλων ελάχιστης τομής στην Ποιοτική Ανάλυση» (Qualitative Importance Analysis). Ο πίνακας απεικονίζει την κατανομή του αριθμού των συνόλων ελάχιστης τομής, που βρέθηκαν σε κάθε σειρά των

συνόλων τομής που υπάρχουν. Όλα τα σύνολα ελάχιστης τομής γράφονται στη «Σειρά 1» (Order 1).

4.2.2.2 Ανάλυση δένδρου λαθών με τη μέθοδο ποσοτικής ανάλυσης

Η μέθοδος «Ποσοτική Ανάλυση» (Numerical Probability) ακολουθεί την «Ποιοτική Ανάλυση» (Minimal Cut Sets), γιατι έχει απλοποιηθεί το δένδρο λαθών και οι υπολογισμοί δεν θα είναι πολύπλοκοι και χρονοβόροι. Πρέπει να ορίσουμε τις ιδιότητες της Ποσοτικής Ανάλυσης. Επιλέγουμε τις προκαθορισμένες επιλογες, που έχει η ανάλυση και φαίνονται στην Εικόνα 4.3.



Εικόνα 4.3

Όταν πατήσουμε το OK, τότε εμφανίζεται μια αναφορά με τα αποτελέσματα της ανάλυσης. Στο παρακάτω κείμενο είναι γραμμένα τα αποτελέσματα που παρουσιάζονται στην αναφορά.

Probabilities Analysis
==========

Tree : 655-593.fta
Time : Mon Aug 01 13:33:40 2005

Number of primary events = 8
Number of minimal cut sets = 8
Order of minimal cut sets = 8

Unit time span = 1.000000

Minimal cut set probabilities :

1	AUCTIONHOUSE	1.000000E-004
2	AUCTIONHOUSE1	1.000000E-004
3	BUY	1.000000E-004
4	BUY_1	1.000000E-004
5	REG	1.000000E-004
6	REG_1	1.000000E-004
7	SEL	1.000000E-004
8	SEL_1	1.000000E-004

Probability of top level event (minimal cut sets up to order 8 used):

1 term	+8.000000E-004	= 8.000000E-004 (upper bound)
2 term	-2.800000E-007	= 7.997200E-004 (lower bound)
3 term	+5.599997E-011	= 7.997201E-004 (upper bound)
4 term	-6.999996E-015	= 7.997201E-004 (lower bound)
5 term	+5.599997E-019	= 7.997201E-004 (upper bound)
6 term	-2.799999E-023	= 7.997201E-004 (lower bound)
7 term	+7.999998E-028	= 7.997201E-004 (upper bound)
8 term	-9.999998E-033	= 7.997201E-004 (lower bound)

Exact value : 7.997201E-004

Primary Event Analysis:

Event	Failure contrib.	Importance
AUCTIONHOUSE	1.000000E-004	12.50%
AUCTIONHOUSE1	1.000000E-004	12.50%
BUY	1.000000E-004	12.50%
BUY_1	1.000000E-004	12.50%
REG	1.000000E-004	12.50%
REG_1	1.000000E-004	12.50%
SEL	1.000000E-004	12.50%
SEL_1	1.000000E-004	12.50%

Τα αποτελέσματα αναφέρουν ότι υπάρχουν οκτώ στοιχειώδη γεγονότα και οκτώ σύνολα ελάχιστης τομής. Οι σειρές εύρεσης στις οποίες θα αναλυθούν τα σύνολα ελάχιστης τομής είναι επίσης οκτώ. Αναφέρονται επίσης οι πιθανότητες των συνόλων ελάχιστης τομής. Όλα τα σύνολα ελάχιστης τομής είναι ισοπίθανα και η πιθανότητά τους ισούται με αυτήν των στοιχειώδων γεγονότων, δηλαδή με 1.000000E-004. Στο πλαίσιο «Πιθανότητα του γεγονότος της κορυφής χρησιμοποιώντας τα σύνολα ελάχιστης τομής μέχρι την σειρά οκτώ» (Probability of top level event with minimal

cut sets up to order 8 used) υπολογίζονται οι οκτώ πρώτοι όροι της συνάρτησης της μεθόδου. Ο πρώτος όρος είναι άνω όριο της πιθανότητας του γεγονότος της κορυφής, ο δεύτερος είναι κάτω όριο της πιθανότητας του γεγονότος της κορυφής, ο τρίτος είναι καλύτερο άνω όριο της πιθανότητας του γεγονότος της κορυφής και αυτο ισχύει και για τους υπόλοιπους όρους. Η πιθανότητα του γεγονότος της κορυφής γράφεται στο «Ακριβής τιμή» (Exact value) και ισούται με τον τελευταίο όρο, που είναι και το μεγαλύτερο κάτω όριο της πιθανότητας του γεγονότος της κορυφής, με τιμή 7.997201E-004. Ο τελευταίος πίνακας, που ονομάζεται Basic Event Analysis (Ανάλυση Βασικού Γεγονότος), περιέχει μια λίστα όλων των στοιχειώδων γεγονότων του δένδρου λαθών και την αντίστοιχη συμβολή της αποτυχίας τους στην πραγματοποίηση του γεγονότος της κορυφής. Η συμβολή αυτή εκφράζεται και ως ποσοστό σημαντικότητας του κάθε στοιχειώδους γεγονότος. Παρατηρούμε ότι όλα τα στοιχειώδη γεγονότα μπορούν να συμβάλουν με το ίδιο ποσοστό στην πραγματοποίηση του γεγονότος της κορυφής (αποτυχία της Υπηρεσίας Δημοπρασιών).

4.2.2.3 Ανάλυση του δένδρου λαθών με τη μέθοδο Monte Carlo προσομοίωση

Η μέθοδος αυτή προσφέρει μεγαλύτερη ακρίβεια στα αποτελέσματα σε σχέση με την Ποσοτική Ανάλυση με κόστος όμως στον χρόνο. Θα ορίσουμε τις ιδιότητες της Προσομοίωσης Monte Carlo. Παρόμοια με τις προηγούμενες αναλύσεις θα επιλέξουμε τις προκαθορισμένες επιλογές που φαίνονται στην Εικόνα 4.4.

Εικόνα 4.4

Όταν πατήσουμε το OK, τότε εμφανίζεται μια αναφορά με τα αποτελέσματα της ανάλυσης. Στο παρακάτω κείμενο είναι γραμμένα τα αποτελέσματα που παρουσιάζονται στην αναφορά.

Monte Carlo Simulation
==========

Tree : 655-593.fta
Time : Mon Aug 01 14:20:44 2005

Note: Only runs with at least one component failure are simulated

Number of primary events = 8
Number of tests = 10000
Unit Time span used = 1.000000

Number of system failures = 10000

Probability of at least = 7.997200E-004 (exact)
one component failure

Probability of top event = 7.997201E-004 (+/- 7.997201E-006)

Rank	Failure mode	Failures	Estimated Probability	Importance
1	AUCTIONHOUSE	1338	1.070025E-004 (+/- 2.925271E-006)	13.38%
2	REG_1	1270	1.015644E-004 (+/- 2.849967E-006)	12.70%
3	REG	1243	9.940520E-005 (+/- 2.819509E-006)	12.43%
4	BUY	1242	9.932523E-005 (+/- 2.818375E-006)	12.42%
5	BUY_1	1237	9.892537E-005 (+/- 2.812696E-006)	12.37%
6	SEL	1232	9.852551E-005 (+/- 2.807006E-006)	12.32%
7	SEL_1	1225	9.796570E-005 (+/- 2.799020E-006)	12.25%
8	AUCTIONHOUSE1	1209	9.668615E-005 (+/- 2.780681E-006)	12.09%
9	AUCTIONHOUSE BUY	1	7.997200E-008 (+/- 7.997200E-008)	0.01%
10	BUY SEL	1	7.997200E-008 (+/- 7.997200E-008)	0.01%
11	BUY BUY_1	1	7.997200E-008 (+/- 7.997200E-008)	0.01%
12	BUY_1 REG_1	1	7.997200E-008 (+/- 7.997200E-008)	0.01%

Compressed:

Rank	Failure mode	Failures	Estimated Probability	Importance
1	AUCTIONHOUSE1	1209	9.668615E-005 (+/- 2.780681E-006)	12.09%
2	SEL_1	1225	9.796570E-005 (+/- 2.799020E-006)	12.25%
3	SEL	1233	9.860548E-005 (+/- 2.808145E-006)	12.33%
4	BUY_1	1239	9.908531E-005 (+/- 2.814969E-006)	12.39%
5	BUY	1245	9.956514E-005 (+/- 2.821777E-006)	12.45%
6	REG	1243	9.940520E-005 (+/- 2.819509E-006)	12.43%
7	REG_1	1271	1.016444E-004 (+/- 2.851089E-006)	12.71%
8	AUCTIONHOUSE	1339	1.070825E-004 (+/- 2.926363E-006)	13.39%

Primary Event Analysis:

Event	Failure contrib.	Importance
AUCTIONHOUSE	1.070825E-004	13.39%
AUCTIONHOUSE1	9.668616E-005	12.09%
BUY	9.956514E-005	12.45%
BUY_1	9.908532E-005	12.39%
REG	9.940520E-005	12.43%
REG_1	1.016444E-004	12.71%
SEL	9.860548E-005	12.33%
SEL_1	9.796571E-005	12.25%

Τα αποτελέσματα αναφέρουν ότι υπάρχουν οκτώ στοιχειώδη γεγονότα, ο αριθμός των test είναι 10000 και το Unit Time span είναι 1.000000. Ο αριθμός των αποτυχιών του συστήματος είναι 10000. Η πιθανότητα τουλάχιστον ένα από τα συστατικά να αποτύχει είναι 7.997200E-004. Η πιθανότητα πραγματοποίησης του γεγονότος της κορυφής είναι 7.997201E-004 (+/- 7.997201E-006).

Στον επόμενο πίνακα παρουσιάζονται όλα τα συνόλα ελάχιστης τομής που βρέθηκαν στο δένδρο λαθών. Κάθε γραμμή του πίνακα περιέχει: το συνόλο ελάχιστης τομής, τον αριθμό των αποτυχιών που οφείλονται σε αυτό, την πιθανότητα ένα από τα γεγονότα του συνόλου τομής να συμβεί και το ποσοστό σημαντικότητας του συνόλου τομής σε σχέση με τα υπόλοιπα που βρέθηκαν. Τα συνόλα ελάχιστης τομής αποτυγχάνουν περίπου ισάριθμες φορές με μικρό προβάδισμα στο AUCTIONHOUSE και επομένως έχουν περίπου και τα ίδια αποτελέσματα και στις υπόλοιπες στήλες του πίνακα. Τα συνόλα ελάχιστης τομής παρουσιάζονται σε φθίνουσα σειρά ανάλογα με τα αριθμητικά αποτελέσματά τους.

Ο πίνακας, που ονομάζεται Compressed, είναι ίδιος με τον προηγούμενο, αλλά τα συνόλα τομής που είναι λιγότερο μινιμαλιστικά από τα υπόλοιπα τα μετατρέπει σε περισσότερο μινιμαλιστικά. Τα υπόλοιπα πεδία προσαρμόζονται σύμφωνα με τα καινούρια στοιχεία. Σε αυτόν τον πίνακα τα τέσσερα τελευταία σύνολα τομής απλοποιούνται και περιλαμβάνονται στα πρώτα. Αυτό γίνεται επειδή δεν ήταν μινιμαλιστικά, δηλαδή αποτελούνταν από άλλα σύνολα ελάχιστης τομής. Τα αριθμητικά αποτελέσματα των συνόλων ελάχιστης τομής είναι ίδια με αυτά του προηγούμενου πίνακα, αλλά παρουσιάζονται σε αντίστροφη σειρά.

Ο τελευταίος πίνακας, που ονομάζεται Basic Event Analysis (Ανάλυση Βασικού Γεγονότος), περιέχει μια λίστα με όλα τα στοιχειώδη γεγονότα και την η συμβολή της αποτυχίας όταν συμβαίνει το γεγονός της κορυφής. Αυτή η συμβολή εκφράζεται και ως ποσοστό σημαντικότητας του κάθε στοιχειώδους γεγονότος. Τα στοιχειώδη γεγονότα που ανήκουν σε σύνολα ελάχιστης τομής πραγματοποιούνται περίπου ίσες φορές. Συνεπώς και η σημαντικότητα του κάθε στοιχειώδους γεγονότος, δηλαδή η συμβολή της αποτυχίας τους όταν πραγματοποιείται το γεγονός της κορυφής (αποτυχία της Υπηρεσίας Δημοπρασιών χωρίς Εφεδρικά τμήματα), είναι περίπου ίδια. Τα αριθμητικά αποτελέσματα αυτού του πίνακα ισούνται με αυτά της τελευταίας στήλης του Compressed, αλλά παρουσιάζονται σε αλφαβητική σειρά.

4.3 Δένδρο λαθών με εφεδρικά τμήματα

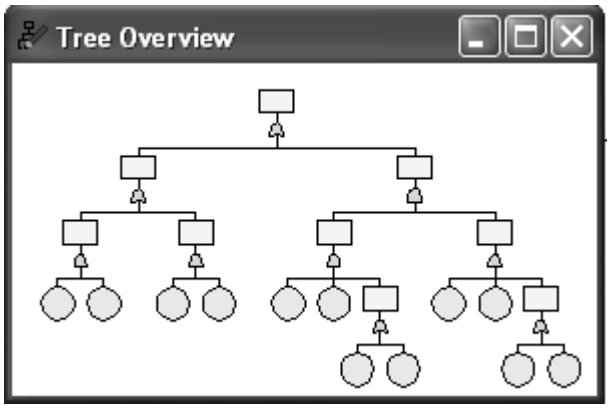
Το με εφεδρικά τμήματα επηρεάζει το δένδρο λαθών στο μέρος όπου εφαρμόζεται αυτή η μέθοδος. Έτσι το δένδρο λαθών θα αλλάξει στο σημείο που αναπτύσσεται στην Υπηρεσία Καταγραφής Δημοπρασίας και το υπόλοιπο κομμάτι θα μείνει ίδιο. Επίσης θα επηρρεαστούν και τα αποτελέσματα των μεθόδων ανάλυσης (Minimal Cut Sets, Numerical Probability και Monte Carlo Simulation).

4.3.1 Κατασκευή του δένδρου λαθών με εφεδρικά τμήματα

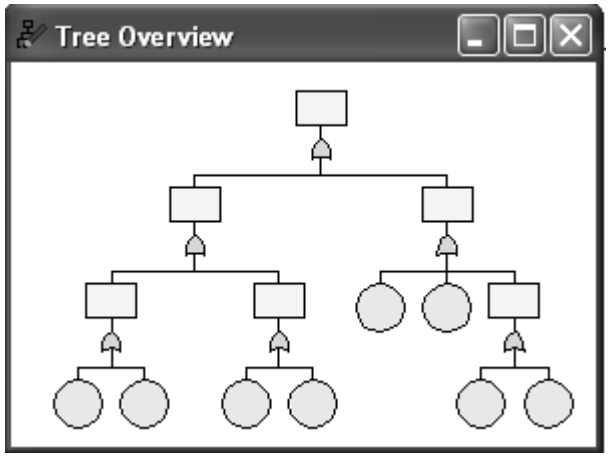
Σύμφωνα με τα προηγούμενα η εφαρμογη της μεθόδου με εφεδρικά τμήματα έχει ως αποτέλεσμα την προσθήκη μιας δεύτερης Υπηρεσίας Καταγραφής Δημοπρασίας στο δένδρο λαθών με τις ίδιες ιδιότητες όπως αυτές του προυπάρχοντος. Το UML διάγραμμα παραμένει ίδιο με αυτό που δημιουργήθηκε από την ανάλυση της αρχικής Υπηρεσίας Δημοπρασιών. Θεώρούμε ως αρχή το δένδρο λαθών χωρίς εφεδρικά τμήματα πάνω στο οποίο θα κάνουμε τις αλλαγές για να δημιουργήσουμε το αντίστοιχο με εφεδρικά τμήματα. Στο ενδιάμεσο γεγονός «Auction Registration Service Failure», τον οποίο μετονομάζουμε σε «Evaluation of data», εισάγουμε μια πύλη OR. Στην πύλη OR τοποθετούμε δύο ενδιάμεσα γεγονότα. Το πρώτο ενδιάμεσο γεγονός ονομάζεται «Auction Registration 1 Service Failure» και είναι η αποτυχία της πρώτης Υπηρεσίας Καταγραφής Δημοπρασίας. Το δεύτερο ενδιάμεσο γεγονός ονομάζεται «Auction Registration 2 Service Failure» και είναι η αποτυχία της δεύτερης Υπηρεσίας Καταγραφής Δημοπρασίας. Η δομή για κάθε

Υπηρεσία Καταγραφής Δημοπρασίας κάτω από το αντίστοιχο του ενδιάμεσου γεγονότος είναι ίδια με αυτή που ήταν για την Υπηρεσία Καταγραφής Δημοπρασίας του δένδρου λαθών χωρίς εφεδρικά τμήματα. Αυτό που αλλάζει είναι οι ονομασίες μερικών γεγονότων σχετικών με την Υπηρεσία Καταγραφής Δημοπρασίας.

Στην Εικόνα 4.5 είναι το δένδρο λαθών με εφεδρικά τμήματα και στην Εικόνα 4.6 το δένδρο λαθών χωρίς εφεδρικά τμήματα. Έτσι μπορούμε να διακρίνουμε τις ομοιότητες και τις διαφορές που αναφέραμε προηγουμένως.



Εικόνα 4.5: (Δένδρο λαθών με εφεδρικά τμήματα)



Εικόνα 4.6: (Δένδρο λαθών χωρίς εφεδρικά τμήματα)

Η προσθήκη στοιχειώδων γεγονότων στο δένδρο λαθών οδηγεί στην προσθήκη εγγραφών στη βάση δεδομένων. Αφού προσθέσαμε δύο επιπλέον γεγονότα στο δένδρο λαθών, θα δημιουργήσουμε τις αντίστοιχες εγγραφές στη βάση δεδομένων. Από τη βάση δεδομένων του δένδρου λαθών χωρίς εφεδρικά τμήματα θα κρατήσουμε τις εγγραφές SEL, SEL_1, BUY, BUY_1, AUCTIONHOUSE KAI AUCTIONHOUSE1. Θα διαγράψουμε τις REG KAI REG_1. Θα προσθέσουμε τέσσερις εγγραφές:

- REG1 με όνομα «Auction Registration Service Data 1 Failure»
- REG1_1 με όνομα «Auction Registration Service 1 Answer Failure»
- REG2 με όνομα «Auction Registration Service 2 Data Failure» και
- REG2_1 με όνομα « Auction Registration Service 2 Answer Failure»

4.3.2 Ανάλυση του δένδρου λαθών με εφεδρικά τμήματα

Η ανάλυση του δένδρου λαθών με εφεδρικά τμήματα θα γίνει με τον ίδιο τρόπο που υλοποιήθηκε το δένδρο λαθών χωρίς εφεδρικά τμήματα. Πριν ξεκινήσουμε την ανάλυση θα πρέπει να ελέγξουμε αν το δένδρο λαθών είναι σωστό. Θα κάνουμε *Validate (Έλεγχος Ορθότητας)* από το *Analysis (Ανάλυση)* για να ελέγξουμε την ορθότητα του δένδρου λαθών. Η αναφορά, που παράγει το λογισμικό και φαίνεται στο επόμενο κειμένο, δείχνει ότι το δένδρο λαθών είναι σωστό.

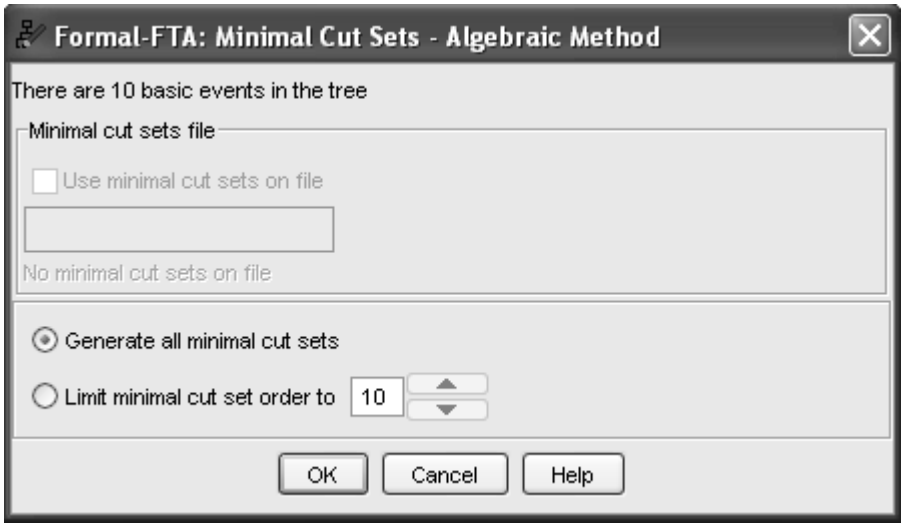
VALIDATION REPORT ON 655-593.fta

TREE VALID

Τώρα μπορούμε να προχωρήσουμε στην ανάλυση του δένδρου λαθών με τις μεθόδους *Minimal Cut Sets... (Σύνολα Ελάχιστης Τομής...), Numerical Probability… (Ποσοτική Ανάλυση)* και *Monte Carlo Simulation… (Προσομοίωση Monte Carlo)* κατά σειρά από το *Analysis (Ανάλυση).*

4.3.2.1 Ανάλυση στο δένδρου λαθών (με εφεδρικά τμήματα) με Minimal Cut Sets (Ποιοτική Ανάλυση)

Η ανάλυση με τη μέθοδο «Ποιοτική Ανάλυση» (Minimal Cut Sets) αρχίζει προσδιορίζοντας τις ιδιότητές της. Θα επιλέξουμε τις προκαθορισμένες επιλογές, που έχει η ανάλυση, και φαίνονται στην Εικόνα 4.7.



Εικόνα 4.7

Minimal Cut Sets
==========

Tree : 655-593.fta
Time : Mon Aug 01 19:33:42 2005

Method : Algebraic

No. of primary events = 10
Minimal cut set order = 1 to 10

Order 1:
1) AUCTIONHOUSE
2) AUCTIONHOUSE1
3) BUY
4) BUY_1
5) SEL
6) SEL_1

Order 2:
1) REG1 REG2
2) REG1 REG2_1
3) REG1_1 REG2
4) REG1_1 REG2_1

Order 3:

Order 4:

Order 5:

Order 6:

Order 7:

Order 8:

Order 9:

Order 10:

Qualitative Importance Analysis:

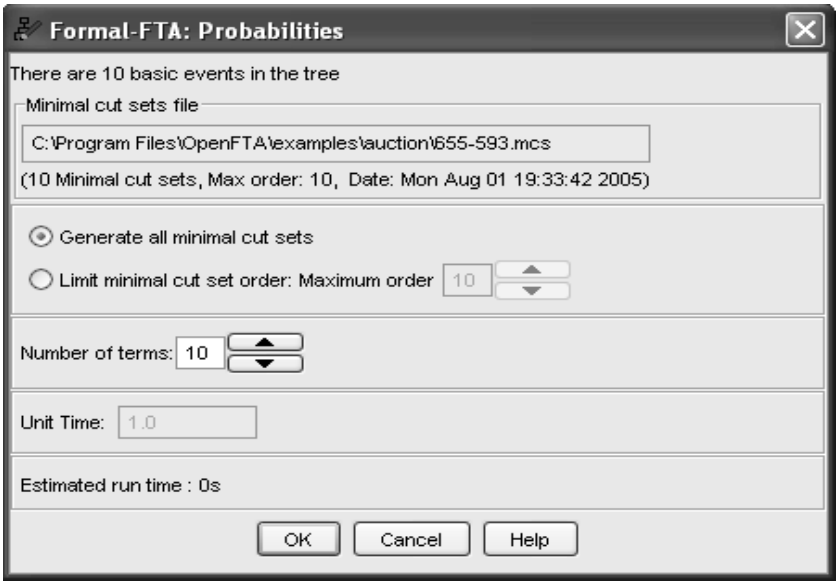
Order	Number
1	6
2	4
3	0
4	0

5	0
6	0
7	0
8	0
9	0
10	0
ALL	10

Τα αποτελέσματα αναφέρουν ότι υπάρχουν δέκα στοιχειώδη γεγονότα και οι σειρές εύρεσης στις οποίες θα αναλυθούν τα σύνολα ελάχιστης τομής είναι επίσης δέκα. Τα σύνολα ελάχιστης τομής AUCTIONHOUSE, AUCTIONHOUSE1, BUY, BUY_1, SEL και SEL_1 ανήκουν στην πρώτη σειρά εύρεσης. Αυτό σημαίνει ότι αυτά τα σύνολα ελάχιστης τομής ανακαλύφθηκαν στο ίδιο επίπεδο και είναι ίδιας σημαντικότητας για την πραγματοποιήση του γεγονότος της κορυφής (αποτυχία της Υπηρεσίας Δημοπρασιών). Τα σύνολα ελάχιστης τομής {REG1 REG2}, {REG1 REG2_1}, {REG1_1 REG2} και {REG1_1 REG2_1} ανήκουν στην δεύτερη σειρά εύρεσης. Αυτό σημαίνει ότι βρέθηκαν στο επόμενο επίπεδο από το προηγούμενο. Αυτό διακρίνεται και από την ανάλυση που γίνεται στον πίνακα «Σημαντικότητα των συνόλων ελάχιστης τομής στην Ποιοτική Ανάλυση» (Qualitative Importance Analysis). Ο πίνακας απεικονίζει την κατανομή του αριθμού των συνόλων ελάχιστης τομής, που βρέθηκαν σε κάθε σειρά των συνόλων τομής που υπάρχουν. Τα σύνολα ελάχιστης τομής γράφονται στη «Σειρά 1» (Order 1) και στη «Σειρά 2» (Order 2).

4.3.2.2 Ανάλυση του δένδρου λαθών με Ποσοτική Ανάλυση (Numerical Probability)

Η μέθοδος «Ποσοτική Ανάλυση» (Numerical Probability) ακολουθεί την «Ποιοτική Ανάλυση» (Minimal Cut Sets), γιατι έχει απλοποιηθεί το δένδρο λαθών και οι υπολογισμοί δεν θα είναι πολύπλοκοι και χρονοβόροι. Πρέπει να ορίσουμε τις ιδιότητες της Ποσοτικής Ανάλυσης. Επιλέγουμε τις προκαθορισμένες επιλογες, που έχει η ανάλυση και φαίνονται στην Εικόνα 4.8.



Εικόνα 4.8

Όταν πατήσουμε το OK, τότε εμφανίζεται μια αναφορά με τα αποτελέσματα της ανάλυσης. Στο παρακάτω κείμενο είναι γραμμένα τα αποτελέσματα που παρουσιάζονται στην αναφορά.

Probabilities Analysis
==========

Tree : 655-593.fta
Time : Mon Aug 01 19:48:35 2005

Number of primary events = 10
Number of minimal cut sets = 10
Order of minimal cut sets = 10

Unit time span = 1.000000

Minimal cut set probabilities :

1	AUCTIONHOUSE	1.000000E-004
2	AUCTIONHOUSE1	1.000000E-004
3	BUY	1.000000E-004
4	BUY_1	1.000000E-004
5	SEL	1.000000E-004
6	SEL_1	1.000000E-004
7	REG1 REG2	9.999999E-009
8	REG1 REG2_1	9.999999E-009
9	REG1_1 REG2	9.999999E-009
10	REG1_1 REG2_1	9.999999E-009

Probability of top level event (minimal cut sets up to order 10 used):

1 term	+6.000400E-004	= 6.000400E-004 (upper bound)
2 terms	-1.500279E-007	= 5.998900E-004 (lower bound)
3 terms	+2.000883E-011	= 5.998900E-004 (upper bound)
4 terms	-1.601633E-015	= 5.998900E-004 (lower bound)
5 terms	+1.202000E-019	= 5.998900E-004 (upper bound)
6 terms	-1.601641E-023	= 5.998900E-004 (lower bound)
7 terms	+2.000880E-027	= 5.998900E-004 (upper bound)
8 terms	-1.500280E-031	= 5.998900E-004 (lower bound)
9 terms	+6.000399E-036	= 5.998900E-004 (upper bound)
10 terms	-9.999946E-041	= 5.998900E-004 (lower bound)

Exact value : 5.998900E-004

Primary Event Analysis:

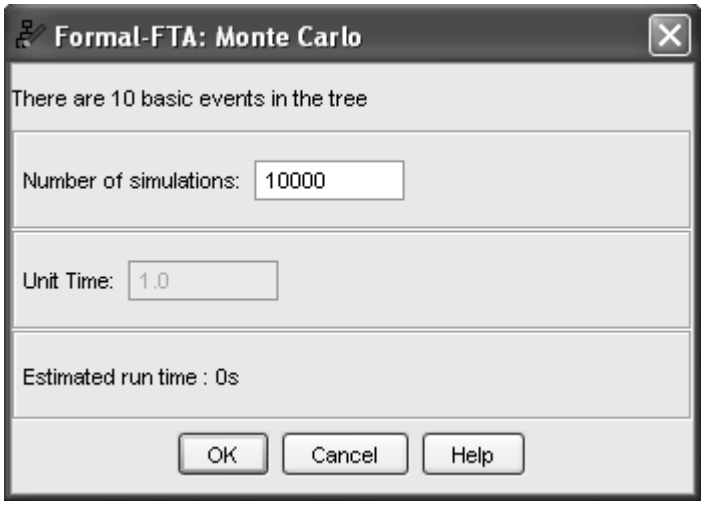
Event	Failure contrib.	Importance
AUCTIONHOUSE	1.000000E-004	16.67%
AUCTIONHOUSE1	1.000000E-004	16.67%
BUY	1.000000E-004	16.67%
BUY_1	1.000000E-004	16.67%
REG1	2.000000E-008	0.00%
REG1_1	2.000000E-008	0.00%
REG2	2.000000E-008	0.00%
REG2_1	2.000000E-008	0.00%
SEL	1.000000E-004	16.67%
SEL_1	1.000000E-004	16.67%

Τα αποτελέσματα αναφέρουν ότι υπάρχουν δέκα στοιχειώδη γεγονότα και δέκα σύνολα ελάχιστης τομής. Οι σειρές εύρεσης στις οποίες θα αναλυθούν τα σύνολα ελάχιστης τομής είναι επίσης δέκα. Αναφέρονται οι πιθανότητες των συνόλων ελάχιστης τομής. Τα σύνολα ελάχιστης τομής, που βρέθηκαν στην πρώτη σειρά, είναι ισοπίθανα με τη τιμή 1.000000E-004. Τα σύνολα ελάχιστης τομής, που βρέθηκαν στην δέυτερη σειρά, είναι ισοπίθανα με τη τιμή 9.999999E-009. Στο πλαίσιο «Πιθανότητα του γεγονότος της κορυφής χρησιμοποιώντας τα σύνολα ελάχιστης τομής μέχρι την σειρά δέκα» (Probability of top level event with minimal cut sets up to order 10 used) υπολογίζονται οι δέκα πρώτοι όροι της συνάρτησης της μεθόδου. Ο πρώτος όρος είναι άνω όριο της πιθανότητας του γεγονότος της κορυφής, ο δεύτερος είναι κάτω όριο της πιθανότητας του γεγονότος της κορυφής, ο τρίτος είναι καλύτερο άνω όριο της πιθανότητας του γεγονότος της κορυφής και αυτο ισχύει και για τους υπόλοιπους όρους. Η πιθανότητα του γεγονότος της κορυφής γράφεται στο «Ακριβής τιμή» (Exact value) και ισούται με τον τελευταίο όρο, που είναι και το μεγαλύτερο κάτω όριο της πιθανότητας του γεγονότος της κορυφής, με τιμή 5.998900E-004. Ο τελευταίος πίνακας, που ονομάζεται Basic Event Analysis (Ανάλυση Βασικού Γεγονότος), περιέχει μια λίστα όλων των στοιχειώδων γεγονότων του δένδρου λαθών και την αντίστοιχη συμβολή της αποτυχίας τους στην πραγματοποίηση του γεγονότος της κορυφής. Η συμβολή αυτή εκφράζεται και ως ποσοστό σημαντικότητας του κάθε

στοιχειώδους γεγονότος. Παρατηρούμε ότι τα στοιχειώδη γεγονότα, που ανήκουν στα σύνολα ελάχιστης τομής της πρώτης σειράς, συμβάλουν με το ίδιο ποσοστό στην πραγματοποίηση του γεγονότος της κορυφής (αποτυχία της Υπηρεσίας Δημοπρασιών) με τιμή 16.67%. Τα στοιχειώδη γεγονότα, που ανήκουν στα σύνολα ελάχιστης τομής της δεύτερης σειράς, έχουν μηδενικό ποσοστό στην πραγματοποίηση του γεγονότος της κορυφής. Αυτό συμβαίνει επειδή η αριθμητικη συμβολή της αποτυχίας τους είναι 2.000000E-008, η οποία είναι διπλάσια από των υπόλοιπων στοιχειώδων γεγονότων 1.000000E-004. Επομένως μπορεί να θεωρηθεί αμελητέα και να παραβλεφθεί.

4.3.2.3 Ανάλυση του δένδρου λαθών με εφεδρικά τμήματα με τη Monte Carlo προσομοίωση

Θα ορίσουμε τις ιδιότητες της Monte Carlo προσομοίωσης. Παρόμοια με τις προηγούμενες αναλύσεις θα επιλέξουμε τις προκαθορισμένες επιλογές που φαίνονται στην Εικόνα 4.9.



Εικόνα 4.9

Όταν πατήσουμε το OK, τότε εμφανίζεται μια αναφορά με τα αποτελέσματα της ανάλυσης. Στο παρακάτω κείμενο είναι γραμμένα τα αποτελέσματα που παρουσιάζονται στην αναφορά.

Monte Carlo Simulation
==========

Tree : 655-593.fta
Time : Mon Aug 01 20:16:42 2005

Note: Only runs with at least one component failure are simulated

Number of primary events = 10
Number of tests = 10000
Unit Time span used = 1.000000

Number of system failures = 5954

Probability of at least = 9.995501E-004 (exact)
one component failure

Probability of top event = 5.951321E-004 (+/- 7.712745E-006)

Rank	Failure mode	Failures	Estimated Probability	Importance
1	SEL	1018	1.017542E-004 (+/- 3.189176E-006)	17.10%
2	AUCTIONHOUSE	1002	1.001549E-004 (+/- 3.164014E-006)	16.83%
3	SEL_1	999	9.985505E-005 (+/- 3.159274E-006)	16.78%
4	BUY_1	986	9.855564E-005 (+/- 3.138651E-006)	16.56%
5	BUY	979	9.785595E-005 (+/- 3.127490E-006)	16.44%
6	AUCTIONHOUSE1	966	9.655654E-005 (+/- 3.106656E-006)	16.22%
7	REG1_1 REG2_1	1	9.995501E-008 (+/- 9.995501E-008)	0.02%
8	AUCTIONHOUSE REG1_1	1	9.995501E-008 (+/- 9.995501E-008)	0.02%
9	BUY_1 REG2_1	1	9.995501E-008 (+/- 9.995501E-008)	0.02%
10	BUY BUY_1	1	9.995501E-008 (+/- 9.995501E-008)	0.02%

Compressed:

Rank	Failure mode	Failures	Estimated Probability	Importance
1	AUCTIONHOUSE1	966	9.655654E-005 (+/- 3.106656E-006)	16.22%
2	BUY	980	9.795591E-005 (+/- 3.129087E-006)	16.46%
3	BUY_1	988	9.875555E-005 (+/- 3.141833E-006)	16.59%
4	SEL_1	999	9.985505E-005 (+/- 3.159274E-006)	16.78%
5	AUCTIONHOUSE	1003	1.002549E-004 (+/- 3.165593E-006)	16.85%
6	SEL	1018	1.017542E-004 (+/- 3.189176E-006)	17.10%
7	REG1_1 REG2_1	1	9.995501E-008 (+/- 9.995501E-008)	0.02%

Primary Event Analysis:

Event	Failure contrib.	Importance
AUCTIONHOUSE	1.002549E-004	16.85%
AUCTIONHOUSE1	9.655654E-005	16.22%
BUY	9.795591E-005	16.46%
BUY_1	9.875555E-005	16.59%
REG1	0.000000E+000	0.00%
REG1_1	9.995501E-008	0.02%
REG2	0.000000E+000	0.00%
REG2_1	9.995501E-008	0.02%
SEL	1.017542E-004	17.10%
SEL_1	9.985505E-005	16.78%

Τα αποτελέσματα αναφέρουν ότι υπάρχουν δέκα στοιχειώδη γεγονότα, ο αριθμός των test είναι 10000 και το Unit Time span είναι 1.000000. Ο αριθμός των αποτυχιών του συστήματος είναι 5954. Η πιθανότητα τουλάχιστον ένα από τα συστατικά να αποτύχει είναι 9.995501E-004. Η πιθανότητα πραγματοποίησης του γεγονότος της κορυφής είναι 5.951321E-004 (+/- 7.712745E-006).

Στον επόμενο πίνακα παρουσιάζονται όλα τα σύνολα ελάχιστης τομής που βρέθηκαν στο δένδρο λαθών. Κάθε γραμμή του πίνακα περιέχει: το σύνολο ελάχιστης τομής, τον αριθμό των αποτυχιών που οφείλονται σε αυτό, την πιθανότητα ένα από τα γεγονότα του συνόλου τομής να συμβεί και το ποσοστό σημαντικότητας του συνόλου τομής σε σχέση με τα υπόλοιπα που βρέθηκαν. Τα σύνολα ελάχιστης τομής, που ανήκουν στην πρώτη σειρά, αποτυγχάνουν περίπου ισάριθμες φορές με μικρό προβάδισμα στο AUCTIONHOUSE και επομένως έχουν περίπου και τα ίδια

αποτελέσματα και στις υπόλοιπες στήλες του πίνακα. Τα σύνολα ελάχιστης τομής, που ανήκουν στην δεύτερη σειρά, αποτυγχάνουν από μια και μοναδική φορά το καθένα. Οπότε και η σημαντικότητά τους είναι αμελητέα. Τα σύνολα ελάχιστης τομής παρουσιάζονται σε φθίνουσα σειρά ανάλογα με τα αριθμητικά αποτελέσματά τους.

Ο πίνακας, που ονομάζεται Compressed, είναι ίδιος με τον προηγούμενο, αλλά τα σύνολα τομής που είναι λιγότερο μινιμαλιστικά από τα υπόλοιπα, τα μετατρέπει σε περισσότερο μινιμαλιστικά. Τα υπόλοιπα πεδία προσαρμόζονται σύμφωνα με τα καινούρια στοιχεία. Σε αυτόν τον πίνακα τα τρία τελευταία σύνολα τομής διαγράφονται, επειδή θεωρούνται μικρής αξίας στην ανάλυση. Τα αριθμητικά αποτελέσματα των συνόλων ελάχιστης τομής είναι ίδια με αυτά του προηγούμενου πίνακα, αλλά παρουσιάζονται σε αντίστροφη σειρά. Στο τέλος υπάρχει και ένα σύνολο ελάχιστης τομής από αυτά που ανήκουν στη δεύτερη σειρά, το οποίο μπορεί να προστέθηκε λόγω μικρής ακρίβειας ανάλυσης του λογισμικού.

Ο τελευταίος πίνακας, που ονομάζεται Basic Event Analysis (Ανάλυση Βασικού Γεγονότος), περιέχει μια λίστα με όλα τα στοιχειώδη γεγονότα και τη συμβολή της αποτυχίας όταν συμβαίνει το γεγονός της κορυφής. Αυτή η συμβολή εκφράζεται και ως ποσοστό σημαντικότητας του κάθε στοιχειώδους γεγονότος. Σε αυτόν τον πίνακα υπάρχουν στοιχειώδη γεγονότα που ανήκουν σε σύνολα ελάχιστης τομής πρώτης και δεύτερης σειράς. Τα στοιχειώδη γεγονότα που ανήκουν σε σύνολα ελάχιστης τομής δεύτερης σειράς θεωρούμε ότι παίζουν ασήμαντο ρόλο και δεν θα τα περιγράψουμε καθόλου. Τα στοιχειώδη γεγονότα που ανήκουν σε σύνολα ελάχιστης τομής πρώτης σειράς πραγματοποιούνται περίπου ίσες φορές. Συνεπώς και η σημαντικότητα του κάθε στοιχειώδους γεγονότος, δηλαδή η συμβολή της αποτυχίας τους όταν πραγματοποιείται το γεγονός της κορυφής (αποτυχία της Υπηρεσίας Δημοπρασιών με «*εφεδρικά τμήματα*»), είναι περίπου ίδια. Αυτή η συμβολή εκφράζεται και ως ποσοστό σημαντικότητας του κάθε στοιχειώδους γεγονότος. Τα αριθμητικά αποτελέσματα αυτού του πίνακα ισούνται με αυτά της τελευταίας στήλης του Compressed, αλλά παρουσιάζονται σε αλφαβητική σειρά.

4.4 Σύγκριση των αποτελεσμάτων των δύο δένδρων λαθών και εξαγωγή συμπερασμάτων

Σε αυτό το κεφάλαιο θα εξετάσουμε και τις διαφορές που προκαλεί στα αποτελέσματα της ανάλυσης του δένδρου λαθών η ύπαρξη ή όχι της μεθόδου «Επεξεργασία με εφεδρικά τμήματα». Αυτό θα μας επιβεβαιώσει τους λόγους που χρησιμοποιήσαμε τη μέθοδο αυτή, δηλαδή αν όντως αυξάνεται ή όχι η αξιοπιστία του συστήματος. Αυτό είναι πολύ σημαντικό, γιατί η χρήση της «*Επεξεργασίας με εφεδρικά τμήματα*» αυξάνει το κόστος του συστήματος. Επομένως αν δεν μας προσφέρει τα αναμενόμενα, είναι περιττή η χρήση της. Για να είμαστε ακριβής στα συμπεράσματά μας, θα πρέπει να εξετάσουμε ένα προς ένα τα στάδια της κατασκευής και ανάλυσης του δένδρου λαθών. Οι διαφορές και οι ομοιότητες των δένδρων λαθών με και χωρίς «*Επεξεργασία με εφεδρικά τμήματα*» καταγράφηκαν κατά τη διάρκεια της κατασκευής τους, οπότε δεν χρειάζεται να εξεταστεί τώρα αυτό το στάδιο. Αν θέλετε να τους θυμηθείτε, ανατρέξτε στις σελίδες 79-80. Στη συνέχεια θα εξετάσουμε και θα συγκρίνουμε τα δένδρα λαθών στο στάδιο της ανάλυσής τους.

4.4.1 Σύγκριση των δένδρων λαθών στο στάδιο της ανάλυσης

Καταρχήν θα ξεκινήσουμε από το μενού των ιδιοτήτων που εμφανίζονται κάθε φορά που επιλέγουμε να γίνει «*Ποιοτική ανάλυση*» του δένδρου λαθών, οι οποίες έχουν τις ίδιες τιμές εκτός από τον αριθμό των συνόλων ελάχιστης τομής. Το δένδρο λαθών με «Με εφεδρικά τμήματα» έχει δύο σύνολα ελάχιστης τομής περισσότερα. Αυτό συμβαίνει εξαιτίας του επιπλέον συστατικού και ισχύει για τα μενού ιδιοτήτων της «*Ποσοτικής ανάλυσης*» και της προσομοίωσης «*Monte Carlo*». Η FTA Αναφορά της «*Ποιοτικής ανάλυσης*» του δένδρου λαθών χωρίς «*Επεξεργασία με εφεδρικά τμήματα*» δείχνει ότι τα οκτώ σύνολα ελάχιστης τομής ανήκουν στην πρώτη σειρά εύρεσης. Αντίθετα για το άλλο δένδρο τα έξι από τα δέκα σύνολα ελάχιστης τομής ανήκουν στην πρώτη σειρά εύρεσης και τα υπόλοιπα στη δεύτερη. Αυτό μπορεί να ερμηνευτεί, αν σκεφτούμε το λόγο που χρησιμοποιήσαμε τη μέθοδο της «*Επεξεργασίας με εφεδρικά τμήματα*», δηλαδή για να αυξήσουμε την αξιοπιστία του συστήματος υποβαθμίζοντας την πιθανότητα να συμβεί ένα ή περισσότερα στοιχειώδη γεγονότα. Υποβαθμίζοντας αυτή την πιθανότητα, τα σύνολα ελάχιστης τομής που περιέχουν αυτά τα στοιχειώδη γεγονότα συμβάλλουν λιγότερο στην αποτυχία του συστήματος. Συνεπώς η σειρά εύρεσης αυτών των συνόλων ελάχιστης τομής αυξάνεται, πράγμα που επιβεβαιώνεται και από τα στοιχεία της FTA Αναφοράς. Τέλος παρατηρούμε και τα τέσσερα σύνολα ελάχιστης τομής του δένδρου λαθών με «*Επεξεργασία με εφεδρικά τμήματα*» που ανήκουν στη δεύτερη σειρά εύρεσης, είναι αυτά που προέρχονται από τα συστατικά που έχουν «*Επεξεργασία με εφεδρικά τμήματα*».

Η σύγκριση των αποτελεσμάτων της «*Ποιοτικής ανάλυσης*» και της προσομοίωσης «*Monte Carlo*» είναι που θα μας δώσουν τα σημαντικότερα και πιο ενδιαφέροντα στοιχεία και με τα οποία θα ασχοληθούμε τώρα. Τα αποτελέσματα από την FTA Αναφορά της ανάλυσης του δένδρου λαθών χωρίς «*Επεξεργασία με εφεδρικά τμήματα*» είναι:

- Η πιθανότητα αποτυχίας του γεγονότος της κορυφής είναι 7,997201 E -004.
- Το ποσοστό συμβολής του κάθε στοιχειώδους γεγονότος στην αποτυχία του γεγονότος της κορυφής είναι 12,50%.

Ενώ τα αποτελέσματα από την FTA Αναφορά της ανάλυσης του δένδρου λαθών με «*Επεξεργασία με εφεδρικά τμήματα*» είναι:

- Η πιθανότητα αποτυχίας του γεγονότος της κορυφής είναι 5,998900 E -004.
- Το ποσοστό συμβολής, των έξι στοιχειωδών γεγονότων που ανήκουν στα σύνολα ελάχιστης τομής της πρώτης σειράς εύρεσης, στην αποτυχία του γεγονότος της κορυφής είναι 16,67% και περίπου 0,02% για τα υπόλοιπα τέσσερα στοιχειώδη γεγονότα που ανήκουν σε σύνολα ελάχιστης τομής της δεύτερης σειράς.

Συγκρίνοντας αυτά τα αποτελέσματα συμπεραίνουμε ότι η μέθοδος της «*Επεξεργασίας με εφεδρικά τμήματα*» μειώνει κατά το ¼ την πιθανότητα αποτυχίας του γεγονότος της κορυφής. Επίσης γίνεται σχεδόν μηδενική και η πιθανότητα συμβολής δύο στοιχειώδη γεγονότα, που ανήκουν στο ίδιο συστατικό. Επομένως το συγκεκριμένο συστατικό (υλικό μέρος) του συστήματος γίνεται πιο αξιόπιστο και το σύστημα προσφέρει μεγαλύτερη ασφάλεια και διαθεσιμότητα στους χρήστες.

Το ίδιο συμπέρασμα απορρέει και από την σύγκριση των αποτελεσμάτων της προσομοίωσης «*Monte Carlo*». Για το δένδρο λαθών χωρίς «*Επεξεργασία με εφεδρικά τμήματα*» που είναι:

- Η ακριβής τιμή (exact value) της πιθανότητας τουλάχιστον ένα συστατικό να αποτύχει είναι 7,997200 E -004.
- Η πιθανότητα αποτυχίας του γεγονότος κορυφής είναι 7,997201 E -004 (+/- 7,997201 E -006).
- Στον πίνακα Compressed παρουσιάζονται τα σύνολα ελάχιστης τομής που είναι τα σημαντικότερα στην αποτυχία του συστήματος. Στον πίνακα περιλαμβάνονται και τα οκτώ σύνολα ελάχιστης τομής που βρέθηκαν στην πρώτη σειρά εύρεσης.
- Το ποσοστό συμβολής του κάθε στοιχειώδους γεγονότος στην αποτυχία του γεγονότος κορυφής κυμαίνεται από 12,09 μέχρι 13,39.

Αντίθετα τα αποτελέσματα για το δένδρο λαθών με «*Επεξεργασία με εφεδρικά τμήματα*» είναι:

- Η ακριβής τιμή (exact value) της πιθανότητας τουλάχιστον ένα συστατικό να αποτύχει είναι 9,995501 E -004.
- Η πιθανότητα αποτυχίας του top γεγονότος είναι 5,951321 E -004 (+/- 7,712745 E -006).
- Στον πίνακα Compressed παρουσιάζονται τα σύνολα ελάχιστης τομής, που είναι τα σημαντικότερα στην αποτυχία του συστήματος. Στον πίνακα περιλαμβάνονται και τα έξι από τα οκτώ σύνολα ελάχιστης τομής που βρέθηκαν στην πρώτη σειρά εύρεσης. Αυτά που βρέθηκαν στη δεύτερη σειρά εύρεσης παραλείπονται, επειδή θεωρείται ασήμαντος ο ρόλος τους.
- Το ποσοστό συμβολής των έξι στοιχειωδών γεγονότων της πρώτης σειράς εύρεσης στην αποτυχία του γεγονότος κορυφής κυμαίνεται από 16,22 μέχρι 17,10, ενώ για υπόλοιπα τέσσερα της δεύτερης σειράς εύρεσης κυμαίνεται από 0,00 μέχρι 0,02.

Η πιθανότητα να αποτύχει τουλάχιστον ένα συστατικό αυξάνεται με τη χρήση της μεθόδου «*Επεξεργασίας με εφεδρικά τμήματα*» κατά ¼. Αυτό γίνεται γιατί μειώνονται τα στοιχειώδη γεγονότα που παίζουν σημαντικό ρόλο στην αποτυχία του γεγονότος κορυφής. Έτσι στα εναπομείναντα στοιχειώδη γεγονότα διαμοιράζεται η παραπάνω πιθανότητα. Αντίθετα η πιθανότητα αποτυχίας του γεγονότος κορυφής αυξάνεται, το οποίο απορρέει και από τις προηγούμενες αναλύσεις. Στον πίνακα Compressed, στον οποίο εμφανίζονται τα σύνολα ελάχιστης τομής που έχουν το σημαντικότερο ρόλο, μειώνεται ο αριθμός των συνόλων ελάχιστης τομής και περιλαμβάνονται μόνο αυτά που ανήκουν στην πρώτη σειρά εύρεσης. Τέλος το

ποσοστό συμβολής του κάθε στοιχειώδους γεγονότος στην αποτυχία του γεγονότος κορυφής αυξάνεται, επειδή επηρεάζεται ανάλογα με την πιθανότητα αποτυχίας τουλάχιστον ενός συστατικού.

Μετά από αυτή την συγκριτική εξέταση των αποτελεσμάτων των μεθόδων ανάλυσης μπορούμε να θεωρήσουμε με βεβαιότητα ότι η μέθοδος της «*Επεξεργασίας με εφεδρικά τμήματα*» επιδρά θετικά στην αξιοπιστία και στη διαθεσιμότητα του συστήματος. Αν θέλουμε να αντιμετωπίσουμε προβλήματα αξιοπιστίας σε ένα τμήμα του συστήματος, τότε μπορούμε να εφαρμόσουμε αυτή τη μέθοδο. Είναι μια πρώτη καλή λύση, ανάλογα και με το κόστος υλοποίησης, μέχρι να βρούμε τα ελαττώματα του συστήματος. Σε αρκετά πραγματικά συστήματα είναι μια δημοφιλής τεχνική σε κρίσιμα σημεία του συστήματος εξαιτίας της γρήγορης υλοποίησής του. Αλλά επειδή είναι μια δαπανηρή διεργασία η προσθήκη επιπλέον υλικού, γίνονται προσπάθειες να μεταφερθεί το πρόβλημα στο λογισμικό.

5. Δένδρα Επίθεσης

Στις προηγούμενες ενότητες παρουσιάσθηκαν διάφοροι αλγόριθμοι ανάλυσης των Δένδρων Λαθών. Σε αυτή την ενότητα θα περιγραφούν και τα Δένδρα Επίθεσης, που χρησιμοποιούνται και για την ανάλυση της ασφάλειας και της αξιοπιστίας διάφορων συστημάτων όπως ακριβώς και τα Δένδρα Λαθών. Η αρχική ιδέα ήταν να δημιουργηθεί ένας γράφος που να αναπαριστά την διαδικασία λήψης αποφάσεων των πολύ καλά ενημερωμένων εισβολέων. Η ρίζα του δένδρου απεικονίζει δυνατούς στόχους ενός εισβολέα. Τα φύλλα αναπαριστούν τρόπους για την επίτευξη του στόχου. Οι κόμβοι κάτω από τον κόμβο-ρίζα είναι γενικοί τρόποι με τους οποίους μπορεί να επιτευχθεί ο στόχος. Όσο πιο χαμηλά πηγαίνουμε προς τα κάτω στο δένδρο, τόσο πιο συγκεκριμένες γίνονται οι επιθέσεις. Αυτά είναι προβλήματα που δεν τα αντιμετωπίζουν οι ομάδες σχεδιασμού. Οπότε το βάρος της ανακάλυψης τέτοιων "κενών" είναι δουλειά των αναλυτών σε συνεργασία με τους σχεδιαστές του συστήματος. Μπορεί τα Δένδρα Επιθέσεων (Attack Trees) και τα Δένδρα Λαθών να ασχολούνται με το ίδιο θέμα, αλλά από τον ορισμό τους διαφέρουν.

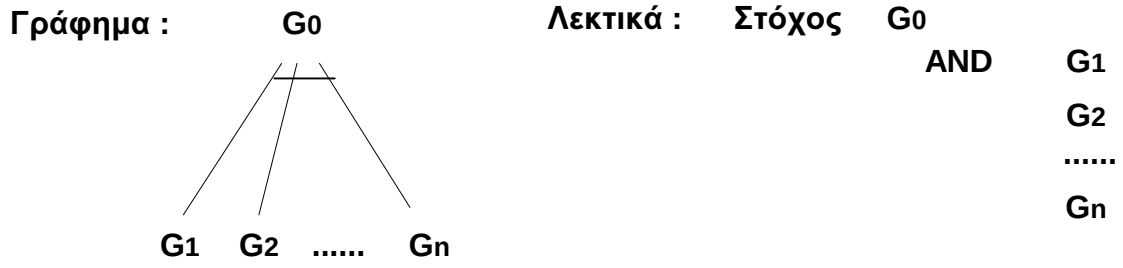
5.1 Διαφορές και ομοιότητες Δένδρα Επιθέσεων – Δένδρα Λαθών

Τα Δένδρα Επιθέσεων αντιμετωπίζουν το θέμα της αποτυχίας του συστήματος πιο γενικά και προσπαθούν να βρουν όλα τα πιθανά σημεία όπου μπορεί να δημιουργηθεί πρόβλημα είτε εσωτερικό (βλάβη) είτε εξωτερικό (προσβολή από εξωγενή παράγοντα). Αντίθετα τα Δένδρα Λαθών ασχολούνται κυρίως με εσωτερικά προβλήματα του συστήματος, δηλαδή με σφάλματα που μπορεί να γίνουν και να οδηγήσουν στην αποτυχία της σωστής λειτουργίας του. Επίσης μια ακόμα σημαντική επιλογή στα Δένδρα Επιθέσεων είναι ότι μπορεί να δημιουργηθεί μια βάση δεδομένων με τα ελαττώματα του συστήματος καθώς και τον τρόπο επίλυσής τους. Αυτή η βάση δεδομένων μπορεί να χρησιμοποιηθεί στο μέλλον για ως ευρετήριο λύσεων όταν αντιμετωπιστεί κάποιο ανάλογο πρόβλημα σε ένα μελλοντικό σύστημα. Επίσης μπορεί κάποιος να επαναχρησιμοποιήσει πλάνα επίθεσης (Attack Pattern) που έχουν ήδη αναπτυχθεί. Αυτή είναι και η πρακτική χρήση των Δένδρων Επιθέσεων πέρα από το θεωρητικό κομμάτι σε πραγματικά συστήματα. Η επαναχρησιμοποίηση υποστηρίζεται από δύο δομές τα πλάνα επίθεσης και τα αρχεία επίθεσης (Attack Profiles). Τα πλάνα επίθεσης χαρακτηρίζουν ένα συγκεκριμένο τύπο επίθεσης και τα αρχεία επίθεσης χρησιμοποιούνται για να οργανώνουν τα πλάνα επίθεσης και να κάνουν εύκολη την αναζήτησή τους και την εφαρμογή τους.

Στο στάδιο της κατασκευής, τα Δένδρα Επιθέσεων κατασκευάζονται όπως και τα Δένδρα Λαθών, αλλά οι κόμβοι τους αναφέρονται σε διαφορετικές έννοιες. Χρησιμοποιούν πύλες AND και OR. Ένας κόμβος αναλύεται σε μια από τις παρακάτω περιπτώσεις:

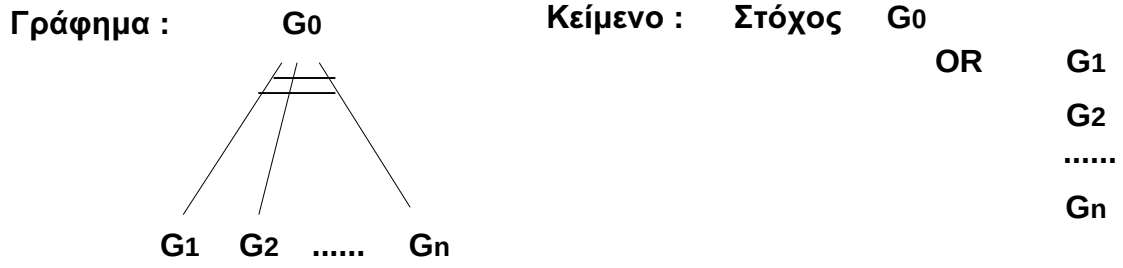
- ένα σύνολο κόμβων-υποστόχων, από τους οποίους πρέπει να επιτύχουν όλοι για να ισχύει ο αρχικός κόμβος-στόχος και οι οποίοι συνδέονται μεταξύ τους με μια πύλη AND
- ένα σύνολο κόμβων-υποστόχων, από τους οποίους πρέπει να επιτύχει τουλάχιστον ένας όλοι για να ισχύει ο αρχικός κόμβος-στόχος και οι οποίοι συνδέονται μεταξύ τους με μια πύλη OR

Τα Δένδρα Επιθέσεων παρουσιάζονται είτε γραφικά είτε λεκτικά. Το Σχήμα 5.1 απεικονίζει μια πύλη AND, δηλαδή ένα στόχο G_0 που μπορεί να επιτύχει, αν επιτύχουν οι στόχοι από G_1 μέχρι G_n.



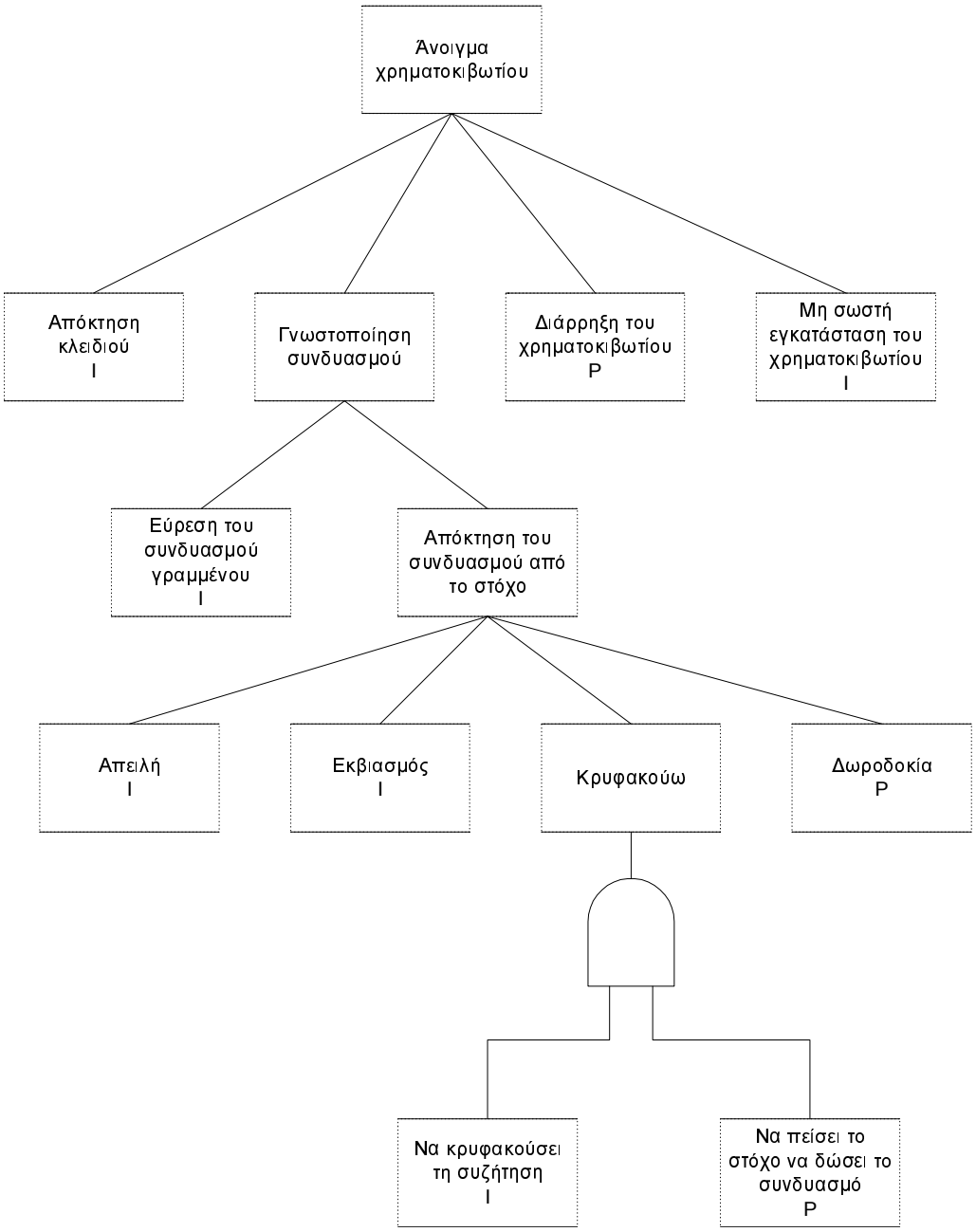
Σχήμα 5.4: πύλη AND

Το Σχήμα 5.2 απεικονίζει μια πύλη OR, δηλαδή ένα στόχο G_0 που μπορεί να επιτύχει, αν επιτύχει τουλάχιστον ένας από τους στόχους από G_1 μέχρι G_n.



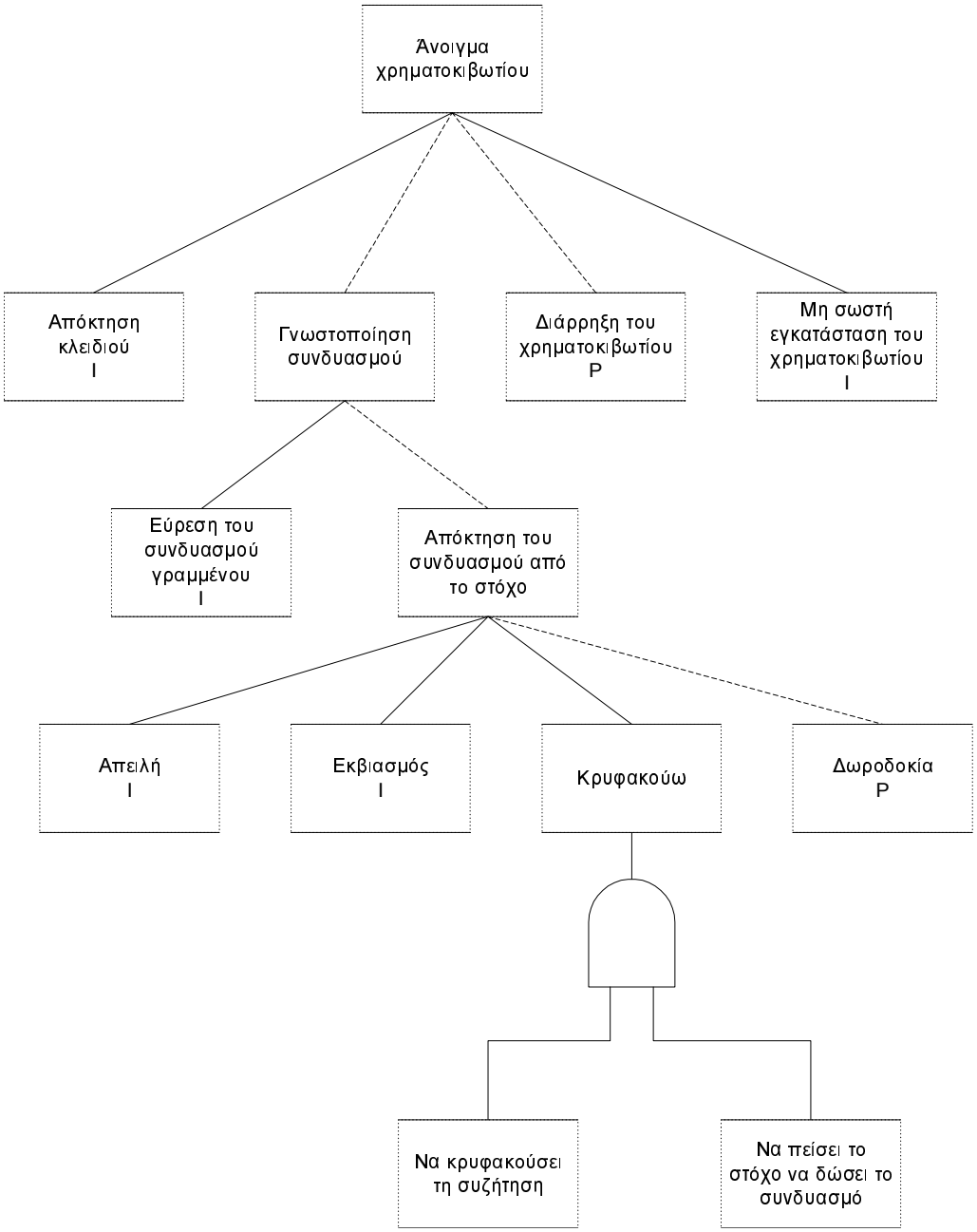
Σχήμα 5.2: πύλη OR

Συνδέοντας τους κόμβους με τις πύλες AND και OR δημιουργείται ένας μεθοδικός τρόπος για την περιγραφή της ασφάλειας του συστήματος, δηλαδή τα Δένδρα Επιθέσεων. Στη δομή του δένδρου, ο στόχος περιγράφεται στον κόμβο ρίζα και οι τρόποι με τους οποίους μπορεί να επιτευχθεί αναφέρονται στα φύλλα. Ακολουθεί ένα παράδειγμα στο Σχήμα 5.3.



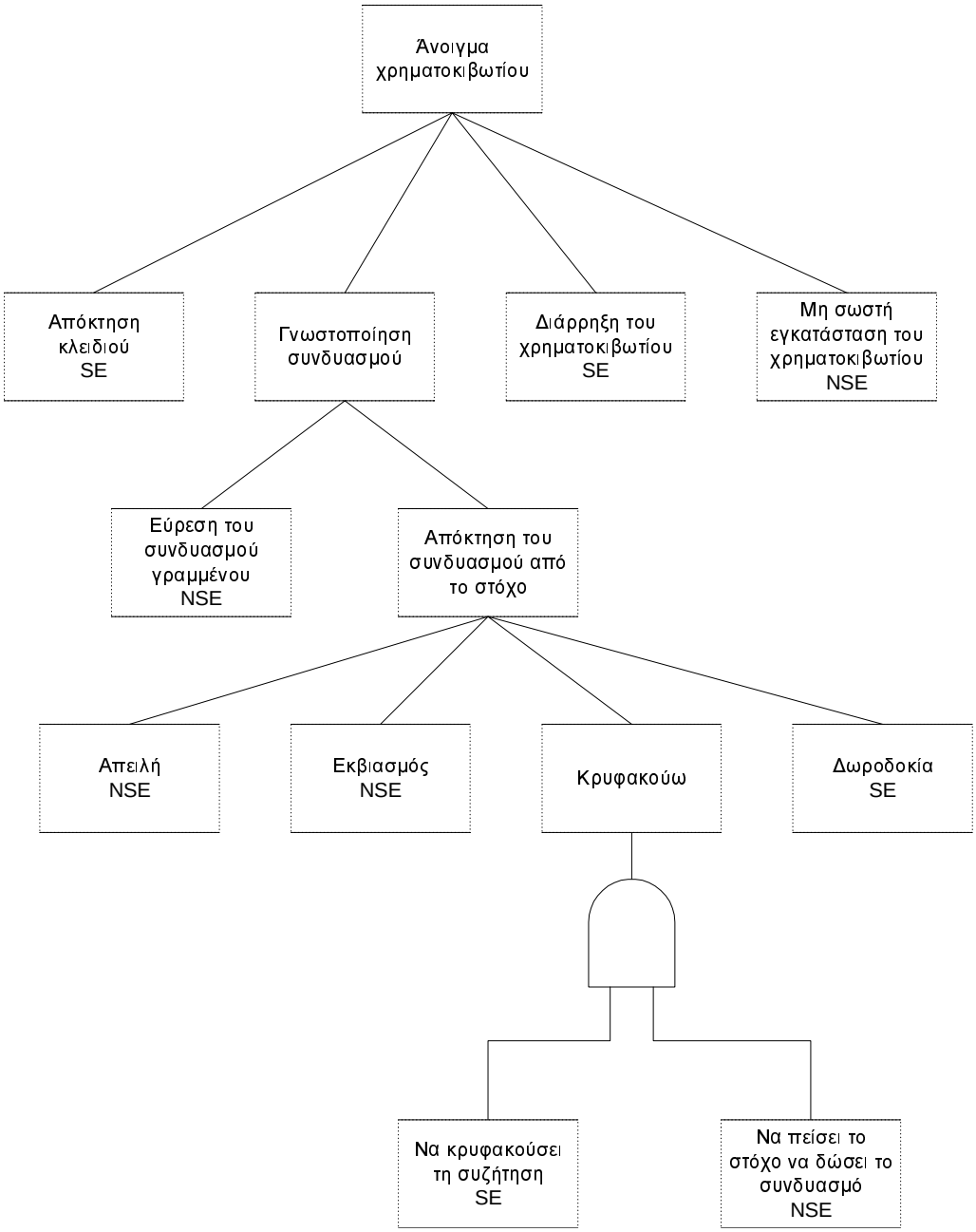
Σχήμα 5.5: Attack Tree

Τέλος μια σημαντική διαφορά είναι ότι μπορούμε να αποδώσουμε οποιαδήποτε τιμή Boolean στους κόμβους-φύλλα και μετά να αναπαραχθούν προς τα επάνω και στους υπόλοιπούς κόμβους του δένδρου. Στο Σχήμα 3 αποδόθηκαν σε όλους τους κόμβους-φύλλα οι τιμές P-Πιθανό και I-Απίθανο και στη συνέχεια μπορούμε ακολουθώντας τους κανόνες για τις πύλες AND και OR να παραχθούν οι τιμές και για τους υπόλοιπους κόμβους. Μετά από αυτή την διαδικασία το δένδρο γίνεται όπως στο Σχήμα 5.4.

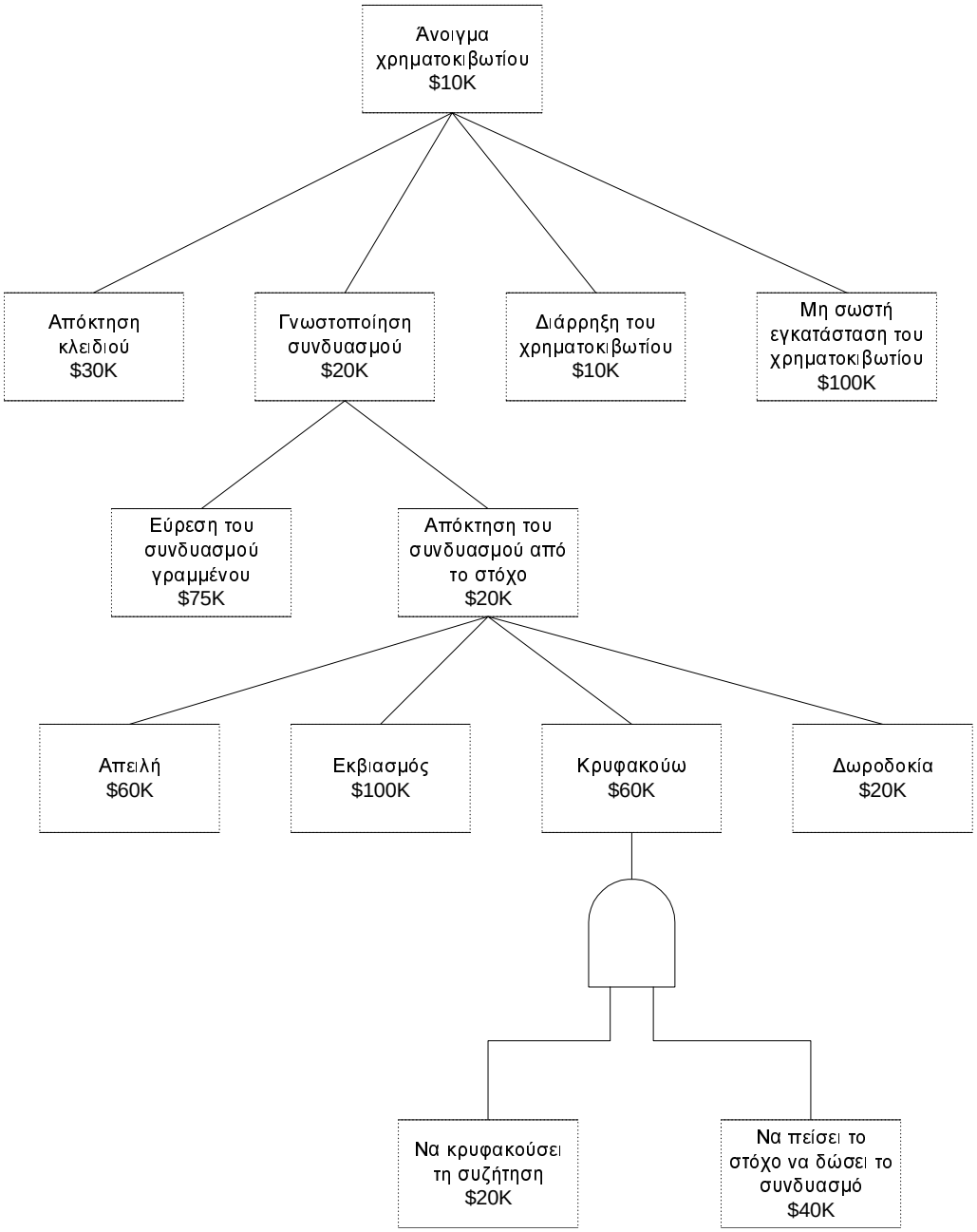


Σχήμα 5.6: Attack Tree

Μερικές από τις τιμές που μπορούμε να αναθέσουμε είναι: εύκολο έναντι δύσκολο, ακριβό έναντι φθηνό, παρεισφρητικό έναντι μη παρεισφρητικό, νόμιμο έναντι παράνομο, χρήση ειδικού εξοπλισμού έναντι μη χρήση ειδικού εξοπλισμού. Στη συνέχεια ακολουθούν δύο παραδείγματα Δένδρων Επίθεσης που οι κόμβοι–φύλλα έχουν τιμές «χρήση ειδικού εξοπλισμού (SE) έναντι μη χρήση ειδικού εξοπλισμού (NSE)» για αυτό του Σχήματος 5.5 και το ακριβές κόστος του κάθε κόμβου στο Σχήμα 5.6.


Άνοιγμα χρηματοκιβωτίου
Απόκτηση κλειδιού SE
Γνωστοποίηση συνδυασμού
Διάρρηξη του χρηματοκιβωτίου SE
Μη σωστή εγκατάσταση του χρηματοκιβωτίου NSE
Εύρεση του συνδυασμού γραμμένου NSE
Απόκτηση του συνδυασμού από το στόχο
Απειλή NSE
Εκβιασμός NSE
Κρυφακούω
Δωροδοκία SE
Να κρυφακούσει τη συζήτηση SE
Να πείσει το στόχο να δώσει το συνδυασμό NSE

Σχήμα 7.5



Σχήμα 5.8

Πέρα από αυτές τις τιμές Boolean που μπορεί να πάρουν οι κόμβοι ενός Δένδρου Επιθέσεων, υπάρχουν και συνεχείς τιμές όπως η πιθανότητα επιτυχημένης επίθεσης, δηλαδή η πιθανότητα ένας εισβολέα θα προσπαθήσει να κάνει μιας επίθεσης, κλπ. Σε κάθε πραγματικό Δένδρο Επιθέσεων, οι κόμβοι θα έχουν πολλές διαφορετικές τιμές αναφερόμενες σε πολλές διαφορετικές μεταβλητές, είτε Boolean είτε συνεχείς. Διαφορετικές τιμές κόμβων μπορούν να συνδυαστούν και να μάθουμε ακόμα περισσότερα για τα ελαττώματα του συστήματος. Κάθε φορά μπορούμε να κάνουμε και μια διαφορετική «ερώτηση» για ένα χαρακτηριστικό επίθεσης στο Δένδρο Επιθέσεων και να πάρουμε μια διαφορετική απάντηση που θα είναι και μια καινούρια πληροφορία για το σύστημα.

Όλα αυτά βέβαια για να δουλεύουν σωστά, πρέπει να «παντρέψουμε» τα Δένδρα Επίθεσης με τις πληροφορίες που έχουμε για τους εισβολείς. Κάθε εισβολέας έχει και διαφορετικές ικανότητες που πρέπει να τις λάβουμε υπόψιν μας.

6. Ανακεφαλαίωση

Τα δέντρα λαθών κατασκευάζονται και αναλύονται με σκοπό να μειωθεί η πιθανότητα αποτυχίας για ένα σύστημα. Έτσι ελαχιστοποιώντας αυτή την πιθανότητα μπορούμε να αποφύγουμε τις πιθανές επακόλουθες ανθρώπινες (π.χ. θάνατος,αρρώστια), οικονομικές (π.χ. απώλεια κεφαλαίου) και περιβαλλοντικές (π.χ. μόλυνση του αέρα,της θάλασσας) απώλειες. Τα δέντρα λαθών λοιπόν, μπορούν να βοηθήσουν στην αναγνώριση των γεγονότων, που οδηγούν στην αποτυχία του συστήματος. Έτσι το σύστημα στη συνέχεια μπορεί να βελτιωθεί, να ξανασχεδιαστεί αν αυτό είναι απαραίτητο και να μειωθούν έτσι οι κίνδυνοι που το απειλούν.

Στο 1^{ο} Κεφάλαιο παρουσιάσαμε τη δομή των δέντρων λαθών, το τρόπο κατασκευής τους, τα σύμβολα που χρησιμοποιούνται για την αναπαράσταση των γεγονότων, καθώς και το πώς αυτά συσχετίζονται μεταξύ τους.

Στο 2^{ο} Κεφάλαιο είδαμε αναλυτικά τις μεθόδους ανάλυσης αξιοπιστίας λογισμικού, που βασίζονται στα δέντρα λαθών. Την ποιοτική και την ποσοτική ανάλυση, καθώς και την Monte Carlo προσομοίωση. Σκοπός μας ήταν να κατανοήσει ο αναγνώστης πως λειτουργούν οι διάφορες αυτές τεχνικές και να ανακαλύψει τον τρόπο που αυτές μπορούν να βοηθήσουν στην ανάλυση ενός συστήματος.

Στο 3^{ο} Κεφάλαιο περιγράψαμε αναλυτικά τη λειτουργία του λογισμικού OpenFTA. Το λογισμικό αυτό, που εντοπίσαμε στο διαδίκτυο, βοηθάει στο να γίνονται γρηγορότερα και με μεγαλύτερη αξιοπιστία οι υπολογισμοί των μεθόδων, που χρησιμοποιούνται στην ανάλυση των δένδρων λαθών. Αυτό που στην ουσία κάνει το OpenFTA είναι να υπολογίζει την πιθανότητα να αποτύχει το σύστημα (το οποίο περιγράφεται στον κόμβο-ρίζα) αναλύοντας το δένδρο που κατασκευάσαμε.

Στο 4^{ο} Κεφάλαιο παρουσιάσαμε μια on-line Υπηρεσία Δημοπρασιών, στην οποία μπορεί να συμετέχει κάποιος μέσω του Διαδικτύου. Αυτό έγινε για να μπορέσει ο αναγνώστης να κατανοήσει καλύτερα τον τρόπο σκέψης και τη τεχνική για την κατασκευή δένδρων λαθών, καθώς και πως λειτουργούν οι διάφορες μέθοδοι ανάλυσης αξιοπιστίας σε ένα λογισμικό. Επίσης εφαρμόσαμε όσα παρουσιάστηκαν στο προηγούμενο κεφάλαιο για την υλοποίηση του δένδρου λαθών της συγκεκριμένης Διαδικτυακής Υπηρεσίας.

Επιπλέον στη συνέχεια παραθέτουμε χρήσιμη Βιβλιογραφία για όσους ενδιαφέρονται να μελετήσουν περαιτέρω τα Δένδρα λαθών. Τέλος, σε όλη τη διάρκεια του κειμένου, όπου κρίνεται απαραίτητο, υπάρχουν ειδικοί σύνδεσμοι για το διαδίκτυο, έτσι ώστε να μπορεί ο αναγνώστης να τους επισκευθεί, αν βέβαια το επιθυμεί.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Ernest J. Henley, Hiromitsu Kumamoto, “Reliability Engineering and Risk Assessment”, Prentice Hall, 1981.

2. Judith Stafford, John D. McGregor, “Issues in Predicting the Reliability of Composed Components”, Proceedings of the 5th ICSE Workshop on Component-Based Software Engineering, Orlando, Florida, May 2002.

3. Frank Ortmeier, Wolfgang Reif, “Safety Optimization: A Combination of Fault Tree Analysis and Optimization Techniques”, 2004.

4. John D. McGregor, Judith A. Stafford, Il-Hyung Cho, “Measuring Component Reliability”, 2003.

5. Dave Mason, “Propabilistic Analysis for Component Reliability Composition”, Proceedings of the 5th ICSE Workshop on Component-Based Software Engineering, Orlando, Florida, May 2002.

6. John Viega, Gary McGraw, “Risk Analysis: Attack Trees and Other Tricks”, August 2002, http://www.sdmagazine.com/print.

7. Andrew P. Moore, Robert J. Ellison, Richard C. Linger, “Attack Modeling for Information Security and Survivability”, March 2001.

8. Dr. Dobb, “Attack Trees”, December 1999.

9. Apostolos Zarras, Panos Vassiliadis, Valerie Issarny. “Model-Driven Dependability Analysis of Web Services”, 2004.

10. Formal Software Construction Limited, “Open FTA, Version 1.0, User Manual”, 2005, www.fsc.co.uk.

11. D.Hamlet, Dave Mason, and D.Woit, “Theory of Software Component Reliability”, Proceedings of the 23rd International Conference on Software Engineering, Toronto, Canada, May 2001.

12. J. Musa, “ Software Reliability Engineering, McGraw-Hill”, New York, 1998.

13. Cho, Il-Hyung, John D. Mc Gregor, “Component Specification and Testing Interoperation of Components”, Proceedings of the 3rd International Conference on Software Engineering and Applications, October 1999.

14. K.S.Trivedi, K.Vaidyanathan, K.Goseva-Popstojanova, “Modeling and Analysis of Software Aging and Rejuvenation”, Proceedings of the 33rd Annual Simulation Symposium, Washington D.C., April 2000.

ΛΕΞΙΛΟΓΙΟ ΕΝΝΟΙΩΝ

A

Absorption State = Κατάσταση Απορρόφησης
Analysed Event = Γεγονός Πλήρως αναλυμένο
Attacker = Εισβολέας
Attack Patterns = Πλάνα Επίθεσης
Attack Profiles = Αρχεία Επίθεσης
Attack Trees = Δένδρα Επιθέσεων
Auction House = Οίκος Δημοπρασιών
Auction ID = Κωδικός Δημοπρασίας
Auction Registration Service = Υπηρεσία Καταγραφής Δημοπρασιών
Auction Service = Υπηρεσία Δημοπρασιών

B

Backward Analysis = Ανάλυση Οπίσθιας Ροής
Basic Event = Βασικό Γεγονός
Basic Initiating Event = Βασικό Γεγονός Εκκίνησης
Block Diagram = Διάγραμμα Μπλοκ

C

Command Faults = Σφάλματα Εντολής
Common Cause = Συνήθης Αιτία
Common Mode Failure Analysis = Ανάλυση Αποτυχίας Κοινής-Κατάστασης
Components Faults = Σφάλματα Συστατικών
Conditioning Event = Υπό Συνθήκη Γεγονός
Constant Failure Rate/Unit Time = Ρυθμός Αποτυχίας

D

Dormant Failure = Μη Ανιχνευθείσα Αποτυχία
Default Choices = Προκαθορισμένες Επιλογές

E

Exclusive OR Gate = Πύλη Αποκλειστκού OR
External Event = Εξωγενές Γεγονός

F

Fault Tree = Δένδρο λαθών
Forward Analysis = Ανάλυση Εμπρόσθιας Ροής

I

Intermediate Event = Ενδιάμεσο Γεγονός
Invalid = Λάθος
Inclusion-Exclusion = Συνυπολογισμός-Αποκλεισμού

K

KITT (Kinetic Tree Theory) = Θεωρία Δένδρου Κίνησης

M

Minimal cut set = Σύνολο Ελάχιστης Τομής
Minimal path set = Σύνολο Ελάχιστου Μονοπατιού
M-out-of-N Voting Gate = Πύλη Καταμέτρησης

N

Not analysed Event = Γεγονός όχι Πλήρως Αναλυμένο

P

Primary Event = Στοιχειώδες Γεγονός
Primary Failure = Στοιχειώδης Αποτυχία
Priority AND Gate = Πύλη AND με Προτεραιότητα

R

Redudancy = Επεξεργασία Με Εφεδρικά Τμήματα

S

Secondary Failures = Δευτερεύοντες Αποτυχίες
System Failure = Αποτυχία του Συστήματος
Structure Functions = Συναρτήσεις Δομής

T

Top Event = Γεγονός Κορυφής
Transfer-IN Triangle = Τρίγωνο Μεταφορά στο
Transfer-OUT Triangle = Τρίγωνο από Μεταφορά
Truth Table = Πίνακας Αληθείας

U

UML Diagram = Διάγραμμα UML
Undeveloped Event = Γεγονός μη Αναπτύξιμο

User Manual = Εγχειρίδιο Χρήσης

W

Web Service = Διαδικτυακή Υπηρεσία