ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΑΡΑΓΩΓΗΣ
ΚΑΙ ΔΙΟΙΚΗΣΗΣ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ:
ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ανάλυση επικινδυνότητας χειρισμού εκσκαφέα με ανεστραμμένο κάδο με χρήση της μεθόδου STPA

Σπουδαστής
Κατίκας Ανδρέας
(Α.Μ. 2014019042)

Επιβλέπων Καθηγητής
Κοντογιάννης Θωμάς

Νοέμβριος 2018

Η παρούσα Διπλωματική Εργασία
εκπονήθηκε στα πλαίσια των σπουδών
για την απόκτηση του Μεταπτυχιακού Διπλώματος Ειδίκευσης
«Οργάνωση και Διοίκηση»
που απονέμει το
Τμήμα Μηχανικών Παραγωγής και Διοίκησης
του Πολυτεχνείου Κρήτης

Η παρούσα διπλωματική εργασία του Κατίκα Ανδρέα εγκρίνεται από τους κ.κ.

Κοντογιάννης Θωμάς	Επιβλέπων Εργασίας
Μουστάκης Βασίλειος	Καθηγητής
Ατσαλάκης Γεώργιος	Καθηγητής

Περιεχόμενα

Περίληψη

Η τεχνολογική πρόοδος του τελευταίου αιώνα είναι αδιαμφισβήτητα ραγδαία και αυτό έχει σαν αποτέλεσμα την ανάπτυξη νέων σύνθετων συστημάτων οργάνωσης της ίδιας της κοινωνίας, στην οποία κυριαρχούν η πολυπλοκότητα και η υψηλή εξειδίκευση. Τα χαρακτηριστικά αυτά των κοινωνιών θέτουν ως ύψιστη προτεραιότητα τους, την μείωση των ατυχημάτων στο ελάχιστο ενώ δείχνουν μηδενική ανοχή στις ανθρώπινες απώλειες καθώς περιμένουν από το νέο αυτό σύστημα να τους προστατεύσει λόγω της υψηλής εξειδίκευσης.

Γενικότερα, παρά την προσπάθεια μείωσης του, ατυχήματα συμβαίνουν συνεχώς καθημερινά γύρω μας και είναι αποτέλεσμα ενός συνόλου γεγονότων ή παραλείψεων που οφείλονται είτε σε ανθρώπινο παράγοντα είτε σε αστοχία μηχανημάτων εξοπλισμού και μπορεί να οδηγήσει είτε σε ανθρώπινο τραυματισμό ή απώλεια είτε σε φθορά εξοπλισμού. Η πρόληψη των ατυχημάτων περιλαμβάνει την ανάπτυξη μεθόδων για την ελαχιστοποίηση των παραγόντων που μπορεί να οδηγήσουν σε ατύχημα. Πλέον αποτελεί ύψιστη προτεραιότητα για κάθε επιχείρηση, η εξασφάλιση ενός περιβάλλοντος εργασιακής ασφάλειας, πετυχαίνοντας έτσι υψηλότερη απόδοση των εργαζομένων της και αποφεύγοντας τις οικονομικές απώλειες ή την δυσφήμιση από ένα δυσάρεστο συμβάν. Μέθοδοι για την πρόληψη των ατυχημάτων αποτελούν ο εντοπισμός των επικίνδυνων καταστάσεων και η λήψη μέτρων αποφυγής τους, η συνεχής εκπαίδευση του προσωπικού, τα αναλυτικά εγχειρίδια τεχνικών εργασιών και ο συνεχής έλεγχος για την εξασφάλιση μια ποιοτικής και ασφαλούς εργασίας της επιχείρησης.

Στην παρούσα διπλωματική θα αναλύσουμε όλες τις ενέργειες που εκτελούνται κατά την διάρκεια χρήσης ενός εκσκαφικού μηχανήματος με ανεστραμμένο κάδο από τον χειριστή του μηχανήματος και θα γίνει προσπάθεια εντοπισμού όλων των επισφαλών διαδικασιών (κίνδυνοι) που δυνητικά μπορεί να οδηγήσουν σε ατύχημα. Ουσιαστικά πρόκειται για μια ανάλυση επικινδυνότητας της χρήσης εκσκαφικού μηχανήματος με ανεστραμμένο κάδο η οποία θα γίνει με τη χρήση της μεθόδου STPA (Systems Theoretic Process Analysis). Μέσα από την μέθοδο αυτή θα προσπαθήσουμε να εντοπίσουμε τις ενέργειες εκείνες που είναι επικίνδυνες ή μη αποδεκτές κατά την χρήση ενός εκσκαφέα, να ορίσουμε περιορισμούς ασφαλείας για την αποτροπή αυτών των επισφαλών ενεργειών και τέλος να προσδιορίσουμε τις αιτίες που οδήγησαν σε αυτές τις επικίνδυνες ενέργειες δηλαδή να εντοπίσουμε την ρίζα του προβλήματος.

Η παρούσα διπλωματική έχει διαρθρωθεί σε πέντε (5) Κεφάλαια, το περιεχόμενο των οποίων παρουσιάζεται συνοπτικά παρακάτω.

Στο Κεφάλαιο 1^{ο} πραγματοποιείται μια γενική εισαγωγή για την διάρθρωση και το περιεχόμενο της παρούσας διπλωματικής.

Στο Κεφάλαιο 2^{ο} γίνεται μια γενική αναφορά στα εσκαπτικά μηχανήματα, τις ιδιότητες και τα χαρακτηριστικά τους. Ιδιαίτερη αναφορά γίνεται στον εκσκαφέα με ανεστραμμένο κάδο, ο όποιος και αποτελεί αντικείμενο μελέτης της παρούσας διπλωματικής. Συγκεκριμένα πέρα από τις γενικές πληροφορίες για αυτόν και τα βασικά του εξαρτήματα γίνεται διαχωρισμός των βασικών εργασιών χειρισμού του εκσκαφέα σε στάδια έτσι ώστε να γίνουν πλήρως κατανοητές και διακριτές οι διάφορες

φάσεις της εκσκαφής ενώ ιδιαίτερη έμφαση δίνεται στις πρακτικές ασφαλούς λειτουργείας του.

Στο Κεφάλαιο 3ο πραγματοποιείται μια θεωρητική ανασκόπηση της μεθόδου STPA με την οποία πρόκειται να γίνει η ανάλυση επικινδυνότητας της χρήσης εκσκαφικού μηχανήματος. Αρχικά, γίνεται μια αναφορά στο θεωρητικό υπόβαθρο των πρώτων αναλύσεων επικινδυνότητας που αναπτύχθηκαν, των Μοντέλων Αιτιότητας Ατυχημάτων, που χρησιμοποιούνται εδώ και πολλά χρόνια στην ανάλυση επικινδυνότητας και στη συνέχεια παρουσιάζονται κάποια παραδοσιακά μοντέλα αιτιότητας αλυσιδωτών γεγονότων (Swiss Cheese Model, Fault Tree Analysis, FMEA & FMECA). Στη συνέχεια, ακολουθεί μια συλλογιστική προσέγγιση των μοντέρνων και βελτιωμένων μοντέλων επικινδυνότητας μέσω της Θεωρίας Συστημάτων και των Μοντέλων Διαδικασιών, έχοντας ως βασικό πρότυπο την μέθοδο ανάλυσης STAMP. Ενώ στο τέλος του Κεφαλαίου αναπτύσσεται αναλυτικά κάθε βήμα της θεωρίας της μεθόδου STPA προκειμένου να γίνει πλήρως οικεία και κατανοητή.

Στο Κεφάλαιο 4ο γίνεται εφαρμογή της μεθόδου STPA στη χρήση εκσκαφικού μηχανήματος με ανεστραμμένο κάδο σε μία προσπάθεια εντοπισμού των επισφαλών πρακτικών λειτουργείας του εκσκαφέα και αποτροπής αυτών. Αρχικά, πραγματοποιείται προσδιορισμός των θεμελίων του συστήματος δηλαδή εντοπισμός των ατυχημάτων και των κινδύνων του συστήματος και κατασκευάζεται το πρότυπο δομής ελέγχου όπου παρέχεται μια λειτουργική αναπαράσταση του συστήματος. Στη συνέχεια, αφού έχουν προσδιοριστεί τα θεμέλια του συστήματος, γίνεται ο εντοπισμός των επισφαλών ενεργειών ελέγχου για κάθε εργασία κατά τον χειρισμό του εκσκαφέα και κατόπιν αναπτύσσονται οι περιορισμοί ασφαλείας προκειμένου να αποτρέψουν τις επισφαλείς ενέργειες που έχουν εντοπιστεί. Τελευταίο αλλά πιο σημαντικό βήμα της ανάλυσης STPA που αναπτύσσεται αποτελεί ο εντοπισμός των αιτιωδών παραγόντων δηλαδή των αιτιών που οδηγούν σε μια επισφαλή ενέργεια αλλά και των αιτιών που μπορεί να οδηγήσουν σε παραβίαση των περιορισμών ασφαλείας.

Στο Κεφάλαιο 5ο παρουσιάζονται συγκεντρωτικά όλα τα αποτελέσματα αλλά και τα συμπεράσματα της ανάλυσης επικινδυνότητας που αναπτύχθηκε στην παρούσα διπλωματική.

Κεφάλαιο 1ο Εκσκαπτικά μηχανήματα και επικινδυνότητα

1.1 Επικινδυνότητα εργασιών με εκσκαπτικά μηχανήματα

Ο εξοπλισμός βαρέων κατασκευών είναι βαρέα επαγγελματικά οχήματα ειδικά σχεδιασμένα για την εκτέλεση τεράστιων εργασιών κάτω από τεράστια δύναμη. Ο εξοπλισμός βαρέων κατασκευών απέφερε σημαντικά οφέλη στην ανθρωπότητα από όταν η πρώτη χωματουργική μηχανή εισήχθη το 1835. Με τη βοήθεια αυτών των μηχανών, συστάθηκε όλος ο σύγχρονος πολιτισμός και η ανθρωπότητα ήταν σε θέση να δημιουργήσει αξιοσημείωτες δομές όπως δρόμους, φράγματα, κανάλια, ουρανοξύστες κλπ. Αποτελούν λοιπόν βασικοί συντελεστές στο σύγχρονο τρόπο ζωής της ανθρωπότητας.

Πολυάριθμοι τύποι εξοπλισμού βαρέων κατασκευών είναι διαθέσιμοι προς χρήση σε εργολάβους από διάφορες βιομηχανίες, όπως στα ορυχεία και τις κατασκευές, για την εκτέλεση μιας ευρείας ποικιλίας δραστηριοτήτων. Διάφοροι τύποι εξοπλισμού βαρέων κατασκευών χρησιμοποιούνται σε διαφορετικούς τύπους έργων ή σε δραστηριότητες μιας εργασίας σε διαφορετικά επίπεδα. Ο εξοπλισμός αυτός περιλαμβάνει φορτωτές, εκσκαφείς, αποξεστές δρόμων, εμπρόσθιους φορτωτές, ισοπεδωτές, μπουλντόζες, συμπιεστές, ασφαλτοστρωτήρες, ανατρεπόμενα φορτηγά, κυλίνδρους, μπετονιέρες, τράκτορες, οχήματα μεταφοράς, φορτηγά νερού και άλλα.

Στη σημερινή αναπτυσσόμενη βιομηχανία κατασκευών, οι ανάγκες και η φαντασία της ανθρωπότητας έχουν ωθήσει τους κατασκευαστές να βελτιώσουν τον εξοπλισμό τους. Αυτά τα οφέλη μερικές φορές σημαίνουν πιο ισχυρό, μεγαλύτερο και ταχύτερο εξοπλισμό. Ως εκ τούτου, με τη βοήθεια της συνεχώς αναπτυσσόμενης τεχνολογίας δημιουργούνται νέοι, πιο ισχυροί και πιο παραγωγικοί εξοπλισμοί. Αυτό το δραματικά αυξημένο ποσοστό παραγωγικότητας κάνει αυτά τα μηχανήματα απαραίτητα στα εργοτάξια. Ωστόσο, αυτά τα οφέλη φέρνουν και κινδύνους. Λόγω του μεγέθους τους, της φύσης της λειτουργίας τους και τη ισχύς τους, ο εξοπλισμός βαρέων κατασκευών μπορεί να γίνει μια απειλητική για τη ζωή ανησυχία για όσους τα λειτουργούν και εργάζονται γύρω από αυτά.

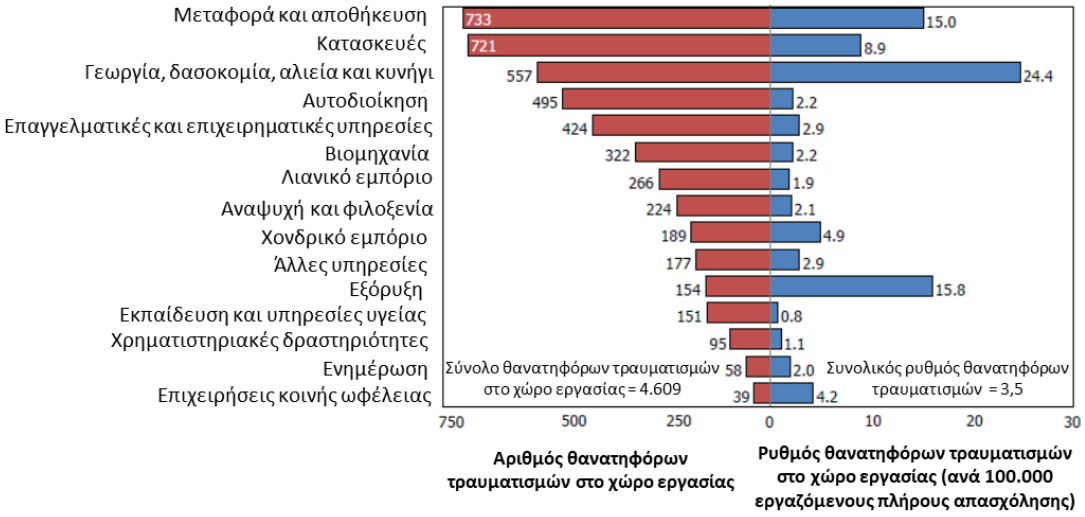
Από τότε που τα μηχανήματα αναπτύχθηκαν για πρώτη φορά, ένα μεγάλο τίμημα σε τραυματισμούς και απώλειες έχει καταβληθεί για αυτήν την ευκολία. Οι κατασκευαστικές εργασίες παραμένουν ένα από τα πιο επικίνδυνα επαγγέλματα λόγω των μεταβλητών, σύνθετων καθηκόντων και δραστηριοτήτων τους. Οι εργαζόμενοι στα εργοτάξια αντιμετωπίζουν συχνά επικίνδυνες και απειλητικές για τη ζωή τους συνθήκες. Η κατασκευαστική βιομηχανία στην αμερικάνικη βιομηχανία αντιπροσωπεύει περίπου το 7% του συνολικού εργατικού δυναμικού αλλά οι απώλειες εργαζομένων στον τομέα των κατασκευών αντιπροσωπεύει περίπου το 20% όλων των βιομηχανικών ατυχημάτων. Έχοντας περισσότερες από μία δραστηριότητες και πολλαπλές συναλλαγές σε ένα εργοτάξιο την ίδια στιγμή αυξάνεται σημαντικά ο κίνδυνος ενός ατυχήματος που μπορεί να οδηγήσει σε τραυματισμό ή θάνατο.

Η αυξημένη ανησυχία για τη συχνότητα και την έκταση των βιομηχανικών ατυχημάτων και των κινδύνων υγείας των εργαζομένων οδήγησαν το 1970 τις ΗΠΑ στην ανάπτυξη ενός νόμου για την Επαγγελματική Ασφάλεια και Υγεία, ο οποίος θέσπισε συγκεκριμένες απαιτήσεις ασφάλειας και υγείας για όλες σχεδόν τις

βιομηχανίες και οδήγησε στην δημιουργία ενός εποπτικού οργανισμού. Έκτοτε έχει δημιουργηθεί η ανάγκη για συλλογή και διαχείριση πληροφοριακών συστημάτων ασφαλείας με σκοπό τον προγραμματισμό, τη διαχείριση, την παρακολούθηση, την υποβολή εκθέσεων και την παροχή υπηρεσιών και βοήθειας.

Αυτό οδήγησε στην ανάπτυξη μιας βάσης δεδομένων που περιλαμβάνει όλες τις αναφορές διερεύνησης ατυχημάτων που σχετίζονται με την εργασία, οι οποίες είναι πληροφορίες επιθεώρησης του χώρου εργασίας των ατυχημάτων, όπου σημειώθηκε κάποια απώλεια ή καταστροφή και περιπτώσεων καταγεγραμμένων τραυματισμών. Αυτές οι αναφορές περιλαμβάνουν πληροφορίες όπως ημερομηνία και ώρα του ατυχήματος, σύντομη περιγραφή του ατυχήματος, πληροφορίες σχετικά με τον τραυματισμένο εργαζόμενο, τη φύση και την προέλευση του τραυματισμού, τους αιτιώδεις παράγοντες (ανθρώπινος παράγοντας, περιβαλλοντικός παράγοντας), και τα αποτελέσματα της.

Τα εργοτάξια είναι μοναδικοί χώροι που περιλαμβάνουν πολλές εγγενώς επικίνδυνες εργασίες υπό δύσκολες συνθήκες. Σύμφωνα με τις πληροφορίες που προκύπτουν από την βάση δεδομένων που έχει αναπτυχθεί, σε ένα σύνολο 4.609 θανατηφόρων ατυχημάτων στο χώρο εργασίας κατά το έτος 2011 οι 721 θάνατοι σημειώθηκαν στην κατασκευαστική βιομηχανία αντιπροσωπεύοντας περίπου το 16% επί του συνόλου των θανάτων. Αυτό αντιστοιχεί σε ένα ποσοστό θνησιμότητας 8,9 απασχολούμενοι ανά 100.000 το έτος 2011, το οποίο είναι ελαφρώς χαμηλότερο από το 2010. Αυτοί οι αριθμοί κάνουν τη βιομηχανία των κατασκευών να είναι η δεύτερη πιο επικίνδυνη βιομηχανία στις Ηνωμένες Πολιτείες ελάχιστα πίσω από τις βιομηχανίες μεταφορών και αποθήκευσης.

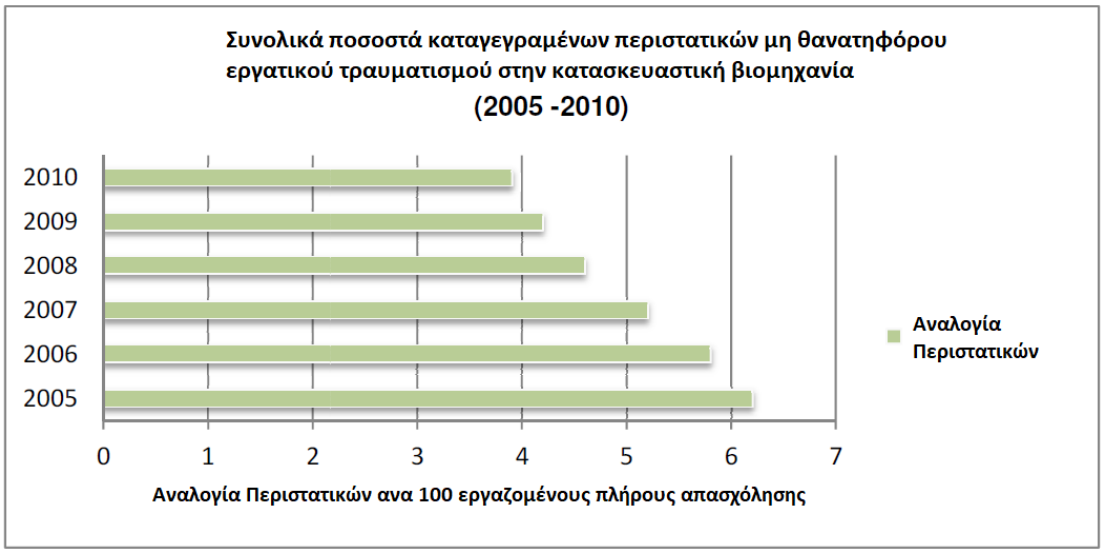


Σχήμα 1: Στατιστικά θανατηφόρων ατυχημάτων στις ΗΠΑ ανά βιομηχανία κατά το έτος 2011

Σύμφωνα με πληροφορίες από τα στατιστικά στοιχεία, μεταξύ όλων των θανάτων, οι πτώσεις είναι η κύρια αιτία θανάτου στις κατασκευαστικές εργασίες. Το 2010, το 35% των θανατηφόρων ατυχημάτων στον κατασκευαστικό κλάδο αφορούσε πτώσεις και ολισθήσεις ενώ το περίπου το 10% αναγνωρίστηκαν ως συγκρούσεις αντικειμένων ή εξοπλισμού. Περίπου το 75% των θανάτων που προκλήθηκαν από συγκρούσεις περιλαμβάνουν βαρύ εξοπλισμό. Οπότε καταλήγουμε στο συμπέρασμα ότι ένα στα τέσσερα ατυχήματα από συγκρούσεις οχημάτων έχει σαν αποτέλεσμα σε

μια απώλεια εργάτη από τον κατασκευαστικό κλάδο, περισσότερο από κάθε άλλη επαγγελματική δραστηριότητα.

Επίσης παρατηρείτε ότι ο κατασκευαστικός κλάδος έχει ένα υψηλό ποσοστό περιστατικών μη θανατηφόρων εργατικών τραυματισμών. Το ποσοστό αυτό ήταν 3,9 ανά 100 εργαζόμενους με πλήρες ωράριο το 2010 (Σχήμα 2). Αυτά τα ποσοστά εμφάνισης αντιπροσωπεύουν τον αριθμό των τραυματισμών και ασθενειών ανά 100 εργαζομένους πλήρους απασχόλησης και υπολογίζεται σύμφωνα με τον τύπο (N/ΕΩ) x 200000 όπου N ο αριθμός των τραυματισμών και ασθενειών, ΕΩ οι εργατοώρες δηλαδή το σύνολο των ωρών απασχόλησης όλων των εργαζομένων κατά τη διάρκεια του ημερολογιακού έτους και 200.000 είναι η βάση για 100 ισοδύναμους εργαζομένους πλήρους απασχόλησης οι οποίοι εργάζονται 40 ώρες την εβδομάδα, 50 εβδομάδες ετησίως.



Σχήμα 2: Στατιστικά τραυματισμών και ασθενειών στην κατασκευαστική βιομηχανία κατά το 2010

1.2 Χωματουργικά μηχανήματα

Τα χωματουργικά μηχανήματα αποτελούν το κύριο μηχανικό εξοπλισμό για την κατασκευή τεχνικών έργων, για τα οποία απαιτούνται:

- Εκσκαφείς κ φορτηγά για τις μετακινήσεις χωμάτινων όγκων προκειμένου να σχηματισθούν οι κατάλληλες κοιλότητες (λάκκοι, τάφροι, χαντάκια αγωγών και διώρυγες)
- Διαμορφώσεις και ισοπεδώσεις εδαφών
- Συμπυκνώσεις για σταθεροποίηση χωμάτινων όγκων
- Θρυμματισμός και ανάμιξη του εδάφους με άλλα υλικά

Σε ένα χωματουργικό έργο, όπως άλλωστε σε κάθε δομικό έργο, διακρίνουμε τρεις κυρίες φάσεις εργασίας:

Εκσκαφή ➔Μεταφορά➔Διάστρωση

Από τις τρεις αυτές βασικές φάσεις, η πρώτη και η τρίτη θεωρούνται ως οι κύριες φάσεις εργασίας για την παραγωγή έργου.

Οι χωματουργικές μηχανές διακρίνονται αντίστοιχα σε:

i. μηχανές εκσκαφής και φορτώσεως,
ii. μεταφορικές μηχανές
iii. μηχανές αποθέσεως, διαστρώσεως και συμπυκνώσεως.

Στην πρώτη κατηγορία ανήκουν όλες οι μηχανές , οι οποίες χρησιμοποιούνται στη χαλάρωση, εκσκαφή, εξόρυξη και φόρτωση υλικών. Στην δεύτερη κατηγορία ανήκουν τα μεταφορικά μέσα όπως ελαστικοφόρα οχήματα. Στην τρίτη κατηγορία ανήκουν οι μηχανές αποθέσεως, διαστρώσεως και συμπυκνώσεως, όπως είναι οι αποθέτες, οι διάφορες μορφές επιπέδων εκσκαφέων, οι συμπυκνωτές εδάφους και πολλά ακόμα.

Ανάλογα με την θέση λειτουργίας του μηχανήματος διακρίνονται σε χερσαία και πλωτά μηχανικά μέσα. Εκσκαφέας , οποίος είναι τοποθετημένος πάνω σε πλωτό μέσο και σκάβει τα πρανή διώρυγας, χαρακτηρίζεται ως πλωτός εκσκαφέας ενώ εκσκαφέας ο οποίος είναι τοποθετημένος στην όχθη και σκύβει τον πυθμένα λιμανιού χαρακτηρίζεται ως χερσαίος εκσκαφέας.

1.3 Μηχανικός εκσκαφέας γενικής χρήσεως

Είναι βασικό εκσκαπτικό μηχάνημα της κατηγόριας των χερσαίων εκσκαφέων, ο οποίος μετατρέπεται σε πλωτός εκσκαφέας, όταν τοποθετηθεί πάνω σε πλωτήρα. Οι εκσκαφείς είναι συνήθως μηχανήματα αυτοπροωθούμενα και σπανίως αποτελούν πρόσθετο εξοπλισμό εγκαταστημένα επί φορτηγών μεταφοράς υλικών ή σε άλλα μηχανήματα έργων.

Χαρακτηριστικό στοιχείο των εκσκαφέων είναι ο ειδικός κάδος με σκληρά δόντια ή κοφτερά χείλη , ο οποίος υπό κατάλληλη γωνία μπορεί να εισχωρεί στο έδαφος και να παραλαμβάνει ποσότητες από τα υλικά εδάφους. Οι κάδοι των εκσκαφέων σκάβουν το έδαφος , παραλαμβάνουν υλικό και έχουν τη δυνατότητα να το αποθέσουν σε επιθυμητή θέση ή σε όχημα μεταφοράς.

1.4 Κατηγοριοποίηση – Διάκριση εκσκαφέων γενικής χρήσης

Χαρακτηρίζονται ως εκσκαφείς γενικής χρήσεως, γιατί μπορούν με αλλαγή του εκσκαπτικού μηχανήματος να πάρουν διάφορες μορφές και να χρησιμοποιηθούν σε διαφορετικές εργασίες. Το εκσκαπτικό μηχάνημα προσαρμόζεται στο βασικό κατασκεύασμα και οι διάφορες μορφές και παραλλαγές αυτών μπορούν να προσεγγισθούν με την διάκριση σε:

1) Εκσκαφείς με μετωπικό κάδο φορτώσεως (Shovel)

Είναι μηχανήματα εξοπλισμένα με κάδο, συνήθως ηλεκτρικά τροφοδοτούμενα, που χρησιμοποιούνται για την εκσκαφή και φόρτωση της γης ή του κατακερματισμένου πετρώματος και για την εξόρυξη ορυκτών. Οι εκσκαφείς αυτοί είναι τύπου σχοινιού/καλωδίου, όπου ο βραχίονας εκσκαφής ελέγχεται και τροφοδοτείται με βαρούλκα και χαλύβδινα σχοινιά, παρά με υδραυλικά συστήματα όπως στους πιο κοινούς υδραυλικούς εκσκαφείς.

Εικόνα 1: Στα αριστερά φαίνεται ένας υδραυλικός εκσκαφέας με μετωπικό κάδο φόρτωσης ενώ στα δεξιά ένας ίδιου τύπου με συρματόσχοινα

2) Εκσκαφείς με ανεστραμμένο κάδο (Backhoe ή τσάπα)

Αποτελείται από έναν κάδο εκσκαφής στο τέλος ενός αρθρωτού βραχίονα δύο τμημάτων. Συνήθως τοποθετείται στο πίσω μέρος ενός ελκυστήρα ή ενός μπροστινού φορτωτή, ο οποίος σχηματίζει έναν «φορτωτή εκσκαφέα». Το τμήμα του βραχίονα που βρίσκεται πλησιέστερα προς το όχημα είναι γνωστό ως βραχίονας, ενώ το τμήμα που φέρει τον κάδο είναι γνωστό ως βύθισμα (ή ράβδος ρυμούλκησης). Η μπούμα είναι γενικά συνδεδεμένη με το όχημα μέσω ενός στροφέα, ο οποίος επιτρέπει στον βραχίονα να περιστρέφεται αριστερά και δεξιά, συνήθως σε ένα σύνολο γύρω στις συνολικά 180 έως 200 μοίρες.

Εικόνα 2: Χαρακτηριστικός εκσκαφέας με ανεστραμμένο κάδο

3) Εκσκαφείς με συρόμενο κάδο (Dragline)

Οι εκσκαφείς αυτοί θεωρούνται κομμάτι βαρέος εξοπλισμού και χρησιμοποιούνται σε οικοδομικές εργασίες και σε εξορύξεις. Αποτελούνται από ένα μεγάλο κουβά που αναρτάται από μια μπούμα (μια μεγάλη δομή τύπου δοκού) με συρματόσχοινα. Ο κάδος χειρίζεται με τη βοήθεια πολλών σχοινιών και αλυσίδων. Το

σχοινί ανύψωσης, που τροφοδοτείται από μεγάλους πετρελαιοκινητήρες ή ηλεκτροκινητήρες, στηρίζει τον κάδο και το συγκρότημα ανυψωτή-συνδέσμου από το βραχίονα. Με επιδέξιο ελιγμό του ανυψωτήρα και των οδοντωτών τροχών ο κάδος ελέγχεται για τις διάφορες λειτουργίες του. Μια σχηματική απεικόνιση ενός εκσκαφέα με σύστημα κάδου dragline φαίνεται παρακάτω.

Εικόνα 3: Μηχανικός εκσκαφέας με συρόμενο κάδο

4) Εκσκαφείς με αρπαγή (Clamshell ή αχιβάδα)

Πρόκειται για εκσκαφείς με ανοιγόμενο κάδο διπλής όψης συναρμολογημένο σε βαρύ εξοπλισμό, όπως ένα υδραυλικό εκσκαφέα ή γερανό. Συνδέεται με ένα υπόστεγο ή ένα βραχίονα και χρησιμοποιεί ειδικά σχεδιασμένα δόντια στην άκρη κοπής για να σκάψει σε κατακόρυφη κατεύθυνση. Όταν ο κάδος ανυψωθεί, οι δύο πλευρές κλείνουν, δημιουργώντας μια κίνηση που είναι γνωστή ως αρπαγή. Όταν ο κάδος χαμηλώνει, οι δύο πλευρές ανοίγουν και απελευθερώνουν τα υλικά που περιέχονται στο χέρι του.

Εικόνα 4: Υδραυλικού τύπου εκσκαφέας με αρπαγή

5) Εκσκαφείς γερανοί (Crane)

Πρόκειται για κοινούς εκσκαφείς που χρησιμοποιούνται για την ανύψωση και μεταφορά υλικών όπου για τον σκοπό αυτό έχουν προσαρμοσμένα στην άκρη του βραχίονα ειδικούς ιμάντες πρόσδεσης.

Εικόνα 5: Τύπος εκσκαφέα – γερανού

6) Εκσκαφείς πασσαλομπήκτες (Pile Driving Excavator)

Είναι ένα τύπος εκσκαφέα που χρησιμοποιεί έναν οδηγό πασσάλων (pile driving) για την οδήγηση κα τοποθέτηση πασσάλων στο έδαφος προκειμένου να παρέχουν στήριξη θεμελίων για κτίρια ή άλλες δομές. Ο οδηγός αυτός αποτελείται από ένα ψηλό πλαίσιο στο οποίο είτε ένα βάρος ανεβαίνει και πέφτει σε μια κεφαλή πασσάλου ή στο οποίο ένα σφυρί ατμού οδηγεί τον πάσσαλο.

Εικόνα 6: Εκσκαφέας πασσαλομπήκτης

Οι εκσκαφείς γενικής χρήσεως διακρίνονται σε μηχανικούς εκσκαφείς, όταν η μετάδοση κινήσεως στα λειτουργικά στοιχεία γίνεται με μηχανικά μέσα, δηλαδή οδοντωτούς τροχούς, συρματόσχοινα, αλυσίδες και στους υδραυλικούς εκσκαφείς όταν η μετάδοση κινήσεως γίνεται με υδροδυναμική ή υδροστατική ενέργεια. Σήμερα χρησιμοποιούνται σχεδόν κατά αποκλειστικότητα υδραυλικής μετάδοσης κίνησης εκσκαφείς, λόγω των μεγάλων πλεονεκτημάτων τα οποία παρουσιάζουν.

Ανάλογα με τον τρόπο μετακινήσεις τους, όπως και πολλά μηχανήματα έργων, διακρίνονται σε ελαστικοφόρους και σε ερπυστριοφόρους εκσκαφείς.

Πλεονεκτήματα των ερπυστριοφόρων εκσκαφέων είναι ότι ασκούν μικρή επιφανειακή πίεση πάνω στο έδαφος (λόγω μεγαλύτερης κατανομής), που τους επιτρέπει να εργάζονται και σε μαλακά εδάφη.

Αντίθετα τα τροχοφόρα οχήματα αναπτύσσουν μεγάλη ταχύτητα και μπορούν ευκολότερα να μετακινηθούν από το ένα μέτωπο εργασίας σε άλλο ή από εργοτάξιο σε εργοτάξιο.

1.5 Χαρακτηριστικά στοιχεία εκσκαφέων

Η μορφή των κάδων και η χωρητικότητα τους, όταν ανταποκρίνεται στην αναγκαία ισχύ εκσκαφής για δεδομένο έδαφος, χαρακτηρίζει την απόδοση του εκσκαφέα, σε συνάρτηση με το βαθμό πλήρωσης και τον αριθμό των πληρώσεων ανά μονάδα χρόνου.

Για αυτό η χωρητικότητα του μέγιστου κάδου για κάθε μηχάνημα δίδεται από τους κατασκευαστές εκσκαφέων, ως χαρακτηριστικό στοιχείο του μεγέθους (διαστάσεων και ισχύος) του μηχανήματος. Ο βαθμός πλήρωσης του κάδου εξαρτάται από το είδος του εδάφους (ομοιογένεια και συνεκτικότητα) και την περιεκτικότητα του σε υγρασία. Ο βαθμός πλήρωσης μπορεί να είναι μεγαλύτερος ή μικρότερος από την μονάδα.

Ο αριθμός πληρώσεων και αντίστοιχα ο αριθμός εκκενώσεων ενός κάδου εκσκαφέα , εξαρτάται από:

- Την ταχύτητα λειτουργίας των μηχανισμών που ελέγχουν τις κινήσεις των κάδων.
- Τη μηχανική συμπεριφορά και τη σύσταση του εδάφους
- Τη μορφή των στοιχείων διείσδυσης στο έδαφος (δόντια , χείλη) και το μέγεθος της τομής στο έδαφος.
- Τη διαδρομή του κάδου από θέση εκσκαφής μέχρι τη θέση εκφόρτωσης
- Τη γωνία και την ταχύτητα διείσδυσης του κάδου στο έδαφος και την ταχύτητα εκκένωσης του.

Τα αναφερθέντα στοιχεία είναι αυτονόητο ότι αλληλοεπηρεάζονται σημαντικά ενώ στην αποδοτικότητα του μηχανήματος σημαντική επίδραση έχει η δεξιοτεχνία του χείριστη, όσο και η σχετική θέση μηχανήματος - περιοχής εκσκαφής - θέση απόρριψης.

Οι κατασκευαστές εκσκαφέων συχνά προβάλλουν με έμφαση τη δυνατότητα των μηχανημάτων τους να εργασθούν και σε κατεύθυνση που σχηματίζει γωνία με την πορεία τους.

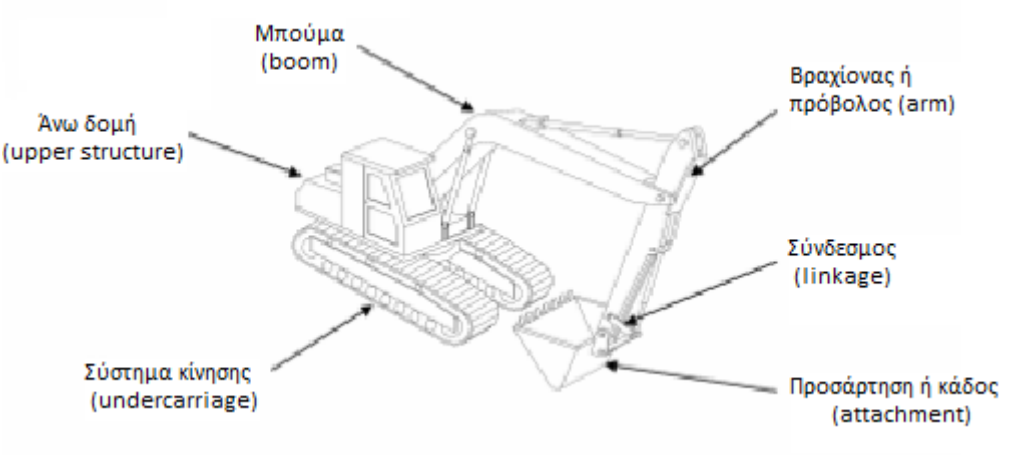
Κύρια χαρακτηριστικά των εκσκαφέων πέραν των προαναφερθέντων είναι ακόμη:

- Τα όρια της περιοχής δράσης (ακτίνα δράσης) του κάδου σε οριζόντιο επίπεδο.
- Τα ακραία όρια όπως το μέγιστο βάθος, το μέγιστο ύψος και η ακραία ακτίνα εκφόρτωσης.

- Η ανυψωτική ικανότητα και η μέγιστη δύναμη εισχώρησης στο έδαφος για δεδομένη θέση
- Οι ακραίες διαστάσεις (ελάχιστες τιμές) και το βάρος για να εξετάζεται εκάστοτε η δυνατότητα προσέγγισης στη θέση εργασίας, όπως και τα δεδομένα μετακινήσεις ή μεταφοράς σε σημαντική απόσταση.
- Η δυνατότητα χρησιμοποίησης διάφορων τύπων κάδων και η ευκολία πραγματοποίησης ελιγμών κατά την εκσκαφή για παράδειγμα σκάψιμο υπό γωνία

Στην παρούσα διπλωματική θα προσπαθήσουμε να εντοπίσουμε τα λάθη και τις παραβλέψεις που μπορεί να οδηγήσουν σε μια επισφαλή κατάσταση από την χρήση εκσκαφικού μηχανήματος με ανεστραμμένο κάδο χρησιμοποιώντας την μέθοδο STPA για την μοντελοποίηση του προβλήματος.

1.6 Βασικά εξαρτήματα εκσκαφέα με ανεστραμμένο κάδο



Εικόνα 7: Εξαρτήματα εκσκαφέα με ανεστραμμένο κάδο

Όπως φαίνεται και από την παραπάνω Εικόνα τα βασικά εξαρτήματα που απαρτίζουν έναν εκσκαφέα με ανεστραμμένο κάδο είναι:

- η προσάρτηση ή κάδος (attachment), νοείται μια αφαιρούμενη συσκευή (εργαλείο εργασίας) τοποθετημένη είτε απευθείας στον σύνδεσμο (linkage) είτε σε ένα βραχίονα προσάρτησης ενός εκσκαφέα για την εκπλήρωση της πρωταρχικής λειτουργίας του εκσκαφέα
- ο βραχίονας ή πρόβολος (arm) ο οποίος κινεί ουσιαστικά τον κάδο για να μαζέψει το υλικό από το έδαφος
- ο σύνδεσμος (linkage) ο οποίος συνδέει τον κάδο με τον βραχίονα
- η μπούμα (boom) χρησιμοποιείται για να επιτρέψει την ανύψωση καθώς και το χαμήλωμα του φορτίου
- η άνω δομή του εκσκαφέα (upper structure) που αποτελείται από τον κινητήρα, την καμπίνα του χειριστή και από την προστατευτική δομή πτώσης ή ανατροπής του μηχανήματος
- το σύστημα κίνησης (undercarriage)

1.7 Βασικές εργασίες εκσκαφέα

Οι βασικές κινήσεις και οι βασικές εργασίες που εκτελεί ένας εκσκαφέας κατά το έργο της εκσκαφής είναι:

- Εκσκαφή: Κατέβασμα του προβόλου (βραχίονα) και ώθηση του κάδου μέσα στο έδαφος, ώστε να γεμίσει.
- Μετατόπιση υλικού στον τόπο εκφόρτωσης: Ανύψωση κάδου και προβόλου, εφόσον αυτό χρειάζεται και περιστροφή του σκάφους.
- Εκφόρτωση: Άνοιγμα του πυθμένα ή ανατροπή του κάδου.
- Επιστροφή: Περιστροφή του σκάφους και τοποθέτηση του προβόλου και του κάδου για επανάληψη της εκσκαφής.

1.8 Στάδια χειρισμού εκσκαφέα

Στην εργασία αυτή όπως ήδη έχει αναφερθεί θα προσπαθήσουμε να εντοπίσουμε τα λάθη και τις παραβλέψεις κατά τον χειρισμό ενός εκσκαφέα και να προσπαθήσουμε να διορθώσουμε αυτές τις επισφαλείς καταστάσεις έτσι ώστε να οδηγηθούμε σε μια ασφαλέστερη χρήση του εκσκαφέα. Για να το επιτύχουμε αυτό θα πρέπει να προσδιορίσουμε και στη συνέχεια να αναλύσουμε τα στάδια χειρισμού του εκσκαφέα (συνήθης διαδικασία χειρισμού) προκειμένου να επιχειρήσουμε να εντοπίσουμε αστοχίες και λάθη κυρίως στο χειρισμό του μηχανήματος.

Ο χειριστής στην πλειοψηφία των περιπτώσεων, αν όχι πάντα, πρέπει να έχει την κατάλληλη εκπαίδευση, εξειδίκευση, και εξοικείωση με το μηχάνημα που θα εργαστεί έτσι ώστε και να είναι αποδοτικός στην εργασία του αλλά και να εργασθεί με ασφάλεια και για αυτόν και για τους γύρω του. Για αυτό ίσως χρειαστεί αρκετές ώρες προετοιμασίας έως ότου αισθανθεί ότι έχει τον απόλυτο έλεγχο του μηχανήματος του.

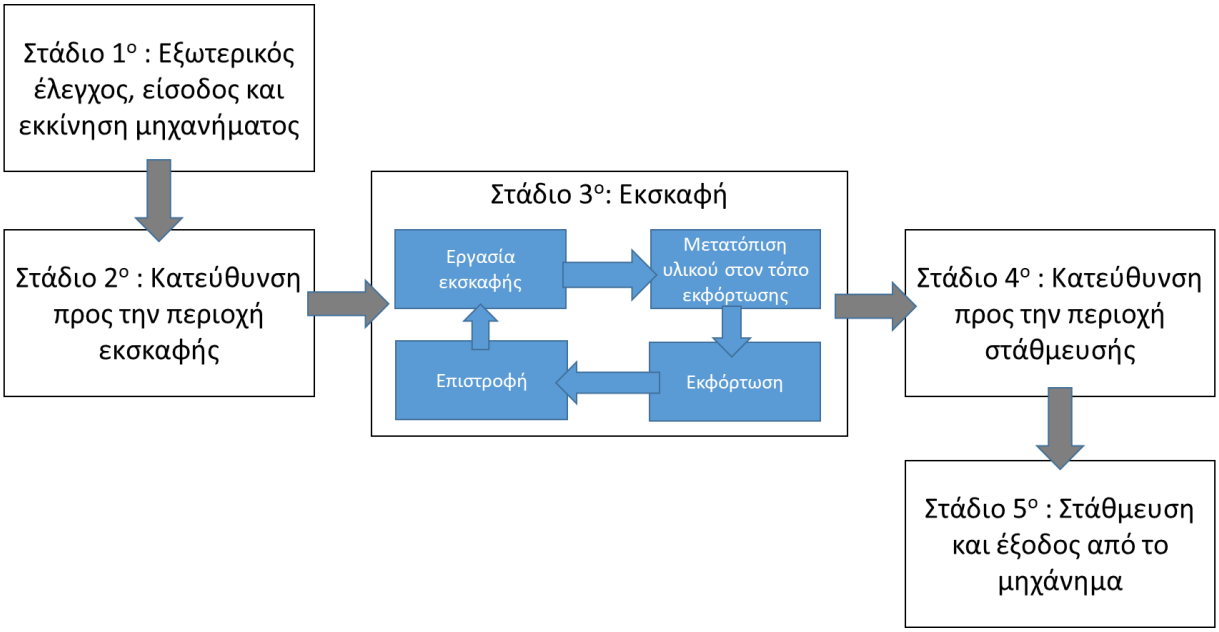
Επίσης, πρέπει να μελετήσει με μεγάλη προσοχή το εγχειρίδιο χρήσης και συντήρησης που συνοδεύει τον εκσκαφέα και να το έχει πάντα σε σημείο εύκολα προσβάσιμο μέσα στο μηχάνημα, για να το συμβουλευτεί όταν θα του χρειαστεί. Δυστυχώς στη χώρα μας τα περισσότερα εγχειρίδια δεν μεταφράζονται, έρχονται γραμμένα κυρίως στα Αγγλικά και αυτό θα μπορούσαμε αμέσως να το εντοπίσουμε σαν ένα στοιχείο που θα μπορούσε να γίνει αιτία παραλήψεων ή κακής συντήρησης του εκσκαφέα.

Ένας χειριστής εκσκαφέα, πρέπει να διενεργεί έλεγχο στα βασικά μέρη του μηχανήματος του πριν την κάθε χρήση του, ώστε να είναι σίγουρος ότι το μηχάνημα είναι σε καλή (εξωτερική) κατάσταση.

Η τυπική διαδικασία χειρισμού μετά τον απαραίτητο έλεγχο που πρέπει να διενεργήσει ο χειριστής, είναι η είσοδος του στο μηχάνημα, η έναρξη λειτουργίας του μηχανήματος, η κατεύθυνση προς την περιοχή εκσκαφής, η εκσκαφή, η εκφόρτωση του υλικού εκσκαφής ο τερματισμός λειτουργίας του μηχανήματος, αφού με ασφάλεια το σταθμεύσει και η έξοδος του από αυτό. Όλα αυτά πρέπει να γίνονται με συνέπεια και υπευθυνότητα ώστε να διασφαλίζονται τόσο η ασφάλεια του χειριστή αλλά και των άλλων εργαζομένων που βρίσκονται στο χώρο της εκσκαφής όσο και του ίδιου του μηχανήματος.

Λαμβάνοντας υπόψη όλα όσα αναφέρθηκαν παραπάνω μπορούμε να καταλήξουμε ότι τα στάδια χειρισμού ενός εκσκαφέα μπορούν να συνοψιστούν σε 5 στάδια τα οποία είναι τα εξής:

- Στάδιο1ο: Εξωτερικός έλεγχος, είσοδος και εκκίνηση μηχανήματος
- Στάδιο 2ο: Κατεύθυνση προς την περιοχή εκσκαφής
- Στάδιο 3ο: Εκσκαφή (κύρια φάση εργασίας η οποία αναλύθηκε σε υποεργασίες στο κεφ 2.8)
- Στάδιο 4ο: Κατεύθυνση προς την περιοχή στάθμευσης
- Στάδιο 5ο: Στάθμευση και έξοδος από το μηχάνημα



Εικόνα 8: Στάδια χειρισμού ενός εκσκαφικού μηχανήματος

1.9 Πρακτικές Ασφαλούς λειτουργίας του εκσκαφέα

Στη συνέχεια θα αναφερθούμε σε κάποιες βασικές πρακτικές που θα πρέπει να ακολουθήσει ο χειριστής κατά την λειτουργία του εκσκαφέα έτσι ώστε να είναι ασφαλής η λειτουργία του τόσο για αυτόν όσο και για τους γύρω του. Προκειμένου να προσδιοριστούν με ακρίβεια και σαφήνεια οι πρακτικές θα τις ομαδοποιήσουμε σύμφωνα με τα στάδια λειτουργίας του εκσκαφέα που αναφέραμε και πιο πάνω. Ούτως ή άλλως για να επιτευχθεί μια ασφαλής λειτουργία του εκσκαφέα πρέπει να εξασφαλιστεί ότι σε όλα τα στάδια λειτουργίας θα τηρηθούν οι πρακτικές ασφαλούς λειτουργίας του. Οπότε ανάλογα με το στάδιο χειρισμού του εκσκαφέα οι πρακτικές για την ασφαλή λειτουργία του παρουσιάζονται παρακάτω

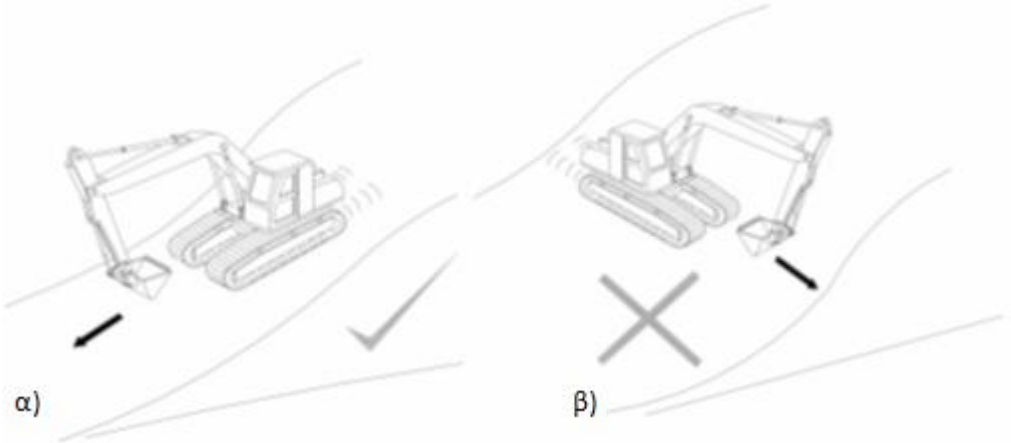
<u>Στάδιο 1ο: Εξωτερικού ελέγχου, εισόδου και εκκίνησης του μηχανήματος</u>

- Ο χειριστής ενός εκσκαφέα πρέπει να διαβάσει και να κατανοήσει τις πληροφορίες ασφαλείας σχετικά με τον εκσκαφέα από το σχετικό εγχειρίδιο του κατασκευαστή. Είναι σημαντικό ο φορέας εκμετάλλευσης, εκτός από την κατοχή των απαραίτητων πιστοποιήσεων, να έχει επαρκείς γνώσεις σχετικά με τις ασφαλείς διαδικασίες και τις προφυλάξεις ασφαλείας κατά τη λειτουργία του εκσκαφέα.

- Αναφορά θα πρέπει να γίνεται στα σχετικά αρχεία συντήρησης για να πιστοποιείται αν ο εκσκαφέας βρίσκεται σε κατάσταση κατάλληλη για χρήση.
- Ο χειριστής θα πρέπει να πραγματοποιεί μια επιθεώρηση του εκσκαφέα σε ασφαλή θέση, ακολουθούμενη από δοκιμή λειτουργίας. Ο χειριστής θα πρέπει να διακόψει τη λειτουργία του εκσκαφέα και να αναφέρει στον επιβλέποντα εάν ο εκσκαφέας δεν λειτουργεί κανονικά ή έχει κάποιο πρόβλημα λειτουργίας.
- Ο χειριστής πρέπει να θέσει σε λειτουργία στον εκσκαφέα το σύστημα συγκράτησης του χειριστή (ζώνης ασφαλείας).
- Πριν την εκκίνηση και εκτέλεση οποιουδήποτε ελέγχου του εκσκαφέα, ο χειριστής πρέπει να ελέγξει τον περιβάλλοντα χώρο γύρω από το μηχάνημα ώστε να βεβαιωθεί ότι κανένας δεν κινδυνεύει από τον μηχανισμό όταν αρχίσει να κινείται.
- Ο χειριστής κατά την είσοδο του στην καμπίνα του χειριστή, θα πρέπει να κάνει χρήση των σκαλοπατιών και των χειρολαβών του μηχανήματος ώστε να αποφευχθεί να χτυπήσει κατά την είσοδο του σε αυτή.

<u>Στάδιο 2ο: Κατεύθυνση προς την περιοχή εκσκαφής</u>

- Ο χειριστής πρέπει να ελέγξει την περιοχή εργασίας για να επαληθεύσει τις επικρατούσες συνθήκες και να λάβει τα απαραίτητα μέτρα (ισοπέδωση ή η συμπίεση του εδάφους ή η παροχή στήριξης) ώστε να λειτουργήσει με ασφάλεια, όπως:
  i. την κλίση του εδάφους και την τοποθεσία του ανοίγματος ή της τάφρου
  ii. τη συμπαγή κατάσταση του εδάφους (π.χ. μαλακό) και τη κατάσταση του οδοστρώματος και
  iii. την παρουσία προσώπων, εμποδίων και αντικειμένων κοινής ωφέλειας (όπως καλωδιώσεις ηλεκτρισμού ή τηλεφωνίας και σωληνώσεων ύδρευσης).
- Ο χειριστής πρέπει να ακολουθεί αυστηρά τις προφυλάξεις ασφαλείας που συνιστώνται στα εγχειρίδια του κατασκευαστή, ώστε ο εκσκαφέας να λειτουργεί και να πορεύεται σε πλαγιές εάν η περιοχή εργασίας είναι εντός της αποδεκτής γωνίας κλίσης.
- Όταν ο εκσκαφέας πορεύεται σε μια πλαγιά, πρέπει να κινείται ευθεία προς τα πάνω και προς τα κάτω στη γωνία κλίσης με χαμηλή ταχύτητα (Εικ. 9α). Δεν πρέπει να οδηγείται εγκάρσια της πλαγιάς (Εικ. 9β).

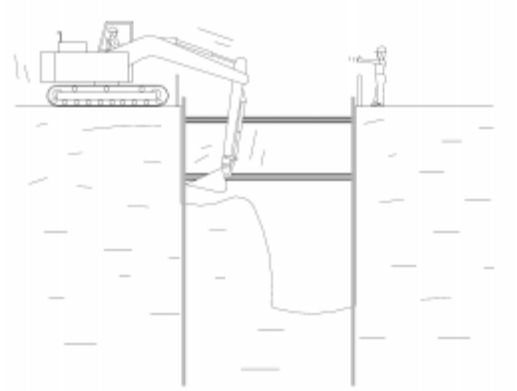


Εικόνα 9: α) Ορθή και β) εσφαλμένη οδήγησή εκσκαφέα κατά μήκος μια πλαγιάς

- Όταν ένας εκσκαφέας οδηγείτε σε κλίση, ο χειριστής πρέπει να διατηρεί την ταχύτητα οδήγησης σε χαμηλά επίπεδα. Για εκσκαφέα με γραναζωτό κιβώτιο ταχυτήτων, ο χειριστής θα πρέπει να διατηρεί το κιβώτιο σε χαμηλή σχέση μετάδοσης, και σε καμία περίπτωση δεν πρέπει να το μετατοπίσει σε ουδέτερη θέση (αποσύμπλεξη).
- Όταν ένας εκσκαφέας κινείται, ο χειριστής πρέπει να έχει κατεβασμένο το προσάρτημα (κάδο) ώστε να μην εμποδίζει την ορατότητα του και να αυξήσει τη σταθερότητα.

Στάδιο 3ο: Εκσκαφή

- Ο χειριστής πρέπει να εκτελεί τους χειρισμούς στον εκσκαφέα σταθερά και να αποφεύγει ξαφνικές ή απότομες κινήσεις.
- Ο χειριστής πρέπει να ακολουθεί τις διαδικασίες λειτουργίας του εκσκαφέα όπως συνιστάται στα εγχειρίδια του κατασκευαστή.
- Ο εκσκαφέας δεν πρέπει να φορτώνεται πέρα από το ασφαλές φορτίο εργασίας του, όπως ορίζεται από τα εγκεκριμένα πιστοποιητικά του.
- Κατά το χειρισμό φορτίου με προσάρτημα κάδου στον εκσκαφέα, το βάρος του προσαρτήματος και του βραχίονα στήριξης του προσαρτήματος, θα πρέπει να υπολογίζεται ως μέρος του φορτιού του εκσκαφέα.
- Σε καταστάσεις όπου ο χειριστής του εκσκαφέα δεν έχει πλήρη και χωρίς περιορισμούς ορατότητα της προσάρτησης κατά τη διάρκεια της εργασίας, θα πρέπει να υπάρχει ένας άνθρωπός να παρέχει σήματα στον χειριστή (Εικ. 10).



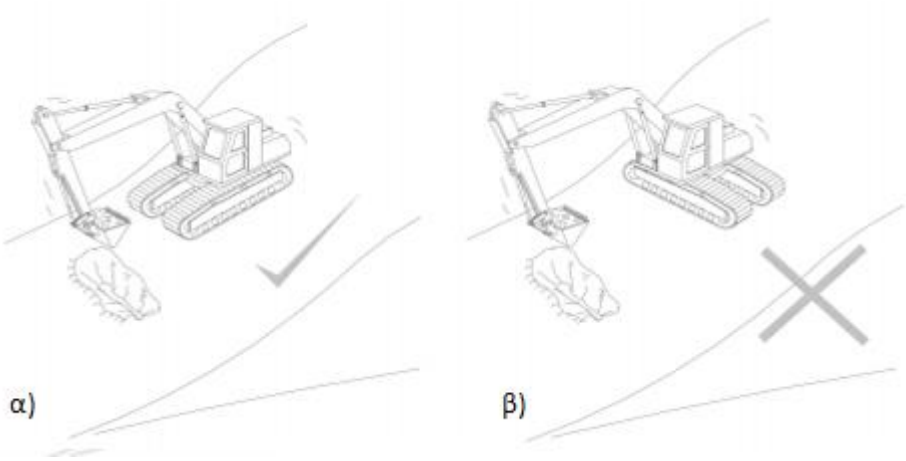
Εικόνα 10: Εργάτης παρέχει σήματα για την καθοδήγηση του χειριστή λόγω μη επαρκής ορατότητας κατά την εκσκαφή

- Κατά τη διάρκεια της εκσκαφής, ο εκσκαφέας και η θέση στην οποία απορρίπτεται το υλικό εκσκαφής θα πρέπει να βρίσκεται σε επαρκή απόστασή μακριά από την χείλος της εκσκαφής.
- Ο εκσκαφέας για να εργασθεί με ασφάλεια σε κλίση κατά μήκος μιας πλαγιάς, θα πρέπει να προσδιοριστεί η γωνία κλίσης του χώρου εργασίας με κατάλληλες μεθόδους (όπως τοπογραφική μελέτη ή χρήση εξοπλισμού ένδειξης της γωνίας κλίσης εγκατεστημένου στον εκσκαφέα) και να εξακριβωθεί από τα εγχειρίδια του κατασκευαστή, αν η εργασία που πρόκειται να εκτελεσθεί βρίσκεται εντός ορίου από τη μέγιστη συνιστώμενη γωνία κλίσης λειτουργίας του εκσκαφέα.

- Για να αποφευχθεί η ολίσθηση ενός εκσκαφέα κατά τη λειτουργία σε πλαγιά εντός της αποδεκτής γωνίας κλίσης, οι ερπύστριες ή οι τροχοί θα πρέπει να ασφαλίζονται (chocked) στην κατηφορική πλευρά.

- Για να αποφευχθεί η ανατροπή ενός εκσκαφέα σε πλαγιά, ο χειριστής θα πρέπει να δείξει ιδιαίτερη προσοχή όταν στρέφει τη μπούμα του εκσκαφέα.

- Για μέγιστη σταθερότητα κατά την εργασία σε κλίση, οι ερπυστριοφόροι ή οι τροχοί καθώς και το πλαίσιο του εκσκαφέα πρέπει να τοποθετηθούν κατά μήκος της πλαγιάς (Εικ. 11α και Εικ. 11β).



Εικόνα 11: Τοποθέτηση εκσκαφέα κατά την εκτέλεση της εργασίας α) Ορθή και β) Λανθασμένη

- Όταν ένας εκσκαφέας πρέπει να λειτουργεί κοντά στην άκρη μιας πλαγιάς κλίσης (είτε σε ανάχωμα είτε σε εκσκαφή), θα πρέπει να ληφθούν προληπτικά μέτρα όπως παροχή σήμανσης ή ανέγερσης περιφράξεων, μπλοκ παρεμπόδισης, προειδοποιητικά σήματα κλπ. στην άκρη της πλαγιάς ώστε να προειδοποιούν τον χειριστή.

- Οι εκσκαφείς για λειτουργία σε πλαγιές πρέπει να φέρουν προστατευτική δομή και σύστημα συγκράτησης του χειριστή για περιπτώσεις ανατροπής.

- Τα στηρίγματα σε ελαστικοφόρους εκσκαφείς ή τα εύκαμπτα μέρη επέκτασης σε ερπυστριοφόρους εκσκαφείς, θα πρέπει να χρησιμοποιούνται όποτε είναι δυνατόν κατά τη διάρκεια της λειτουργίας, για τη στάθμιση της μηχανής και τη βελτίωση της σταθερότητας.

Στάδιο 4ο: Κατεύθυνση προς την περιοχή στάθμευσης

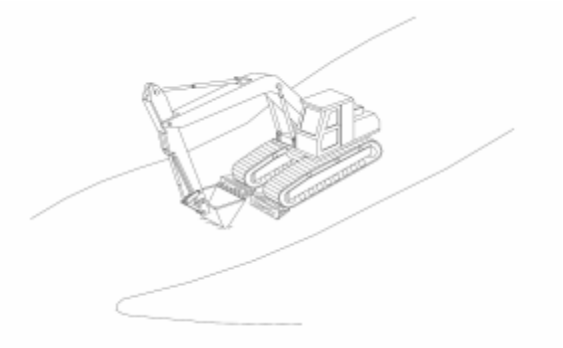
Ταυτίζεται με αυτά που αναφέρθηκαν στο Στάδιο 2ο παραπάνω.

Στάδιο5ο: Στάθμευση και έξοδος από το μηχάνημα

- Πριν την απενεργοποίηση του εκσκαφέα, ο χειριστής πρέπει να χαμηλώσει την προσάρτηση (κάδο) στο έδαφος.
- Πριν αποχωρήσει από τον εκσκαφέα, ο χειριστής θα πρέπει να τον έχει σταθμεύσει σε επίπεδο και σταθερό έδαφος με τον κινητήρα σβηστό, εφαρμοσμένο το φρένο στάθμευσης, το κλειδί του διακόπτη εκκίνησης του κινητήρα να έχει αφαιρεθεί, τα παράθυρα και η πόρτα της καμπίνας του

χειριστή κλειστά με την πόρτα κλειδωμένη και το κλειδί της πόρτας να έχει και αυτό αφαιρεθεί.

- ❖ Η θέση στην οποία σταθμεύετε ο εκσκαφέας δεν πρέπει να παρεμποδίζει την κίνηση, τα σήματα κυκλοφορίας, την ορατότητα άλλων οδηγών οχημάτων ή άλλες δραστηριότητες στο χώρο.
- ❖ Αν είναι απαραίτητο να σταθμεύσει ο εκσκαφέας σε έδαφος με κλίση, οι ερπύστριες ή οι τροχοί θα πρέπει να ασφαλιστούν στην κατηφορική πλευρά (Εικόνα 12).



Εικόνα 12: Στάθμευση εκσκαφέα σε έδαφος με κλίση

- ❖ Κατά την έξοδο του από το μηχάνημα, ο χειριστής θα πρέπει να κάνει χρήση των σκαλοπατιών και των χειρολαβών του μηχανήματος για λόγους ασφαλής εξόδου του από την καμπίνα.

Πέρα όμως από τις βασικές πρακτικές ασφαλούς λειτουργίας του εκσκαφέα που αναφέρθηκαν παραπάνω για κάθε στάδιο λειτουργίας του, υπάρχουν και κάποιες άλλες γενικότερες πρακτικές ασφαλείας που δεν μπορούν να ενταχθούν σε κάποιο συγκεκριμένο στάδιο λειτουργίας του εκσκαφέα αλλά είναι απαραίτητες για την ασφαλή του χρήση και αναφέρονται παρακάτω.

- Οι εργασίες θα πρέπει να αναστέλλονται σε καιρικές συνθήκες όπου η κατάσταση λειτουργίας του εκσκαφέα είναι δυνητικά επικίνδυνη.
- Όταν ένας εκσκαφέας εργάζεται κοντά σε οποιαδήποτε σταθερή κατασκευή, τότε θα πρέπει να διατηρηθεί μια ελεύθερη δίοδος μεταξύ του εκσκαφέα και της δομής και να ληφθούν εύλογα μέτρα για να αποτραπεί η πρόσβαση προσώπων σε αυτόν τον τόπο, όπως με περίφραξη.
- Όταν ένας εκσκαφέας χρησιμοποιείται σε οδικά έργα, θα πρέπει συμμορφώνεται με τις απαιτήσεις βάσει των Κανονισμών Οδικής Ασφάλειας σχετικά με το φωτισμό, την σήμανση και τη φύλαξη των οδικών έργων. Εάν από την χρήση του εκσκαφέα προκύπτει κάποιος κίνδυνος για τα διερχόμενα οχήματα τότε ένας άλλος εργαζόμενος πρέπει να χρησιμοποιηθεί για την ρύθμιση της κυκλοφορίας έτσι ώστε να αποφεύγονται τα ατυχήματα.
- Για χρησιμοποιηθεί ένας εκσκαφέας σε ένα κτίριο, θα πρέπει να επαληθευτεί ότι το φορτίο του δαπέδου μπορεί να υποστηρίξει το βάρος του μηχανήματος. Επίσης θα πρέπει να ελέγχουν το ύψος του δωματίου και τα διάκενα ώστε να διασφαλίσει ότι δεν θα παρουσιαστεί επισφαλής κατάσταση κατά τη χρήση του εκσκαφέα.

- Όταν ένας εκσκαφέας λειτουργεί σε περιοχή με ανεπαρκή φυσικό φωτισμό ή συνθήκες κακής ορατότητας, θα πρέπει να αναπτύσσεται τεχνητός φωτισμός.
- Όταν ένας εκσκαφέας λειτουργεί σε περιοχή με ανεπαρκή φυσικό εξαερισμό, θα πρέπει να ληφθούν μέτρα για την πρόληψη βλαβών λόγω συσσώρευσης τοξικών αερίων ή καπνών.
- Όλα τα εκτεθειμένα κινούμενα μέρη του εκσκαφέα θα πρέπει να προστατεύονται αποτελεσματικά, συμπεριλαμβανομένου και του κιβωτίου μετάδοσης κίνησης.
- Ανάλογα με την κατάσταση εργασίας, θα πρέπει να παρέχεται κατάλληλος εξοπλισμός ατομικής προστασίας τόσο για τον χειριστή όσο και για τους τριγύρω εργαζόμενους.

1.10 Επισφαλείς πρακτικές που πρέπει να αποφεύγονται

Οι επικίνδυνες πρακτικές κατά τη χρήση ενός εκσκαφέα δημιουργούν άσκοπους κινδύνους όχι μόνο για τον χειριστή αλλά και για τους εργαζόμενους που βρίσκονται κοντά. Προκειμένου να αποφευχθούν τα ατυχήματα, θα πρέπει να λαμβάνονται συγκεκριμένα μέτρα ώστε να εξασφαλιστεί ότι ο χειριστής ενός εκσκαφέα δεν εκτελεί τις ακόλουθες επικίνδυνες πρακτικές:

- να αφήσει τον εκσκαφέα χωρίς επιτήρηση με τον κινητήρα του σε λειτουργία
- να αφήσει τον εκσκαφέα χωρίς επιτήρηση με την προσάρτηση σε ανεβασμένη θέση
- εφαρμογή εγκάρσιου φορτίου στον κάδο και στον βραχίονα του εκσκαφέα κατά την εργασία
- οδήγηση του εκσκαφέα με την ώση του κάδου να εφαρμόζει προς τη γη
- εκσκαφή με τον εκσκαφέα σε ασταθή επιφάνεια
- τοποθέτηση του εκσκαφέα πολύ κοντά στην άκρη μιας πλαγιάς ή τάφρου
- μείωση της περιοχής κάτω από τον εκσκαφέα
- χρήση του κάδου του εκσκαφέα ως υποστηρίγματος για τη μετακίνηση του εκσκαφέα κατά μήκος της εκσκαφής ή του εμποδίου
- ανύψωση του εκσκαφέα με τον βραχίονα ως τρόπο για τη διάσωση του μηχανήματος από αστάθεια
- χρήση του κάδου του εκσκαφέα για απομάκρυνση σωρού φύλλων από το έδαφος
- περιστροφή του βραχίονα (μπούμα) του εκσκαφέα ενώ κινείται σε πλαγιά
- χτύπημα του κάδου σκληρά ενάντια στην επιφάνεια εργασίας
- χρήση του κάδου ως πλατφόρμα εργασίας ή φορέα μεταφοράς επιβατών και
- χρήση του κάδου του εκσκαφέα για τη μεταφορά υλικών και αντικειμένων που δεν μπορούν να συγκρατηθούν με ασφάλεια στον κάδο, όπως σωλήνες, ξύλινα δοκάρια και σανίδες.

Κεφάλαιο 2ο Ανάλυση Διαδικασιών με τη Θεωρία Συστημάτων

2.1 Εισαγωγή στην μέθοδο STPA

Η Συστημική Ανάλυση Διαδικασιών Ελέγχου (**Systems Theoretic Process Analysis – STPA)** είναι μια νέα τεχνική ανάλυσης κινδύνων που προτάθηκε από την Leveson. Κύριος στόχος της ανάλυσης κινδύνου είναι ο εντοπισμός των σεναρίων, τα οποία οδηγούν σε αναγνωρισμένους κινδύνους και αυτοί με τη σειρά τους μπορεί να οδηγήσουν σε απώλειες, προκειμένου να εξαλειφθούν ή να ελεγχθούν. Η μέθοδος STPA, ωστόσο, έχει μια αρκετά διαφορετική θεωρητική βάση ή μοντέλο αιτιότητας ατυχημάτων (Accident Causality Model**)**. Η STPA βασίζεται στη Θεωρία Συστημάτων (System Theory) ενώ οι παραδοσιακές τεχνικές ανάλυσης κινδύνων έχουν τη Θεωρία Αξιοπιστίας (Reliability Theory) ως θεμέλιο λίθο. Η χρήση της μεθόδου STPA έχει ως αποτέλεσμα τον εντοπισμό ενός μεγαλύτερου συνόλου αιτιών, πολλές από τις οποίες δεν εμπλέκουν αστοχίες ή αναξιοπιστία. Ενώ οι παραδοσιακές τεχνικές έχουν σχεδιαστεί για την αποτροπή ατυχημάτων αστοχίας στοιχείων του συστήματος (component failure accidents), η STPA αναπτύχθηκε για να αντιμετωπίσει τα ολοένα και συχνότερα ατυχήματα αλληλεπίδρασης των στοιχείων του συστήματος (component interaction accidents), τα οποία προκύπτουν από σχεδιαστικά ελαττώματα ή από επισφαλείς αλληλεπιδράσεις μεταξύ των "λειτουργικών" στοιχείων του συστήματος. Στην πραγματικότητα, οι αιτίες που εντοπίζονται χρησιμοποιώντας την STPA είναι ένα υπερσύνολο αυτών που εντοπίζονται από άλλες τεχνικές. Πολλές από αυτές τις πρόσθετες αιτίες σχετίζονται με νέα είδη τεχνολογίας (όπως υπολογιστές και ψηφιακά συστήματα) και υψηλότερα επίπεδα πολυπλοκότητας στα συστήματα που αναπτύσσονται σήμερα σε σύγκριση με εκείνα που αναπτύχθηκαν πριν από πολλά χρόνια, όπου οι περισσότερες παραδοσιακές τεχνικές αναπτύχθηκαν.

2.2 Μοντέλο Αιτιότητας Ατυχημάτων

Όλες οι αναλύσεις επικινδυνότητας βασίζονται στην αντίληψη του αναλυτή για το πώς και γιατί συμβαίνουν τα ατυχήματα. Εάν τα ατυχήματα ήταν εντελώς τυχαία γεγονότα τα οποία συνεπαγόταν πολύπλοκες και τυχαίες αλληλεπιδράσεις διαφόρων γεγονότων και συνθηκών, τότε δεν θα ήταν δυνατό να εντοπιστούν συγκεκριμένοι συνδυασμοί σεναρίων τα οποία οδηγούν σε απώλειες προτού αυτά συμβούν.

Στην πραγματικότητα, η ιδέα της τυχαίας αιτιότητας είναι η βάση της επιδημιολογικής προσέγγισης για την ασφάλεια, που προτάθηκε αρχικά από τον Gordon στη δεκαετία του 1940. Ενώ η επιδημιολογία συνήθως εφαρμόζεται σε ασθένειες, ο Gordon πρότεινε ότι θα μπορούσε επίσης να εφαρμοστεί σε ατυχήματα και στους τραυματισμούς που προκύπτουν. Αυτό το επιδημιολογικό μοντέλο ατυχημάτων και τραυματισμών υποθέτει ότι τα ατυχήματα προκύπτουν από τυχαίες αλληλεπιδράσεις μεταξύ ενός παράγοντα (φυσική ενέργεια), του περιβάλλοντος και του θύματος. Όπως και στην κλασική επιδημιολογία, αυτή η υπόθεση οδηγεί σε μια αντιδραστική προσέγγιση στην ανάλυση ατυχημάτων. Στην περιγραφική επιδημιολογία ο αριθμός των περιστατικών και τα ποσοστά επιπολασμού και θνησιμότητας σε ατυχήματα μεγάλων πληθυσμιακών ομάδων συλλέγονται και προσδιορίζονται τα γενικά χαρακτηριστικά του πληθυσμού όπως η ηλικία, το φύλο και

η γεωγραφική περιοχή. Η ερευνητική επιδημιολογία χρησιμοποιεί μια διαφορετική προσέγγιση όπου συλλέγονται τα συγκεκριμένα αίτια των τραυματισμών και των θανάτων, προκειμένου να καταρτιστούν εφικτά αντίμετρα.

Μολονότι αυτό το μετά από ατυχήματα επιδημιολογικό μοντέλο αιτιότητας των ατυχημάτων υποδηλώνει κάποιους κοινούς παράγοντες στα ατυχήματα, οι οποίοι μπορούν καθοριστούν μόνο με τη στατιστική αξιολόγηση των δεδομένων των ατυχημάτων. Από τη θετική πλευρά, επειδή δεν λαμβάνονται υπόψη συγκεκριμένες σχέσεις μεταξύ αιτιωδών παραγόντων, προηγούμενες μη αναγνωρισμένες σχέσεις μπορούν να ανακαλυφθούν. Επιπλέον, ο καθοριστικός παράγοντας σε αντίθεση με τις τυχαίες σχέσεις μπορεί να διακριθεί μέσω στατιστικών τεχνικών.

Η εναλλακτική λύση στην υπόθεση της ολικής τυχαιότητας είναι να υποθέσουμε ότι υπάρχει ένα πρότυπο για τα ατυχήματα που μπορεί να χρησιμοποιηθεί προληπτικά για τον εντοπισμό πιθανών αιτίων των ατυχημάτων σε συγκεκριμένα σχέδια συστημάτων. Οι επιδημιολόγοι εργάζονται με μεγάλους πληθυσμούς και με φυσικά (μη σχεδιασμένα) συστήματα. Οι μηχανικοί ασφαλείας είναι πιο πιθανό να εμπλακούν σε ανθρώπινα σχεδιασμένα συστήματα όπου η δομή και οι σχέσεις στο σύστημα είναι γνωστές και, στην πραγματικότητα, έχουν σχεδιαστεί και καταγραφεί. Προληπτικές προσεγγίσεις πρόληψης των ατυχημάτων μπορούν να αναπτυχθούν, οι οποίες εκμεταλλεύονται κοινά πρότυπα σε ατυχήματα, αναλύοντας μια συγκεκριμένη δομή του συστήματος για πρότυπα που μπορεί να οδηγήσουν σε απώλεια.

Για να εντοπιστούν πιθανά πρότυπα στα ατυχήματα, πρέπει να ληφθεί υπόψη ο ορισμός της αιτίας.

Σύμφωνα με το John Stuart Mill (1806-1873) μια **αιτία** είναι ένα σύνολο από επαρκείς συνθήκες. Γενικότερα μπορεί να οριστεί ως το άθροισμα των συνθηκών, θετικών και αρνητικών, συμπεριλαμβανομένου και του συνόλου των απρόβλεπτων περιπτώσεων κάθε περιγραφής, οι οποίες ενεργοποιούν, τις επακόλουθες κατά κανόνα συνέπειες.

Για παράδειγμα, η καύση απαιτεί εύφλεκτο υλικό, πηγή ανάφλεξης και οξυγόνο. Κάθε μία από αυτές τις προϋποθέσεις είναι αναγκαία, αλλά μόνο όταν συνδυαστούν μαζί μπορεί να οδηγήσουν στο γεγονός της «καύσης». Η διάκριση επομένως μεταξύ επαρκών και αναγκαίων συνθηκών είναι σημαντική. Ένα γεγονός λοιπόν μπορεί να οφείλεται σε πέντε συνθήκες, αλλά οι συνθήκες 1 και 2 μαζί μπορεί να είναι σε θέση να παράγουν το αποτέλεσμα, ενώ οι συνθήκες 3, 4 και 5 μπορεί επίσης να το κάνουν. Επομένως, υπάρχουν δύο ομάδες αιτιών (σύνολα συνθηκών που επαρκούν για την εμφάνιση του συμβάντος). Και οι δύο αιτίες (που ονομάζονται αιτιώδη σενάρια) έχουν ένα σύνολο αναγκαίων συνθηκών.

Η φράση "αναγκαία και επαρκής" συνεπάγεται άμεση αιτιότητα και γραμμικές σχέσεις. Η Α προκαλεί την Β, αυτό υποδηλώνει ότι αν συμβεί η Α, τότε και η Β θα συμβεί ενώ η Β δεν θα συμβεί μέχρι να συμβεί η Α. Υπάρχουν όμως πολλές καταστάσεις όπου η έμμεση αιτιότητα είναι σημαντική, δηλαδή όταν η σχέση δεν είναι ούτε αναγκαία ούτε επαρκής. Αυτοί οι παράγοντες μπορούν να επισημανθούν ως συστηματικοί αιτιώδεις παράγοντες.

Ένα παράδειγμα έμμεσης αιτιότητας είναι η οδήγηση υπό την επήρεια αλκοόλ. Η οδήγηση σε κατάσταση μέθης λέγεται ότι προκαλεί ατυχήματα, αλλά η κατανάλωσή αλκοόλ κατά την οδήγηση ενός αυτοκινήτου δεν οδηγεί πάντοτε σε ατύχημα, ενώ παράλληλα ατυχήματα συμβαίνουν και χωρίς να πιούν οι οδηγοί. Μια έμμεση αιτιακή σχέση είναι αυτή στην οποία το X ασκεί μια αιτιακή επίδραση στο Y αλλά μόνο μέσω μιας τρίτης μεταβλητής Z. Σε πιο σύνθετες σχέσεις, η φύση της σχέσης μεταξύ X και Y μπορεί να ποικίλει με την πάροδο του χρόνου, ανάλογα με την τιμή του Z.

Όλα τα παραπάνω αναφέρονται ώστε να γίνει πλήρως κατανοητό, ότι στις προσπάθειες μας να εντοπίσουμε τους κινδύνους και να τους αναλύσουμε έτσι ώστε να δημιουργήσουμε ένα ασφαλέστερο σύστημα, χρησιμοποιούμε χωρίς να το συνειδητοποιήσουμε μοντέλο αιτιότητας ατυχημάτων. Και αυτό γιατί είτε θεωρήσουμε τα ατυχήματα ως ένα ατυχές αλλά αναπόφευκτο αποτέλεσμα τυχαίων γεγονότων (όπως στα επιδημιολογικά μοντέλα), είτε ως αποτέλεσμα μεμονωμένων αστοχιών εξαρτημάτων, ή ως αποτέλεσμα δυσλειτουργικών αλληλεπιδράσεων και ανεπαρκώς ελεγχόμενων διαδικασιών στο σύστημα, αυτές οι υποθέσεις θα καθορίσουν τους τύπους των ατυχημάτων που μπορούμε να αναλύσουμε και να αποτρέψουμε στο σύστημά μας. Το υποκείμενο μοντέλο αιτιότητας ή οι υποθέσεις που θα χρησιμοποιήσουμε θα καθορίσουν το βαθμό επιτυχίας των προσπαθειών μας.

Η ανάλυση κινδύνου μπορεί να περιγραφεί ως "διερεύνηση ενός ατυχήματος πριν συμβεί". Για να γίνει αυτή η υποθετική έρευνα, απαιτούνται κάποιες υποθέσεις σχετικά με την αιτία των ατυχημάτων. Μια σημαντική υπόθεση είναι αν το μοντέλο ατυχήματος περιλαμβάνει μόνο την άμεση αιτιότητα ή αν περιλαμβάνει και την συστημική ή έμμεση αιτιότητα.

Μια μέθοδος ανάλυσης επικινδυνότητας που βασίζεται στη συστημική αιτιότητα μπορεί να εντοπίσει μη άμεσες εξαρτήσεις και σχέσεις. Μια συστημική αιτία μπορεί να είναι μία μέσα σε ένα αριθμό από πολλαπλές αιτίες, μπορεί να απαιτεί κάποιες ειδικές συνθήκες, μπορεί να είναι έμμεσα συνεργαζόμενη μέσω ενός δικτύου πιο άμεσων αιτιών ή μπορεί να απαιτεί ένα μηχανισμό ανάδρασης [Hall 1997, Korzybski 1933, Lakoff 2012, Senge 1990]. Η συστημική αιτιότητα είναι ιδιαίτερα σημαντική όταν μελετάμε οικοσυστήματα, βιολογικά συστήματα, οικονομικά συστήματα και κοινωνικά συστήματα. Τα μηχανικά συστήματα συνηθίζουν να είναι αρκετά απλά έτσι ώστε η άμεση γραμμική αιτιότητα να είναι επαρκής. Όμως, η πολυπλοκότητα έχει φτάσει σε τέτοιο σημείο όπου η συστημική αιτιότητα πρέπει να ληφθεί υπόψη ώστε να σχεδιάσουμε κατάλληλα συστήματα για την ασφάλεια. Το παραδοσιακό μοντέλο ατυχημάτων των αλυσιδωτών άμεσων αιτιωδών γεγονότων δεν είναι πλέον επαρκές.

2.3 Παραδοσιακά Μοντέλα Αιτιότητας Αλυσιδωτών Αστοχιών

Οι παραδοσιακές παραδοχές και τα σχετικά πρότυπα που χρησιμοποιούνται για την επεξήγηση των ατυχημάτων (το μοντέλο αιτιώδους ατυχήματος – accident causation model) αποτελούν το μοντέλο των αλυσιδωτών αστοχιών. Τα ατυχήματα θεωρείται ότι προκαλούνται από μια αλυσίδα αποτυχημένων γεγονότων στην διάρκεια του χρόνου, όπου κάθε γεγονός οδηγεί άμεσα στην πρόκληση του επακόλουθου συμβάντος και τελικά υπάρχει μια απώλεια (loss). Για παράδειγμα, τα φρένα αποτυγχάνουν, πράγμα που οδηγεί στο μη σταμάτημα του αυτοκινήτου τη σωστή

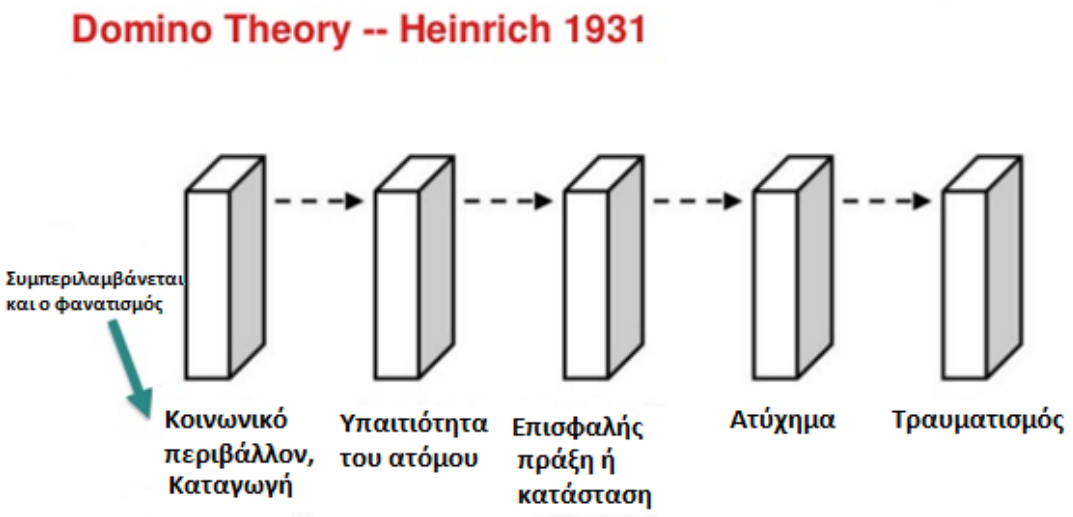
στιγμή, που προκαλεί το αυτοκίνητο να χτυπήσει το προπορευόμενο αυτοκίνητο. Τα γεγονότα που εξετάζονται είναι σχεδόν πάντα αποτυχίες υλικού, ανθρώπινα σφάλματα, αποτυχίες λογισμικού ή ενεργειακά σχετιζόμενα γεγονότα όπως μια έκρηξη.

Χρησιμοποιώντας αυτό το μοντέλο, η λογική προσέγγιση στην ανάλυση κινδύνων είναι να δημιουργηθούν εύλογες αλυσίδες αποτυχημένων γεγονότων που μπορούν να οδηγήσουν στην πρόληψη του ατυχήματος. Αυτές οι εύλογες αλυσίδες μπορούν να χρησιμοποιηθούν για τη δημιουργία αλλαγών στο σχεδιασμό ή στις λειτουργίες του συστήματος, προκειμένου να αποφευχθούν οι αστοχίες. Επειδή τα γεγονότα περιλαμβάνουν αστοχίες, ανθρώπινα σφάλματα ή ανεξέλεγκτη ενέργεια, είναι λογικό να προσπαθήσουμε να αποτρέψουμε τα ατυχήματα αυξάνοντας την αξιοπιστία των στοιχείων του συστήματος ώστε να αποτρέψουμε τις αποτυχίες και να σταματήσουμε την αλυσίδα (για παράδειγμα, να αυξήσουμε την αξιοπιστία των φρένων στο αυτοκίνητο). Θα πρέπει να τονιστεί ότι η αξιοπιστία της συμπεριφοράς των στοιχείων του συστήματος, δηλαδή η πρόληψη γεγονότων αποτυχίας, είναι το θεμέλιο ενός τέτοιου μοντέλου αιτιώδους αιτίου. Οι αποτυχίες θεωρούνται τυχαίες και συνεπώς είναι εύλογο να εκχωρηθεί μια πιθανότητα σε τέτοια γεγονότα αποτυχίας.

Σε ορισμένες βιομηχανίες, και κυρίως στη βιομηχανία μεταποίησης, η τυποποιημένη προσέγγιση για τον σχεδιασμό με ασφάλεια είναι να τεθούν φράγματα μεταξύ των γεγονότων, ιδίως των ενεργειακών γεγονότων, ώστε να εμποδίσουν την αλυσίδα από την διάδοση ακόμη και αν τα γεγονότα αποτυχίας μπορεί να συμβούν. Τα γεγονότα που εξετάζονται στη συνέχεια είναι η αποτυχία των φραγμών και όχι απαραίτητα τα γεγονότα αποτυχίας βασικών στοιχείων του συστήματος. Το πρόβλημα λοιπόν μετατοπίζεται στην μείωση της πιθανότητας αποτυχίας των φραγμών, η οποία και πάλι θεωρείται τυχαία. Σε άλλους κλάδους βιομηχανίας, πιο γενικές μορφές μέτρων πρόληψης μπορεί να χρησιμοποιηθούν, όπως εξελιγμένες τεχνικές ανθεκτικές σε σφάλματα και τεχνικές σχεδιασμού ασφαλούς αποτυχίας.

2.3.1 Θεωρία Domino

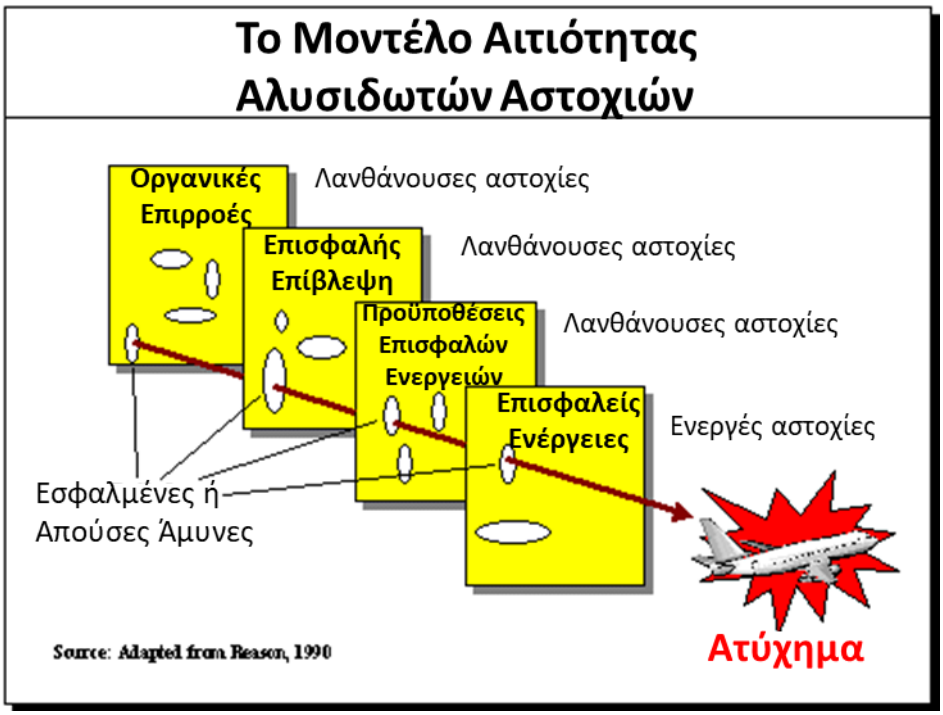
Τα τυπικά μοντέλα αλυσιδωτών αποτυχημένων συμβάντων χρονολογούνται από τη δεκαετία του 1930 και το μοντέλο Domino του Heinrich (Σχήμα 1), το οποίο επικεντρώθηκε στα σφάλματα του χειριστή ως αιτία των ατυχημάτων. Καθώς άρχισε να συσσωρεύεται μεγαλύτερη κατανόηση των πρόσθετων παραγόντων στα ατυχήματα, οι άνθρωποι πρόσθεσαν νέους παράγοντες στην αλυσίδα ντόμινο των συμβάντων, ιδιαίτερα στη δεκαετία του '70, όπως η έλλειψη ελέγχου από την διαχείριση, η συμπεριφορά του επόπτη, τη δομή διαχείρισης και οργάνωσης, και υποβαθμισμένες πρακτικές.



Σχήμα 3: Το πρωτότυπο μοντέλο Domino του Heinrich

2.3.2 Swiss Cheese Model

Το 1990, ο Reason δημιούργησε το δημοφιλές μοντέλο ελβετικού τυριού (Swiss Cheese Model). Υπάρχουν πολλές γραφικές απεικονίσεις του μοντέλου αυτού, όπου κοινός παράγοντας αποτελούν οι φέτες ελβετικού τυριού ενώ η τροχιά των ατυχημάτων παρουσιάζεται ως ένα βέλος μέσα από τις τρύπες του τυριού. Διαφορετικές "ετικέτες" μπορούν να τοποθετηθούν στις φέτες. Μια κοινή εκδοχή του μοντέλου παρουσιάζεται στο Σχήμα 4.



Σχήμα 4: Μια εκδοχή του Swiss Cheese Model

Η μόνη σημαντική διαφορά μεταξύ του μοντέλου του ελβετικού τυριού και των προηγούμενων μοντέλων του Heinrich και άλλων ήταν η υποκατάσταση με ελβετικές

φέτες τυριού των ντόμινο ή άλλων γραφικών. Οι οπές του τυριού αντιπροσωπεύουν αποτυχημένους ή απουσιάζοντες φραγμούς ή άμυνες. Σε ένα σενάριο ατυχήματος, θεωρείται ότι ταξινομούνται τυχαία, γεγονός που υποθέτει ότι κάθε "φέτα" είναι ανεξάρτητη, το οποίο είναι πολύ απίθανο σε οποιοδήποτε πραγματικό σύστημα. Η ανάγκη να ευθυγραμμιστούν οι οπές (συμβάντα αποτυχίας) ώστε να συμβεί ένα ατύχημα, συνεπάγεται επίσης μια απαίτηση προτεραιότητας για τα συμβάντα αστοχίας. Οι οργανωτικές επιρροές πρέπει να προηγούνται (και προφανώς να "προκαλούν") της επικίνδυνης εποπτείας η οποία προκαλεί τις προϋποθέσεις για επικίνδυνες πράξεις και οδηγεί τελικά στις επικίνδυνες πράξεις και στις απώλειες.

Το υφιστάμενο μοντέλο αλυσιδωτών αποτυχημένων γεγονότων παρέχει τη βάση για όλες σχεδόν τις σημερινές τεχνικές ανάλυσης κινδύνου (Δέντρα Αστοχιών – Fault Trees, Δέντρα Συμβάντων – Fault Events, Ανάλυση κινδύνων και διαδικασιών – HAZOP, FMEA και FMECA) και την πιθανή εκτίμηση κινδύνου που βασίζεται σε αυτές. Υποστηρίζει επίσης τις περισσότερες από τις τεχνικές σχεδιασμού ενίσχυσης της αξιοπιστίας μας, όπως πλεονασμό, φράγματα, περιθώρια ασφαλείας και υπερβολική σχεδίαση, σχεδιασμό ασφαλούς αστοχίας κ.λπ. Όλες αυτές οι τεχνικές ανάλυσης και σχεδιασμού βασίζονται στις αστοχίες στοιχείων του συστήματος και επομένως στην θεωρία αξιοπιστίας.

2.3.3 Τρόποι Αστοχιών και Ανάλυση Αποτελεσμάτων

Οι τρόποι αστοχιών και η ανάλυση των αποτελεσμάτων (Failure Modes and Effect Analysis - FMEA) είναι μια τεχνική ανάλυσης που αξιολογεί ένα σύστημα προκειμένου να εντοπιστούν πιθανές αστοχίες των στοιχείων της (ή των υποσυστημάτων) και να εκτιμηθούν τα αποτελέσματα αυτών των αστοχιών. Η τεχνική FMEA αναπτύχθηκε από μηχανικούς αξιοπιστίας οι οποίοι εργάζονταν σε στρατιωτικά συστήματα τη δεκαετία του 1950 και από τότε έχει υιοθετηθεί και προσαρμοσθεί από διάφορες βιομηχανίες όπως η άμυνα, η αυτοκινητοβιομηχανία, η ενέργεια και άλλες.

Υπάρχουν πολλοί δυνητικοί τύποι της FMEA ανάλυσης, οι οποίοι μπορούν γενικά να ομαδοποιηθούν σε δύο κατηγορίες ανάλογα με τον τύπο συλλογιστικής που χρησιμοποιούν κατά την ανάλυση. Ο πιο κοινός τύπος της FMEA αναφέρεται ως υλιστική FMEA (hardware FMEA) και χρησιμοποιεί επαγωγική συλλογιστική ξεκινώντας από γνωστούς τρόπους αστοχιών και αναλύοντας τα αποτελέσματά τους. Ο δεύτερος τύπος FMEA, μια λειτουργική FMEA, στηρίζεται σε συμπερασματική συλλογιστική ώστε να συναγάγει ποιοι τρόποι μπορεί να οδηγήσουν σε μια συγκεκριμένη αστοχία. Περισσότερες παραλλαγές μπορεί να προκύψουν λαμβάνοντας υπόψη πότε η FMEA λαμβάνει χώρα και από την διαφοροποίηση του κατά πόσον το σύστημα καθορίζεται φυσικά ή είναι μια μηχανική διαδικασία. Η ανάλυση FMEA επεκτείνεται συνήθως σε τρόπους αστοχιών, αποτελέσματα και ανάλυση κρισιμότητας (Failure Modes, Effects and Criticality Analysis – FMECA) προσθέτοντας πληροφορίες σχετικά με την πιθανότητα και την κρισιμότητα των τρόπων αστοχίας.

Η ανάλυση και για τις δύο παραλλαγές FMEA/FMECA ακολουθεί παρόμοια βήματα, ξεκινώντας από την αναγνώριση και απαρίθμηση των τμημάτων του συστήματος (εξαρτήματα ή υποσυστήματα) και των τρόπων αστοχίας τους. Στη συνέχεια, για κάθε τρόπο αστοχίας, οι επιδράσεις σε άλλα συστατικά και οι επιπτώσεις

στο συνολικό σύστημα καταγράφονται. Τα αποτελέσματα μια ανάλυσης FMEA/FMECA καταγράφονται γενικά σε έναν πίνακα όπως φαίνεται στον Πίνακα 1

Πίνακας 1: Παράδειγμα ανάλυσης FMEA

Συστατικό (ή υποσύστημα)	Τρόποι Αστοχίας	Αιτία	Αποτέλεσμα	Κρισιμότητα
Μηχανές Ανύψωσης	Μη λειτουργική	απώλεια ισχύος, ελαττωματικό κύκλωμα, ελαττωματικά ρουλεμάν	το φορτίο δεν μπορεί να ανυψωθεί ή να χαμηλωθεί	3
	Αποτυχία συγκράτησης	σπασμένα ελατήρια, φθαρμένα συνδέσεις	η ροπή συγκράτησης φορτίου της μηχανής θα χαθεί,. μειωμένο επίδοση συγκράτησης του φορτίου	3

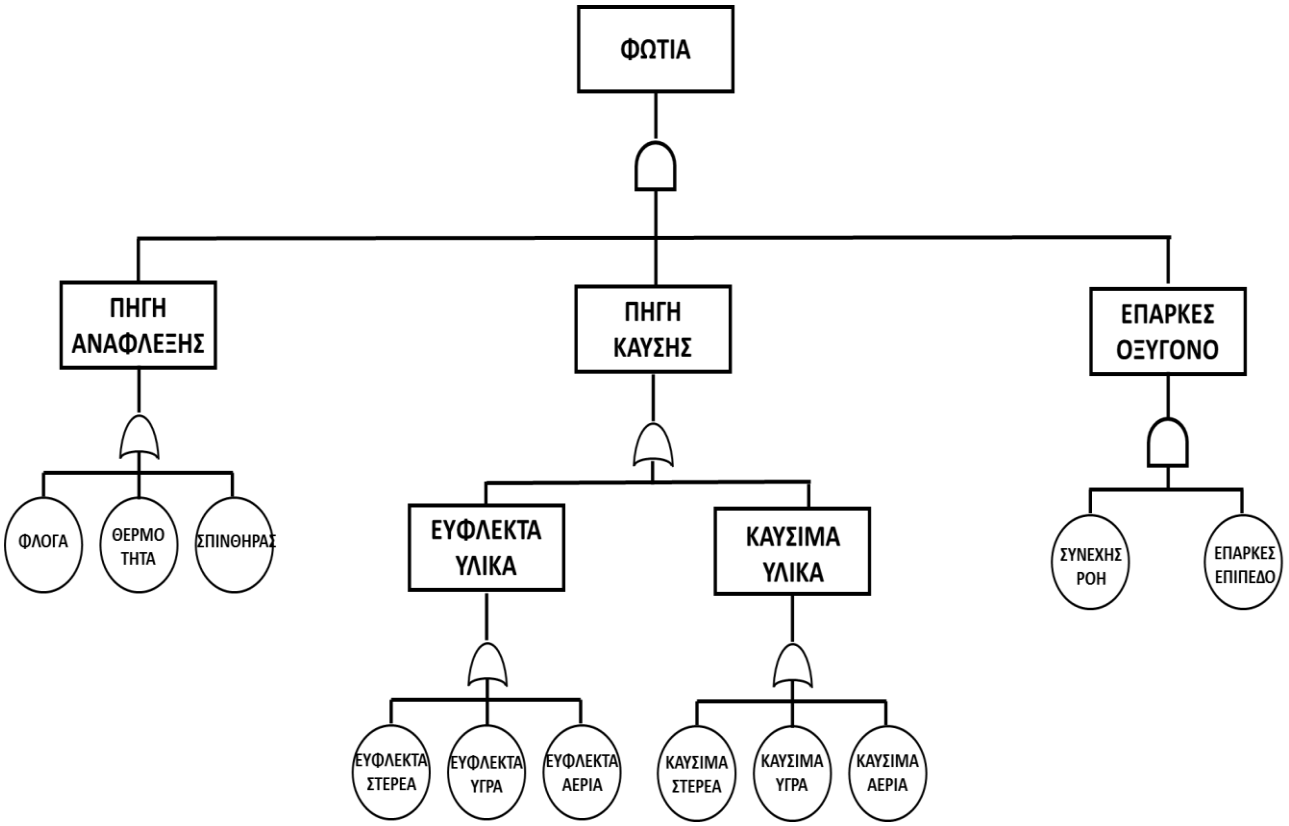
Αφού ολοκληρωθεί η ανάλυση FMEA/FMECA, οι διαθέσιμες πληροφορίες ενδέχεται να χρησιμοποιηθούν για την λήψη αποφάσεων σχετικά με το σύστημα. Οι αστοχίες που έχουν υψηλό επίπεδο κρισιμότητας και πιθανώς να επηρεάσουν σημαντικά το σύστημα θα πρέπει να μελετηθούν περαιτέρω και ενδεχομένως να εξαλειφθούν από το σύστημα. Συχνά η μορφή του πίνακα παρουσιάζεται με πρόσθετες στήλες που καταγράφουν τα επόμενα βήματα όπως προτείνονται από την ομάδα ανάλυσης.

Η τεχνική FMEA/FMECA μπορεί να εντοπίσει αποτελεσματικά αστοχίες ενός σημείου στο σύστημα και να χαρακτηρίσει τις συνέπειές τους. Η απλότητα της μεθόδου είναι θετική καθώς μπορεί να εφαρμοστεί σε μια ευρεία ποικιλία συστημάτων κατά την διάρκεια των περισσότερων φάσεων της διαδικασίας σχεδιασμού. Ωστόσο, η μέθοδος δεν είναι κατάλληλη για την αξιολόγηση πολλαπλών σεναρίων αστοχίας που μπορεί να προκύψουν σε περίπλοκα ολοκληρωμένα συστήματα. Επιπλέον, η εστίαση της τεχνικής FMEA/FMECA στις αστοχίες την εμποδίζει να εντοπίσει τα σενάρια που προκύπτουν από την ενσωμάτωση συστημάτων στα οποία δεν σημειώθηκε καμία αποτυχία.

2.3.4 Ανάλυση Δένδρου Αστοχιών (Fault Tree Analysis)

Σε αντίθεση με την FMEA, η οποία είναι σε μεγάλο βαθμό επαγωγική, η Ανάλυση Δένδρου Αστοχιών είναι μια μέθοδος συμπερασματική που προσδιορίζει τα αίτια των ανεπιθύμητων συμβάντων. Η FTA αναπτύχθηκε αρχικά στις αρχές της δεκαετίας του 1960 στα Bell Laboratories για να αξιολογήσει το σύστημα εκτόξευσης πυραύλων Minuteman και στη συνέχεια αναπτύχθηκε περαιτέρω από την Boeing Company ως ποσοτική και ποιοτική τεχνική, αλλά από τότε έχει υιοθετηθεί από πολλές άλλες βιομηχανίες ως μέρος των διαδικασιών ασφαλείας του συστήματος. Βασικά, μια FTA χρησιμοποιεί Boolean Logic για να περιγράψει τους συνδυασμούς των αιτιωδών γεγονότων που οδηγούν σε κάποιο συγκεκριμένο ανεπιθύμητο γεγονός, που συχνά αναφέρεται ως κίνδυνος. Εάν είναι ποιοτική, το αποτέλεσμα της ανάλυσης είναι μια λίστα με συνδυασμούς πραγμάτων (γεγονότα, περιβαλλοντικοί παράγοντες, αποτυχίες, σφάλματα κ.λπ.) που θα οδηγήσουν σε κίνδυνο. Αν είναι ποσοτική, η FTA θα παράγει μια πιθανότητα εμφάνισης του κινδύνου σε ένα δεδομένο χρονικό διάστημα.

Κάθε FTA ξεκινά από τον εντοπισμό του κορυφαίου συμβάντος, το οποίο μπορεί να είναι ευρύ, όπως η συντριβή ενός οχήματος, ή συγκεκριμένο, όπως ξεφούσκωμα των ελαστικών. Στη συνέχεια, τα αιτιακά γεγονότα που μπορεί να οδηγήσουν στο κορυφαίο συμβάν εντοπίζονται και τοποθετούνται ως διακλαδώσεις κάτω από το κορυφαίο συμβάν. Ένα τυποποιημένο σύνολο συμβόλων χρησιμοποιείται για την κατασκευή του δέντρου αστοχιών και των αστοχιών που συνδυάζονται χρησιμοποιώντας πύλες AND και πύλες OR. Ένα παράδειγμα δένδρου αστοχιών φαίνεται στο Σχήμα 5.



Σχήμα 5: Παράδειγμα Δένδρου Αστοχιών

Μετά την κατασκευή του δένδρου αστοχιών, αναπτύσσεται μια λογικά ισοδύναμη μορφή που σχετίζει τα βασικά συμβάντα με το κορυφαίο συμβάν, που αναφέρεται ως ανεπιθύμητο γεγονός. Εάν οι πιθανότητες ανατίθενται στα βασικά συμβάντα, η πιθανότητα εμφάνισης ενός ανεπιθύμητου γεγονότοςμπορεί να υπολογιστεί χρησιμοποιώντας τη θεωρία πιθανοτήτων. Τα ανεπιθύμητα γεγονότα χρησιμοποιούνται για την περαιτέρω εστίαση της ανάλυσης και βοηθούν τους αναλυτές να δώσουν προτεραιότητα σε υψηλού επιπέδου αιτίες ενός κορυφαίου γεγονότος για περαιτέρω μελέτη και πιθανό μετριασμό.

Η FTA είναι μια από πάνω προς τα κάτω τεχνική, καθόσον αρχίζει με τον εντοπισμό ενός μόνο ανεπιθύμητου συμβάντος και στη συνέχεια λειτουργεί σε επίπεδα μεγαλύτερης λεπτομέρειας προσδιορίζοντας τα αιτιακά γεγονότα. Αυτό είναι ένα ισχυρό χαρακτηριστικό που αποτρέπει τμήματα του συστήματος από το να μείνουν εντελώς ανεξερεύνητα. Ωστόσο, η FTA παρέχει λίγη καθοδήγηση στον αναλυτή καθ΄ όλη τη διάρκεια της ανάλυσης. Αν και είναι μια ισχυρή τεχνική για την ανάλυση των ηλεκτρομηχανικών συστημάτων που επικρατούν κατά την ανάπτυξή της, η FTA δεν

είναι ιδιαίτερα ικανή να αναλύει συστήματα με σημαντικό λογισμικό όπως ενσωματωμένα συστήματα ελέγχου. Το λογισμικό δεν αποτυγχάνει όπως τα φυσικά συστατικά και η FTA δεν παρέχει ένα μέσο για την ανάλυση των λανθασμένων απαιτήσεων που μπορεί να οδηγήσουν σε ανεπιθύμητη συμπεριφορά λογισμικού. Επιπλέον, η κατασκευή ενός Δέντρου Αστοχιών απαιτεί κάποιο αξιόλογο επίπεδο σχεδιαστικής λεπτομέρειας και κατά συνέπεια η FTA κατά την ανάπτυξη του σεναρίου είναι απίθανο να παράγει σημαντικά αποτελέσματα.

2.4 Θεωρία Συστημάτων

Μέχρι τη δεκαετία του 1940 και του 1950, οι επιστήμονες και οι μηχανικοί χρησιμοποίησαν την αναλυτική μείωση για να αντιμετωπίσουν την πολυπλοκότητα. Στην αναλυτική μείωση, η φυσική πολυπλοκότητα αντιμετωπίζεται διαιρώντας το σύστημα σε ξεχωριστά φυσικά συστατικά, ενώ η πολυπλοκότητα συμπεριφοράς απλοποιείται λαμβάνοντας υπόψη μόνο ξεχωριστά γεγονότα με την πάροδο του χρόνου. Οι υποθέσεις στις οποίες βασίζεται η αναλυτική μείωση περιλαμβάνουν την υπόθεση ότι η διαίρεση σε μέρη δεν διαστρεβλώνει το φαινόμενο και ότι οι αλληλεπιδράσεις μεταξύ των υποσυστημάτων και των γεγονότων είναι απλές και άμεσες.

Εναλλακτικά, ορισμένα συστήματα μπορούν να θεωρηθούν ως μία μάζα χωρίς δομή με εναλλακτά μέρη. Ο νόμος των μεγάλων αριθμών χρησιμοποιείται για να περιγράψει τη συμπεριφορά σε όρους μέσων όρων. Η υπόθεση είναι ότι τα συστατικά είναι επαρκώς τακτικά και τυχαία στη συμπεριφορά τους ώστε μπορούν να μελετηθούν στατιστικά. Δυστυχώς, τα περισσότερα από τα κρίσιμα για την ασφάλεια συστήματα σήμερα είναι πολύ περίπλοκα για πλήρη ανάλυση και πολύ οργανωμένα για στατιστικές.

Η θεωρία των συστημάτων αναπτύχθηκε για να αντιμετωπίσει αυτά τα σύγχρονα συστήματα. Αποτελεί τη βάση της μηχανικής συστημάτων (system engineering), όπου το σύνολο θεωρείται ότι υπερβαίνει το άθροισμα των μερών και μια από πάνω προς τα κάτω ανάλυση και ανάπτυξη χρησιμοποιείται. Η θεωρία των συστημάτων ασχολείται με ιδιότητες (αποκαλούμενες αναδυόμενες ιδιότητες) που μπορούν να αντιμετωπιστούν μόνο με επαρκή ολιστική προσέγγιση, λαμβάνοντας υπόψη όλες τις τεχνικές και κοινωνικές πτυχές. Αυτές οι ιδιότητες προκύπτουν στις σχέσεις και τις αλληλεπιδράσεις μεταξύ των στοιχείων του συστήματος ή των συμβάντων συμπεριφοράς. Δηλαδή, η θεωρία των συστημάτων αντιμετωπίζει τα συστήματα ως σύνολο και όχι τα συστατικά και τα γεγονότα ξεχωριστά.

Στη θεωρία συστημάτων, αντί να σπάσουν τα συστήματα σε αλληλεπιδρώντα συστατικά, τα συστήματα θεωρούνται (μοντελοποιούνται) ως μια ιεραρχία οργανωτικών επιπέδων. Στο χαμηλότερο επίπεδο οδικής κυκλοφορίας, υπάρχουν τα επιμέρους οχήματα, όπως τα αυτοκίνητα και τα φορτηγά. Στο επόμενο επίπεδο υπάρχει ο σχεδιασμός των δρόμων, ο οποίος ελέγχει την κίνηση των μεμονωμένων οχημάτων και τις αλληλεπιδράσεις τους. Σε υψηλότερο επίπεδο, μπορεί κανείς να συλλάβει ολόκληρο το σύστημα των οδών, συμπεριλαμβανομένων των οδών, αλλά και τους κανόνες και τις πολιτικές που επιβάλλονται στους οδηγούς των οχημάτων.

Τα επίπεδα της ιεραρχίας χαρακτηρίζονται από αναδυόμενες ιδιότητες. Αυτές οι ιδιότητες είναι μη αναγώγιμες από την άποψη ότι δεν μπορούν να οριστούν αποκλειστικά όσον αφορά τις ιδιότητες των επιμέρους συστατικών. Η αλληλεπίδραση μεμονωμένων στοιχείων του συστήματος οδηγεί σε αναδυόμενη συμπεριφορά.

Η ασφάλεια είναι μια αναδυόμενη ιδιότητα. Με την εξέταση των στοιχείων ενός πυρηνικού σταθμού ηλεκτροπαραγωγής, για παράδειγμα, μεμονωμένες βαλβίδες και σωλήνες και σύρματα και δοχεία συγκράτησης, δεν είναι δυνατόν να καθοριστεί εάν ο πυρηνικός σταθμός ηλεκτροπαραγωγής θα είναι ασφαλής. Αυτό απαιτεί κατανόηση του τρόπου με τον οποίο τα επιμέρους στοιχεία συνδέονται και αλληλοεπιδρούν, δηλαδή ολόκληρο το σχεδιασμό του συστήματος. Ενδεχομένως να υπάρχουν κάποιες τοπικές ιδιότητες ασφαλείας των επιμέρους συστατικών, όπως αιχμηρές άκρες που θα μπορούσαν να κόψουν όποιον έρχεται σε επαφή μαζί τους, αλλά ο κίνδυνος της «ανεξέλεγκτης έκλυσης ραδιενεργού υλικού» δεν μπορεί να αξιολογηθεί εξετάζοντας μόνο τα μεμονωμένα συστατικά χωρίς κατανόηση του συνολικού σχεδιασμού του συστήματος (φυσικές και λογικές συνδέσεις) και του τρόπου αλληλεπίδρασης των στοιχείων.

Στη θεωρία συστημάτων, κάθε ιεραρχικό επίπεδο ενός συστήματος ελέγχει τις σχέσεις μεταξύ των στοιχείων στο επόμενο κατώτερο επίπεδο. Δηλαδή, τα επίπεδα επιβάλλουν περιορισμούς στον βαθμό ελευθερίας της συμπεριφοράς των συστατικών κάτω από αυτά. Αυτή η έννοια των περιορισμών στη συμπεριφορά παίζει σημαντικό ρόλο στη STAMP. Οι ιδιότητες ασφαλείας ελέγχονται με την επιβολή περιορισμών στη συμπεριφορά και την αλληλεπίδραση των στοιχείων του συστήματος. Για παράδειγμα, σε ένα σύστημα ελέγχου εναέριας κυκλοφορίας, ένας περιορισμός ασφαλείας είναι ότι πρέπει πάντα να υπάρχει ελάχιστη απόσταση μεταξύ αερομεταφερόμενων αεροσκαφών. Εξ ορισμού, τότε, τα ατυχήματα συμβαίνουν όταν οι περιορισμοί ασφαλείας δεν επιβάλλονται.

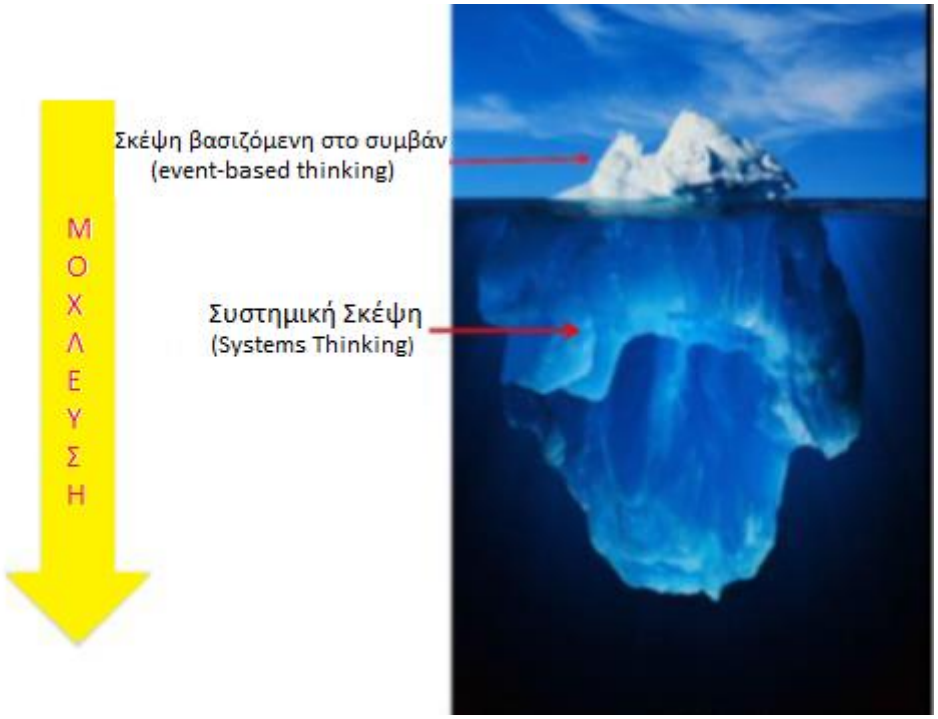
Χρησιμοποιώντας τη θεωρία των συστημάτων, μπορούμε να ξεπεράσουμε τις απλές άμεσες σχέσεις μεταξύ των συνιστωσών και να εξετάσουμε τις έμμεσες και μη γραμμικές σχέσεις, καθώς και τους τύπους ελέγχου, όπως ο έλεγχος στη ροή προς τα εμπρός και την ανατροφοδότηση. Αυτές οι πιο σύνθετες σχέσεις μεταξύ συστατικών και συμβάντων δεν μπορούν να περιγραφούν εύκολα χρησιμοποιώντας μόνο πλαίσια με βέλη μεταξύ τους, πράγμα που φυσικά συνεπάγεται άμεση αιτιότητα. Αυτό, δυστυχώς, το καθιστά αδύνατο να περιγράψουμε γραφικά την αιτία ενός ατυχήματος χρησιμοποιώντας κουτιά και βέλη χωρίς να χάνουμε σημαντικές πληροφορίες και σχέσεις. Η STAMP έχει επικριθεί διότι δεν οδηγεί σε ωραία γραφικά μοντέλα των αιτιών ενός ατυχήματος, ειδικά σε αυτά που παρουσιάζονται σε μία σελίδα. Συμφωνούμε ότι τα απλά γραφικά μοντέλα είναι πολύ ισχυρά, αλλά χάνουν σημαντικές πληροφορίες όταν δείχνουν μόνο άμεσες σχέσεις. Στην καλύτερη περίπτωση, πολλοί τύποι γραφικών μοντέλων (όπως τα δυναμικά μοντέλα συστήματος για να δείξουν τη δυναμική και τα μοντέλα τύπου STAMP για να δείξουν τη στατική δομή) θα χρειαστούν μαζί με τη φυσική γλώσσα για να περιγράψουν επαρκώς τα αίτια ενός ατυχήματος.

2.5 Συστημική Προσέγγιση

Η συστημική προσέγγιση (Systems Thinking) είναι ένας όρος που υποδηλώνει διαδικασίες και τρόπους σκέψης που ακολουθούν τις αρχές της θεωρίας των συστημάτων και ενσωματώνουν τη συστημική αιτιότητα. Ο Senge (1990) αναφέρει ότι η συστημική προσέγγιση μετατοπίζει την έμφαση από την υπαιτιότητα του ατόμου στο γενικό σύστημα και τις οργανωσιακές διαδικασίες για την ασφάλεια. Αυτό υποδηλώνει ότι όλοι μοιράζονται την ευθύνη για τα προβλήματα που δημιουργούνται σε ένα σύστημα. Με τη συστημική σκέψη, αναγνωρίζουμε ότι "η αιτία" συχνά βρίσκεται στην ίδια τη δομή και οργάνωση του συστήματος. Αυτή η διαρθρωτική συνείδηση, μας δίνει τη δυνατότητα να ρωτήσουμε ποιες είναι οι υπερβολικές δομές που συγκρατούν το σύστημα μαζί.

Ο σχεδιασμός ενός ασφαλέστερου κόσμου απαιτεί όχι μόνο την επίλυση των άμεσων προβλημάτων αλλά και την κατασκευή ενός συστήματος που μαθαίνει και βελτιώνεται με την πάροδο του χρόνου. Δεν αρκεί να εντοπίσουμε μια συγκεκριμένη δομή που υποκρύπτει ένα συγκεκριμένο πρόβλημα, αυτό μπορεί να οδηγήσει στην επίλυση ενός προβλήματος, αλλά δεν θα αλλάξει τον τρόπο σκέψης που προκάλεσε το πρόβλημα.

Με την εφαρμογή της συστημικής προσέγγισης στον τομέα της ασφαλείας, θα μπορέσουμε να χειριστούμε πιο πολύπλοκους και αιτιώδεις παράγοντες στην τεχνική ασφάλειας (Εικόνα 13).

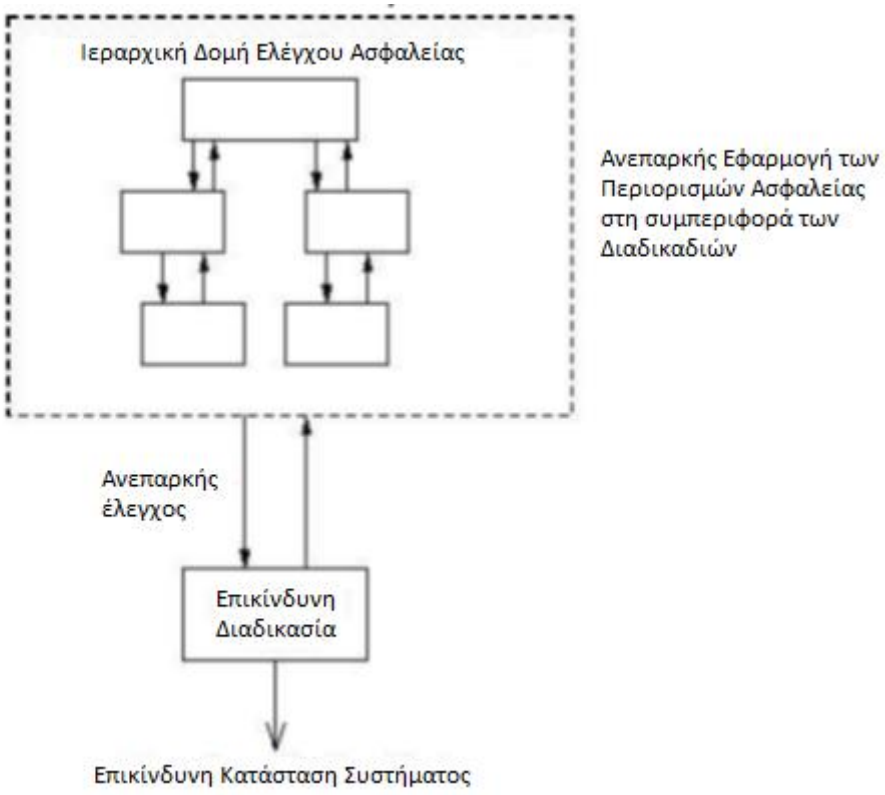


Εικόνα 13: Με τη χρήση της συστημικής σκέψης παρέχεται η μόχλευση που χρειάζεται ώστε να ξεπεράσουμε την βασισμένη σε απλά γεγονότα σκέψη και να μειώσουμε τα ατυχήματα σε σύνθετα συστήματα

2.6 Συστημική Θεώρηση Ατυχημάτων και Διαδικασιών

Συμφωνα με τη Συστημική Θεώρηση Ατυχημάτων και Διαδικασιών (Systems-Theoretic Accident Model and Processes – STAMP), η ασφάλεια είναι μια αναδυόμενη ιδιότητα που προκύπτει όταν τα στοιχεία του συστήματος αλληλεπιδρούν μεταξύ τους μέσα σε ένα ευρύτερο περιβάλλον. Υπάρχει ένα σύνολο περιορισμών ασφαλείας που σχετίζονται με τα στοιχεία του συστήματος - φυσικά, ανθρώπινα και κοινωνικά - που επιβάλλουν την ιδιότητα της ασφάλειας. Τα ατυχήματα εμφανίζονται όταν οι αλληλεπιδράσεις των στοιχείων του συστήματος παραβιάζουν τους περιορισμούς ασφαλείας, το οποίο σημαίνει ότι δεν επιβάλλονται κατάλληλοι περιορισμοί στις αλληλεπιδράσεις.

Ο στόχος των διαδικασίων ασφάλειας , επομένως, είναι να ελέγξει τη συμπεριφορά των στοιχείων και του συστήματος ως ένα σύνολο ώστε να διασφαλιστεί ότι οι περιορισμοί ασφαλείας επιβάλλονται. Στην εικόνα παρακάτω φαίνεται ένα απλοποιημένο γράφημα του μοντέλου STAMP το οποίο εξηγεί σύντομα ότι τα ατυχήματα συμβαίνουν όταν το σύστημα εισέλθει σε μια επικίνδυνη κατάσταση, η οποία με τη σειρά της συμβαίνει λόγω ανεπαρκούς ελέγχου στη μορφή επιβολής των περιορισμών ασφαλείας στη συμπεριφορά του συστήματος.



Εικόνα 14: Απλοποιημένη απεικόνιση του μοντέλου STAMP

Στη STAMP, τα ατυχήματα περιλαμβάνουν μια πολύπλοκη και δυναμική διαδικασία. Δεν είναι απλώς αλυσίδες συμβάντων αστοχίας στοιχείων του συστήματος. Η ασφάλεια λοιπόν μπορεί να αντιμετωπιστεί ως πρόβλημα δυναμικού ελέγχου και όχι ως πρόβλημα αξιοπιστίας των στοιχείων του συστήματος. Για παράδειγμα, στο διαστημικό λεωφορείο Challenger ο δακτύλιος O-ring δεν έλεγξε την απελευθέρωση των προωθητικών αερίων σφραγίζοντας ένα διάκενο στο πεδίο ένωσης. Το O-ring

απέτυχε, αλλά το μεγαλύτερο πρόβλημα δεν ήταν μόνο αυτή η αποτυχία, αλλά ότι αυτή η αποτυχία οδήγησε σε παραβίαση ενός περιορισμού ασφαλείας του συστήματος.

Τα περισσότερα μοντέλα ατυχημάτων δίνουν έμφαση στις αστοχίες των στοιχείων του συστήματος παραλείποντας άλλους τύπους παραγόντων αποτυχίας, όπως σφάλματα σχεδιασμού του συστήματος, ελαττώματα στις απαιτήσεις λογισμικού, λάθη στη λήψη αποφάσεων από τον άνθρωπο, μετακίνηση του συνολικού συστήματος προς καταστάσεις υψηλότερου κινδύνου κλπ. Ένα μοντέλο αιτιότητας βασιζόμενο στον έλεγχο περιλαμβάνει τόσο την αποτυχία να ελέγξει τις αστοχίες των στοιχείων του συστήματος ή των αποτελεσμάτων που προκαλούν, όσο και τις περιπτώσεις όπου οι αλληλεπιδράσεις μεταξύ των στοιχείων (συνολικός σχεδιασμός του συστήματος) ήταν το πρόβλημα και όχι οι αστοχίες των στοιχείων του συστήματος. Επομένως, η STAMP επεκτείνει το κλασικό μοντέλο συμπεριλαμβάνοντας το ως υποσύνολο.

Για να κατανοήσουμε το "γιατί" πίσω από τα ατυχήματα, πρέπει να δούμε πέρα από τα γεγονότα, τους λόγους για τους οποίους συνέβησαν αυτά τα γεγονότα. Στην ουσία, η STAMP έχει ως αποτέλεσμα μια αλλαγή στην έμφαση των μοντέλων από την αποτροπή αστοχιών - αποτυχιών στην επιβολή περιορισμών ασφαλείας στη συμπεριφορά του συστήματος (το οποίο περιλαμβάνει την αποτροπή αποτυχιών αλλά και πολλά περισσότερα).

Η STAMP περιλαμβάνει τρεις βασικές έννοιες:

i. περιορισμούς ασφαλείας που περιγράφηκαν παραπάνω (safety constrains)
ii. ιεραρχικές δομές ελέγχου ασφάλειας (hierarchical safety control structures)
iii. μοντέλα διαδικασιών (process models).

2.6.1 Ιεραρχικές δομές ελέγχου ασφάλειας

Μια ιεραρχική δομή ελέγχου ασφάλειας είναι ένα παράδειγμα της πιο γενικής θεωρίας συστημάτων στην έννοια της ιεραρχικής δομής ελέγχου. Ο στόχος της δομής ελέγχου ασφάλειας (Safety Control Structures) είναι η επιβολή περιορισμών ασφαλείας και κατά συνέπεια η εξάλειψη ή η μείωση των απωλειών.

Δύο βασικές δομές ιεραρχικού ελέγχου αποτελούν η ανάπτυξη του συστήματος και οι λειτουργίες του συστήματος μαζί με τις μεταξύ τους αλληλεπιδράσεις. Μεταξύ κάθε επιπέδου του συστήματος υπάρχει ένας βρόγχος ελέγχου ανάδρασης όπως ορίζεται και στη θεωρία συστημάτων. Τα υψηλότερα επίπεδα ελέγχου παρέχουν μια συνολική πολιτική ασφαλείας, πρότυπα και διαδικασίες και λαμβάνουν αναδράσεις σχετικά με τις επιπτώσεις τους σε διάφορους τύπους αναφορών, συμπεριλαμβανομένων των αναφορών περιστατικών και ατυχημάτων. Τα κατώτερα επίπεδα εφαρμόζουν αυτές τις πολιτικές και διαδικασίες. Η ανάδραση παρέχει τη δυνατότητα εκμάθησης και βελτίωσης της αποτελεσματικότητας των ελέγχων ασφαλείας.

Ένας κατασκευαστής αεροσκαφών, για παράδειγμα, μπορεί να έχει μόνο το σύστημα ανάπτυξης του αεροσκάφους υπό άμεσο έλεγχο, αλλά η ασφάλεια αφορά τόσο την ανάπτυξη όσο και την επιχειρησιακή χρήση του αεροσκάφους και καμία δεν μπορεί να επιτευχθεί επιτυχώς μεμονωμένα: η ασφάλεια πρέπει να σχεδιαστεί στο

αεροσκάφος και η ασφάλεια κατά τη διάρκεια λειτουργίας του εξαρτάται εν μέρει από τον αρχικό σχεδιασμό και εν μέρει από τον αποτελεσματικό έλεγχο των λειτουργιών. Οι κατασκευαστές πρέπει να γνωστοποιούν στους πελάτες τους τις παραδοχές σχετικά με το επιχειρησιακό περιβάλλον στο οποίο βασίστηκε η αρχική ανάλυση ασφάλειας, για παράδειγμα, την ποιότητα και τις διαδικασίες συντήρησης, καθώς και πληροφορίες σχετικά με τις ασφαλείς διαδικασίες λειτουργίας του αεροσκάφους. Το επιχειρησιακό περιβάλλον, με τη σειρά του, παρέχει ανατροφοδότηση στον κατασκευαστή σχετικά με την απόδοση του συστήματος κατά τη διάρκεια λειτουργίας του.

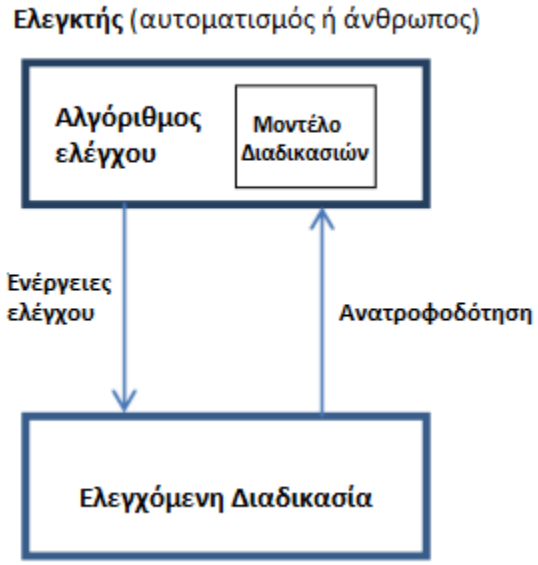
Πρόσθετες δομές ελέγχου μπορούν να συμπεριληφθούν, οι οποίες έχουν ευθύνη για μια διαφορετική πτυχή του συστήματος, όπως μια δομή ελέγχου για την προστασία του κοινού (έλεγχος της δημόσιας υγείας) παρέχοντας άμεση επέμβαση σε παραβιάσεις των περιορισμών ασφαλείας που μπορούν να οδηγήσουν σε επιπτώσεις στην υγεία ή το περιβάλλον.

Κάθε στοιχείο της ιεραρχικής δομής ελέγχου ασφάλειας έχει ευθύνες για την επιβολή των περιορισμών ασφαλείας που είναι κατάλληλες για το συγκεκριμένο στοιχείο και μαζί αυτές οι ευθύνες θα πρέπει να έχουν ως αποτέλεσμα στην επιβολή ενός συνολικού περιορισμού του συστήματος ασφάλειας. Μέρος του ορισμού της δομής ελέγχου ασφάλειας είναι ο προσδιορισμός των προσδοκιών, των ευθυνών, της εξουσίας και της ευθύνης σε σχέση με την επιβολή περιορισμών ασφαλείας για κάθε στοιχείο σε κάθε επίπεδο. Αυτές οι ευθύνες, η εξουσία, κ.λπ., στο σύνολό τους πρέπει να επιβάλλουν τους περιορισμούς ασφαλείας του συστήματος στο φυσικό σχεδιασμό, στις λειτουργίες, στη διαχείριση, στις κοινωνικές αλληλεπιδράσεις και στην κουλτούρα.

2.6.2 Μοντέλα διαδικασιών

Οι βρόχοι ελέγχου υπάρχουν μεταξύ κάθε επιπέδου της δομής ελέγχου της ασφάλειας, ακόμη και μεταξύ εκείνων στο επίπεδο διαχείρισης και οργάνωσης. Κάθε μηχανισμός ελέγχου (controller) περιέχει έναν αλγόριθμο απόφασης για το ποιες ενέργειες ελέγχου (control actions) πρέπει να παρέχει. Αυτός ο αλγόριθμος χρησιμοποιεί ένα μοντέλο της τρέχουσας κατάστασης του συστήματος που ελέγχει, ώστε να βοηθήσει στη λήψη αυτής της απόφασης. Στην Εικόνα 15 φαίνεται ένας πολύ απλός βρόχος ελέγχου με ανάδραση. Στον μηχανισμό ελέγχου έχουν εκχωρηθεί απαιτήσεις για την επιβολή της ελεγχόμενης διαδικασίας συμπεριφοράς, την οποία εκτελεί εκδίδοντας δράσεις ελέγχου για να αλλάξει την κατάσταση της ελεγχόμενης διαδικασίας. Για τους μηχανισμούς ελέγχου σε μια δομή ελέγχου ασφαλείας, οι καθορισμένες απαιτήσεις πρέπει να εξασφαλίζουν ότι οι περιορισμοί ασφαλείας διατηρούνται στην ελεγχόμενη διαδικασία.

Σε ένα σύστημα ελέγχου της εναέριας κυκλοφορίας, για παράδειγμα, ο ελεγκτής εναέριας κυκλοφορίας μπορεί να αναλάβει την ευθύνη για τη διατήρηση ασφαλούς διαχωρισμού μεταξύ των αεροσκαφών. Ο ελεγκτής εκδίδει συμβουλές στο αεροσκάφος για να διασφαλίσει ότι δεν θα προκύψει απώλεια του ελάχιστου κινδύνου διαχωρισμού.



Εικόνα 15: Απλοποιημένο σχεδιάγραμμα ροής διαδικασιών σε ένα βρόχο ελέγχου

Ο αλγόριθμος ελέγχου χρησιμοποιεί πληροφορίες σχετικά με την κατάσταση των διαδικασιών (που περιέχεται στο μοντέλο διαδικασιών) για να παράγει εκείνες τις ενέργειες ελέγχου που θα επιτρέψουν στην διαδικασία να φέρει σε πέρας τις απαιτήσεις (δηλαδή τη διατήρηση των περιορισμών ασφαλείας) που έχουν ανατεθεί σε αυτόν τον συγκεκριμένο μηχανισμό ελέγχου. Σε ένα ανθρώπινο μηχανισμό ελέγχου, το μοντέλο της διαδικασίας ονομάζεται συνήθως «ψυχικό μοντέλο». Αυτό το μοντέλο διαδικασίας περιλαμβάνει υποθέσεις σχετικά με τον τρόπο λειτουργίας και την τρέχουσα κατάσταση της ελεγχόμενης διαδικασίας.

Για παράδειγμα, εάν ένας απλός θερμοστάτης ελέγχει τη θερμοκρασία σε ένα δωμάτιο, θα καθορίσει εάν η θερμοκρασία του δωματίου είναι στο καθορισμένο σημείο ρύθμισης. Αν όχι, ο μηχανισμός ελέγχου δημιουργεί ένα έλεγχο. Ένας τρόπος που μπορεί να συμβεί ένα ατύχημα σε ένα τέτοιο σύστημα είναι όταν το μοντέλο διαδικασιών του μηχανισμού ελέγχου γίνεται ασύμβατο με την πραγματική κατάσταση της ελεγχόμενης διαδικασίας και ο μηχανισμός ελέγχου παρέχει μια επισφαλή ενέργεια ελέγχου στη διαδικασία. Όταν υπάρχουν πολλαπλοί μηχανισμοί ελέγχου, οι οποίοι παρέχουν οδηγίες ελέγχου στην ίδια διαδικασία (συμπεριλαμβανομένης της περίπτωσης όπου οι πολλαπλοί μηχανισμοί ελέγχου μπορεί να είναι μείγμα ανθρώπων και υπολογιστών), τα ατυχήματα μπορούν επίσης να προκύψουν όταν παρέχονται αντιφατικές ενέργειες ελέγχου, ίσως λόγω ασυμβατότητας μεταξύ των μεμονωμένων μοντέλων διαδικασιών του μηχανισμού ελέγχου. Πρόκληση για το σχεδιασμό μιας αποτελεσματικής δομής ελέγχου ασφάλειας αποτελεί η παροχή των απαραίτητων αναδράσεων και εισροών ώστε να διατηρηθούν τα μοντέλα σε συνέπεια (συμβατότητα) με την πραγματική κατάσταση της ελεγχόμενης διαδικασίας αλλά και μεταξύ τους.

Υπάρχουν τέσσερις γενικοί τύποι επισφαλούς ενέργειας ελέγχου:

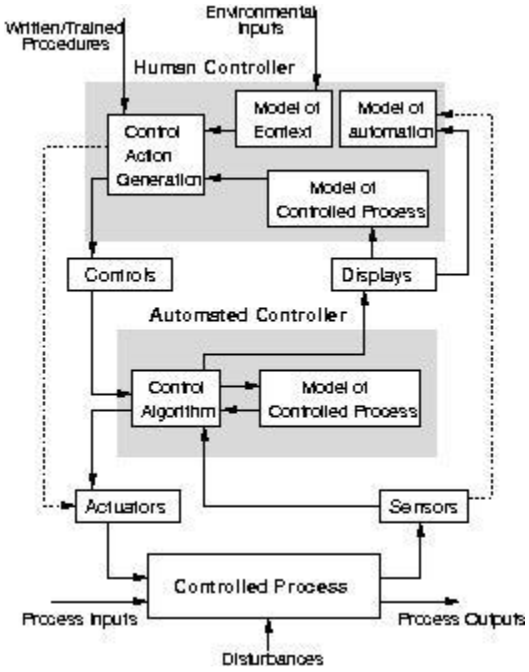
1. Μια επισφαλήσ ενέργεια ελέγχου πραγματοποιείται η οποία δημιουργεί μια επικίνδυνη κατάσταση (π.χ., ένας ελεγκτής εναέριας κυκλοφορίας εκδίδει συμβουλές που οδηγούν σε απώλεια διαχωρισμού δυο αεροσκαφών που διαφορετικά δεν θα συνέβαινε)
2. Μια απαιτούμενη ενέργεια ελέγχου δεν πραγματοποιείται ώστε να αποφευχθεί μια επισφαλήσ κατάσταση (π.χ. ο ελεγκτής εναέριας κυκλοφορίας δεν εκδίδει μια συμβουλή που απαιτείται για να διατηρηθεί ο ασφαλής διαχωρισμός)
3. Μια ενδεχομένως ασφαλή ενέργεια ελέγχου πραγματοποιείται πολύ αργά, πολύ νωρίς ή σε λάθος σειρά
4. Μια ασφαλής ενέργεια ελέγχου πραγματοποιείται για υπερβολικά μεγάλη διάρκεια ή σταματάει πολύ σύντομα (π.χ. ο πιλότος εκτελεί έναν απαιτούμενο ελιγμό ανόδου αλλά συνεχίζει το πέρασμα από το επιτρεπόμενο επίπεδο πτήσης)

Υπάρχει και ένα πέμπτο σενάριο όπου μια ενέργεια ελέγχου που απαιτείται για την επιβολή ενός περιορισμού ασφαλείας (αποφυγή κινδύνου) πραγματοποιείται αλλά δεν ακολουθείται. Η αιτία αυτού του πέμπτου σεναρίου συνεπάγεται την ανεπαρκή συμπεριφορά (ίσως αποτυχία ή καθυστέρηση) ενός τμήματος του βρόχου ελέγχου εκτός του μηχανισμού ελέγχου (όπως η διαδικασία ελέγχου, οι αισθητήρες ή οι σύνδεσμοι επικοινωνίας).

Αυτά τα πέντε σενάρια είναι ένα πολύ καλύτερο μοντέλο αιτιωδών ατυχημάτων που σχετίζονται με ενέργειες ενός ανθρώπου ή ενός υπολογιστή σε αντίθεση με ένα απλό μοντέλο που λέει ότι «απέτυχαν» χωρίς άλλες πληροφορίες για το γιατί. Χωρίς να κατανοήσουμε τα αίτια των «αποτυχιών», οι επιλογές για την εξάλειψή τους ή για τη μείωση τους είναι περιορισμένες. Η STPA χρησιμοποιεί τους τέσσερις τύπους επισφαλών ενεργειών ελέγχου μαζί με τον πέμπτο λόγο για επισφαλή έλεγχο για τον εντοπισμό δυνητικών αιτιών επικίνδυνων συμπεριφορών, συνυπολογίζοντας αυτές που σχετίζονται είτε με λογισμικό είτε με τον άνθρωπο. Τα αναγνωρισμένα σενάρια (αιτίες κινδύνου) μπορούν στη συνέχεια να χρησιμοποιηθούν για την εξάλειψη των αιτίων από το σύστημα ή, εάν αυτό δεν είναι εφικτό ή πρακτικό, για τον περιορισμό τους. Ο περιορισμός αυτός μπορεί να συνεπάγεται την αλλαγή οποιουδήποτε τμήματος του βρόγχου ελέγχου (τις καθορισμένες ευθύνες, τον σχεδιασμό της ελεγχόμενης διαδικασίας, τον αλγόριθμο ελέγχου, το μοντέλο διαδικασίας, τις ενέργειες ελέγχου, τη σχεδιαζόμενη ανατροφοδότηση, το σύνδεσμο επικοινωνίας κ.λπ.).

Αν η STPA χρησιμοποιείται από την αρχή στη διαδικασία δημιουργίας και σχεδίασης του συστήματος, τα αποτελέσματα της ανάλυσης μπορούν να χρησιμοποιηθούν για να δημιουργηθούν οι απαιτήσεις του συστήματος και του υποσυστήματος και να δημιουργηθεί ένας ασφαλέστερος σχεδιασμός από την αρχή, ώστε οι αλλαγές να μην χρειαστούν αργά στην διαδικασία σχεδιασμού και ανάπτυξης.

Στην Εικόνα 16 φαίνεται ένα πιο λεπτομερές (και ρεαλιστικό) μοντέλο, όπου μια ελεγχόμενη διαδικασία (controlled process) ελέγχεται από έναν αυτομα-τοποιημένο μηχανισμό ελέγχου (automated controller), ο οποίος, με τη σειρά του, ελέγχεται από έναν ανθρώπινο μηχανισμό ελέγχου (human controller).



Εικόνα 16: Ένα πιο λεπτομερές μοντέλο ελέγχου

Οι πληροφορίες σχετικά με την κατάσταση της ελεγχόμενης διεργασίας (ανάδραση) παρέχονται από αισθητήρες (sensors) ενώ οι ενέργειες ελέγχου εφαρμόζονται στην ελεγχόμενη διαδικασία από ενεργοποιητές (actuators). Ένας αυτοματοποιημένος ελεγκτής συχνά διαμεσολαβεί μεταξύ των ανθρώπινων ελεγκτών και της ελεγχόμενης διαδικασίας. Ο άνθρωπος μπορεί να έχει άμεση πρόσβαση στους ενεργοποιητές αλλά συνήθως εκδίδει οδηγίες στον αυτοματοποιημένο μηχανισμό ελέγχου μέσω φυσικών ή ηλεκτρονικών χειρισμών. Η αυτοματοποιημένη διαδικασία μπορεί επίσης να βοηθήσει στην ανάδραση και να την παρέχει στον ανθρώπινο μηχανισμό ελέγχου μέσω διαφόρων τύπων απεικονίσεις. Οι διακεκομμένες γραμμές υποδεικνύουν εάν ο ανθρώπινος μηχανισμός ελέγχου έχει άμεση πρόσβαση στους ενεργοποιητές και τους αισθητήρες ή αν όλες οι ενέργειες πληροφόρησης και ελέγχου πρέπει να περάσουν από μια αυτοματοποιημένη συσκευή. Σε μερικά πλήρως αυτοματοποιημένα συστήματα, δεν υπάρχει ανθρώπινος μηχανισμός ελέγχου να ελέγχει άμεσα τη φυσική διαδικασία, αν και υπάρχουν άνθρωποι σε υψηλότερα επίπεδα της δομής ελέγχου.

Ο αλγόριθμος ελέγχου στον αυτοματοποιημένο μηχανισμό ελέγχου (ο οποίος έχει προσχεδιαστεί και αλλάζει σπάνια) χρησιμοποιεί τις πληροφορίες του σχετικά με την τρέχουσα κατάσταση της ελεγχόμενης διαδικασίας για να προσδιορίσει εάν κάποια ενέργεια ελέγχου απαιτείται να σταλεί στους ενεργοποιητές ώστε να εφαρμόσει τις απαιτήσεις ελέγχου για την επιβολή των περιορισμών ασφαλείας. Αυτός ο αλγόριθμος δημιουργείται από έναν άνθρωπο χρησιμοποιώντας ένα μοντέλο διαδικασίας με βάση ποιες αυτός σκέφτεται ότι θα είναι οι λειτουργικές καταστάσεις της ελεγχόμενης διαδικασίας. Επισφαλείς αυτοματοποιημένοι αλγόριθμοι ελέγχου μπορεί να προκύψουν εάν ο σχεδιαστής του αλγορίθμου έχει μια εσφαλμένη κατανόηση της απαιτούμενης συμπεριφοράς του αυτοματοποιημένου μηχανισμού ελέγχου.

Το μοντέλο διαδικασίας στον αυτοματοποιημένο μηχανισμό ελέγχου ενημερώνεται περιοδικά μέσω της ανάδρασης από την ελεγχόμενη διαδικασία η οποία

μεταδίδεται μέσω αισθητήρων και διαβάζεται από τον αλγόριθμο ελέγχου του αυτοματοποιημένου μηχανισμού ελέγχου και χρησιμοποιείται για την αλλαγή του εσωτερικού μοντέλου διαδικασίας.

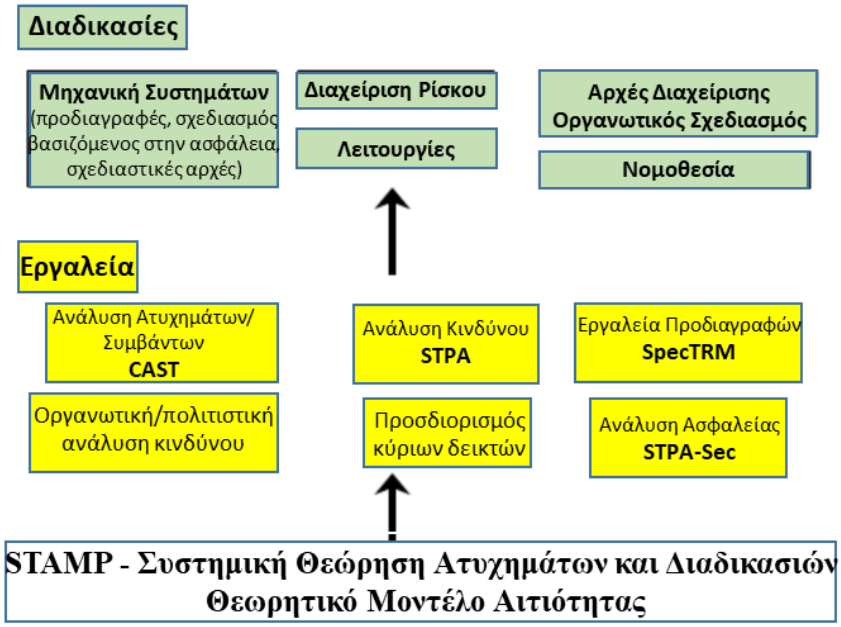
Σε αντίθεση με τον αυτοματοποιημένο μηχανισμό ελέγχου, ο ανθρώπινος είναι μια γεννήτρια ενεργειών ελέγχου αντί ενός σταθερού αλγόριθμου. Οι άνθρωποι μπορεί να είναι εφοδιασμένοι με κανόνες ή διαδικασίες που πρέπει να ακολουθηθούν, αλλά ένα πλεονέκτημα της ύπαρξης ενός ανθρώπου στον βρόγχο είναι η ευελιξία στο να αλλάξει τις διαδικασίες ή να δημιουργήσει νέες σε μια κατάσταση που δεν είχε προβλεφθεί ή να βελτιώσει τον αλγόριθμο ελέγχου χωρίς να χρειάζεται να περάσει από μια μακρά διαδικασία σχεδιασμού και υλοποίησης.

Μια υπεραπλούστευση της Εικόνα 15 είναι ότι υπάρχει μόνο ένας μηχανισμός ελέγχου και μία ελεγχόμενη διαδικασία, ενώ στην πραγματικότητα μπορεί να υπάρχουν πολλοί περισσότερες από καθεμιά. Πολλαπλοί μηχανισμοί ελέγχου για την ίδια διαδικασία ή διαδικασίες οι οποίες χρειάζονται κάποιο τρόπο συντονισμού με τις ενέργειες ελέγχου ώστε να αποφευχθεί μια επικίνδυνη κατάσταση του συστήματος.

Συνοψίζοντας, χρησιμοποιώντας το μοντέλο αιτιότητας ατυχημάτων STAMP, τα ατυχήματα συμβαίνουν όταν η δομή ελέγχου ασφαλείας δεν επιβάλλει τους περιορισμούς ασφαλείας του συστήματος και επικίνδυνες καταστάσεις προκύπτουν από:

1. Μη διαχειρίσιμες περιβαλλοντικές διαταραχές ή συνθήκες
2. Μη διαχειρίσιμες ή μη ελεγχόμενες αστοχίες των στοιχείων του συστήματος
3. Επισφαλείς αλληλεπιδράσεις μεταξύ των στοιχείων του συστήματος
4. Ανεπαρκώς συντονισμένες ενέργειες ελέγχου από πολλαπλούς μηχανισμούς ελέγχου

Το ενδεχόμενο για ένα επισφαλή έλεγχο μπορεί να υπάρχει στον αρχικό σχεδιασμό της δομής ελέγχου ασφαλείας ή η δομή ελέγχου ασφάλειας και οι έλεγχοι της ενδέχεται να υποβαθμιστούν με την πάροδο του χρόνου, επιτρέποντας στο σύστημα να μετακινηθεί σε καταστάσεις αυξανόμενου κινδύνου.



Εικόνα 17: Εργαλεία και διαδικασίες που μπορούν να ενσωματωθούν στην STAMPστο μέλλον

Η STAMP είναι μόνο ένα μοντέλο αιτιωδών ατυχημάτων και δεν είναι μια τεχνική ανάλυση αστοχιών. Χρησιμοποιώντας τη STAMP ως θεωρητική βάση, ωστόσο, μπορούν να κατασκευαστούν νέα και πιο ισχυρά εργαλεία και διαδικασίες. Η Εικόνα 17 δείχνει μερικά από αυτά τα εργαλεία και τις διαδικασίες που μπορούν να εφαρμοστούν στην STAMP στο μέλλον.

2.7 Χρήση STPA στην Ανάλυση Επικινδυνότητας

Η μέθοδος STPA (Systems Theoretic Process Analysis, Συστημική Ανάλυση Διαδικασιών Ελέγχου) είναι μια τεχνική ανάλυσης κινδύνου που ενσωματώνει το μοντέλο αιτιότητας ατυχημάτων της STAMP. Ως εκ τούτου, βασίζεται στη θεωρία ελέγχου συστημάτων αντί της αξιοπιστίας του εξοπλισμού που χαρακτηρίζει τις προηγούμενες τεχνικές ανάλυσης κινδύνου. Οπως όλες οι τεχνικές ανάλυσης κινδύνου, η STPA έχει σκοπό τη συγκέντρωση πληροφοριών σχετικά με το πώς μπορεί να προκύψουν κίνδυνοι (σενάρια). Αυτές οι πληροφορίες μπορούν στη συνέχεια να χρησιμοποιηθούν για την εξάλειψη, τη μείωση και τον έλεγχο των κινδύνων στο σχεδιασμό, την ανάπτυξη, την κατασκευή και τις λειτουργίες του συστήματος.

Η STPA δεν παράγει μια αριθμητική εκτίμηση της πιθανότητας σχετικά με τον κίνδυνο. Ο μόνος τρόπος για να υπολογιστεί η πιθανότητα ενός ατυχήματος σε σύνθετα συστήματα είναι να παραλείψουμε σημαντικούς αιτιώδεις παράγοντες που δεν είναι στοχαστικοί ή για τους οποίους δεν υπάρχουν αξιόπιστες πληροφορίες (ιδιαίτερα για νέους σχεδιασμούς για τους οποίους δεν υπάρχουν ιστορικά στοιχεία). Η εκτίμηση πιθανοτήτων που δεν αντικατοπτρίζουν με ακρίβεια τον πραγματικό κίνδυνο μπορεί να είναι παραπλανητικές και ίσως οδηγήσουν σε εφησυχασμό. Ετσι, ειναι δυνατόν να μην διορθωθούν καποια σχεδιαστικά ελαττάματα και να οδηγησούν σε ατυχήματα.

Σε αντίθεση με τις παραδοσιακές τεχνικές ανάλυσης επικινδυνότητας, η STPA είναι ισχυρότερη όσον αφορά τον εντοπισμό των πιο αιτιωδών παραγόντων και επικίνδυνων σεναρίων, ιδίως εκείνων που σχετίζονται με το λογισμικό, το σχεδιασμό του συστήματος και την ανθρώπινη συμπεριφορά. Ο ισχυρισμός αυτός μπορεί να υποστηριχθεί τόσο από θεωρητικό επιχείρημα όσο και από την εμπειρία με τη χρήση του σε μια μεγάλη ποικιλία συστημάτων.

Επειδή η STPA είναι μια ιεραρχική προσέγγιση ελέγχου των συστημάτων μπορεί να χρησιμοποιηθεί νωρίς στη διαδικασία ανάπτυξης του συστήματος για τη δημιουργία υψηλού επιπέδου απαιτήσεων και περιορισμούς ασφαλείας. Αυτές οι υψηλού επιπέδου απαιτήσεις μπορούν να βελτιωθούν χρησιμοποιώντας την STPA για καθοδήγηση στη διαδικασία σχεδιασμού του συστήματος και τη δημιουργία λεπτομερών απαιτήσεων ασφαλείας για τα μεμονωμένα στοιχεία του συστήματος. Στο σχεδιασμό με κατεύθυνση την ασφάλεια:

- Η ανάλυση επικινδυνότητας επηρεάζει και διαμορφώνει τις πρώτες σχεδιαστικές αποφάσεις και
- Η ανάλυση επικινδυνότητας επαναλαμβάνεται και διαμορφώνεται καθώς εξελίσσεται ο σχεδιασμός.

Αυτή η διαδικασία σχεδιασμού με προσανατολισμό στην ασφάλεια είναι εξαιρετικά χρήσιμη, καθώς το κόστος της επανεπεξεργασίας όταν τα ελαττώματα σχεδιασμού βρίσκονται αργά είναι τεράστιο. Όταν η ανάλυση επικινδυνότητας μπορεί

να γίνει νωρίς και σε συμφωνία με τις αποφάσεις σχεδιασμού, το κόστος καθίσταται αμελητέο.

Η STPA όπως και οι άλλες τεχνικές μπορεί να χρησιμοποιηθεί σε ένα ολοκληρωμένο σχεδιασμό ή σε ένα υπάρχον σύστημα. Σε ειδική περίπτωση, μπορεί να χρησιμοποιηθεί (όπως και άλλες τεχνικές ανάλυσης κινδύνου) και στη διερεύνηση των ατυχημάτων με σκοπό τη δημιουργία τυποποιημένων σεναρίων τα οποία μπορούν να αξιολογηθούν ως προς τη συνάφεια τους με τα πραγματικά γεγονότα που συνέβησαν.

Υπάρχουν και άλλα μοναδικά χαρακτηριστικά της STPA. Επειδή λειτουργεί στην ιεραρχική δομή ελέγχου ασφαλείας, μπορεί να χρησιμοποιηθεί τόσο στο τεχνικό σχεδιασμό όσο και στον οργανωτικό σχεδιασμό. Για παράδειγμα, μπορεί να εντοπιστεί η επίδραση της λήψης αποφάσεων της διοίκησης και της συμπεριφοράς στα ατυχήματα. Μπορεί επίσης να χρησιμοποιηθεί στη κλασσική ανάλυση κινδύνου έργων αλλά και σε άλλα είδη ανάλυσης κινδύνου.

2.8 Διαδικασία ανάπτυξης μιας ανάλυσης STPA

Η STPA υποστηρίζει και βασίζεται σε μια ιεραρχική θεώρηση της μηχανικής των συστημάτων. Αυτό το γεγονός δεν πρέπει να αποτελεί έκπληξη καθώς η θεωρία συστημάτων παρέχει ένα κοινό θεωρητικό υπόβαθρο και για τα δύο. Η διαδικασία μπορεί να χωριστεί σε τέσσερα μέρη, αν και οι διάφορες δραστηριότητες θα μπορούσαν να αλληλοσυνδεθούν και, στις πιο αποτελεσματικές χρήσεις, η STPA γίνεται μια επαναληπτική διαδικασία με λεπτομέρειες που προστίθενται καθώς ο σχεδιασμός του συστήματος εξελίσσεται:

1. Καθορισμός των θεμελίων των διαδιακασιών του συστήματος για την ανάλυση και την ανάπτυξη του συστήματος
2. Κατασκευή δομής λειτουργικού ελέγχου του συστήματος
3. Αναγνώριση των δυνητικά επισφαλών ενέργειων ελέγχου και χρήση αυτών ώστε να αναπτυχθούν απαιτήσεις και περιορισμοί ασφαλείας
4. Προσδιορισμός των αιτιών των δυνητικά επισφαλών ενέργειων ελέγχου

2.8.1 Καθορισμός των θεμελίων της μηχανικής συστημάτων

Η STPA ξεκινά από τις βασικές δραστηριότητες της πρώιμης μηχανικής του συστήματος που σχετίζονται με την ασφάλεια: καθορίζοντας ποια ατυχήματα ή απώλειες θα ληφθούν υπόψη κατά την ανάπτυξη, αναγνωρίζοντας τους κινδύνους που συνδέονται με αυτά τα ατυχήματα και προσδιορίζοντας τις απαιτήσεις ασφαλείας (περιορισμούς). Αφού προσδιοριστούν αυτές οι θεμελιώδεις πληροφορίες, προστίθεται μια ειδική STPA διαδικασία που σχεδιάζει την προκαταρκτική (υψηλού επιπέδου) δομή του λειτουργικού ελέγχου. Η πραγματική ανάλυση STPA θα χρησιμοποιήσει αυτή τη δομή ελέγχου.

2.8.1.1 Ατυχήματα

Ατύχημα (accidents) είναι ένα ανεπιθύμητο και απρογραμμάτιστο γεγονός το οποίο έχει σαν αποτέλεσμα μια απώλεια, συμπεριλαμβανομένης απώλειας ανθρώπινης ζωής ή τραυματισμό ανθρώπου, υλικές ζημίες, ρύπανση του περιβάλλοντος, αποτυχία αποστολής, οικονομικές ζημιές κλπ.

Ο καθορισμός του τι πρέπει να θεωρηθεί ως απώλεια ή ατύχημα σε ένα συγκεκριμένο σύστημα πρέπει να γίνει από εκείνους που έχουν αναλάβει αυτή την ευθύνη, επειδή περιλαμβάνει κατανομή πόρων και προσπάθειών και αυτά τα πράγματα δεν είναι ποτέ απεριόριστα. Για ορισμένους τύπους εξαιρετικά επικίνδυνων συστημάτων, όπως τα πυρηνικά όπλα, η κυβέρνηση συνήθως παίρνει αυτή την απόφαση. Σε ορισμένες βιομηχανίες όπου η ασφάλεια είναι ζωτικής σημασίας για την επιβίωση της βιομηχανίας, όπως η εμπορική αεροπορία, συχνά η απόφαση λαμβάνεται από εθνικές ή διεθνείς ενώσεις. Εναλλακτικά, η απόφαση μπορεί απλώς να είναι τοπική σε μια συγκεκριμένη εταιρεία, μπορεί να είναι μια απαίτηση που επιβάλλεται από ασφαλιστικές εταιρείες ή μπορεί να προκύψει από ζητήματα ευθύνης.

Πίνακας 2: Παραδείγματα ατυχημάτων και κινδύνων

Σύστημα	**Ατύχημα**	**Κίνδυνος**
Αυτόματο σύστημα ελέγχου ταχύτητας	Δυο οχήματα συγκρούονται	Ανεπαρκής απόσταση μεταξύ οχήματος και ενός εμπρός ή πίσω
Χημική μονάδα	Άνθρωποι πεθαίνουν ή τραυματίζονται εξαιτίας της έκθεσης του σε χημικές ουσίες	Χημικές ουσίες στον αέρα ή στο έδαφος μετά την απελευθέρωση από τη μονάδα
Σύστημα ελέγχου πόρτας τρένου	Ο επιβάτης πέφτει έξω από το τρένο	1. Η πόρτα είναι ανοιχτή όταν ξεκινάει το τρένο 2. Η πόρτα είναι ανοιχτή ενώ το τρένο κινείται 3. Η πόρτα δεν μπορεί να ανοίξει σε περίπτωση έκτακτης ανάγκης 4. Κλείσιμο της πόρτας ενώ κάποιος βρίσκεται στην πόρτα

Σε κάθε περίπτωση, ο ορισμός του τι πρέπει να θεωρηθεί ατύχημα ή μη αποδεκτή απώλεια σε ένα σύστημα πρέπει να γίνει πριν ξεκινήσουν οι προσπάθειες ασφαλείας, διότι καθορίζει τους στόχους και το εύρος των προσπαθειών. Παραδείγματα του τι συνήθως θεωρείται ότι είναι ατυχήματα σε διάφορους τύπους συστημάτων παρουσιάζεται παραπάνω στον Πίνακα 2.

2.8.1.2 Κίνδυνοι

Όπως και στο παραδοσιακό σύστημα ασφαλείας, όλα ξεκινούν από τους κινδύνους (hazards). Αυτή η έννοια συχνά χρησιμοποιείται με διαφορετικό τρόπο σε διαφορετικές βιομηχανίες, οπότε ο ορισμός της είναι απαραίτητος. Όταν η έννοια του κινδύνου δεν χρησιμοποιείται ή απλώς εξομοιώνεται με μια "αποτυχία", τότε η ασφάλεια δεν αντιμετωπίζεται επαρκώς και η ασφάλεια αντικαθίσταται από την αξιοπιστία. Καμία από αυτές τις δύο διαφορετικές ιδιότητες του συστήματος δεν συνεπάγεται την άλλη, οπότε η αντικατάσταση αυτή σημαίνει ότι η ασφάλεια δεν αντιμετωπίζεται.

Υπάρχουν διάφοροι ορισμοί του όρου "κίνδυνος" με κάποιους από αυτούς να είναι ασαφείς και να μην μπορούν να λειτουργήσουν σωστά. Ένας τέτοιος ορισμός αναφέρει ότι "Ο κίνδυνος είναι μια κατάσταση που αποτελεί προαπαιτούμενο για οδηγηθούμε σε ένα ατύχημα ή συμβάν". Το μειονέκτημα αυτού του ορισμού είναι ότι υπάρχει ένας πολύ μεγάλος αν όχι άπειρος αριθμός συνθηκών που προηγούνται ενός

ατυχήματος. Τα αεροσκάφη που βρίσκονται στον ελεγχόμενο εναέριο χώρο είναι προαπαιτούμενο για ένα ατύχημα ή περιστατικό, αλλά δεν μπορούμε να εξαλείψουμε αυτήν την κατάσταση από ένα σύστημα ελέγχου εναέριας κυκλοφορίας, δηλαδή να μην επιτρέψουμε αεροσκάφη στον εναέριο χώρο. Ομοίως, ένα προαπαιτούμενο για (ή μια κατάσταση που θα μπορούσε να οδηγήσει σε) μια σύγκρουση μεταξύ δύο αυτοκινήτων είναι ότι περισσότερα από ένα αυτοκίνητα είναι στον αυτοκινητόδρομο την ίδια στιγμή.

Ο ορισμός που χρησιμοποιείται στην STPA περιορίζει τους κινδύνους να είναι οι συνθήκες ή οι καταστάσεις όπου κανείς δεν θέλει ποτέ να συμβούν, όπως η παραβίαση ελάχιστων προτύπων διαχωρισμού μεταξύ των αεροσκαφών στον ελεγχόμενο εναέριο χώρο ή η ανεπαρκής απόσταση φρεναρίσματος μεταξύ αυτοκινήτων σε ένα σύστημα ελέγχου ταχύτητας ταξιδιού. Αυτές οι συνθήκες, αφού εντοπιστούν, μπορούν να εξαλειφθούν ή να ελεγχθούν στο σχεδιασμό και τις λειτουργίες του συστήματος. Όλα τα προαπαιτούμενα για ένα ατύχημα δεν μπορούν να ληφθούν υπόψη καθώς περιλαμβάνουν όλες σχεδόν τις συνθήκες που συμβαίνουν κατά τη διάρκεια κανονικών λειτουργιών.

Η μέθοδος STPA χρησιμοποιεί τον ακόλουθο πιο σαφή ορισμό για την έννοια του "κίνδυνου" όπου αναφέρεται ως "μια κατάσταση του συστήματος ή ένα σύνολο συνθηκών τα οποία μαζί με τη χείριστη περίπτωση περιβαλλοντικών συνθηκών θα οδηγήσουν σε ατύχημα (απώλεια)".

Υπάρχουν δύο σημαντικές πτυχές αυτού του ορισμού. Η πρώτη είναι ότι ένας κίνδυνος πρέπει να βρίσκεται μέσα στα όρια του συστήματος πάνω στον οποίο έχουμε τον έλεγχο. Για παράδειγμα, ένας κίνδυνος για ένα αεροσκάφος δεν είναι το βουνό ή ο καιρός, επειδή ο σχεδιαστής του αεροσκάφους ή το σύστημα ελέγχου της εναέριας κυκλοφορίας δεν έχει κανένα έλεγχο στον καιρό ή στην τοποθέτηση ενός βουνού. Σε αντίθεση, ο κίνδυνος μπορεί να είναι το αεροσκάφος να περάσει πολύ κοντά από το βουνό ή το αεροσκάφος να βρίσκεται σε μια περιοχή με κακοκαιρία. Και οι δύο αυτοί ορισμοί παρέχουν πιθανούς τρόπους αποφυγής του κίνδυνου όταν σχεδιάζετε το σύστημα. Ένας άλλος τρόπος για να εκφραστεί αυτό είναι ότι ο κίνδυνος πρέπει να είναι στον χώρο σχεδιασμού εκείνων που χτίζουν το σύστημα ή στον επιχειρησιακό χώρο εκείνων που το λειτουργούν.

Η δεύτερη πτυχή του ορισμού είναι ότι θα πρέπει να υπάρξει ένα σύνολο συνθηκών χείριστης περίπτωσης στο περιβάλλον που θα οδηγήσουν σε μια απώλεια. Εάν δεν υπάρχει σύνολο συνθηκών χείριστης περίπτωσης εκτός ή εντός των ορίων του συστήματος που θα συνδυαστεί με τον κίνδυνο ώστε να οδηγήσει σε απώλεια, τότε αυτό δεν χρειάζεται να εξεταστεί σε μια ανάλυση κινδύνου. Ακόμα και αν δύο αεροσκάφη παραβιάζουν τον ελάχιστο διαχωρισμό, οι πιλότοι μπορεί να δουν ο ένας τον άλλον και να αποφύγουν μια σύγκρουση, αλλά υπάρχουν και οι συνθήκες χείριστης περίπτωσης υπό τις οποίες το ατύχημα δεν μπορεί να αποφευχθεί, όπως χαμηλή ορατότητα, έλλειψη προσοχής από το πλήρωμα πτήσης, και γωνίες στον ορίζοντα όπου το άλλο αεροσκάφος δεν φαίνεται. Ως εκ τούτου, είναι ένας κίνδυνος.

Η χρήση του όρου "αποτυχία (failure)" σε ένα κίνδυνο δεν είναι σωστή τις περισσότερες φορές. Και αυτό γιατί πρώτα από όλα μια "αποτυχία" είναι ένα γεγονός και όχι μια κατάσταση του συστήματος και κατά δεύτερον παρέχει λίγες πληροφορίες σχετικά με τον κίνδυνο. Γενικότερα μια αποτυχία μπορεί να οδηγήσει σε μια

επικίνδυνη κατάσταση του συστήματος, αλλά είναι μια πιθανή αιτία μιας επικίνδυνης κατάστασης, όχι η κατάσταση ή ο κίνδυνος ο ίδιος.

Ένας κίνδυνος του συστήματος είναι μια κατάσταση σε επίπεδο συστήματος. Οποιαδήποτε αναφορά στα υποσυστήματα (όπως η αποτυχία ενός υποσυστήματος) δεν αποτελεί κατάσταση του συστήματος, αν και μπορεί να οδηγήσει σε μία. Τη στιγμή που οι κίνδυνοι αναγνωρίζονται, μη λεπτομερής σχεδιασμός, συμπεριλαμβανομένων των στοιχείων, υπάρχει. Για παράδειγμα, τα "φρένα ή το γκάζι λειτουργούν ψευδώς" δεν αποτελεί κίνδυνο για ένα σύστημα ελέγχου ταχύτητας ταξιδιού, ενώ η μη ελεγχόμενη επιτάχυνση ή επιβράδυνση είναι.

Ακόμη και αν μια ανάλυση γίνει μετά το σχεδιασμό ή και αν ακόμα το σύστημα υπάρχει ήδη, ξεκινώντας με τον καθορισμό των κινδύνων σε επίπεδο συστήματος (και όχι βάσης της συμπεριφοράς επικινδυνότητας που σχετίζεται με τα υποσυστήματα) είναι σημαντικό. Αλλαγές μπορεί να χρειαστεί να γίνουν στον σχεδιασμό, συμπεριλαμβανομένης της αλλαγής των στοιχείων ή των ευθυνών τους. Αν η ανάλυση ξεκινά από τους κινδύνους που καθορίζονται με βάση τα στοιχεία του συστήματος, οι αλλαγές που αφορούν άλλα στοιχεία είναι πολύ λιγότερο πιθανό να ληφθούν υπόψη από εκείνους που προσπαθούν να εξαλείψουν το πρόβλημα.

Η λίστα με τους κινδύνους θα πρέπει να είναι πολύ μικρή, μικρότερη από 10 και σίγουρα μικρότερη από 20 κινδύνους. Αν στη λίστα περιλαμβάνονται περισσότεροι κίνδυνοι, τότε η ανάλυση έχει ξεκινήσει από πολύ χαμηλό επίπεδο αφαίρεσης. Στην προσέγγιση της «μηχανικής συστημάτων» (systems engineering), ο στόχος είναι να ξεκινάει από ένα υψηλό επίπεδο αφαίρεσης και στη συνέχεια να εκκαθαρίσει κάθε επίπεδο σε ένα πιο λεπτομερές επίπεδο. Με αυτόν τον τρόπο είναι λιγότερο πιθανό να χαθεί κάτι ή να υπάρχουν κενά ή πλεονασμοί στη λίστα.

Όπως αναφέρθηκε και πιο πάνω μια λίστα με πολλούς κινδύνους είναι δύσκολο (και ίσως αδύνατο) να διαπιστωθεί αν έχει χαθεί ή ξεχαστεί κάτι λόγω του μεγάλου μεγέθους της λίστας και των πάρα πολλών διαφορετικών επιπέδων αφαίρεσης. Ένας από τους πιο ισχυρούς τρόπους όπου τα ανθρώπινα μυαλά αντιμετωπίζουν την πολυπλοκότητα είναι η ιεραρχική αφαίρεση και η εκκαθάριση. Αρχίζοντας σε ένα υψηλό επίπεδο αφαίρεσης με μια μικρή λίστα και στη συνέχεια βελτιώνοντας αυτή την λίστα με μια πιο λεπτομερή λίστα σε κάθε βήμα (από πάνω προς τα κάτω), μπορεί κανείς να είναι πιο σίγουρος για την πληρότητα, διότι κάθε μία από τις μακρύτερες λίστες αιτιών μπορούν να εντοπιστούν σε μία ή περισσότερες από τις μικρές λίστες εκκίνησης (και αντίστροφα). Με αυτή τη διαδικασία εντοπισμού, είναι επίσης ευκολότερο για τους αναθεωρητές να βρουν οποιαδήποτε ατέλεια. Η ανθρώπινη συμμετοχή και επανεξέταση των αποτελεσμάτων στην ανάλυση θα είναι πάντοτε απαραίτητη και επομένως η ατέλεια θα είναι πάντοτε πιθανή. Ωστόσο, η διάρθρωση της διαδικασίας με τρόπο που βελτιστοποιεί την ανθρώπινη επεξεργασία και επανεξέταση των αποτελεσμάτων θα μειώσει κάθε πιθανή ατέλεια.

2.8.1.3 Περιορισμοί ασφαλείας συστήματος - απαιτήσεις

Μόλις προσδιοριστούν οι κίνδυνοι υψηλού επιπέδου του συστήματος, μπορούν να μεταφραστούν σε απαιτήσεις ή περιορισμούς ασφαλείας (system safety constrains or requirements). Αυτή η διαδικασία είναι πολύ απλή αλλά σημαντική επειδή

μεταφράζει τους κινδύνους στις απαιτήσεις και τους περιορισμούς που χρειάζονται οι μηχανικοί και οι σχεδιαστές στις διαδικασίες ελέγχου του συστήματος. Μερικά παραδείγματα παρουσιάζονται στον Πίνακα 3.

Πίνακας 3: Παραδείγματα κινδύνων και των περιορισμών ασφαλείας τους

Κίνδυνος (Hazard)	**Περιορισμός Ασφαλείας - Απαιτήσεις (Safety Constraint - Requirements)**
Μη επαρκής απόσταση μεταξύ δυο οχημάτων	Τα οχήματα δεν πρέπει ποτέ να παραβιάζουν τις ελάχιστες απαιτήσεις διαχωρισμού
Χημικά στον αέρα μετά από απελευθέρωση από ένα εργοστάσιο	Χημικές ουσίες δεν πρέπει ποτέ να απελευθερώνονται ακούσια από ένα εργοστάσιο
Η πόρτα του τρένου είναι ανοιχτή όταν αυτό ξεκινάει	Το τρένο δεν πρέπει να ξεκινάει ενώ οι πόρτες του είναι ανοιχτές
Η πόρτα του τρένου είναι ανοιχτή ενώ αυτό κινείται	Οι πόρτες του τρένου δεν πρέπει να είναι ποτέ ανοιχτές ενώ αυτό κινείται

Οι δύο αυτοί όροι ("περιορισμός" και "απαιτήσεις") έχουν πολύ κοντινή εννοιολογική σημασία και συνδέονται στενά μεταξύ τους με αποτέλεσμα να είναι δύσκολος ο διαχωρισμός τους.

Μια συχνά χρήσιμη διάκριση αποτελεί η χρήση του όρου "απαίτηση" ώστε να σημαίνει τη συμπεριφορά που απαιτείται για την ικανοποίηση της αποστολής ή των στόχων του συστήματος, ενώ οι "περιορισμοί" περιγράφουν τα όρια για το πώς οι στόχοι της αποστολής μπορούν να επιτευχθούν. Η ασφάλεια μπορεί να περιλαμβάνεται και στις δύο περιπτώσεις, όταν μέρος του στόχου ή της αποστολής του συστήματος είναι η διατήρηση της ασφάλειας, όπως ο έλεγχος της εναέριας κυκλοφορίας. Σε άλλα συστήματα όμως, οι στόχοι της αποστολής και οι περιορισμοί ασφαλείας δεν επικαλύπτονται. Σε μια χημική μονάδα, για παράδειγμα, η αποστολή και οι απαιτήσεις της αποστολής περιλαμβάνουν την παραγωγή χημικών ενώ οι περιορισμοί ασφαλείας περιορίζουν τον τρόπο παραγωγής των χημικών. Οι συγκρούσεις μεταξύ στόχων και περιορισμών μπορούν πιο εύκολα να προσδιοριστούν και να επιλυθούν εάν διακρίνονται.

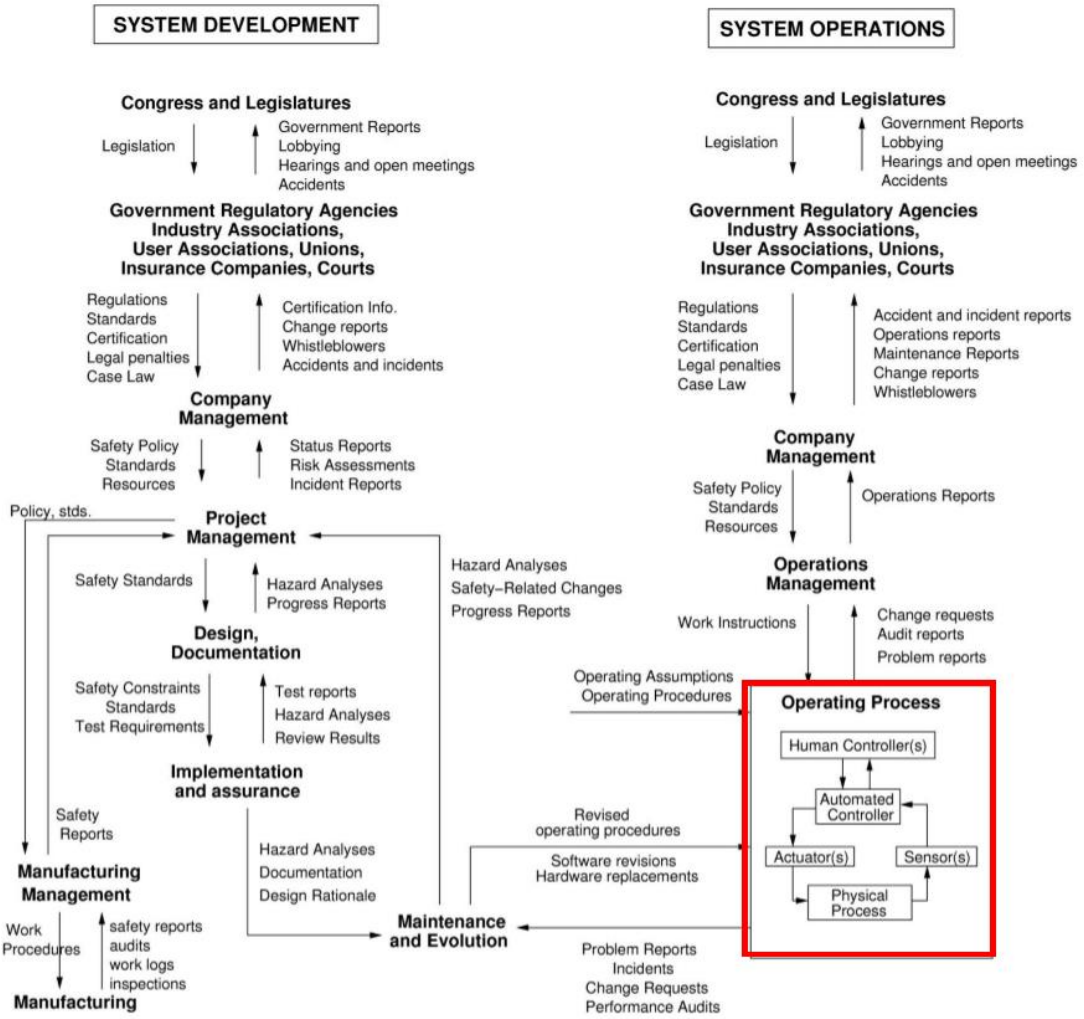
Ένας άλλος παράγοντας διαχωρισμού είναι ότι οι απαιτήσεις δεν μπορούν να έχουν αρνητικό χαρακτήρα (επειδή δεν μπορούν να ελεγχθούν) ενώ ταυτόχρονα οι περιορισμοί ασφαλείας δεν μπορούν να μεταβληθούν αποτελεσματικά σε μια θετική υποθετική δήλωση "θα". Αυτός ο διαχωρισμός είναι ιδιαίτερα χρήσιμος καθώς δίνει την δυνατότητα στους σχεδιαστές του συστήματος να ξεπεράσουν εύκολα κάποια εμπόδια, δημιουργώντας μια λίστα με τις "Δεν Πρέπει (Must Not)" δηλώσεις τις οποίες ονομάζουμε "Περιορισμούς του Συστήματος" και μία άλλη λίστα στην οποία περιλαμβάνονται όλες οι "θα" δηλώσεις οι οποίες καλούνται "Απαιτήσεις".

2.8.2 Δομή λειτουργικού ελέγχου

Η προσπάθεια που έχει περιγράφει μέχρι στιγμής (αναγνώρισης των ατυχημάτων, των κινδύνων και των απαιτήσεων ασφάλειας υψηλού επιπέδου) είναι κοινή σε όλες τις προσπάθειες των μηχανικών ασφάλειας (ή θα πρέπει να είναι) ανεξάρτητα από το είδος του μοντέλου αιτιότητας ατυχήματος ή της τεχνικής ανάλυσης επικινδυνότητας που χρησιμοποιείται. Οι μοναδικές προσπάθειες της STPA ξεκινούν

σε αυτό το σημείο. Η δημιουργία της δομής ελέγχου ασφαλείας (functional control structure) δεν αποτελεί μέρος της STPA αλλά είναι μια προσπάθεια τεκμηρίωσης του συστήματος απαραίτητη για την εκτέλεση της STPA. Ενώ πολλές από τις πτυχές που εμπλέκονται στη δημιουργία της δομής λειτουργικού ελέγχου θα περιλαμβάνουν τυπικές ενέργειες ελέγχου του συστήματος, όπως η κατανομή των απαιτήσεων του συστήματος στα στοιχεία του συστήματος, η χρήση ενός διαγράμματος λειτουργικού ελέγχου για την τεκμηρίωση αυτών των αποφάσεων δεν είναι τυποποιημένη.

Τα πιο πολύπλοκα συστήματα έχουν λεπτομερείς περιγραφές φυσικού σχεδιασμού και τεκμήρια, αλλά οι πληροφορίες σχετικά με τη λειτουργική συμπεριφορά του συστήματος είναι στην καλύτερη περίπτωση διάσπαρτες σε όλα τα τεκμήρια και μερικές φορές είναι δύσκολο να κατανοηθούν. Το μοντέλο λειτουργικού ελέγχου παρέχει μια συνοπτική, γραφική περιγραφή του λειτουργικού σχεδιασμού.



Εικόνα 18: Παράδειγμα δομής ελέγχου ασφαλείας μιας βιομηχανίας

Γενικότερα για τον ανθρώπινο νου θεωρείται ότι είναι πιο εύκολο να κατανοήσει και να παράγει διαγράμματα λειτουργικού ελέγχου ξεκινώντας με ένα πολύ απλό, υψηλού επιπέδου μοντέλο και στη συνέχεια προσθέτοντας λεπτομέρειες (επαναπροσδιορίζοντας το μοντέλο) σε βήματα. Το πρώτο βήμα μπορεί να περιέχει μόνο ένα μηχανισμό ελέγχου και μια ελεγχόμενη διαδικασία ή ίσως μερικά επίπεδα ελέγχου (ανθρώπινα και αυτοματοποιημένα). Στη συνέχεια, καθορίζεται ποιος ελέγχει

ποιον ή τι. Μόλις προσδιοριστεί η βασική δομή, μπορούν να προστεθούν λεπτομέρειες οι οποίες είναι οι ευθύνες και το μοντέλο διαδικασίας για κάθε μηχανισμό ελέγχου, οι ενέργειες ελέγχου και η ανατροφοδότηση. Οι ευθύνες είναι οι βασικές απαιτήσεις υψηλού επιπέδου για τα στοιχεία του συστήματος. Όσο η ανάλυση προχωρά, οι ευθύνες και οι απαιτήσεις σχετικά με την ασφάλεια του μηχανισμού ελέγχου θα προσδιορίζονται. Ενδέχεται επίσης να υπάρχει επικοινωνία μεταξύ των μηχανισμών ελέγχου ελεγκτών και αυτή η επικοινωνία πρέπει να παρουσιαστεί. Παραπάνω φαίνεται ένα παράδειγμα λειτουργικής δομής ελέγχου μιας βιομηχανίας.

2.8.3 Εντοπισμός επισφαλών ενεργειών ελέγχου (STPA Βήμα 1)

Ενώ είναι βολικό να χωριστεί η ανάλυση της STPA σε δύο βήματα, πρώτα να αναγνωριστούν οι επισφαλείς ενέργειες ελέγχου και στη συνέχεια οι αιτίες των επικίνδυνων ενεργειών ελέγχου, ο διαχωρισμός αυτός δεν είναι απαραίτητος. Τα δύο βήματα μπορούν να ενσωματωθούν με διάφορους τρόπους, για παράδειγμα, προσδιορίζοντας μια επισφαλή ενέργεια ελέγχου και αναζητώντας αμέσως τις αιτίες της.

Οι τέσσερις τύποι επικίνδυνων ενεργειών ελέγχου που περιεγράφηκαν και παραπάνω είναι:

- Δεν εφαρμόζεται μια ενέργεια ελέγχου που απαιτείται για την ασφάλεια
- Εφαρμόζεται μια επισφαλής ενέργεια ελέγχου που οδηγεί σε κίνδυνο
- Μια ενδεχομένως ασφαλής ενέργεια ελέγχου εφαρμόζεται πολύ αργά, πολύ νωρίς ή σε λάθος αλληλουχία
- Μια ασφαλής ενέργεια ελέγχου διακόπτεται πολύ σύντομα ή εφαρμόζεται για πάρα πολύ καιρό (για συνεχή ή μη διακριτή ενέργεια ελέγχου)

Υπάρχει ένας πέμπτος τρόπος με τον οποίο μπορεί να υπονομευθεί η ασφάλεια -παρέχεται μια απαιτούμενη ενέργεια ελέγχου, αλλά δεν ακολουθείται- αλλά αυτή η πέμπτη δυνατότητα θα αντιμετωπιστεί στο Βήμα 2 της ανάλυσης STPA.

Έχει διαπιστωθεί ότι ένας πίνακας είναι ένας κατάλληλος τρόπος καταγραφής των συγκεκριμένων επισφαλών ενεργειών ελέγχου αλλά οποιαδήποτε μορφή μπορεί να χρησιμοποιηθεί. Η γενική μορφή του πίνακα που χρησιμοποιείται είναι:

Πίνακας 4: Παρουσίαση ευρημάτων επισφαλών ενεργειών ελέγχου

Ενέργεια ελέγχου	**Δεν εφαρμόζεται μια ασφαλής ενέργεια ελέγχου**	**Εφαρμόζεται μια επισφαλής ενέργεια ελέγχου**	**Εφαρμόζεται πολύ αργά/πολύ νωρίς ή σε λάθος σειρά**	**Σταματά πολύ σύντομα ή εφαρμόζεται για μεγάλο διάστημα**

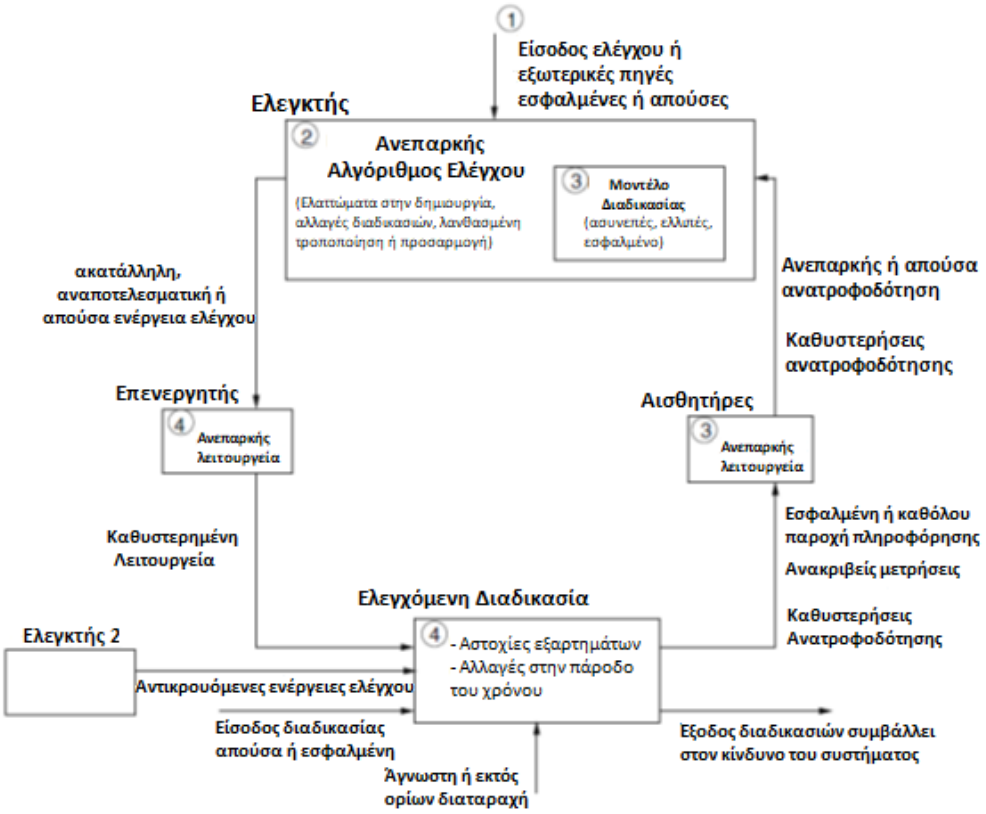
Η διακοπή της ανάλυσης μετά το Βήμα 1 μπορεί να οδηγήσει σε παραλείψεις στις απαιτήσεις και σε επισφαλές σχεδιασμό. Το Βήμα 2, το οποίο προσδιορίζει τις αιτίες των επισφαλών ενεργειών ελέγχου καθώς και τις αιτίες για τις οποίες οι απαιτούμενες ενέργειες ελέγχου μπορούν να εφαρμοστούν σωστά, εντοπίζει περισσότερες απαιτήσεις και παρέχει βοήθεια στον μηχανικό για τον εντοπισμό αλλαγών στο σχεδιασμό για την εξάλειψη ή τον μετριασμό του επισφαλούς ελέγχου.

2.8.4 Προσδιορισμός των αιτιών των επισφαλών ενεργειών ελέγχου (STPA Βήμα 2)

Μόλις προσδιοριστούν οι ενέργειες ελέγχου ασφάλειας (ή όταν εντοπιστούν οποιεσδήποτε από τις επισφαλείς ενέργειες ελέγχου), το δεύτερο και τελευταίο βήμα της STPA είναι να εντοπίσει τα πιθανά αίτια (σενάρια που οδηγούν σε) επισφαλούς ελέγχου. Εδώ εξετάζεται και το πέμπτο είδος σεναρίου, η ανεπαρκής εκτέλεση μιας ενέργειας ελέγχου που απαιτείται για την ασφάλεια.

Το βήμα 2 της STPA απαιτεί την πιο σκεπτόμενη και προηγούμενη εμπειρία από τον αναλυτή και μέχρι στιγμής υπάρχει πολύ λιγότερη βοήθεια σε σύγκριση με το Βήμα 1. Επομένως, διαπιστώνεται μερικές φορές ότι η STPA διακόπτεται μετά το Βήμα 1 ενώ το βήμα 2 είναι πολύ κρίσιμο. Το βήμα 2 της STPA προσδιορίζει πρόσθετες απαιτήσεις ασφάλειας τόσο στο σύστημα ελέγχου στον βρόχο που αναλύεται όσο και στο συνολικό σύστημα. Είναι επίσης εκεί όπου δημιουργούνται οι πληροφορίες για να βοηθήσουν τους σχεδιαστές να εξαλείψουν ή να μετριάσουν τις πιθανές αιτίες των κινδύνων. Ο σημαντικότερος λόγος για τον οποίο γίνεται μια ανάλυση κινδύνου είναι για να εξάγουμε τις αιτιώδεις πληροφορίες που παράγονται από το Βήμα 2.

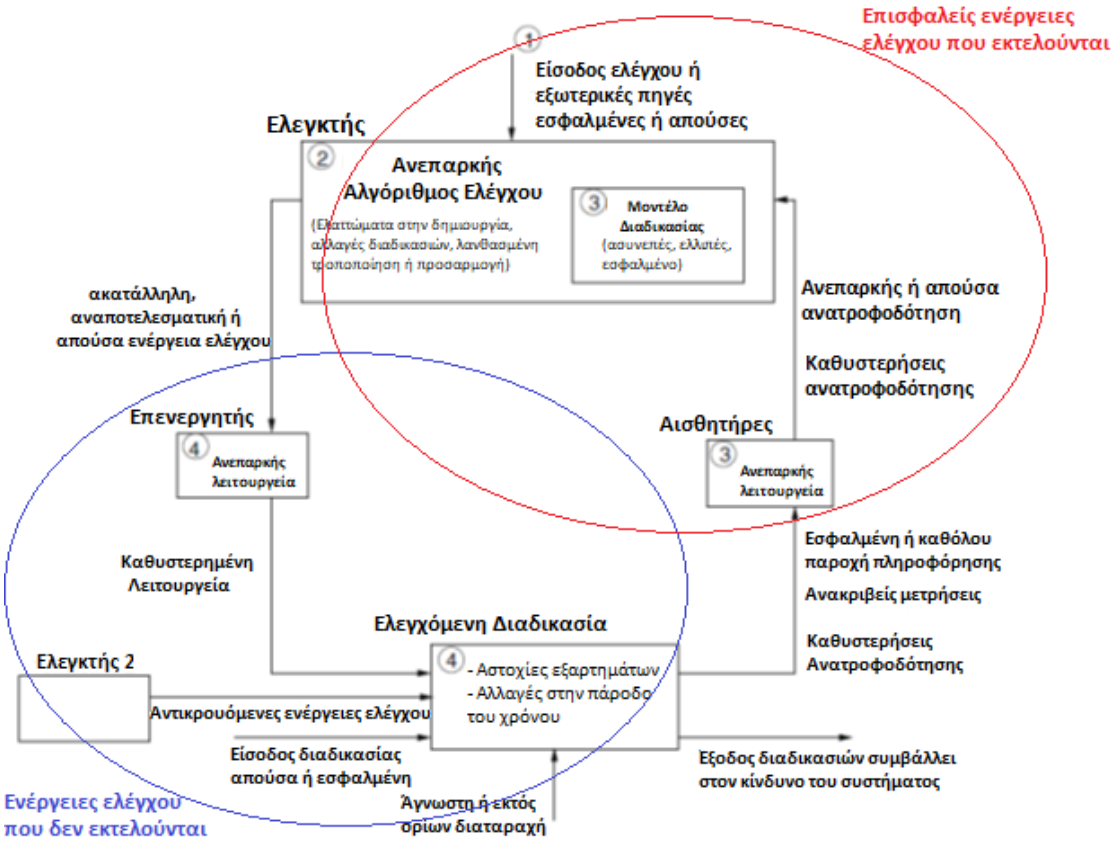
Βασικά, η διαδικασία του Βήματος 2 περιλαμβάνει την εξέταση του βρόχου ελέγχου και των τμημάτων του και τον προσδιορισμό του τρόπου με τον οποίο θα μπορούσαν να οδηγήσουν σε επισφαλή έλεγχο. Το Σχήμα 6 δείχνει τα πράγματα που μπορεί να πάνε λάθος στον βρόγχο ελέγχου.



Σχήμα 6: Πράγματα τα οποία μπορεί να πάνε στραβά σε ένα βρόχο ελέγχου

Πρέπει να ληφθεί μέριμνα ώστε να μην μετατραπεί αυτό το βήμα σε μια μορφή της FMEA ανάλυσης απλά κοιτάζοντας κάθε μία από τις "κατευθυντήριες λέξεις" στο Σχήμα 4 και βλέποντας αν αυτές οδηγούν σε κίνδυνο. Ο στόχος δεν είναι να βρεθούν απλώς αποτυχίες ή ανεπαρκής λειτουργία μεμονωμένων στοιχείων στον βρόχο ελέγχου, αλλά να βρεθούν σενάρια και συνδυασμοί προβλημάτων που θα μπορούσαν να οδηγήσουν σε επισφαλή σύστημα ελέγχου. Η διαδικασία θα πρέπει να ξεκινήσει με τις επισφαλείς ενέργειες ελέγχου και στη συνέχεια θα πρέπει να καθοριστεί ο τρόπος με τον οποίο θα μπορούσαν να συμβούν καθώς και το πώς οι ενέργειες που απαιτούνται για την ασφάλεια ενδέχεται να μην εκτελούνται σωστά.

Επειδή υπάρχουν κοινά ελαττώματα που οδηγούν σε ατυχήματα, υπάρχει η ελπίδα για μεγαλύτερη βοήθεια για το Βήμα 2 στο μέλλον, ορισμένες από τις οποίες θα μπορούσαν να υποστηριχθούν από την αυτοματοποίηση. Το βήμα 2 είναι ένας καλός χώρος για μικρές ομάδες μηχανικών να δουλέψουν μαζί περιπτώσεις καταιγισμού ιδεών (brainstorming). Το Βήμα 1 μπορεί να επιτευχθεί από ένα μόνο άτομο με μεταγενέστερη εξέταση από άλλους. Αλλά η αναγνώριση των αιτιών ενισχύεται από τη συμμετοχή πολλών ανθρώπων. Συνήθως η αιτία δημιουργίας μιας επισφαλούς ενέργειας ελέγχου μπορεί να βρεθεί στη δεξιά πλευρά του βρόχου, ενώ η αιτία της μη εκτέλεσης μιας ενέργειας ελέγχου ή της αδυναμίας της να εκτελεστεί επαρκώς βρίσκεται στην αριστερή πλευρά, αν και αυτός ο κανόνας δεν είναι πάντα αληθής. (Σχήμα 7)



Σχήμα 7: Πιθανά ελαττώματα ελέγχου που σχετίζονται με τμήματα του βρόγχου ελέγχου

Οι καθυστερήσεις στον βρόχο αποτελούν σημαντική παρατήρηση στην αιτιώδη ανάλυση. Οι καθυστερήσεις του βρόχου μπορούν να οδηγήσουν σε (προσωρινά) μη

συμβατά μοντέλα διεργασιών με τη διαδικασία και επομένως να οδηγήσουν σε ένα σύστημα ελέγχου που παρέχει ανασφαλείς ελέγχους. Ενδέχεται επίσης να υπάρχουν προβλήματα στην ενημέρωση του μοντέλου διαδικασίας.

Συνοψίζοντας, το Βήμα 2 της STPA ανάλυσης μπορεί εύκολα να αναπτυχθεί ακολουθώντας τα παρακάτω βήματα:

- Κάθε σενάριο επισφαλούς ενέργειας ελέγχου του Βήματος 1 λαμβάνεται υπόψη και αναλύεται ξεχωριστά για τον προσδιορισμό των αιτιωδών σεναρίων.
- Αναγνώριση των αιτιών μιας επικίνδυνης ενέργειας ελέγχου ή μιας ενέργειας ελέγχου που παρέχεται από το σύστημα αλλά δεν εκτελείται για κάθε σενάριο
- Ανάπτυξη λειτουργιών σχεδίασης (έλεγχοι) που θα χρησιμοποιηθούν για την προστασία του συστήματος από τα σενάρια που προέκυψαν

Κεφάλαιο 3ο Εφαρμογή μεθόδου STPA στην ανάλυση κινδύνων

Στο παρών κεφάλαιο λαμβάνοντας υπόψη την γνώση από τα προηγούμενα κεφάλαια θα προσπαθήσουμε με τη χρήση της μεθόδου STPA να κάνουμε ανάλυση επικινδυνότητας της χρήσης εκσκαφικού μηχανήματος και να εντοπίσουμε τις επικίνδυνες και επισφαλές πρακτικές (ενέργειες ελέγχου) χρήσης του καθώς και τις αιτίες τους (αιτιώδη σενάρια) και τέλος να προτείνουμε κάποιες διορθωτικές ενέργειες για την προστασία του συστήματος από τις επικίνδυνες αυτές πρακτικές που εντοπίστηκαν.

3.1 Προσδιορισμός ατυχημάτων συστήματος

Όπως αναφέραμε και στο παραπάνω κεφάλαιο ατύχημα είναι ένα οποιοδήποτε ανεπιθύμητο ή μη προγραμματισμένο συμβάν που οδηγεί σε απώλεια (loss). Το τι θεωρείται απώλεια είναι υποκειμενικό και εξαρτάται από τα ενδιαφερόμενα μέρη του συστήματος να τις εντοπίσουν. Οι πιο κοινές απώλειες που πρέπει να αποφευχθούν περιλαμβάνουν την ανθρώπινη ζωή, τον τραυματισμό των ανθρώπων, τη ζημιά σε ακίνητα και τη περιβαλλοντική ρύπανση ενώ η ιδέα μπορεί να επεκταθεί ώστε να περιλαμβάνει την απώλεια λειτουργικότητας, ώστε να μπορεί να θεωρηθεί ατύχημα η απώλεια της αποστολής ή η δυσλειτουργία του συστήματος. Παρακάτω παρατίθενται τα ατυχήματα σχετικά με τον χειρισμό εκσκαφικού μηχανήματος με παραδείγματα και σύντομες περιγραφές τα οποία προσπαθούν να περιγράψουν στο σύνολο τους όλες τις περιπτώσεις απωλειών. Ωστόσο, μερικές γνωστές εξαιρέσεις και παραλείψεις συζητούνται μετά την παρουσίαση των ατυχημάτων.

A-1: Τραυματισμός (ή απώλεια) χειριστή

Περιγραφή: Περιλαμβάνει όλα τα ατυχήματα τα οποία μπορεί να οδηγήσουν σε τραυματισμό (ή απώλεια) του χειριστή ανεξαρτήτως αν συμπεριλαμβάνονται και σε άλλη κατηγορία ατυχήματος ταυτόχρονα.

Παράδειγμα: Υπέρβαση ορίου φόρτωσης του εκσκαφέα σε επίπεδο με κλίση με αποτέλεσμα την ανατροπή του και τον τραυματισμό του χειριστή.

A-2: Φθορά ή καταστροφή του εκσκαφικού μηχανήματος

Περιγραφή: Περιλαμβάνονται όλες οι λανθασμένες ενέργειες που μπορεί να οδηγήσουν σε φθορά μικρής ή μεγάλης έκτασης του εκσκαφικού μηχανήματος και έως και καταστροφής του.

Παράδειγμα: Παράλειψη ελέγχου της στάθμης ελαίου του κινητήρα πριν την εκκίνηση του μηχανήματος. Σε πραγματική κατάσταση μειωμένης στάθμης ελαίου στον κινητήρα, αυτό θα προκαλέσει φθορά και έως ολική καταστροφή του κινητήρα του εκσκαφικού μηχανήματος.

Α-3: Τραυματισμός (ή απώλεια)τρίτων εργαζόμενων ή περαστικών

Περιγραφή: Περιγράφονται τα ατυχήματα τα οποία έχουν σαν αποτέλεσμα τον τραυματισμό ή την απώλεια οποιουδήποτε ανθρώπου (είτε εργαζόμενου στο χώρο είτε περαστικού) γύρω από την περιοχή εκσκαφής.

Παράδειγμα: Πορεία του εκσκαφέα με ανασηκωμένο τον κάδο φόρτωσης με αποτέλεσμα την μειωμένη ορατότητα του χειριστή η οποία μπορεί να οδηγήσει σε σοβαρό τραυματισμό είτε κάποιου εργαζόμενου στο χώρο είτε κάποιου περαστικού.

Α-4: Φθορά εξοπλισμού ή εγκαταστάσεων γύρω από την περιοχή εκσκαφής

Περιγραφή: Συμπεριλαμβάνονται τα ατυχήματα που αφορούν φθορά ή καταστροφή είτε εξοπλισμού είτε εγκαταστάσεων γύρω από την περιοχή του τόπου εκσκαφής λόγω κακών εκτιμήσεων και χειρισμών του χειριστή είτε κακής μελέτης του έργου.

Παράδειγμα: Μη ορθά μελετημένη εκσκαφή σε χώρο εντός πόλεως με αποτέλεσμα την καταστροφή σωληνώσεων υδροδότησης της πόλης.

Πίνακας 5: Ατυχήματα συστήματος (System Level Accidents)

Ατύχημα	Περιγραφή
Α-1	Τραυματισμός (ή απώλεια) χειριστή
Α-2	Φθορά ή καταστροφή του εκσκαφικού μηχανήματος
Α-3	Τραυματισμός (ή απώλεια) τρίτων εργαζόμενων ή περαστικών
Α-4	Φθορά εξοπλισμού ή εγκαταστάσεων γύρω από την περιοχή εκσκαφής

Θα πρέπει να αναφέρουμε ότι για λόγους απλοποίησης του εξεταζόμενου προβλήματος, στα παραπάνω σενάρια ατυχημάτων δεν έχουν συμπεριληφθεί περιπτώσεις ατυχημάτων που οφείλονται σε κάποιο κατασκευαστικό σφάλμα ή σε κάποιο σφάλμα ή παράλειψη συντήρησης του μηχανήματος.

3.2 Προσδιορισμός κινδύνων συστήματος

Το επόμενο βήμα μετά τον εντοπισμό των μη αποδεκτών απωλειών και των σχετικών ατυχημάτων είναι ο προσδιορισμός των κινδύνων του συστήματος. Κίνδυνος είναι μια κατάσταση του συστήματος ή ένα σύνολο συνθηκών που μπορεί να οδηγήσουν σε ατύχημα (απώλεια). Μια σημαντική διάκριση μεταξύ ατυχημάτων και κινδύνων είναι ότι τα ατυχήματα μπορεί να περιλαμβάνουν παράγοντες εκτός των ορίων του συστήματος (δηλαδή εκτός του ελέγχου του σχεδιαστή), ενώ οι κίνδυνοι πρέπει να επικεντρώνονται σε αυτούς που βρίσκονται μέσα στα όρια του συστήματος και στον διαθέσιμο σχεδιαστικό χώρο. Ακολουθούν παραδείγματα και σύντομες περιγραφές των επικίνδυνων καταστάσεων κατά την διαδικασίας εκσκαφής που μπορούν να οδηγήσουν στα ατυχήματα που εντοπίστηκαν προηγουμένως:

Η-1: Παράλειψη επιθεώρησης εκσκαφέα πριν και μετά την λειτουργία του

Περιγραφή: Ο κίνδυνος αυτός περιγράφει όλες τις πιθανές ενέργειες που μπορεί να παραληφθούν για το έλεγχο της λειτουργικής κατάστασης του μηχανήματος πριν και μετά από την λειτουργία του εκσκαφέα που μπορεί να οδηγήσουν σε φθορά εξαρτημάτων του μηχανήματος έως και ολική καταστροφή και ακόμα και σε τραυματισμό ή απώλεια του χειριστή σε ακραία περίπτωση.

Παράδειγμα: Η στάθμη ελαίου του κινητήρα είναι κάτω από την ελάχιστα επιτρεπόμενη και ο χειριστής εκκινεί και λειτουργεί το μηχάνημα χωρίς να εντοπίσει αυτή την κατάσταση λόγω παράλειψης ελέγχου του ενδείκτη. Αποτέλεσμα αυτής της κατάστασης είναι η φθορά του κινητήρα που μπορεί να οδηγήσει έως και την καταστροφή του κινητήρα.

Η-2: Μη τήρηση των κανόνων ασφαλούς κίνησης και στάθμευσης του εκσκαφέα

Περιγραφή: Αυτός ο κίνδυνος αναφέρεται σε όλες τις λανθασμένες ενέργειες που μπορεί να συμβούν κατά την οδήγηση ή στάθμευση του εκσκαφέα και είναι επικίνδυνες για την ασφαλή εκτέλεση της εργασίας του. Πιο συγκεκριμένα, σε αυτή την ομάδα κινδύνων περιλαμβάνεται η οδήγηση του εκσκαφέα με μεγάλη ταχύτητα ή με μειωμένη ορατότητα, η στάθμευση του σε κλίση ή η λειτουργεία του σε κλίση μεγαλύτερη της επιτρεπόμενης καθώς και η στάθμευση και λειτουργεία του πολύ κοντά στο χείλος μίας πλαγίας κ.ά.

Παράδειγμα: Στάθμευση του εκσκαφέα σε έδαφος με κλίση.

Η-3: Απότομες κινήσεις εκσκαφέα κατά την εκσκαφή

Περιγραφή: Οι κίνδυνοι που προκύπτουν από απότομες και αδικαιολόγητες κινήσεις που προκαλεί ο χειριστής στον εκσκαφέα.

Παράδειγμα: Χρήση κινητού τηλεφώνου κατά την εκσκαφή με αποτέλεσμα να αποσπάται η προσοχή του χειριστή και να πραγματοποιεί απότομες κινήσεις.

Η-4: Υπέρβαση μέγιστου επιτρεπόμενου βάρους στον κάδο

Περιγραφή: Ο κίνδυνος αυτός αφορά τις περιπτώσεις όπου ο εκσκαφέας φορτώνεται με μεγαλύτερος βάρος από το επιτρεπόμενο.

Παράδειγμα: Προκειμένου να πραγματοποιηθεί η εκσκαφή γρηγορότερα ο χειριστής γεμίζει τον κάδο με μεγαλύτερη ποσότητα υλικού από το επιτρεπόμενο με αποτέλεσμα να ανατραπεί ή να αστοχήσει κάποιο μηχανικό μέρος του εκσκαφέα.

Η-5:Συνθήκες εξωτερικού περιβάλλοντος

Περιγραφή**:** Ο κίνδυνος αυτός περιλαμβάνει όλες τις καταστάσεις που μπορεί να επικρατούν στο εξωτερικό περιβάλλον και θεωρούνται επικίνδυνες για την εκτέλεση της εκσκαφής. Τέτοιες είναι η μη επαρκής σήμανση της περιοχής εκσκαφής, η μη

επαρκής φύλαξη του χώρου εκσκαφής, ο μη επαρκής φωτισμός της περιοχής εκσκαφής, ο μη εντοπισμός σωληνώσεων και καλωδιώσεων κοινωφελούς ωφελείας πριν την εκσκαφή καθώς και οποιαδήποτε άλλη κατάσταση του περιβάλλοντος που μπορεί να θεωρηθεί επικίνδυνη.

Παράδειγμα: Είσοδος στο εργοτάξιο ανθρώπων – περαστικών που δεν έχουν κάποια δουλειά να βρίσκονται εκεί, θέτοντας έτσι σε κίνδυνο την προσωπική τους ασφάλεια το οποίο μπορεί να οδηγήσει σε σοβαρό τραυματισμό τους.

Πίνακας 6: Κίνδυνοι συστήματος (System level hazards)

Κίνδυνος	**Περιγραφή**	**Ατύχημα**
H-1	Παράλειψη επιθεώρησης εκσκαφέα πριν και μετά την λειτουργία του	A-1, A-2
H-2	Μη τήρηση των κανόνων ασφαλούς κίνησης και στάθμευσης του εκσκαφέα	A-1, A-2, A-3, A-4
H-3	Απότομες κινήσεις εκσκαφέα κατά την εκσκαφή	A-3
H-4	Υπέρβαση μέγιστου επιτρεπόμενου βάρους στον κάδο	A-1, A-2
H-5	Συνθήκες εξωτερικού περιβάλλοντος	A-3, A-4

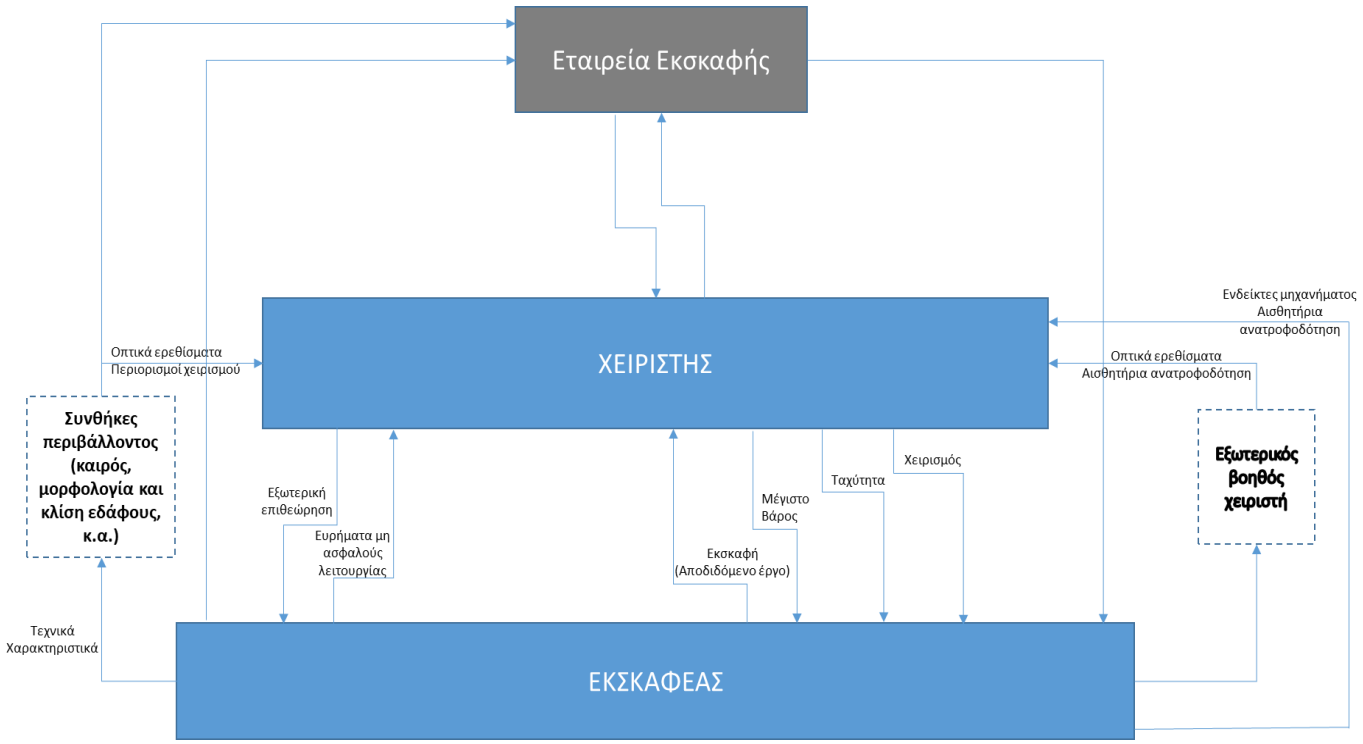
3.3 Πρότυπο δομής ελέγχου

Ο εντοπισμός των ατυχημάτων και των κινδύνων αποτελεί συνήθης πρακτική σε αναλύσεις συστημάτων ασφάλειας. Το επιπρόσθετο θεμελιώδες κομμάτι που απαιτείται για την εκτέλεση της STPA είναι μια δομή ελέγχου του συστήματος. Η δομή ελέγχου του συστήματος είναι μια λειτουργική αναπαράσταση του συστήματος ως ιεραρχικοί βρόγχοι ελέγχου. Η απεικόνιση του συστήματος με μια λειτουργική δομή ελέγχου παρέχει ένα μέσο για την παρουσίαση πολλών πληροφοριών με έναν απλό, γραφικό τρόπο που μπορεί να γίνει κατανοητός από αναλυτές από διαφορετικούς κλάδους. Οι ίδιες πληροφορίες σχετικά με το σχεδιασμό και τη λειτουργία του συστήματος μπορούν να ενσωματωθούν και σε τεχνικά έγγραφα, όπως διαγράμματα καλωδιώσεων, ψευδοκώδικα ή έγγραφα απαιτήσεων. Ωστόσο, οι βασικές λειτουργικές πληροφορίες ενδέχεται να κρύβονται πίσω από τις λεπτομέρειες σχεδίασης του σχετικού κλάδου. Η δομή ελέγχου αποτελείται από λειτουργικά μπλοκ (blocks) που συνδέονται με βέλη που αντιπροσωπεύουν τις ενέργειες ελέγχου (control actions) καθώς και την ανατροφοδότηση (feedback). Κατά την κατασκευή της δομής ελέγχου, ο αναλυτής αναθέτει ευθύνες σε κάθε λειτουργικό μπλοκ και τις συνδέει με μια ιεραρχία. Με τον τρόπο αυτό με ένα ουδέτερο τρόπο εξασφαλίζει ότι όλοι οι φορείς του συστήματος έχουν μια κοινή κατανόηση του σχεδιασμού και της λειτουργίας του συστήματος.

Οι δομές ελέγχου που χρησιμοποιούνται σε αυτή την ανάλυση έχουν ένα κοινό φορμάτ που προέρχεται από παρόμοιες αρχιτεκτονικές των τριών χαρακτηριστικών (feature). Όπως αναφέρθηκε και προηγουμένως, κάθε χαρακτηριστικό είναι ένα δικτυακό-φυσικό σύστημα στο οποίο πολλαπλά στοιχεία υλισμού διαχειρίζονται συστατικά υλικού από ενσωματωμένο ελεγκτή. Από λειτουργικής άποψης, η κοινή

αρχιτεκτονική έχει τρία βασικά ιεραρχικά επίπεδα: τον άνθρωπο χειριστή του μηχανήματος, την οντότητα της εταιρείας εκσκαφής και το μηχάνημα τον εκσκαφέα. Το ίδιο σύστημα μπορεί να αναπτυχθεί με πολύ περισσότερες λεπτομέρειες και με πολλά ακόμη επίπεδα ιεραρχίας, αν και για μια ανάλυση υψηλού επιπέδου αυτό το επίπεδο αφαίρεσης είναι κατάλληλο. Σε μια προσπάθεια σχεδιασμού με ασφάλεια, κάθε ένα από τα λειτουργικά μπλοκ και οι σύνδεσμοί τους θα πρέπει να επεκταθούν σε μεγαλύτερη λεπτομέρεια καθώς οι χώροι σχεδιασμού είναι περιορισμένοι και οι αποφάσεις εφαρμογής έχουν ληφθεί. Το σχήμα 6 παρακάτω παρέχει ένα πρότυπο για τις δομές ελέγχου που αποτελούν μέρος αυτής της ανάλυσης.

Τα μπλοκ στο Σχήμα 6 αντιπροσωπεύουν λειτουργικές οντότητες οι οποίες μπορεί να αντιστοιχούν σε φυσικές οντότητες ή μη. Η παραδοχή που χρησιμοποιείται εδώ είναι ότι τα μπλοκ υψηλότερα στη δομή έχουν εξουσία πάνω σε μπλοκ χαμηλότερα στη δομή (ο χειριστής βρίσκεται στην κορυφή καθώς αυτός λαμβάνει όλες τις αποφάσεις για την διαδικασία εκσκαφής) και ότι οι ενέργειες ελέγχου κινούνται προς τα κάτω, ενώ η ροή ανατροφοδότησης προς τα πάνω και στα πλάγια. Για οπτική απλότητα, μόνο ένα βέλος σε μια δεδομένη κατεύθυνση εμφανίζεται ανάμεσα σε δύο μπλοκ - έτσι ένα βέλος αντιπροσωπεύει μια διαδρομή και όχι μια μεμονωμένη εντολή ή ένα κομμάτι ανάδρασης. Οι πολλαπλοί όροι που επισημαίνονται σε ένα βέλος αντιπροσωπεύουν το σύνολο των ενεργειών ελέγχου (control actions) ή των μεταβλητών ανάδρασης (feedback variables), ανάλογα με την κατεύθυνση, που μπορεί να υπάρχουν στη διαδρομή που υποδεικνύεται από το βέλος.



Σχήμα 8: Μια τυπική δομή ελέγχου

Τα μπλε τετράγωνα και τα μονοπάτια στο Σχήμα 6 είναι κοινά και στα τρία χαρακτηριστικά της συγκεκριμένης μελέτης. Το γκρίζο τμήμα είναι η εταιρεία εκσκαφής και τα μοναδικά της μονοπάτια ελέγχου και ανάδρασης. Κανένα από αυτά τα χαρακτηριστικά δεν μεταβάλλει τα άλλα λειτουργικά μπλοκ σε αυτό το επίπεδο ανάλυσης και έτσι μπορεί να διαμοιραστεί αυτό το κοινό πρότυπο. Τα μπλε ορθογώνια με διακεκομμένες (Επικρατούσες συνθήκες περιβάλλοντος & Εξωτερικός βοηθός χειριστή) περιλαμβάνουν την αναγνώριση ότι το σύστημα χειριστή-μηχανήματος δεν υπάρχει σε απομόνωση. Το μπλοκ του εξωτερικού βοηθού έχει σαν σκοπό να υποβοηθήσει τον χειριστή κατά τη διάρκεια της εκσκαφής υποδεικνύοντας επικίνδυνες περιοχές ενώ το μπλοκ του περιβάλλοντος αντιπροσωπεύει τις συνθήκες του περιβάλλοντος που επικρατούν στην περιοχή εκσκαφής και περιλαμβάνουν τις καιρικές συνθήκες, την μορφολογία του εδάφους, την κλίση του εδάφους, την εκσκαφή στην άκρη μία πλαγιάς, ανθρώπους που εργάζονται γύρω στο εργοτάξιο κλπ. Τα τεχνικά χαρακτηριστικά του μηχανήματος σε συνδυασμό με την εκτίμηση των περιβαλλοντικών συνθηκών έχουν σαν αποτέλεσμα διάφορα οπτικά ερεθίσματα στον χειριστή καθώς επίσης θέτουν περιορισμούς στον χειρισμό του εκσκαφέα. Η ανατροφοδότηση και οι ενέργειες ελέγχου της πρότυπης δομής παρουσιάζονται αναλυτικά στους Πίνακες 7 και 8.

Πίνακας 7: Ενέργειες Ελέγχου (Control Actions) Χειριστή

Ενέργεια Ελέγχου	**Περιγραφή**
Εξωτερική Επιθεώρηση	Αφορά μια σειρά από ενέργειες – επιθεωρήσεις που εκτελεί ο χειριστής πριν και μετά την χρήση του μηχανήματος προκειμένου να εντοπιστούν τυχόν σφάλματα ή αποκλίσεις για την ασφαλή λειτουργεία του και να διορθωθούν προτού γίνουν επικίνδυνα π.χ. χαμηλή στάθμη ελαίου κινητήρα, διαρροή υδραυλικού κ.α
Μέγιστο Βάρος	Είναι το μέγιστο επιτρεπόμενο βάρος εκσκαφής και μεταφοράς υλικού στον κάδο του εκσκαφέα που προβλέπεται από τον κατασκευαστή στα τεχνικά χαρακτηριστικά του εκσκαφέα και δεν πρέπει να παραβιάζεται
Ταχύτητα	Μέγιστη ταχύτητα κίνησης εκσκαφέα και μεταφοράς υλικού ώστε να κινείται με ασφάλεια ώστε να μην ανατραπεί
Χειρισμός	Οι κινήσεις του εκσκαφέα κατά την εργασία εκσκαφής οι οποίες θα πρέπει να είναι προσεκτικές, αργές και με ακρίβεια και όχι απότομες ή νευρικές καθώς όμως και οι κινήσεις μετακίνησης του
Συνθήκες Περιβάλλοντος	Πριν την χρήση του μηχανήματος για την εκσκαφή θα πρέπει να αξιολογηθούν οι επικρατούσες συνθήκες του περιβάλλοντος για την ασφαλή χρήση του όπως οι καιρικές συνθήκες, η κλίση του εδάφους, η μορφολογία και η υφή του εδάφους, ο φωτισμός του χώρου, η περίφραξη του εργοταξίου κ.ά.

Πίνακας 8: Σήματα Ανατροφοδότησης (Feedback signals)

Ανατροφοδότηση	**Περιγραφή**
Ευρήματα επισφαλούς λειτουργίας κατά την επιθεώρηση	Τα πιθανά ευρήματα τα οποία μπορεί να εντοπιστούν κατά την επιθεώρηση πριν και μετά την λειτουργεία του εκσκαφέα και επηρεάζουν την λειτουργικότητα του και την ασφαλή λειτουργεία του μηχανήματος όπως μια διαρροή υδραυλικού, μια ρωγμή στα κινητά μέρη του εκσκαφέα, κάποιο εύρημα στον κινητήρα κ.ά.
Ενδείκτες μηχανήματος	Περιλαμβάνει πληροφορίες κρίσιμες για την λειτουργική κατάσταση του εκσκαφέα όπως η θερμοκρασία ελαίου του κινητήρα, θερμοκρασία του υδραυλικού υγρού, προειδοποίηση για βλάβη κινητήρα, ενδείκτης καυσίμου, ταχύμετρο και άλλες προειδοποιητικές ενδείξεις.
Οπτικά ερεθίσματα	Το τι βλέπει και αντιλαμβάνεται ο χειριστής έξω από το παρμπρίζ του
Αισθητήρια Ανατροφοδότηση	Αυτό που ο χειριστής αισθάνεται και εισπράττει από τη συμπεριφορά του εκσκαφέα κατά τη λειτουργεία του όπως: δυσκολία κίνησης μοχλού βραχίονα, ασυνήθιστος θόρυβος του κινητήρα, συνθήκες εδάφους (ανώμαλο έδαφος) κ.ά.
Περιορισμοί Χειρισμού	Οι περιορισμοί χρήσης ή χειρισμού του εκσκαφέα οι οποίοι προκύπτουν έπειτα από αξιολόγηση των συνθηκών του περιβάλλοντός σε συνάρτηση με τα τεχνικά χαρακτηριστικά του μηχανήματος και τους γενικούς κανόνες ασφαλούς εργασίας
Εκσκαφή	Είναι το αποδιδόμενο έργο του εκσκαφέα το οποίο εξαρτάται από διάφορους παράγοντες όπως τις συνθήκες περιβάλλοντος, τα τεχνικά χαρακτηριστικά του εκσκαφέα, τους χειρισμούς και την ταχύτητα εκσκαφής κ.ά.
Εξωτερικός βοηθός χειριστή	Οι πληροφορίες που μεταδίδονται στον χειριστή από τον βοηθό του για εξωτερικούς κινδύνους καθώς και οδηγίες εκσκαφής(κατευθυντήριες) σε επικίνδυνά σημεία.

3.4 Εντοπισμός επισφαλών ενεργειών ελέγχου

Αφού προσδιοριστούν οι κίνδυνοι και τα ατυχήματα του συστήματος και κατασκευαστεί και η πρότυπη δομή ελέγχου είμαστε έτοιμοι να προχωρήσουμε στο 1^{ο} βήμα της ανάλυσης STPA δηλαδή στον εντοπισμό και την αναγνώριση των επισφαλών ενεργειών ελέγχου. Όπως αναλύθηκε και στο προηγούμενο κεφάλαιο υπάρχουν τέσσερις τρόποι όπου μια ενέργεια ελέγχου μπορεί να αναπτυχθεί και να χαρακτηριστεί επισφαλής. Αυτές λοιπόν οι επισφαλείς ενέργειες μπορούν να οργανωθούν σε πίνακες ανά ενέργεια ελέγχου που εκτελεί ο χειριστής ώστε να καθοδηγηθεί πιο εύκολα το brainstorming. Στους Πίνακες 9, 10, 11, 12 & 13 που ακολουθούν παρουσιάζονται οι ενέργειες ελέγχου που σχετίζονται με αποφάσεις (ενέργειες) που λαμβάνει ο χειριστής κατά το χειρισμό εκσκαφικού μηχανήματος από πριν ακόμα την εκκίνηση του έως και το πέρας της λειτουργείας του και μπορεί να χαρακτηριστούν επικίνδυνες.

Πίνακας 9: Επισφαλείς ενέργειες ελέγχου κατά την εξωτερική επιθεώρηση του εκσκαφέα

Ενέργεια Ελέγχου	**Δεν εφαρμόζεται**	**Εφαρμόζεται εσφαλμένα**	**Πολύ νωρίς ή πολύ αργά**	**Μεγάλη διάρκεια ή πολύ σύντομα**
Εξωτερική επιθεώρηση	UCA-EX-1:Δεν εφαρμόζεται έλεγχος της κατάστασης των ερπυστριών ή των ελαστικών του εκσκαφέα	UCA-EX-2: Εφαρμόζεται έλεγχος της μηχανής ενώ αυτή είναι σε λειτουργία	UCA-EX-3: Εφαρμόζεται πολύ αργά η ζώνη ασφαλείας στην καμπίνα του χειριστή	UCA-EX-4: Εφαρμόζεται έλεγχος υδραυλικού συστήματος κίνησης για πολύ σύντομο διάστημα και δεν διαπιστώνεται δυσλειτουργία κίνησης
	UCA-EX-5: Δεν εφαρμόζεται έλεγχος της στάθμης ελαίου του κινητήρα	UCA-EX-6: Εφαρμόζεται καθαρισμός τζαμιών καμπίνας χωρίς την χρήση αντιολισθητικών υποδημάτων	UCA-EX-7: Εφαρμογή διόρθωσης θέσης καθίσματος πολύ αργά	UCA-EX-8: Εφαρμόζεται έλεγχος πίεσης φρένων για πολύ σύντομο διάστημα και δεν διαπιστώνεται πιθανή απώλεια πίεσης
	UCA-EX-9: Δεν εφαρμόζεται χρήση προστατευτικού εξοπλισμού κατά την προσέγγιση αλλά και κατά την λειτουργεία του εκσκαφέα	UCA-EX-10: Εφαρμόζεται έλεγχος στάθμης ελαίου και υδραυλικού ενώ είναι σε λειτουργεία ο εκσκαφέας με αποτέλεσμα λανθασμένη ένδειξη	UCA-EX-11: Εφαρμόζεται κίνηση του εκσκαφέα πολύ σύντομα πριν ανεβάσει τις σωστές πιέσεις	UCA-EX-12: Εφαρμόζεται λειτουργία του κινητήρα υπό έντονο θόρυβο για μεγάλο διάστημα
	UCA-EX-13: Δεν εφαρμόζεται έλεγχος του μηχανήματος για τυχόν διαρροές (καύσιμο, υδραυλικά, λάδι,)	UCA-EX-14: Εφαρμόζεται έλεγχος των κινούμενων επιφανειών ενώ είναι ο εκσκαφέας σε λειτουργεία		
	UCA-EX-15: Δεν εφαρμόζεται έλεγχος της στάθμης του υδραυλικού υγρού	UCA-EX-16: Εφαρμόζεται εκκίνηση χωρίς προθέρμανση του κινητήρα		
	UCA-EX-17: Δεν εφαρμόζεται έλεγχος του χώρου του κινητήρα για ξένα αντικείμενα ή παρουσία εύφλεκτων υγρών	UCA-EX-18: Εφαρμόζεται είσοδος στο χώρο της καμπίνας χωρίς τη χρήση των ειδικών χειρολαβών		
	UCA-EX-19: Δεν εφαρμόζεται έλεγχος στην δομή αλλά και στον βραχίονα του εκσκαφέα για φθαρμένα ή κατεστραμμένα μέρη	UCA-EX-20: Εφαρμόζεται θεώρηση μιας διαρροής καυσίμου ή υδραυλικού ως ασήμαντη		
	UCA-EX-21: Δεν εφαρμόζεται έλεγχος καθαριότητας των τζαμιών καμπίνας			
	UCA-EX-22: Δεν εφαρμόζεται τοποθέτηση ζώνης ασφαλείας κατά το χειρισμό του εκσκαφέα			
	UCA-EX-23: Δεν εφαρμόζεται έλεγχος ενδείξεων οργάνων			
	UCA-EX-24: Δεν εφαρμόζεται έλεγχος υδραυλικού συστήματος πριν την εκσκαφή			
	UCA-EX-25: Δεν εφαρμόζεται έλεγχος στα φώτα του εκσκαφέα			

Πίνακας 10: Επισφαλείς ενέργειες ελέγχου λόγω παραβίασης του μέγιστου επιτρεπόμενου βάρους εκσκαφής

Ενέργεια Ελέγχου	Δεν εφαρμόζεται	Εφαρμόζεται εσφαλμένα	Πολύ νωρίς ή πολύ αργά	Μεγάλη διάρκεια ή πολύ σύντομα
Μέγιστο Βάρος		UCA-EX-26: Εφαρμόζεται εκσκαφή υλικού μεγαλύτερου βάρους προκειμένου να εκτελεστεί γρηγορότερα η εκσκαφή		UCA-EX-27: Εφαρμόζεται μέγιστο φορτίο για μεγάλη διάρκεια με την μπούμα σε έκταση
		UCA-EX-28: Εφαρμόζεται εγκάρσιο φορτίο στον κάδο ή βραχίονα		

Πίνακας 11: Επισφαλείς ενέργειες ελέγχου κατά τον χειρισμό του εκσκαφέα

Ενέργεια Ελέγχου	Δεν εφαρμόζεται	Εφαρμόζεται εσφαλμένα	Πολύ νωρίς ή πολύ αργά	Μεγάλη διάρκεια ή πολύ σύντομα
Χειρισμός	UCA-EX-29: Δεν εφαρμόζεται έκταση των στη στηριγμάτων του εκσκαφέα για μεγαλύτερη σταθερότητα	UCA-EX-30: Εφαρμόζεται κίνηση με τον βραχίονα εκταμένο		UCA-EX-31: Εφαρμόζεται χρήση κινητού τηλεφώνου κατά την εκσκαφή είτε για σύντομο είτε για μεγάλο διάστημα
	UCA-EX-32: Δεν εφαρμόζεται χρήση τροχοεμποδηστηριών κατά την εκσκαφή σε πλαγιά	UCA-EX-33: Εφαρμόζεται κίνηση με τον βραχίονα να βρίσκεται σε επαφή με το έδαφος ή σε πολύ κοντινή απόσταση		UCA-EX-34: Εφαρμόζεται σε σκληρό έδαφος η μέγιστη ισχύ του μηχανήματος για μεγάλο διάστημα
	UCA-EX-35: Δεν εφαρμόζεται έλεγχος για την διατήρηση του φορτίου (γωνία έκτασης του βραχίονα προς βάρος υλικού)	UCA-EX-36: Εφαρμόζονται κατά την κίνηση του απότομες μανούβρες και κλειστές στροφές		
	UCA-EX-37: Δεν εφαρμόζεται κατέβασμα κάδου κατά την στάθμευση	UCA-EX-38: Εφαρμόζεται κίνηση εγκάρσια στην πλαγιά και όχι κάθετα σε αυτήν		
	UCA-EX-39: Δεν εφαρμόζεται αφαίρεση του κλειδιού της μηχανής κατά την στάθμευση	UCA-EX-40: Εφαρμόζεται απομάκρυνση από τον εκσκαφέα ενώ βρίσκεται σε λειτουργεία ή με τον βραχίονα σε έκταση		
	UCA-EX-41: Δεν εφαρμόζονται το χειρόφρενο κατά την στάθμευση	UCA-EX-42: Εφαρμόζεται χρήση του εκσκαφέα για μεταφορά υλικών που δεν μπορούν να προσδεθούν		
	UCA-EX-43: Δεν εφαρμόζεται ασφάλιση στους τροχούς κατά την εκσκαφή σε πλαγιά	UCA-EX-44: Εφαρμόζεται εκσκαφή πολύ κοντά στο χείλος της εκσκαφής		
	UCA-EX-45: Δεν εφαρμόζεται χρήση των αντιολισθητικών σκαλοπατιών και χειρολαβών	UCA-EX-46: Εφαρμόζεται στάθμευση σε όχι επίπεδο έδαφος		

Πίνακας 12: Επισφαλείς ενέργειες ελέγχου λόγω παραβίασης των ορίων ταχύτητας

Ενέργεια Ελέγχου	Δεν εφαρμόζεται	Εφαρμόζεται εσφαλμένα	Πολύ νωρίς ή πολύ αργά	Μεγάλη διάρκεια ή πολύ σύντομα
Ταχύτητα	UCA-EX-48: Δεν εφαρμόζεται χαμηλή ταχύτητα και χαμηλή σχέση κιβωτίου σε κίνηση σε πλαγιά	UCA-EX-49: Εφαρμόζεται ταχύτητα μεγαλύτερη από την επιτρεπόμενη		
		UCA-EX-50: Εφαρμόζονται απότομες μεταβολές στην ταχύτητα		

Πίνακας 13: Επισφαλείς ενέργειες ελέγχου λόγω περιβαλλοντικών συνθηκών κατά την εκσκαφή

Ενέργεια Ελέγχου	Δεν εφαρμόζεται	Εφαρμόζεται εσφαλμένα	Πολύ νωρίς ή πολύ αργά	Μεγάλη διάρκεια ή πολύ σύντομα
Περιβάλλον	UCA-EX-51: Δεν εφαρμόζεται σε περιπτώσεις μη καλής ορατότητας η χρήση βοηθού χειριστή (ή δεν ακολουθούνται οι οδηγίες που παρέχει)	UCA-EX-52: Εφαρμόζεται εκσκαφή σε πλαγιά με κλίση μεγαλύτερη από την επιτρεπόμενη	UCA-EX-53: Εφαρμόζονται σήματα από τον βοηθό σε μια επικίνδυνη κατά-σταση πολύ αργά	UCA-EX-54: Εφαρμόζεται εκσκαφή σε σκληρό έδαφος για μεγάλο χρονικό διάστημα (overstressing)
	UCA-EX-55: Δεν εφαρμόζεται επαρκής σηματοδότηση και περίφραξη του χώρου εκσκαφής	UCA-EX-56: Εφαρμόζεται εκσκαφή σε μη επιτρεπτές – ακραίες καιρικές συνθήκες		
	UCA-EX-57: Δεν εφαρμόζεται έλεγχος του περιβάλλοντα χώρου για εμπόδια ή άλλους ανθρώπους	UCA-EX-58: Εφαρμόζεται εκσκαφή σε περιοχή με καλώδια και σωλήνες κοινής ωφελείας χωρίς να γίνει μελέτη		
	UCA-EX-59: Δεν εφαρμόζεται επαρκής φωτισμός στον χώρο εκσκαφής	UCA-EX-60: Εφαρμόζεται λειτουργία κοντά σε άλλο μηχάνημα		
	UCA-EX-61: Δεν εφαρμόζεται εξαερισμός σε κλειστό χώρο	UCA-EX-62: Εφαρμόζεται μεταφορά προσωπικού μέσα στον κάδο του εκσκαφέα		
		UCA-EX-63: Εφαρμόζεται εκσκαφή σε μαλακό έδαφος		
		UCA-EX-64: Εφαρμόζεται κίνηση σε έδαφος με λακκούβες και εξογκώματα		

Μετά τον εντοπισμό περιπτώσεων στις οποίες οι ενέργειες ελέγχου μπορούν να οδηγήσουν σε κίνδυνο, πρέπει να ληφθούν μέτρα ώστε να μην εκδίδονται σε τέτοιες καταστάσεις. Περιορισμοί ασφαλείας μπορούν και πρέπει να αναπτυχθούν, έτσι ώστε αν ακολουθηθούν, το σύστημα να μην εισέλθει σε επικίνδυνη κατάσταση ως αποτέλεσμα της έκθεσης σε μια από αυτές τις ενέργειες ελέγχου. Οι περιορισμοί ασφαλείας για την χρήση εκσκαφικού μηχανήματος παρατίθενται στον Πίνακα 14.

Πίνακας 14: Περιορισμοί Ασφαλείας συστήματος (Safety Constrains)

Περιορισμοί Ασφαλείας	Σχετικές επισφαλείς ενέργειες ελέγχου	Λογική - Αιτιολογία
SC-EX-1: Ο χειριστής δεν πρέπει να απομακρύνεται σε καμία περίπτωση ενώ αυτό βρίσκεται σε λειτουργεία	UCA-EX-10,14,40	Είναι πολύ επικίνδυνο, η απομάκρυνση από τον εκσκαφέα ενώ είναι σε λειτουργεία καθώς δεν υπάρχει έλεγχος σε αυτόν και μπορεί να χτυπήσει είτε ο ίδιος ο χειριστής είτε κάποιος άλλος άνθρωπος τριγύρω
SC-EX-2: Χρήση κατάλληλου εγχειριδίου checklist για την εκτέλεση της εξωτερικής επιθεώρησης πριν και μετά την εκσκαφή	UCA-EX-1,5,9,13,16,17,19, 21,23,24,25,37,41	Επειδή μπορεί εύκολα να παραλειφθεί ή να ξεχαστεί κάποια εργασία εξωτερικού ελέγχου το checklist βοηθά ώστε να τσεκαριστούν και να εκτελεστούν μια μία όλες οι επιθεωρήσεις
SC-EX-3: Ο χειριστής θα πρέπει να ακολουθεί πιστά όλες τις οδηγίες ασφαλούς χρήσης και χειρισμού του εκσκαφέα και να εκπαιδεύεται συνεχώς και να εξετάζεται για τις γνώσεις του αυτές σε τακτά χρονικά διαστήματα	UCA-EX-2,4,7,8,10,11,12,18, 20,22,27,28,29,30,32, 33,35,36,38,41,43,44, 45,46,47,48,50,60	Πρέπει συνεχώς ο χειριστής να εκπαιδεύεται και να εξετάζεται για τις γνώσεις του και να ελέγχεται επί του πρακτέου για την πιστή εφαρμογή των κανόνων ασφαλούς χρήσης του εκσκαφέα ώστε να διορθώνονται λάθος πρακτικές και να φρεσκάρονται οι γνώσεις
SC-EX-4: Απαρέγκλιτη χρήση προστατευτικού ατομικού εξοπλισμού (κράνος, ωτοασπίδες, γάντια, παπούτσια αντιολισθητικά, φωσφορίζων γιλεκάκι) πριν την προσέγγιση στον εκσκαφέα	UCA-EX-6,9,38	Είναι απαραίτητη και αυτονόητη η χρήση τους για την υγεία και την προσωπική προστασία του εργαζομένου
SC-EX-5: Χρήση ειδικού συστήματος όπου χωρίς την τοποθέτηση των ζωνών ασφαλείας να μην εκκινεί ο εκσκαφέας ή χρήση διαπεραστικού ήχου εντός της καμπίνας αν δεν γίνει η χρήση της	UCA-EX-3,22	Για λόγους ευκολίας πολλές φορές οι χειριστές παραλείπουν την χρήση της ζώνης ασφαλείας καθώς δεν την θεωρούν σημαντική για αυτό το λόγο είναι απαραίτητη η χρήση ενός προειδοποιητικού μηχανισμού
SC-EX-6: Μη παρέκκλιση από τα μέγιστα επιτρεπόμενα όρια του εκσκαφέα	UCA-EX-26,34,49,52,54	Απόκλιση οποιαδήποτε στιγμή από τα μέγιστα επιτρεπόμενα όρια χρήσης του κατασκευαστή είναι πολύ επικίνδυνη και μπορεί να έχει σοβαρές συνέπειες και για το μηχάνημα αλλά και για τον χειριστή
SC-EX-7: Μη χρήση εκσκαφέα για εξυπηρέτηση άλλων σκοπών και διευκολύνσεων	UCA-EX-42,62	Ο εκσκαφέας είναι σχεδιασμένος για την εκσκαφή υλικού και την τοπική απομάκρυνση του υλικού από το χώρο και όχι για την εξυπηρέτηση και υποβοήθηση άλλων σκοπών
SC-EX-8: Σήμανση εντός της καμπίνας βασικών κανόνων ασφαλείας χειρισμού και μέγιστων επιτρεπόμενων ορίων του εκσκαφέα	UCA-EX-36,49,50	Η σήμανση τους μέσα στην καμπίνα βοηθά τον χειριστή να της έχει συνέχεια υπόψιν του αλλά και να μην τα μπερδεύει με άλλα μοντέλα εκσκαφέων
SC-EX-9: Προϋπόθεση ώστε να πάρει τα κλειδιά του εκσκαφέα είναι η παράδοση του κινητού τηλεφώνου πριν την έναρξη των εργασιών και χρήση μόνο ασυρμάτου για την ενδοεπικοινωνία καθώς και η αντίστροφη διαδικασία	UCA-EX-31,39	Αποφυγή χρήσης κινητού τηλεφώνου κατά την εκσκαφή συνήθεια που είναι πολύ επικίνδυνη και κατά την αντίστροφη διαδικασία αποφεύγεται να ξεχαστεί το κλειδί πάνω στην μηχανή
SC-EX-10: Χρήση εξωτερικού βοηθού – παρατηρητή σε κάθε περίπτωση εκσκαφής ανεξαρτήτου συνθηκών χειριστή	UCA-EX-44,51,53	Η χρήση του σε όλες τις περιπτώσεις θα βοηθήσει στην άμεση πληροφόρηση και προειδοποίηση του χειριστή για οποιαδήποτε αλλαγή στις επικρατούσες συνθήκες ή για μία κάποια επικίνδυνη κατάσταση
SC-EX-11: Χρήση προειδοποιητικών πινακίδων σηματοδότησης του χώρου εργασίας καθώς και περίφραξη αυτού	UCA-EX-55	Είναι απαραίτητο μέτρο για την προειδοποίηση και προφύλαξη από επικίνδυνα σημεία τόσο του χειριστή όσο και των περαστικών
SC-EX-12: Τήρηση κανόνων διασφάλισης ασφαλούς περιβάλλοντος εργασίας (είτε καιρικές είτε εργασιακές) και διακοπή αυτής εάν δεν το ευνοούν οι περιβαλλοντικές συνθήκες	UCA-EX-56,57,58,59, 61,63,64	Οι καιρικές συνθήκες όπως ο καιρός, το έδαφος αλλά και οι εργασιακές όπως ο επαρκής φωτισμός αποτελούν απαραίτητα στοιχεία της ασφαλούς εκτέλεσης της εκσκαφής και δεν πρέπει να παραβιάζονται και να αμελούνται ποτέ

Παρατηρώντας τον Πίνακα 14 βλέπουμε ότι άλλοι περιορισμοί ασφαλείας είναι αυτονόητοι όπως η "Χρήση προστατευτικού εξοπλισμού" ενώ άλλοι όπως η "Παράδοση κινητού τηλεφώνου" μπορεί να χαρακτηριστούν ως σκληροί ή υπερβολικοί γιατί το κινητό τηλέφωνο αποτελεί ένα βασικό και αναπόσπαστο αγαθό της καθημερινότητας. Επίσης από τον πίνακα ξεχωρίζει η σπουδαιότητα της ασφαλούς χρήσης του εκσκαφέα σύμφωνα με τα μνημόνια του κατασκευαστή αλλά και η συνεχής εκπαίδευση και αξιολόγηση του χειριστή ώστε να διασφαλίζεται η υψηλή γνώση και δεξιοτεχνία του στο αντικείμενο. Η υψηλή σημαντικότητα αυτού του περιορισμού απορρέει από τον μεγάλο αριθμό των σχετιζόμενων επισφαλών ενεργειών. Σημαντικός επίσης μπορεί να χαρακτηριστεί ο περιορισμός της "Χρήσης ενός τυποποιημένου checklist" ώστε να μην παραλείπεται, αμελείται ή εκτελείται σε λάθος σειρά κάποιο βήμα της εξωτερικής επιθεώρησης.

Όπως αναφέρθηκε προηγουμένως, ένας στόχος αυτής της διπλωματικής εργασίας είναι να παράσχει κάποια στοιχεία σχετικά με τον τρόπο με τον οποίο η STPA μπορεί να βοηθήσει στην τελειοποίηση εκτέλεσης μιας διαδικασίας ώστε να αποτραπούν οι επισφαλείς καταστάσεις κατά την χρήση εκσκαφικού μηχανήματος. Έως τώρα στην ανάλυση έγινε εντοπισμός των επισφαλών ενεργειών και προσπάθεια αποτροπής αυτών μέσω των περιορισμών ασφαλείας που προτάθηκαν καθώς όμως η ανάλυση προχωράει προς τα εμπρός, θα γίνει προσπάθεια εμβάθυνσης στο πρόβλημα δηλαδή προσδιορισμού της ρίζας του προβλήματος ή ακόμα καλύτερα των αιτιών που οδηγούν σε αυτές τις επισφαλείς καταστάσεις.

3.5 Εντοπισμός αιτιωδών παραγόντων ανάπτυξης επισφαλών ενεργειών

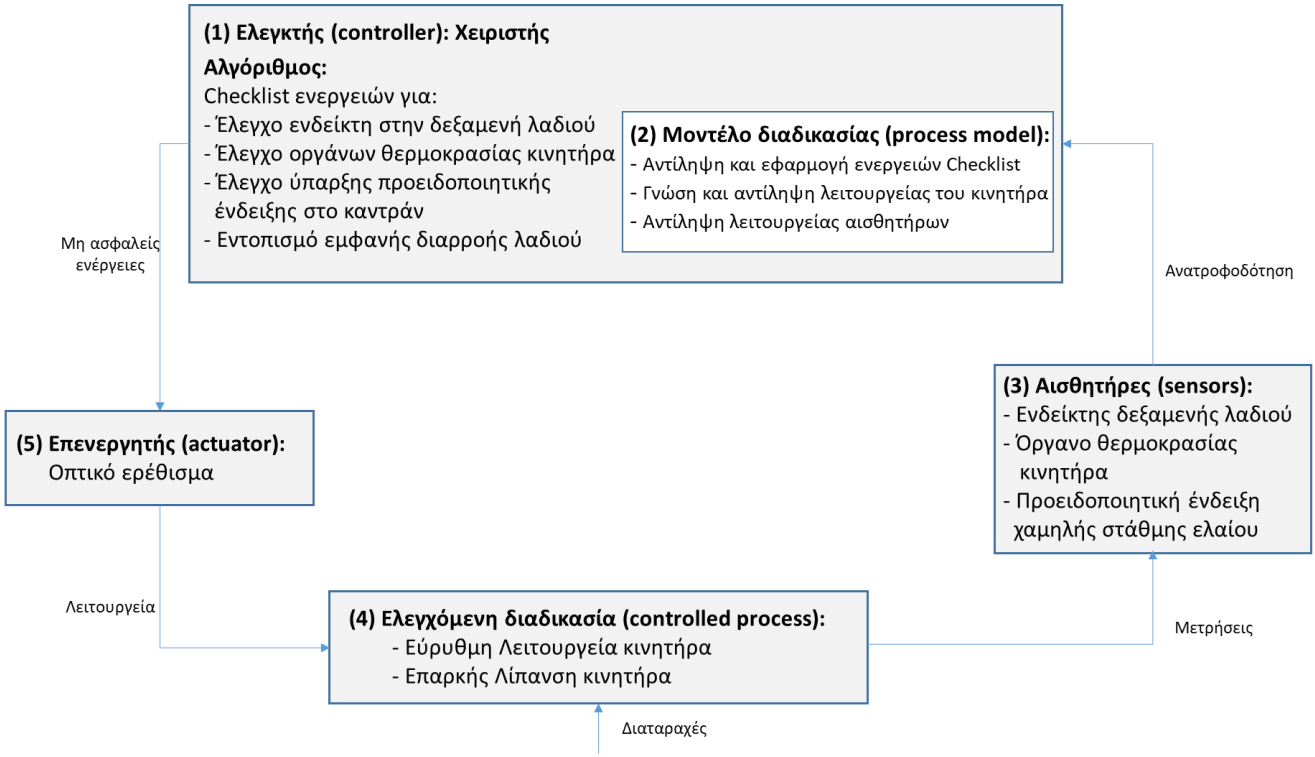
Το Βήμα 1ο της ανάλυσης STPA προσδιορίζει πότε είναι επισφαλές και/ή δυσλειτουργικό για ένα σύστημα ελέγχου (ελεγκτή) να εκδίδει ή να μην εκδίδει εντολές. Το Βήμα 2ο της ανάλυσης STPA βασίζεται σε αυτό και καθοδηγεί τον αναλυτή στην αναγνώριση των αιτιών που το σύστημα ελέγχου (ελεγκτής) μπορεί να εκδώσει μια εντολή όταν είναι ακατάλληλη, να μην εκδώσει μια εντολή όταν είναι απαραίτητη και γιατί μια σωστά εκδοθείσα εντολή μπορεί να εκτελεστεί λανθασμένα. Αυτή η καθοδήγηση προέρχεται από το Σχήμα 6 και 7 όπως περιγράφηκε παραπάνω το οποίο έχει ένα βασικό βρόχο ελέγχου που απεικονίζει την εκπλήρωση (ή όχι) μίας μόνο ενέργειας ελέγχου. Ένα σύστημα ελέγχου (ελεγκτής) εκδίδει εντολές σε έναν επενεργητή (actuator) που στη συνέχεια ενεργεί σε κάποια ελεγχόμενη διαδικασία (controlled process). Οι πτυχές αυτής της ελεγχόμενης διαδικασίας μετριούνται με αισθητήρες (sensors) που παρέχουν ανατροφοδότηση στον ελεγκτή. Ο ελεγκτής λαμβάνει αυτή την ανατροφοδότηση και δημιουργεί ένα μοντέλο διαδικασίας (process model), δηλαδή την κατανόησή του για την κατάσταση της ελεγχόμενης διαδικασίας, την οποία στη συνέχεια χρησιμοποιεί σε συνδυασμό με τον αλγόριθμο ελέγχου για τη λήψη αποφάσεων σχετικά με την έκδοση μιας δεδομένης εντολής.

Ο βρόγχος ελέγχου του Βήματος 2 της STPA όπως τονίσαμε ήδη αναφέρεται, σε μία, κάθε φορά επισφαλή ενέργεια ελέγχου. Παρακάτω θα αναπτύξουμε βρόγχους ελέγχου για μια επισφαλή ενέργεια από κάθε κατηγορία ενέργειας ελέγχου που

πραγματοποιεί ο χειριστής ώστε να εντοπιστούν ευκολότερα κα να γίνουν πιο ξεκάθαρες οι αιτίες που οδηγούν στην ανάπτυξη επισφαλών ενεργειών.

- Βρόγχος ελέγχου και εντοπισμός αιτιών για επισφαλή ενέργεια σχετικά με την εξωτερική επιθεώρηση

Στο Σχήμα 9 παρουσιάζεται ο βρόγχος ελέγχου της επισφαλούς ενέργειας ελέγχου 5 (UCA-EX-5) σχετικά δηλαδή με την μη εφαρμογή ελέγχου της στάθμης ελαίου του κινητήρα πριν την εκκίνηση του μηχανήματος ενώ ταυτόχρονα προσπαθείτε να γίνει σύνδεση μεταξύ της ελεγχόμενης διαδικασίας με τον χειριστή και τον εκσκαφέα.



Σχήμα 9: Βρόγχος ελέγχου επισφαλής ενέργειας UCA-EX-5

Στον Πίνακα 15 εντοπίζονται οι αιτιώδεις παράγοντες οι οποίοι μπορούν να οδηγήσουν στην επισφαλή εκτίμηση της καλής κατάστασης της μηχανής αξιολογώντας τα δεδομένα του βρόγχου ελέγχου που φαίνεται στο Σχήμα 9. Η συγκεκριμένη επισφαλή ενέργεια ελέγχου που εξετάζεται από τον Πίνακα 9 είναι:

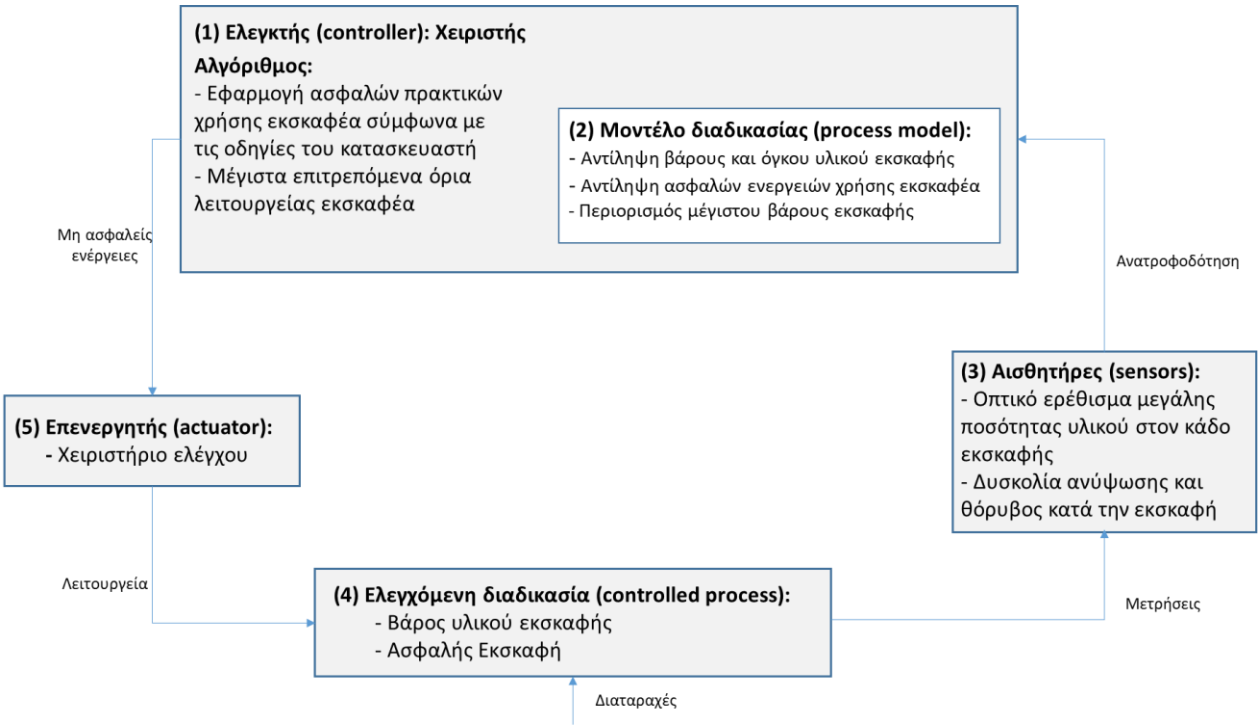
UCA-EX-5: Δεν εφαρμόζεται έλεγχος της στάθμης ελαίου του κινητήρα

Πίνακας 15: Αιτιώδεις παράγοντες ανάπτυξης επισφαλής ενέργειας UCA-EX-5

Συστατικό/Σύνδεση	Σχετιζόμενοι Αιτιώδεις Παράγοντες
(2) Μοντέλο διαδικασίας	• Παράλειψη εκτέλεσης επιθεώρησης • Ελλιπής εκπαίδευση και γνώση του μηχανήματος και των οργάνων του • Λανθασμένη εκτίμηση ενδείξεων οργάνων • Λανθασμένη εκτίμηση διαρροής
(3) Αισθητήρες	• Κάποιο/α από τα όργανα δεν λειτουργεί σωστά και δεν παίρνουμε σωστές ενδείξεις • Βρώμικα όργανα με αποτέλεσμα να μην είναι ξεκάθαρες οι ενδείξεις • Φθαρμένες ή κομμένες καλωδιώσεις που οδηγούν στα όργανα τα δεδομένα του κινητήρα • Σπασμένος ο ενδείκτης λαδιού του κινητήρα
(5) Επενεργητής - Οπτικό ερέθισμα	• Είναι αφηρημένος από προσωπικά προβλήματα ή κουρασμένος και δεν δείχνει την απαιτούμενη προσοχή

➢ <u>Βρόγχος ελέγχου και εντοπισμός αιτιών για επισφαλή ενέργεια σχετικά με το μέγιστο βάρος</u>

Στο Σχήμα 10 παρουσιάζεται ο βρόγχος ελέγχου της επισφαλούς ενέργειας σχετικά με το μέγιστο βάρος με αριθμό κωδικοποίησης UCA-EX-27 και αφορά την εφαρμογή μέγιστου φορτίου για μεγάλη διάρκεια με την μπούμα σε έκταση κινητήρα πριν την εκκίνηση του μηχανήματος. Προσπαθείτε πάλι να γίνει σύνδεση μεταξύ της ελεγχόμενης διαδικασίας και του χειριστή ώστε να καταστούν σαφείς όλες οι διαδικασίες της συγκεκριμένης ενέργειας και να εντοπιστούν έτσι ευκολότερα οι αιτίες που οδηγούν στην επισφαλή ενέργεια.



Σχήμα 10: Βρόγχος ελέγχου επισφαλής ενέργειας UCA-EX-27

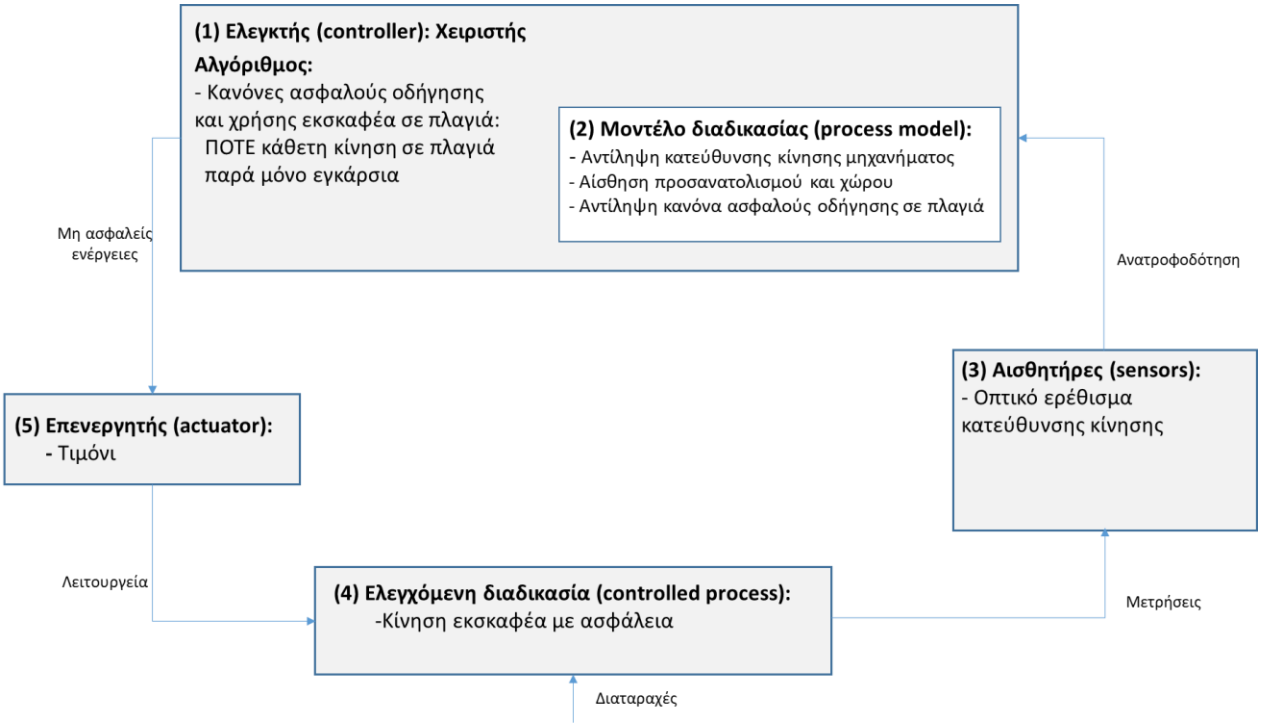
Στον Πίνακα 16 εντοπίζονται οι αιτιώδεις παράγοντες οι οποίοι μπορούν να οδηγήσουν στην επισφαλή κατάσταση εφαρμογής μέγιστου βάρους για μεγάλη διάρκεια αξιολογώντας τα δεδομένα του βρόγχου ελέγχου που φαίνεται στο Σχήμα 10. Η συγκεκριμένη επισφαλή ενέργεια ελέγχου που εξετάζεται από τον Πίνακα 10 είναι:

UCA-EX-27: Εφαρμόζεται μέγιστο φορτίο για μεγάλη διάρκεια με την μπούμα σε έκταση

Πίνακας 16: Αιτιώδεις παράγοντες ανάπτυξης επισφαλής ενέργειας UCA-EX-27

Συστατικό/Σύνδεση	Σχετιζόμενοι Αιτιώδεις Παράγοντες
(2) Μοντέλο διαδικασίας	• Ελλιπής εκπαίδευση και γνώση του μηχανήματος • Μη εξοικείωση με τον τύπο εκσκαφέα • Σύγχυση του μέγιστου επιτρεπόμενου βάρους με άλλο τύπο εκσκαφέα • Μη τήρηση του μέγιστου επιτρεπόμενου βάρους εκσκαφής προκειμένου να εκτελεστεί γρηγορότερα η εκσκαφή • Λανθασμένη εκτίμηση της ποσότητας εκσκαφής
(3) Αισθητήρες	• Αφηρημένος κατά την εκτέλεση της εκσκαφής οπότε δεν προσέχει την ποσότητα υλικού που βρίσκεται στον κάδο εκσκαφής • Δεν γίνεται αντιληπτή η δυσκολία ανύψωσης λόγω μεγάλου όγκου εκσκαφής • Λανθασμένη εκτίμηση του αυξανομένου θορύβου μηχανής από την προσπάθεια ανύψωσης μεγάλου όγκου υλικού
(5) Επενεργητής - Χειριστήριο ελέγχου	• Μη καλή λειτουργικότητα ή αστοχία του χειριστηρίου με αποτέλεσμα να μείνει η μπούμα σε έκταση με το υλικό εκσκαφής εντός του κάδου για μεγάλη διάρκεια

➢ <u>Βρόγχος ελέγχου και εντοπισμός αιτιών για επισφαλή ενέργεια σχετικά με το χειρισμό του εκσκαφέα</u>



Σχήμα 11: Βρόγχος ελέγχου επισφαλής ενέργειας UCA-EX-38

Στο Σχήμα 11 παρουσιάζεται ο βρόγχος ελέγχου για την επισφαλή ενέργεια σχετικά με το χειρισμό του εκσκαφέα με κωδικό UCA-EX-38 και αφορά την κίνηση του εκσκαφικού μηχανήματος σε πλαγιά. Ο βρόγχος ελέγχου προσπαθεί να ρίξει φως σε όλες τις πτυχές αυτής της ενέργειας ελέγχου και να εντοπίσει τις αιτίες παρέκκλισης από τους κανόνες ασφαλούς οδήγησης.

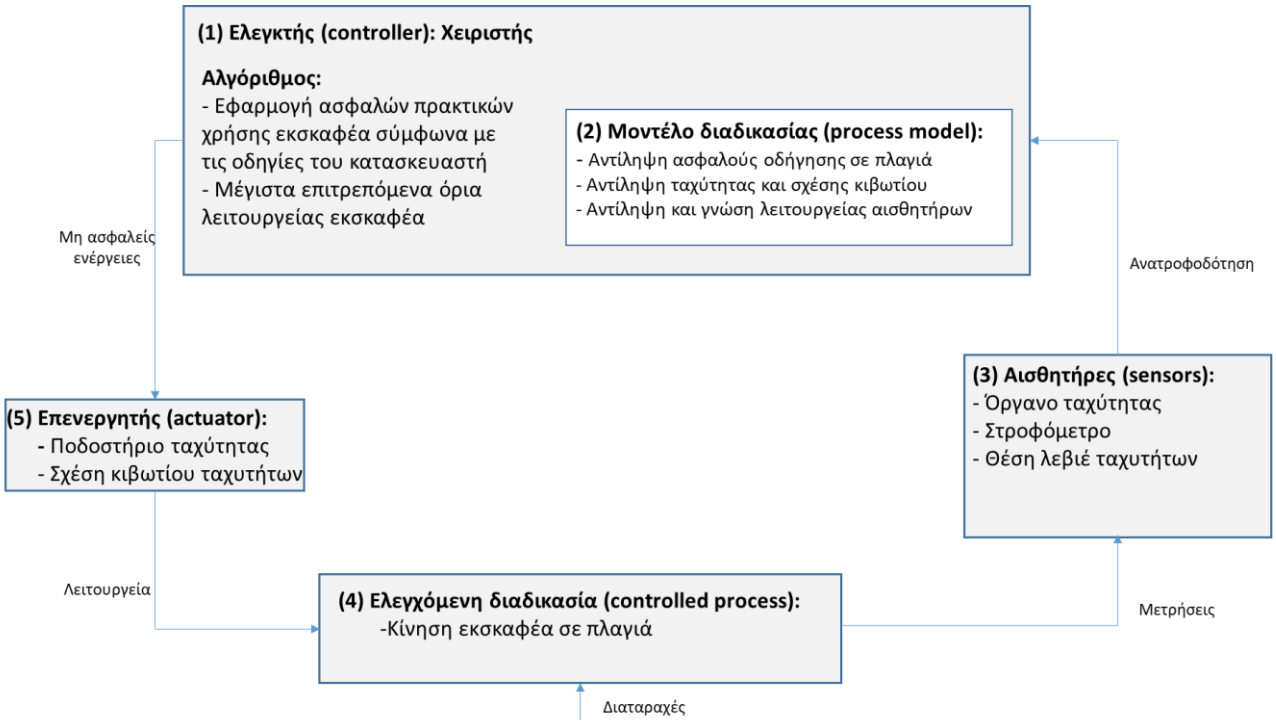
Στον Πίνακα 17, όπως και προηγουμένως, εντοπίζονται οι αιτιώδεις παράγοντες οι οποίοι μπορούν να οδηγήσουν στην ανάπτυξη της επισφαλής ενέργειας χειρισμού του εκσκαφέα αξιολογώντας τα δεδομένα του βρόγχου ελέγχου που φαίνεται στο Σχήμα 11. Η συγκεκριμένη επισφαλή ενέργεια ελέγχου που εξετάζεται από τον Πίνακα 11 είναι:

UCA-EX-38: Εφαρμόζεται κίνηση εγκάρσια στην πλαγιά και όχι κάθετα σε αυτήν

Πίνακας 17: Αιτιώδεις παράγοντες ανάπτυξης επισφαλής ενέργειας UCA-EX-38

Συστατικό/Σύνδεση	Σχετιζόμενοι Αιτιώδεις Παράγοντες
(2) Μοντέλο διαδικασίας	• Μη τήρηση κανόνα ασφαλούς κίνησης σε πλαγιά με σκοπό να φτάσει γρηγορότερα στο σημείο εκσκαφής • Ελλιπής εκπαίδευση και γνώση των κανόνων ασφαλούς κίνησης του εκσκαφικού μηχανήματος • Λανθασμένη αίσθηση προσανατολισμού
(3) Αισθητήρες	• Λανθασμένη αντίληψη κατεύθυνσης κίνησης λόγω απόσπασης προσοχής ή κούρασης
(5) Επενεργητής - Τιμόνι	• Μη λειτουργικότητα ή αστοχία του τιμονιού με αποτέλεσμα να μην είναι δυνατός ο έλεγχος κατεύθυνσης του εκσκαφέα

➢ <u>Βρόγχος ελέγχου και εντοπισμός αιτιών για επισφαλή ενέργεια σχετικά με την ταχύτητα κίνησης</u>



Σχήμα 12: Βρόγχος ελέγχου επισφαλής ενέργειας UCA-EX-48

Στο Σχήμα 12 αναπτύσσεται ο βρόγχος ελέγχου για την επισφαλή ενέργεια σχετιζόμενη με την ταχύτητα κίνησης του εκσκαφέα και πιο συγκεκριμένα την μη εφαρμογή χαμηλής ταχύτητας και χαμηλής σχέσης στο κιβώτιο ταχυτήτων κατά την κίνηση σε πλαγιά (UCA-EX-48). Ο βρόγχος ελέγχου παρακάτω προσπαθεί να συνδέσει όλα τα αλληλοεπηρεαζόμενα μέρη του συστήματος με την ενέργεια ώστε να εντοπιστούν ευκολότερα οι αιτίες πρόκλησης αυτής της επισφαλής κατάστασης.

Στον Πίνακα 18 εντοπίζονται οι αιτιώδεις παράγοντες οι οποίοι μπορούν να οδηγήσουν στην επισφαλή ενέργεια που αναφέρθηκε και παραπάνω αξιολογώντας τα δεδομένα του βρόγχου ελέγχου που φαίνεται στο Σχήμα 12. Η συγκεκριμένη επισφαλή ενέργεια ελέγχου που εξετάζεται από τον Πίνακα 12 είναι:

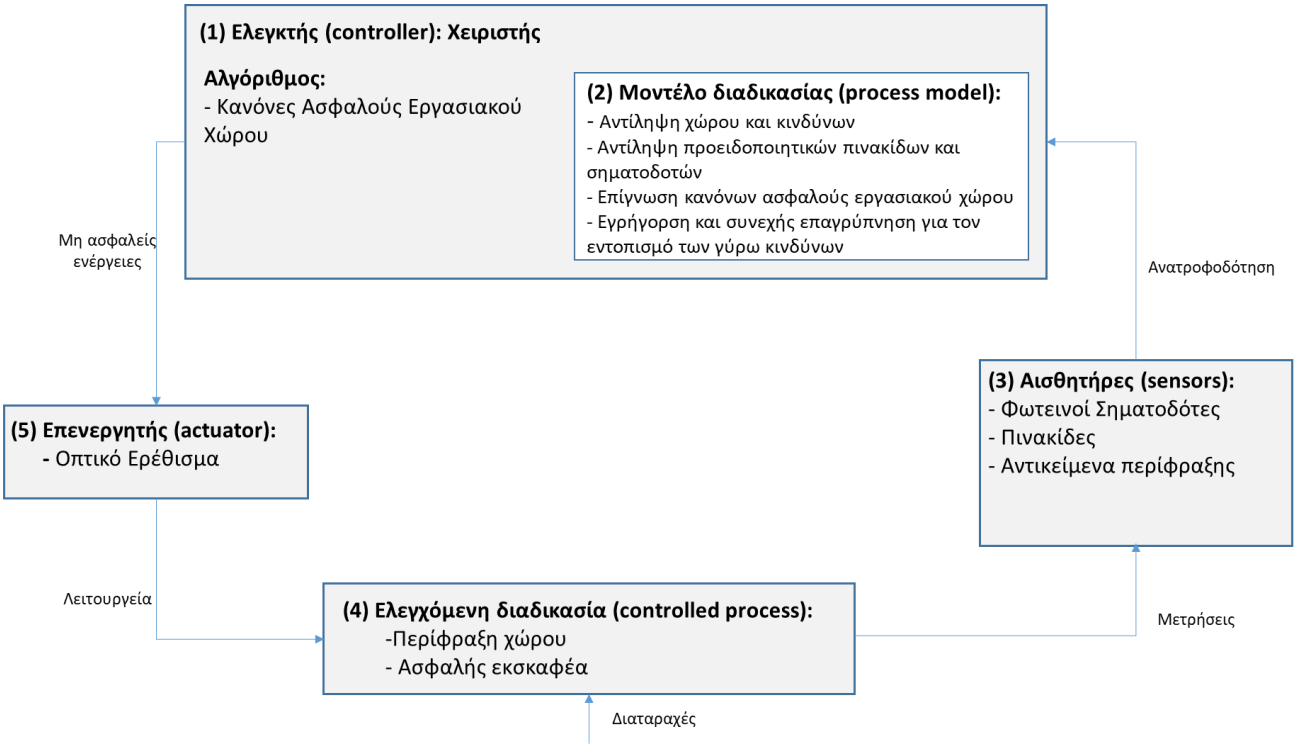
UCA-EX-48: Δεν εφαρμόζεται χαμηλή ταχύτητα και χαμηλή σχέση κιβωτίου σε κίνηση σε πλαγιά

Πίνακας 18: Αιτιώδεις παράγοντες ανάπτυξης επισφαλής ενέργειας UCA-EX-48

Συστατικό/Σύνδεση	**Σχετιζόμενοι Αιτιώδεις Παράγοντες**
(2) Μοντέλο διαδικασίας	• Μη τήρηση κανόνα ασφαλούς κίνησης σε πλαγιά με σκοπό να φτάσει γρηγορότερα στο σημείο εκσκαφής • Ελλιπής εκπαίδευση και γνώση των κανόνων ασφαλούς κίνησης • Υπερβολική εμπιστοσύνη στην προσωπική αντίληψη κίνησης αγνοώντας τις ενδείξεις των αισθητήρων
(3) Αισθητήρες	• Κάποιο/α από τα όργανα δεν λειτουργεί σωστά και δεν παίρνουμε σωστές ενδείξεις • Βρώμικο ταμπλό ενδείξεων με αποτέλεσμα να μην φαίνονται ξεκάθαρα οι ενδείξεις
(5) Επενεργητής - Ποδοστήριο ταχύτητας - Σχέση κιβωτίου ταχυτήτων	• Αστοχία ή δυσλειτουργία αισθητήρα της θέσης του ποδοστηρίου ταχύτητας • Αστοχία του ποδοστηρίου ταχύτητας με αποτέλεσμα να κολλήσει σε μία θέση • Δυσκολία εναλλαγής ταχυτήτων κιβωτίου λόγω μη καλής συντήρησης • Λειτουργεία εκσκαφέα παρά την μη πλήρη λειτουργική κατάσταση μέρους των σχέσεων του κιβωτίου ταχυτήτων

- <u>Βρόγχος ελέγχου και εντοπισμός αιτιών για επισφαλή ενέργεια σχετικά με τον περιβάλλοντα χώρο</u>

Στο Σχήμα 13 αναπτύσσεται ο βρόγχος ελέγχου για την επισφαλή ενέργεια σχετιζόμενη με τις επικρατούσες περιβαλλοντικές συνθήκες και πιο συγκεκριμένα για την μη εφαρμογή περίφραξης και φωτεινής σηματοδότησης στο χώρο εκσκαφής (UCA-EX-55).



Σχήμα 13: Βρόγχος ελέγχου επισφαλής ενέργειας UCA-EX-55

Στον Πίνακα 19 γίνεται προσπάθεια να εντοπιστούν οι αιτιώδεις παράγοντες οι οποίοι μπορούν να οδηγήσουν στην επισφαλή ενέργεια που αναφέρθηκε και παραπάνω αξιολογώντας τα δεδομένα του βρόγχου ελέγχου που φαίνεται στο Σχήμα 13. Η συγκεκριμένη επισφαλή ενέργεια ελέγχου που εξετάζεται από τον Πίνακα 13 είναι:

UCA-EX-55: Δεν εφαρμόζεται επαρκής σηματοδότηση και περίφραξη του χώρου εκσκαφής

Πίνακας 19: Αιτιώδεις παράγοντες ανάπτυξης επισφαλής ενέργειας UCA-EX-55

Συστατικό/Σύνδεση	Σχετιζόμενοι Αιτιώδεις Παράγοντες
(2) Μοντέλο διαδικασίας	• Μη αναγνώριση σημαντικότητας ύπαρξης επαρκής σηματοδότησης και περίφραξης του χώρου για την ασφαλή εκτέλεση της εκσκαφής • Ελλιπής εκπαίδευση και γνώση μέτρων ασφαλούς εργασίας • Μη τήρηση των προειδοποιητικών πινακίδων • Μη συνεχής έλεγχος της περιοχής γύρω από το σημείο εκσκαφής για παρουσία τρίτων με αποτέλεσμα τον τραυματισμό τους
(3) Αισθητήρες	• Μη λειτουργικοί σηματοδότες • Λανθασμένη επιλογή σημείου τοποθέτησης των πινακίδων με αποτέλεσμα να μην είναι εμφανή • Μη επαρκής αριθμός προειδοποιητικών πινακίδων • Τα αντικείμενα περίφραξης δεν επαρκούν για την πλήρη κάλυψη και προστασία του χώρου
(5) Επενεργητής - Οπτικό ερέθισμα	• Δεν δίνει έμφαση, στην επαρκή ή μη, περίφραξη και σηματοδότηση του χώρου λόγω κόπωσης

Παραπάνω αναπτύχθηκαν οι βρόγχοι ελέγχου μίας επισφαλής ενέργειας από κάθε μία κατηγορία ενεργειών ελέγχου προκειμένου να καλυφθεί όλο το φάσμα της χρήσης εκσκαφικού μηχανήματος έτσι ώστε να πλησιάσουμε όσο γίνεται στον εντοπισμό όλων των αιτιωδών παραγόντων που οδηγούν στην ανάπτυξη των επισφαλών καταστάσεων. Αυτή η διαδικασία προσδιορισμού αιτιωδών παραγόντων κανονικά πρέπει να ολοκληρωθεί για κάθε επισφαλή ενέργεια ελέγχου (unsafe control action) και το συνδυασμένο σύνολο από αυτές μπορεί στη συνέχεια να χρησιμοποιηθεί για να γραφτούν οι απαιτήσεις για τα συστατικά του συστήματος που θα συμβάλουν στην επιβολή και βελτίωση των περιορισμών ασφαλείας του συστήματος όπως αυτοί παρουσιάστηκαν προγενέστερα στον Πίνακα 10.

3.6 Εντοπισμός αιτιωδών παραγόντων παραβίασης περιορισμών ασφαλείας

Έπειτα από την ανάπτυξη του βήματος 2^{ο} της ανάλυσης STPA και τον εντοπισμό των αιτιών ανάπτυξης επισφαλών ενεργειών ελέγχου, σειρά έχει ο εντοπισμός των αιτιωδών παραγόντων παραβίασης των περιορισμών ασφαλείας που έχουν τεθεί στο σύστημα. Στο προηγούμενο βήμα, ο εντοπισμός των αιτιωδών παραγόντων έγινε μέσα από την κατασκευή βρόγχων ελέγχου για κάθε επισφαλή ενέργεια που σκοπό είχαν την κατανόηση των ενεργειών ελέγχου προκειμένου να εντοπιστούν τα αδύναμα σημεία που μπορεί να οδηγήσουν στην ανάπτυξη μίας επισφαλής ενέργειας. Στο στάδιο αυτό για τον εντοπισμό των αιτιωδών παραγόντων χρησιμοποιείται ο Πίνακας 14 που αναπτύχθηκε κατά το βήμα 1^{ο} της STPA και περιλαμβάνει τους περιορισμούς ασφαλείας του συστήματος. Πιο συγκεκριμένα για κάθε περιορισμό ασφαλείας του Πίνακα 14 γίνεται προσπάθεια εντοπισμού, μέσω εμπειρικών κανόνων, όλων των αιτιών που μπορούν να οδηγήσουν σε παραβίαση αυτού του περιορισμού. Στον Πίνακα 20 που φαίνεται παρακάτω παρουσιάζονται αναλυτικά ανά περιορισμό ασφαλείας όλες οι αίτιες που εντοπίστηκαν.

Πίνακας 20: Αιτιώδεις παράγοντες παραβίασης των περιορισμών ασφαλείας

Περιορισμοί Ασφαλείας	Αιτιώδεις παράγοντες
SC-EX-1: Ο χειριστής δεν πρέπει να απομακρύνεται σε καμία περίπτωση ενώ αυτό βρίσκεται σε λειτουργεία	• Μη συμμόρφωση με την οδηγία • Θεώρηση αυτού του μέτρου μη σημαντικού με αποτέλεσμα την αγνόηση του • Υπερβολική εμπιστοσύνη του χειριστή στις ικανότητες του στο ότι δεν πρόκειται να συμβεί τίποτα αν απομακρυνθεί
SC-EX-2: Χρήση κατάλληλου εγχειριδίου checklist για την εκτέλεση της εξωτερικής επιθεώρησης πριν και μετά την εκσκαφή	• Μη ύπαρξη checklist ενεργειών επιθεώρησης εκσκαφέα • Τα βήματα της επιθεώρησης έχουν παραληφθεί ή είναι σε λάθος σειρά • Μη ενημερωμένο checklist • Φθαρμένο ή ελλιπές checklist
SC-EX-3: Ο χειριστής θα πρέπει να ακολουθεί πιστά όλες τις οδηγίες ασφαλούς χρήσης και χειρισμού του εκσκαφέα και να εκπαιδεύεται συνεχώς και να εξετάζεται για τις γνώσεις του αυτές σε τακτά χρονικά διαστήματα	• Μη σωστή ή μη επαρκής εκπαίδευση του χειριστή είτε σε θεωρητικό είτε σε πρακτικό επίπεδο • Μη καλή επίγνωση των ασφαλών πρακτικών χρήσης του εκσκαφέα που προβλέπει ο κατασκευαστής ή των χαρακτηριστικών του • Μη συνεχής επανεκπαίδευση ή απουσία αυτής • Μη σωστή, ελλιπής ή ανύπαρκτη επαναξιολόγηση του χειριστή για τον έλεγχο των γνώσεων και δεξιοτήτων του

SC-EX-4: Απαρέγκλιτη χρήση προστατευτικού ατομικού εξοπλισμού (κράνος, ωτοασπίδες, γάντια, παπούτσια αντιολισθητικά, φωσφορίζων γιλεκάκι) πριν την προσέγγιση στον εκσκαφέα	• Μη παροχή του απαραίτητου προστατευτικού εξοπλισμού • Μη σωστή εκπαίδευση και άγνοια της σημαντικότητας αυτών για την προσωπική υγεία και ασφάλεια του χρήστη • Υπερβολική αυτοπεποίθηση του χειριστή ότι δεν πρόκειται να συμβεί τίποτα από την μη χρήση • Αποφυγή χρήσης του εξοπλισμού προκειμένου να εκτελούνται οι εργασίες πιο εύκολα και πιο άνετα
SC-EX-5: Χρήση ειδικού συστήματος όπου χωρίς την τοποθέτηση των ζωνών ασφαλείας να μην εκκινεί ο εκσκαφέας ή χρήση διαπεραστικού ήχου εντός της καμπίνας αν δεν γίνει η χρήση της	• Περιφρόνηση του προειδοποιητικό ήχου και κανονική συνέχιση των εργασιών εκσκαφής • Μη χρήση ειδικού συστήματος ώστε να μην εκκινεί ο εκσκαφέας σε περίπτωση μη τοποθέτησης της ζώνης ασφαλείας • Απενεργοποίηση του προειδοποιητικού ήχου ώστε να μην τον ενοχλεί κατά την εκτέλεση της εργασίας • Χρήση του εκσκαφέα ενώ οι ζώνες ασφαλείας είναι μη λειτουργικές
SC-EX-6: Μη παρέκκλιση από τα μέγιστα επιτρεπόμενα όρια του εκσκαφέα	• Σύγχυση των ορίων με άλλου τύπου εκσκαφέα • Αγνόηση των μέγιστων ορίων του εκσκαφέα • Παράβλεψη αυτών ώστε να εκτελεστεί πιο γρήγορα η δουλειά
SC-EX-7: Μη χρήση εκσκαφέα για εξυπηρέτηση άλλων σκοπών και διευκολύνσεων	• Εσκεμμένη παραβίαση του κανόνα για εξυπηρέτηση προσωπικών σκοπών του χειριστή και επιτάχυνση διαδικασιών εκσκαφής
SC-EX-8: Σήμανση εντός της καμπίνας βασικών κανόνων ασφαλείας χειρισμού και μέγιστων επιτρεπόμενων ορίων του εκσκαφέα	• Ελλιπής σήμανση της καμπίνας με τους βασικούς κανόνες ασφαλείας • Απώλεια ή φθορά της σήμανσης • Αγνόηση των προτροπών της σήμανσης
SC-EX-9: Προϋπόθεση ώστε να πάρει τα κλειδιά του εκσκαφέα είναι η παράδοση του κινητού τηλεφώνου πριν την έναρξη των εργασιών και χρήση μόνο ασυρμάτου για την ενδοεπικοινωνία καθώς και η αντίστροφη διαδικασία	• Παράβλεψη και ολιγωρία στην εφαρμογή του κανόνα • Θεώρηση του μέτρου ως υπερβολικό με αποτέλεσμα την άρνηση παράδοσης του κινητού τηλεφώνου από τον χειριστή
SC-EX-10: Χρήση εξωτερικού βοηθού – παρατηρητή σε κάθε περίπτωση εκσκαφής ανεξαρτήτου συνθηκών χειριστή	• Απειρία και ελλιπής γνώση από τον βοηθό των επικίνδυνων καταστάσεων κατά την χρήση εκσκαφικού μηχανήματος • Αγνόηση από τον χειριστή των υποδείξεων του βοηθού • Νωχελικές και καθυστερημένες υποδείξεις του βοηθού και γενικότερα απόσπαση της προσοχής του από την εργασία του με αποτέλεσμα την μη έγκαιρη προειδοποίηση για μια επισφαλή κατάσταση • Μη χρησιμοποίηση βοηθού σε κάποιες περιπτώσεις για εξοικονόμηση πόρων
SC-EX-11: Χρήση προειδοποιητικών πινακίδων σηματοδότησης του χώρου εργασίας καθώς και περίφραξη αυτού	• Ελλιπής ή μη επαρκής σηματοδότηση ή/και περίφραξη • Τοποθέτηση των πινακίδων σε λάθος ή μη ορατό σημείο • Παραβίαση περίφραξης από τρίτους και είσοδο στο χώρο εκσκαφής
SC-EX-12: Τήρηση κανόνων διασφάλισης ασφαλούς περιβάλλοντος εργασίας (είτε καιρικών είτε εργασιακών) και διακοπή αυτής εάν δεν το ευνοούν οι περιβαλλοντικές συνθήκες	• Μη σωστή μελέτη χώρου εκσκαφής (κλίση, υπέδαφος, σκληρότητα εδάφους κ.ά.) • Μη σωστή εκτίμηση καιρικών συνθηκών • Συνέχιση εργασιών εκσκαφής παρά την επιδείνωση των καιρικών φαινομένων εκτός επιτρεπόμενων ορίων • Μη τήρηση των συνθηκών ασφαλούς εργασίας όπως επαρκής φωτισμός και εξαερισμός του εργασιακού χώρου

Κεφάλαιο 4ο Συμπεράσματα

Ουσιαστικά, έπειτα και από την ολοκλήρωση του εντοπισμού των αιτιωδών παραγόντων παραβίασης των περιορισμών ασφαλείας η μελέτη επικινδυνότητας της χρήσης εκσκαφικού μηχανήματος με ανεστραμμένο κάδο μπορεί να θεωρηθεί ότι ολοκληρώθηκε.

Σκοπός της παρούσας διπλωματικής υπήρξε η μελέτη της χρήσης εκσκαπτικού μηχανήματος με ανεστραμμένο κάδο και η ανάπτυξη ασφαλών πρακτικών και περιορισμών ώστε να μειωθεί στο μέγιστο δυνατό η επικινδυνότητα χρήσης του και να αποφευχθεί και να αποτραπεί οποιοδήποτε ατύχημα (είτε τραυματισμός είτε απώλεια είτε φθορά εξοπλισμού) στο μέλλον. Για τον σκοπό αυτού αναπτύξαμε μια ανάλυση επικινδυνότητας της χρήσης εκσκαφέα με τη βοήθεια της μεθόδου STPA, όπου αυτή η ανάλυση αρχικά στόχευσε στον εντοπισμό των επισφαλών ενεργειών κατά την χρήση του εκσκαφέα, και την ανάπτυξη περιορισμών ασφαλείας για την αποτροπή των επισφαλών αυτών ενεργειών. Πέρα όμως των παραπάνω η ανάλυση αυτή στο τελευταίο της βήμα μας καθοδήγησε στον εντοπισμό των αιτιωδών παραγόντων που μπορεί να οδηγήσουν στην ανάπτυξη μίας επισφαλούς ενέργειας αλλά ακόμα σημαντικότερα και στον εντοπισμό των αιτιών που μπορεί να οδηγήσουν σε παραβίαση των περιορισμών ασφαλείας του συστήματος που. Ο εντοπισμός των αιτιών αυτών αποτελεί την ρίζα του προβλήματος και συμβάλλει στην βελτίωση και αναθεώρηση των διαδικασιών χρήσης του εκσκαφέα.

Ανακεφαλαιώνοντας, στην παρούσα διπλωματική ξεκινήσαμε την ανάλυση με μια θεωρητική αναφορά στα εκσκαπτικά μηχανήματα και τα είδη αυτών ανάλογα με τη χρήση τους ενώ πιο συγκεκριμένα επικεντρωθήκαμε στα χαρακτηριστικά του εκσκαφέα με ανεστραμμένο κάδο και στις ασφαλές πρακτικές χρήσης του. Στη συνέχεια, παρουσιάσαμε διάφορες μεθόδους ανάλυσης επικινδυνότητας δίνοντας έμφαση στα χαρακτηριστικά και στην τεχνική ανάπτυξης της μεθόδου STPA όπου χρησιμοποιείται στην παρούσα διπλωματική.

Ακολούθως, πραγματοποιήθηκε η ανάπτυξη της μεθόδου STPA, ξεκινώντας από τον καθορισμό των θεμελίων της μηχανικής συστημάτων όπου προσδιορίστηκαν τα ατυχήματα και οι κίνδυνοι του συστήματος χειριστή – εκσκαφέα. Η ανάπτυξη και ο σχεδιασμός της δομής λειτουργικού ελέγχου ήταν το επόμενο και αναγκαίο βήμα έτσι ώστε να γίνει σαφής η αλληλεπίδραση μεταξύ του χειριστή και του εκσκαφέα και να προσδιοριστούν οι ενέργειες ελέγχου του συστήματος. Από την δομή λειτουργικού ελέγχου προέκυψαν 5 ενέργειες ελέγχου του χειριστή (εξωτερική επιθεώρηση, μέγιστο βάρος, ταχύτητα, χειρισμός, συνθήκες περιβάλλοντος) σε όλο το φάσμα της χρήσης του και αντίστοιχα προσδιορίστηκαν και οι ανατροφοδοτήσεις του εκσκαφέα προς τον χείριστή.

Έχοντας λοιπόν προσδιορίσει τα θεμέλια και τη δομή του συστήματος προχωρήσαμε στο 1ο Βήμα της ανάλυσης STPA όπου εντοπίστηκαν 64 επισφαλείς ενέργειες από την χρήση του εκσκαφικού μηχανήματος οι οποίες ομαδοποιήθηκαν ανά ενέργεια ελέγχου. Στη συνέχεια βασιζόμενοι σε αυτές τις επισφαλείς ενέργειες αναπτύχθηκαν 12 περιορισμοί ασφαλείας του συστήματος που στόχο έχουν να αποτρέψουν την ανάπτυξη των επισφαλών αυτών ενεργειών. Τα κυριότερα

συμπεράσματα που προέκυψαν από αυτό το βήμα της ανάλυσης είναι ότι τη μεγαλύτερη βαρύτητα για την αποτροπή των περισσοτέρων επισφαλών ενεργειών κατά την χρήση του εκσκαφέα συγκεντρώνουν η σωστή και πλήρης εκπαίδευση του χειριστή, η πιστή εφαρμογή των οδηγιών ασφαλούς χρήσης και χειρισμού του κατασκευαστή και η χρήση ενός τυποποιημένου checklist ενεργειών.

Έπειτα, στο 2ο Βήμα της ανάλυσης STPA αναπτύξαμε τους βρόγχους ελέγχου για 5 επισφαλείς ενέργειες (μια επισφαλή ενέργεια ανά κατηγορία ενεργειών ελέγχου) προκειμένου να εντοπιστούν οι αιτιώδεις παράγοντες ανάπτυξης αυτών των επισφαλών καταστάσεων. Τέλος, χρησιμοποιώντας τους περιορισμούς ασφαλείας που έχουμε ήδη ορίσει στο 1ο Βήμα έγινε μια προσπάθεια εντοπισμού των αιτιωδών παραγόντων οι οποίοι μπορεί να οδηγήσουν σε παραβίαση των περιορισμών αυτών. Με τον τρόπο αυτό μπορεί να εντοπιστούν πιθανά «κενά» ασφαλείας στην οργάνωση του συστήματος το οποίο αυτομάτως μας οδηγεί στην βελτίωση των διαδικασιών και των πρακτικών ασφαλούς χρήσης του εκσκαφέα αναπτύσσοντας νέους περιορισμούς ασφαλείας ή βελτιώνοντας τους ήδη υπάρχοντες έτσι ώστε να αποφευχθεί στο μέλλον η οποιαδήποτε δημιουργία επικίνδυνης κατάστασης.

Βιβλιογραφία

Διεθνής Βιβλιογραφία

Matthew Seth Placke (2014), Application of STPA to the Integration of Multiple, Control Systems: A Case Study and New Approach, Massachusetts Institute Of Technology

Nancy Leveson (2013), An STPA Primer, Version 1, August 2013, Massachusetts Institute Of Technology

David Fox (2014), Inadvertent operation of controls in excavator plant - insight analysis and recommendations for prevention by design, Health and Safety Laboratory

Esref Emrah Kazan (2013), Analysis Of Fatal And Nonfatal Accidents Involving Earthmoving Equipment Operators And On-Foot Workers, Wayne State University

Nancy Leveson (2011), Engineering a Safer World, Systems Thinking Applied to Safety, The MIT Press, Cambridge Massachusetts Institute Of Technology

Yuki Sakaida et al. (2008), The Analysis of Excavator Operation by Skillful Operator, 2008 SICE Annual Conference

Mine Safety and Health Administration (MSHA), Module Number 5, On-the Job Training Modules for surface metal and nonmetal mines, Backhoe and Hydraulic Excavator Operation, USA Department of Labor

R. Burgess-Limerick et al. (2014), Bow-tie analysis of a fatal underground coal mine collision, Human Factors and Ergonomics Society of Australia

INGAA Foundation Inc. (September 2012), Construction Safety Consensus Guidelines, Trenching and Excavation Safety

Prakash Kumar & Arvind Kumar (2016), Methods for Risk Management of Mining Excavator through FMEA and FMECA, The International Journal Of Engineering and Science (IJES) pg 57-63

D. Seward et al. (2000), Safety analysis of autonomous excavator functionality, Reliability Engineering and System Safety pg 29-39

Clark Equipment, Risk Assessment for Bobcat Excavator Models: M Series, Version 1

Occupational Safety and Health Branch (2005), Code of Practice on Safe Use of Excavators, USA Labor Department

Contra Costa Water District (2010), Standard Operating Procedure, Excavation Safety – Safe Working Practices for Excavations

Tom Finnegan (2014), Job Hazard Analysis for Excavate, break out and remove existing tanks, Dakin Service Station Contractors Limited

Martelco Equipment Hire (2014), Safe Work Procedures, Excavator, Advanced Safety Systems Australia and New Zealand (Version 1.3)

Ελληνική Βιβλιογραφία

Κοντογιάννης Θ. (2016), Εργονομικές Προσεγγίσεις στη Διοίκηση και Διαχείρηση της Ασφάλειας, Θεσσαλονίκη: Εκδόσεις Τζιόλα

Καινουριάκη Μαρία (2016), Ανάλυση επικινδυνότητας χειρισμού εκσκαφέα, Πολυτεχνείο Κρήτης, Τμήμα Μηχανικών Παραγωγής και Διοίκησης

Κοντόπουλος Νικόλαος (2008), Μελέτη Σχήματος Οργάνωσης Παραγωγικών Διαδικασιών και Διαδικασιών Υπηρεσιών σε Επιχείρηση Συντήρησης – Αναβάθμισης Μηχανημάτων Έργων, ΤΕΙ Καβάλας, Σχολή Τεχνολογικών Εφαρμογών, Τμήμα Μηχανολογίας