Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ. «Ασφάλεια Ψηφιακών Συστημάτων»

Μεταπτυχιακή Διπλωματική Εργασία

Κυβερνοεπιθέσεις στο cyber-enabled πλοίο

Cyber-attacks against the cyber-enabled ship

Καβαλλιεράτος Γεώργιος

Επιβλέπων: Καθηγητής Κάτσικας Κ. Σωκράτης

Πειραιάς, Ιανουάριος 2018

Περίληψη

Η διαρκής διείσδυση των νέων τεχνολογιών στα συστήματα των πλοίων έχει οδηγήσει τον χώρο της ναυτιλίας στην κατασκευή πλοίων τα οποία είναι εφοδιασμένα με σύγχρονα cyber-physical συστήματα, που επιτρέπουν τον χειρισμό των πλοίων από απόσταση. Αν τα πλοία αυτά δεν κατασκευαστούν λαμβάνοντας υπόψιν τη κυβερνοασφάλεια από το στάδιο του σχεδιασμού τους, σύντομα θα έρθουν αντιμέτωπα με περιστατικά ασφάλειας παρόμοια με αυτά τα οποία έχουμε συναντήσει στη βιομηχανία η οποία έχει ήδη αφομοιώσει συστήματα ICT, χωρίς να καλύψει επαρκώς τα θέματα ασφάλειας που αυτά συνεπάγονται.

Στην παρούσα διπλωματική εργασία έχει αναπτυχθεί μία μορφή της αρχιτεκτονικής ενός cyber-enabled πλοίου, με σκοπό στη συνέχεια να μελετηθεί η ασφάλειά του, πραγματοποιώντας αναλύσεις επιθέσεων και κινδύνων στα συστήματά του. Αφού αναπτύξουμε μία δενδρική δομή της αρχιτεκτονικής, στη συνέχεια εφαρμόσαμε υψηλού επιπέδου ανάλυση απειλών σύμφωνα με τη μεθοδολογία STRIDE, η οποία μας επέτρεψε να παρατηρήσουμε και να αξιολογήσουμε τις πιθανές επιπτώσεις που έχουν αυτές οι απειλές στα συστήματα και τα υποσυστήματα του πλοίου. Επίσης, υπολογίσαμε τα αντίστοιχα επίπεδα κινδύνου που αντιστοιχούν στις απειλές, βασιζόμενοι στη σχετική βιβλιογραφία.

Τα αποτελέσματα της εργασίας αποτελούν τη βάση για περαιτέρω ανάλυση της ασφάλειας των cyber-physical συστημάτων του πλοίου και συμβάλλουν στην ασφαλέστερη λειτουργία του.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου και επιβλέπων στην παρούσα εργασία, κύριο Σωκράτη Κάτσικα για τη καθοδήγησή του και την ευκαιρία που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα.

Ευχαριστίες επίσης θα ήθελα να δώσω στη κοπέλα μου για την στήριξη και τα χρήσιμα σχόλιά της, καθόλη την διάρκεια διεκπεραίωσης της παρούσας εργασίας.

Ιανουάριος 2018

Γιώργος Καβαλλιεράτος

Περιεχόμενα

Κατάλογος εικόνων

Κατάλογος Πινάκων

Κεφάλαιο 1

1.1 Εισαγωγή

Τα αυτόνομα οχήματα αποτελούν πλέον πόλο έλξης τόσο για τη βιομηχανία όσο και για τους πολίτες. Υπάρχουν πολλά παραδείγματα αυτόνομων οχημάτων, όπως είναι οι υπόγειοι σιδηρόδρομοι, οχήματα μεταφορών, drones και οχήματα καθοδήγησης φορτώσεων και εκφορτώσεων (AGV). Τα αυτόνομα πλοία αποτελούν ακόμη ένα παράδειγμα αυτών των οχημάτων, συμβάλλοντας στην ελάττωση της ρύπανσης του περιβάλλοντος και στην ασφαλέστερη και οικονομικότερη πλοήγηση.

Η ανάπτυξη των Τεχνολογιών της Πληροφορίας και Τηλεπικοινωνιών (ΤΠΕ) τα τελευταία χρόνια πυροδότησε την ανάπτυξη σύγχρονων συστημάτων, τα οποία συνέβαλλαν και συμβάλλουν στην αποτελεσματικότερη και ασφαλέστερη λειτουργία των πλοίων, με το πλήθος των μελών του πληρώματος να μειώνεται σημαντικά. [1]

Η ναυτιλιακή βιομηχανία, λόγω του ανταγωνιστικού της χαρακτήρα, καθώς και λόγω του χαμηλού κόστους της υιοθέτησης των ΤΠΕ, πραγματοποιεί ολοένα και μεγαλύτερα βήματα για τον σχεδιασμό και την κατασκευή των αυτόνομων πλοίων. Η ραγδαία ανάπτυξη των ΤΠΕ οδηγεί τη βιομηχανία στην ανάπτυξη ενός νέου μοντέλου πλοίου, η πλοήγηση του οποίου θα γίνεται εξ αποστάσεως, με καινοτόμα συστήματα επικοινωνίας και διασύνδεσης. Εταιρείες όπως η Rolls-Royce σχεδιάζουν πλοία με μειωμένο προσωπικό και μακρόθεν υποστήριξη, τα οποία θα πλεύσουν το 2020 και αυτόνομα πλοία τα οποία θα είναι σε θέση να πλέουν σε ανοιχτές θάλασσες το 2035 [2].

Υπάρχουν δύο εναλλακτικά μοντέλα υλοποίησης του αυτόνομου πλοίου: αυτό του τηλεχειριζόμενου πλοίου και εκείνο του πλήρως αυτόνομου. Στο πρώτο, όλες ο διεργασίες του πλοίου εκτελούνται από απόσταση, από ένα κέντρο ελέγχου το οποίο βρίσκεται στη στεριά, ενώ στο δεύτερο συστήματα αυτόματης λήψης αποφάσεων αναλαμβάνουν τον πλήρη έλεγχο του πλοίου, χωρίς καθόλου ανθρώπινη παρέμβαση.

Το αυτόνομο πλοίο, ανεξάρτητα από το μοντέλο υλοποίησης που ακολουθεί, αποτελεί ένα συνδυασμό συστημάτων βιομηχανικού ελέγχου και συστημάτων πληροφορικής, που είναι γνωστά ως cyber-physical systems, οδηγώντας έτσι στον όρο cyber-enabled ship. Στα συστήματα αυτά η φυσική διεργασία που ελέγχεται είναι τόσο στενά συνδεδεμένη με το σύστημα πληροφορικής που την ελέγχει, ώστε δεν είναι εύκολο (ή και δυνατό) να αποδοθεί ένα αποτέλεσμα στη φυσική διεργασία ή στο σύστημα ελέγχου. Αν και η διάδοση των συστημάτων αυτών οδηγεί σε σημαντικά οφέλη, ωστόσο δημιουργεί μεγάλα ζητήματα ασφάλειας. Τούτο επειδή είναι γνωστό ότι τα περισσότερα συστήματα βιομηχανικού ελέγχου δεν έχουν σχεδιαστεί λαμβάνοντας υπόψιν την ασφάλεια των διεργασιών τους, καθώς παλαιότερα τα συστήματα αυτά δεν διασυνδέονταν στο διαδίκτυο, με αποτέλεσμα τώρα πια να είναι ευάλωτα και ευκόλως προσβάσιμα σε εξωτερικούς παράγοντες, από τη στιγμή που το συνολικό δίκτυο είναι συνδεδεμένο με τον έξω κόσμο. Αυξανόμενες είναι οι αναφορές στις επιθέσεις που έχουν πραγματοποιηθεί επιτυχώς εναντίον συστημάτων βιομηχανικού ελέγχου, καθώς τις περισσότερες φορές οι επιτιθέμενοι εκμεταλλεύονται τις ευπάθειες των συστημάτων του ενδοεπιχειρησακού εξοπλισμού με σκοπό να αποκτήσουν πρόσβαση στο σύστημα ελέγχου [2].

1.2 Αυτόνομο πλοίο

Προκειμένου να ορίσουμε το αυτόνομο πλοίο, θα πρέπει πρώτα να γίνει κατανοητή η έννοια του αυτόνομου. Η ρίζα της λέξης αυτόνομος προέρχεται από τις δύο ελληνικές "αυτός" και "νέμω" που σημαίνει ότι μία αυτόνομη οντότητα είναι σε θέση να λαμβάνει αποφάσεις μόνη της, να είναι ανεξάρτητη [3].

Υπάρχουν πολλοί διαφορετικοί ορισμοί για τις έννοιες του αυτόνομου και της σχετικής έννοιας της μηχανικής νοημοσύνης (machine intelligence) στη βιβλιογραφία. Τα επίπεδα τις αυτονομίας (Levels of Autonomy-LOA) συνήθως χρησιμοποιούντα για να περιγράψουν τον βαθμό αυτονομίας ενός μηχανήματος. Μία από τις περισσότερο γνωστές περιγραφές των επιπέδων αυτονομίας είναι αυτή του Thomas Sheridan, η οποία πραγματοποιεί μία κατηγοριοποίηση δέκα επιπέδων, ξεκινώντας από συστήματα τα οποία δεν λειτουργούν χωρίς ανθρώπινη παρέμβαση, μέχρι συστήματα τα οποία είναι τελείως ανεξάρτητα και δρουν μόνα τους [7].

Επίπεδο	Περιγραφή
10	Ο υπολογιστής αποφασίζει μόνος του, δρα αυτόνομα, αγνοώντας τον ανθρώπινο παράγοντα.
9	Ο υπολογιστής ενημερώνει τον άνθρωπο μόνο εάν ο υπολογιστής το αποφασίσει.
8	Ο υπολογιστής ενημερώνει των άνθρωπο μόνο εάν του ζητηθεί.
7	Ο υπολογιστής δρα αυτόνομα και μόνο αν είναι απαραίτητο ενημερώνει τον άνθρωπο.
6	Ο υπολογιστής επιτρέπει περιορισμένο χρόνο εναντίωσης του ανθρώπου πριν την έναρξη των αυτόνομων διεργασιών.
5	Ο υπολογιστής εκτελεί τις προτεινόμενες ενέργειες εφόσον ο ανθρώπινος παράγοντας το εγκρίνει.
4	Ο υπολογιστής προτείνει μία εναλλακτική επιλογή.
3	Ο υπολογιστής περιορίζει τις εναλλακτικές επιλογές.
2	Ο υπολογιστής προσφέρει ένα πλήρες σύνολο εναλλακτικών.
1	Ο υπολογιστής δεν προσφέρει καμία βοήθεια, ο άνθρωπος είναι υπεύθυνος για όλες τις ενέργειες.

Πίνακας 1.Τα 10 στάδια αυτονομίας του Thomas Sheridan [8]

Μία πρώτη προσπάθεια ορισμού του αυτόνομου πλοίου βασίστηκε στα 10 στάδια αυτονομίας του T.B. Sheridan [4], προσαρμόζοντάς τα στις τέσσερις βασικές λειτουργίες του πλοίου, οι οποίες είναι: 1) συλλογή πληροφοριών, 2) ανάλυση πληροφορίας, 3) λήψη αποφάσεων και επιλογή δράσεων και 4) εφαρμογή των δράσεων [5]. Ο ορισμός όμως αυτός δεν καλύπτει πλήρως τις λειτουργίες του πλοίου, αλλά μόνο μέρη αυτών. Για τον λόγο αυτόν προτάθηκε ένας νέος ορισμός του αυτόνομου πλοίου σύμφωνα με τον οποίο θα υπάρχει ένα σύστημα ελέγχου υπεύθυνο για τον χειρισμό, τον συντονισμό των διαδικασιών και τη συνεχή παρακολούθηση του πλοίου [6].

Η αρχική ιδέα υλοποίησης του αυτόνομου πλοίου είναι να εκτελούνται όλες οι διεργασίες αυτοματοποιημένα χωρίς ανθρώπινη παρέμβαση. Μία τέτοια υλοποίηση περιγράφεται στο ευρωπαϊκό έργο MUNIN [9]. Το MUNIN (Marine Unmanned Navigation through Intelligence in Networks)[1] είναι ένα έργο που ολοκληρώθηκε τον Ιούνη του 2016 και στόχος του ήταν η ανάπτυξη και ο έλεγχος της ιδέας του αυτόνομου πλοίου, οδηγώντας και σε ορισμένες πιλοτικές υλοποιήσεις [9]. Στην περίπτωση που οι αυτοματοποιημένες λειτουργίες αποτύχουν, τότε το πλοίο θα τίθεται υπό τον έλεγχο του κέντρου ελέγχου ξηράς (Shore Control Center) και στην περίπτωση όπου και σε αυτή την επικοινωνία δημιουργηθεί πρόβλημα, το πλοίο θα είναι προγραμματισμένο με συγκεκριμένο τρόπο ώστε να μεταβαίνει στον ασφαλέστερο κοντινό προορισμό, συνήθως με τη βοήθεια πληρώματος το οποίο θα έχει επιβιβαστεί στο πλοίο μέσω του συστήματος των "rendezvous" [11]. Το έργο αυτό στηρίζεται στην άμεση επικοινωνία του πλοίου με το Shore Control Center και στον συνδυασμό των αυτοματοποιημένων διεργασιών με τον ανθρώπινο παράγοντα. Το συμπέρασμα είναι ότι το αυτόνομο πλοίο μπορεί να είναι λειτουργικό με πολλές μορφές αυτονομίας κατά τη διάρκεια του ταξιδιού του, αφού αποτελεί συνδυαστική εφαρμογή λειτουργιών οι οποίες προέρχονται άλλοτε από τον άνθρωπο, άλλοτε από αυτοματοποιημένες διαδικασίες και άλλοτε από τον συνδυασμό των δύο. Ο βαθμός λοιπόν αυτονομίας του πλοίου είναι άμεσα εξαρτώμενος από τον βαθμό εμπλοκής του ανθρώπου.

1.3 Διαφορές Συμβατικού, Τηλεχειριζόμενου και Αυτόνομου πλοίου

Προκειμένου ένα πλοίο να λειτουργεί κανονικά, είτε είναι αυτόνομο είτε όχι, είναι απαραίτητο να εκτελούνται οι εξής λειτουργίες και δραστηριότητες [12]: 1) Συλλογή πληροφοριών (όπως η συλλογή δεδομένων από το σύστημα αισθητήρων), 2) Ανάλυση δεδομένων, 3) Λήψη αποφάσεων (απόφαση για τη μείωση ταχύτητας ή αποφυγή εμποδίου), και 4) Εφαρμογή αυτών των αποφάσεων (ελιγμοί, ή σταμάτημα του πλοίου). Η απουσία του ανθρώπινου παράγοντα, δεν αποτελεί τη μοναδική διαφορά μεταξύ ενός συμβατικού πλοίου και ενός αυτόνομου. Σημαντική διαφορά μεταξύ των δύο αποτελεί και η επεξεργασία, η διαχείριση και η εφαρμογή των αντίστοιχων αποφάσεων που σε ένα συμβατικό πλοίο τις εφαρμόζει το πλήρωμα και ο πλοίαρχος.

1.3.1 Συμβατικά πλοία

Στα συμβατικά πλοία, πολλά συστήματα, όπως π.χ. το Automatic Identification System (AIS), τα Radar και το Long Range Identification and Tracking (LRIT), συγκεντρώνουν πληροφορίες από το περιβάλλον του πλοίου. Το Global Positioning System (GPS) παρέχει πληροφορίες για τη θέση που βρίσκεται το πλοίο και οι επικοινωνίες πραγματοποιούνται μέσω Very High Frequency (VHF) και δορυφορικών συνδέσεων. Επίσης, πολλά είναι τα συστήματα τα οποία συγκεντρώνουν πληροφορίες σχετικά με τα μηχανικά μέρη του πλοίου, το φορτίο κλπ. Όλα τα παραπάνω συστήματα έχουν τη δυνατότητα συλλογής πληροφορίας, ικανοποιώντας τη πρώτη συνθήκη του [12] αλλά δεν παρέχουν σχεδόν κανένα μηχανισμό ανάλυσης δεδομένων και λήψης αποφάσεων. Τα τελευταία χρόνια έχει πραγματοποιηθεί μία σημαντική αλλαγή στη ναυτιλία με την εισαγωγή του e-navigation [13] το οποίο παρέχει πλέον στα πλοία μία σύγχρονη εκδοχή των συστημάτων τους, επιτρέποντάς τους να εφαρμόζουν σε ορισμένες περιπτώσεις και ανάλυση των δεδομένων που συλλέγουν. Παρόλες αυτές τις αυτοματοποιημένες διαδικασίες ο ανθρώπινος

[1] Munin ("mind") ονομαζόταν ένα από τα δύο κοράκια του θεού Όντιν στη Νορβηγική μυθολογία το οποίο πετούσε το πρωί και επέστρεφε το βράδυ μεταφέροντας όλα τα νέα του κόσμου στον Όντιν [10].

παράγοντας μέσα στο πλοίο είναι αναγκαίος για τη διεκπεραίωση των λειτουργιών των συστημάτων, ελέγχοντας τα δεδομένα που παρέχονται σε αυτά. Επίσης, στα συμβατικά σημερινά πλοία, ο ανθρώπινος παράγοντας διαδραματίζει σημαντικό ρόλο στην αναγνώριση πολλών καταστάσεων του πλοίου (Situational Awareness), συνεισφέροντας μέσω τις εμπειρίας και των αισθήσεών του. Αισθητικά ερεθίσματα όπως είναι η οσμή καπνού ή το άκουσμα ενός ασυνήθιστου ήχου υποβοηθούν στο συσχετισμό του αιτίου με τα αντίστοιχα μέρη του πλοίου.

1.3.2 Τηλεχειριζόμενα πλοία

Τα τηλεχειριζόμενα πλοία συνδυάζουν τις τεχνολογίες του συμβατικού με εκείνες του αυτόνομου πλοίου για τη διαπεραίωση των λειτουργιών του. Αυτό σημαίνει ότι όλες οι διεργασίες εκτελούνται από συστήματα τα οποία είναι απαραίτητα και στα συμβατικά, όπως είναι το AIS και το Global Maritime Distress and Safety System (GMDSS), με τη διαφορά ότι η συλλογή και η ανάλυση των δεδομένων όλων αυτών των συστημάτων δεν πραγματοποιείται στο πλοίο από το πλήρωμά του αλλά συνήθως από ένα κέντρο ελέγχου το οποίο βρίσκεται στη στεριά. Σε αυτό το κέντρο βρίσκονται όλοι οι "ρόλοι" που θα έπρεπε να παρίστανται στο πλοίο και μέσω αυτοματοποιημένων και σύγχρονων τεχνολογιών πραγματοποιούν τους απαραίτητους χειρισμούς. Το συγκεκριμένο είδος πλοίων αποτελεί ένα ενδιάμεσο στάδιο μεταξύ του συμβατικού και του αυτόνομου πλοίου, για το οποίο η τεχνολογία και η τεχνογνωσία υπάρχει ήδη στον ναυτιλιακό κλάδο.

1.3.3 Αυτόνομα πλοία

Από την άλλη πλευρά, τα αυτόνομα πλοία βασίζουν τη διεκπεραίωση όλων των λειτουργιών τους σε αυτοματοποιημένα συστήματα τα οποία αποφασίζουν και δρούν από μόνα τους. Τα συστήματα τα οποία φέρει ένα αυτόνομο πλοίο είναι ίδια με αυτά ενός συμβατικού πλοίου, με επιπλέον σύγχρονα συστήματα λήψης αποφάσεων. Για τη σωστή και ομαλή λειτουργία αυτών των συστημάτων, η εισαγωγή των δεδομένων θα πρέπει να είναι ακριβής και διασταυρωμένη από εξιδεικευμένα συστήματα ανάλυσης δεδομένων, αφού απουσιάζει ο ανθρώπινος παράγοντας που πραγματοποιούσε τον αντίστοιχο έλεγχο στο συμβατικό πλοίο.

1.4 Στόχοι της εργασίας

Για την ευκολότερη και αποτελεσματικότερη περιγραφή του προβλήματος με το οποίο ασχολείται η παρούσα εργασία, είναι σκόπιμο να ορίσουμε ορισμένες βασικές έννοιες.

- **Απειλή**: οποιαδήποτε πράξη ή γεγονός που θα επηρέαζε αρνητικά ένα αγαθό του πληροφοριακού συστήματος μέσω μη εξουσιοδοτημένης πρόσβασης, καταστροφής, αποκάλυψης, τροποποίησης των δεδομένων και της διακοπής παροχής υπηρεσιών [14].
- **Επίθεση**: οποιαδήποτε κακόβουλη ενέργεια που σκοπό έχει να συλλέξει, διακόψει, αρνηθεί, αλλοιώσει, ή να καταστρέψει τα αγαθά του πληροφοριακού συστήματος [15].
- **Κίνδυνος**: το ενδεχόμενο ότι μία υπάρχουσα απειλή θα εκμεταλλευτεί μία ευπάθεια του συστήματος προκαλώντας ζημιά στο σύστημα/οργανισμό [14].
- **Συνέπεια**: το μέγεθος της βλάβης η οποία προκύπτει από τα αποτελέσματα των πράξεων της μη εξουσιοδοτημένης πρόσβασης, τροποποίησης, καταστροφής και απώλειας δεδομένων στα αγαθά ενός πληροφοριακού συστήματος [15].

- **Ανάλυση κινδύνων**: η διαδικασία αναγνώρισης των κινδύνων του συστήματος, ο καθορισμός της πιθανότητας εμφάνισης του κάθε κινδύνου, ο αντίκτυπός του περιστατικού που θα προκύψει στο σύστημα, και τα πιθανά αντίμετρα [15].
- **Ανάλυση απειλών**: η εξέταση των πηγών των απειλών σε σχέση με τις ευπάθειες των συστημάτων, προκειμένου να καθοριστούν οι απειλές εναντίον κάθε συστήματος, σε συγκεκριμένο περιβάλλον [15].

Η παρούσα διπλωματική εργασία έχει σκοπό την αναγνώριση των απειλών που δύναται να εκδηλωθούν εναντίον των συστημάτων ενός αυτόνομου πλοίου και στη συνέχεια την εκτίμηση του κινδύνου που προκύπτει για κάθε σύστημα. Αν τα συγκεκριμένα πλοία δεν σχεδιαστούν λαμβάνοντας υπόψιν την ασφάλεια των cyber-physical συστημάτων τους, είναι πολύ πιθανό σύντομα να αντιμετωπίσουν επιθέσεις κυβερνοασφάλειας παρόμοιες με αυτές που έχουν πραγματοποιηθεί σε άλλα βιομηχανικά περιβάλλοντα στα οποία δεν είχαν αναγνωριστεί επαρκώς όλα τα προβλήματα ασφάλειας.

Οι δύο κύριοι στόχοι της εργασίας είναι :

1. Η αναγνώριση των cyber-physical συστημάτων που υπάρχουν σε ένα αυτόνομο πλοίο και η μελέτη της πληροφοριακής αρχιτεκτονικής του.
2. Η αναγνώριση των απειλών και η αποτίμηση των κινδύνων των cyber-physical συστημάτων και υποσυστημάτων του πλοίου.

Η επίτευξη του πρώτου στόχου απαιτεί την αξιολόγηση ήδη υπαρχουσών αρχιτεκτονικών για την εξαγωγή των απαραίτητων συμπερασμάτων. Για την επίτευξη του δεύτερου στόχου, μελετήθηκαν ποικίλες μεθοδολογίες μοντελοποίησης ευπαθειών και απειλών καθώς και αποτίμησης κινδύνου [16] [17] οι οποίες στη συνέχεια εφαρμόστηκαν στην αρχιτεκτονική του πρώτου στόχου. Τα αποτελέσματα της εργασίας δύναται να χρησιμοποιηθούν για τη μελέτη και ανάλυση της ασφάλειας των cyber-enabled πλοίων με σκοπό τη βελτίωση της ασφάλειάς τους.

1.5 Δομή

Η παρούσα εργασία είναι χωρισμένη σε πέντε κεφάλαια. Το δεύτερο κεφάλαιο πραγματοποιεί μία ανασκόπηση του χώρου, περιγράφοντας τις υπάρχουσες μεθοδολογίες εύρεσης και μοντελοποίησης απειλών και επιθέσεων καθώς επίσης και μεθοδολογίες ανάλυσης και υπολογισμού του κινδύνου. Λαμβάνοντας υπόψη τη βιβλιογραφία και τις αντίστοιχες αναφορές που υπάρχουν για τα συστήματα των πλοίων και των αλληλοσυνδέσεών τους, στο τρίτο κεφάλαιο περιγράφεται η αρχιτεκτονική του cyber-enabled πλοίου. Στο τέταρτο κεφάλαιο πραγματοποιείται η εφαρμογή μιας εκ των μεθοδολογιών που έχουν αναφερθεί στο κεφάλαιο 2 καθώς και η ανάλυση των αποτελεσμάτων. Τέλος, στο πέμπτο κεφάλαιο, εξάγονται ορισμένα γενικά συμπεράσματα από την εργασία και συζητείται πώς τα αποτελέσματα μπορούν να συνδράμουν στη βελτίωση της ασφάλειας πληροφοριών (security) αλλά και της φυσικής ασφάλειας (safety) των cyber-enabled πλοίων.

Κεφάλαιο 2

2.1 Μοντελοποίηση Απειλών (Threat Modelling)

Ένα από τα σημαντικά βήματα που πρέπει να ακολουθήσουμε για τη διασφάλιση του cyber-enabled πλοίου είναι η ανάλυση πιθανών απειλών/επιθέσεων. Η ανάλυση των απειλών συμβάλλει στην κατανόηση της πολυπλοκότητας ενός συστήματος και στην αναγνώριση όλων των πιθανών επιθέσεων, ανεξάρτητα κατά πόσο αυτές μπορούν να πραγματοποιηθούν. Η σωστή αναγνώριση των απειλών και η κατάλληλη επιλογή των αντίμετρων που θα εφαρμοστούν μπορούν να μειώσουν σε μεγάλο βαθμό τη δυνατότητα των κακόβουλων να εκμεταλλευτούν ένα σύστημα. Επίσης, συμβάλλει στην ορθότερη διαχείριση των επιχειρησιακών κινδύνων, αυξάνει την επίγνωση ασφάλειας και παρέχει τη δυνατότητα αντιστοίχισης των τεχνικών κινδύνων με επιχειρησιακές συνέπειες.

2.2 Μεθοδολογίες Ανάλυσης Απειλών

Υπάρχουν τρεις προσεγγίσεις που μπορεί να ακολουθεί μια μέθοδος ανάλυσης απειλών/επιθέσεων: έχοντας βάση το αγαθό, το λογισμικό ή τον επιτιθέμενο:

- Η πρώτη προσέγγιση βοηθά στην αναγνώριση πολύπλοκων επιθέσεων και διαδρομών που μπορεί να ακολουθήσει ο επιτιθέμενος για να φτάσει στον στόχο του. Στη συνέχεια, βασιζόμενοι στην ανάλυση κινδύνων, αυτές οι διαδρομές μπορούν να αξιολογηθούν και να προτεραιοποιηθούν. Παραδείγματα τέτοιων μεθόδων αποτελούν τα Attack Trees και τα Attack Graphs.
- Η ανάλυση κινδύνων με βάση το λογισμικό συνήθως χρησιμοποιείται σε αρχιτεκτονικές δικτύων και συστημάτων. Από αυτήν προκύπτουν απειλές και ευπάθειες για το κάθε μέρος του συστήματος, διευκολύνοντας την αποτελεσματικότερη και λιγότερο χρονοβόρα αντιμετώπισή τους. Παραδείγματα τέτοιων μεθόδων αποτελούν οι Data Flow Diagrams (DFD), SDL, STRIDE.
- Τέλος, όταν προσεγγίζουμε την ανάλυση από την πλευρά του επιτιθέμενου, απαιτείται η αναγνώριση των δυνατοτήτων, των στόχων και των κινήτρων του για την εκμετάλλευση των αδυναμιών στο σύστημα. Παράδειγμα τέτοιας μεθόδου αποτελούν τα Attack Trees.

2.2.1 Attack trees

Η μέθοδος των attack trees αποτελεί μία από τις πρώτες μεθόδους ανάλυσης κινδύνων/επιθέσεων. Μας επιτρέπει να αναλύουμε ένα συγκεκριμένο υποσύστημα του συστήματος λαμβάνοντάς υπόψιν τις ευπάθειές του. Η δομή δέντρου που ακολουθεί η μέθοδος αναπαριστά τους διαφορετικούς τρόπους με τους οποίους ένας κακόβουλος χρήστης μπορεί να επιτεθεί στο σύστημα και τα φύλλα αναπαριστούν τις ενέργειες που πρέπει να ακολουθηθούν με σκοπό την επίτευξη του αρχικού στόχου της επίθεσης. Η μέθοδος επιτρέπει την εις βάθος ανάλυση όλων των υποσυστημάτων και τη λεπτομερή αναγνώριση των αντίστοιχων απειλών τους. Η σχεδίασή τους μπορεί να πραγματοποιηθεί με πολλούς τρόπους, ακολουθώντας πέντε στάδια. Η συγκεκριμένη μέθοδος είναι χρήσιμη μόνο σε περιπτώσεις όπου το σύστημα και οι διεργασίες του είναι πλήρως κατανοητά. Στόχος της είναι να αναγνωρίσει όλες τις πιθανές απειλές του συστήματος, συμβάλλοντας στην ορθότερη και αποτελεσματικότερη αντιμετώπισή τους. Σημαντικό μειονέκτημα αποτελεί το ότι δεν παρέχει πληροφορίες για την αρχιτεκτονική του συστήματος, καθώς και για την ανάλυση των υποσυστημάτων. Τέλος, αναπόσπαστο βήμα της μεθόδου

είναι η αποτίμηση του κινδύνου, λαμβάνοντας υπόψη και οικονομικούς παράγοντες, με αποτέλεσμα η εφαρμογή της να απευθύνεται σε έμπειρους χρήστες που γνωρίζουν επαρκώς τα συστήματα. [18]

2.2.2 Data flow diagrams- DFD

Τα DFD αποτελούν ακόμη μία μέθοδο ανάλυσης κινδύνων που με τη βοήθεια γράφων αναπαριστά τα υποσυστήματα και τα δεδομένα τους. Είναι απλά διαγράμματα τα οποία απεικονίζουν τα διαφορετικά στοιχεία των πληροφοριακών συστημάτων. Αποτελούν έναν ακριβή και απλοϊκό τρόπο αναπαράστασης απειλών, αλλά συνήθως χρησιμοποιούνται για την ανάλυση επιθέσεων και την εύρεση ευπαθειών σε διαδικτυακές εφαρμογές όπου οι απειλές είναι συνήθως δικτυακές. Για μικρά και ιδιωτικά δίκτυα η χρήση της συγκεκριμένης μεθόδου δεν ενδείκνυται, λόγω των διαφορετικών προδιαγραφών του εκάστοτε δικτύου. Επίσης, μέσω της συγκεκριμένης ανάλυσης δεν καλύπτονται όλες οι απειλές που μπορούν να εμφανιστούν σε ένα σύστημα, αλλά γίνεται περισσότερο λόγος για την αρχιτεκτονική του συστήματος και για τις ευπάθειες των υποσυστημάτων. Τέλος, δεν είναι εφικτή η πλήρης αναπαράσταση όλων των υποσυστημάτων του συστήματος και των αντίστοιχων διεργασιών τους.

2.2.3 Activity Diagrams-ADs

Τα Activity diagrams (ADs) της UML αναπαριστούν τη ροή των διεργασιών ενός συστήματος. Αποτελεί μία εναλλακτική μέθοδο της DFD και χρησιμοποιείται συχνά ως μέρος άλλων μεθόδων ανάλυσης κινδύνων όπως η SDL της Microsoft [19]. Τα ADs παρέχουν μία εκτενέστερη απεικόνιση του συστήματος συγκριτικά με τα DFD και είναι ικανά να αναπαριστούν πολυπλοκότερα συστήματα από αυτά που μπορεί να χειριστεί η DFD. Το μειονέκτημα και σε αυτήν τη μέθοδο είναι ότι τα ADs δεν είναι ικανά να απεικονίσουν όλες τις πιθανές απειλές και κινδύνους του συστήματος, καθώς υπάρχει περιορισμός στην αναπαράσταση των δεδομένων και των διασυνδέσεων μεταξύ των υποσυστημάτων.

2.2.4 Risk Reduction Overview

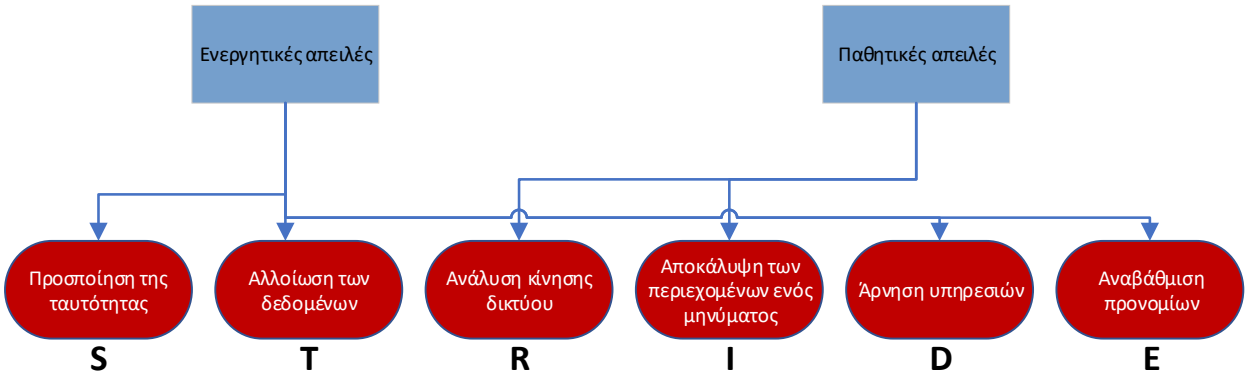
Η Risk Reduction Overview (RRO) είναι η μέθοδος που σκοπό έχει να συσχετίσει έννοιες όπως ο κίνδυνος, τα αντίμετρα και ο εναπομένων κίνδυνος [20]. Βασίζεται σε πέντε διαφορετικά στοιχεία του συστήματος: τον αρχικό κίνδυνο, τον εναπομένοντα κίνδυνο, τον τελικό εναπομένοντα κίνδυνο, τη μέτρηση αυτού και τις αλληλοσυνδέσεις που υπάρχουν μέσα στο σύστημα. Η μέθοδος παρέχει μία συνολική εκτίμηση για την ορθή λήψη αποφάσεων κατά το στάδιο του σχεδιασμού και αποτελεί μία εύκολη μέθοδο ανάλυσης και εκτίμησης των απειλών ενός συστήματος. Σημαντικό μειονέκτημά της είναι ότι η ο αρχικός κίνδυνος θα πρέπει να είναι γνωστός, γεγονός που υποδηλώνει ότι την αδυναμία/ευπάθεια θα πρέπει να την γνωρίζουμε από το στάδιο του σχεδιασμού. [21]

2.2.5 Threat Modeling Framework based on Attack Path Analysis-TMAP

Η Threat Modeling framework based on Attack Path analysis (T-MAP) βασίζεται στη μέθοδο των attack graphs και πραγματοποιεί μία αποτίμηση των κινδύνων του συστήματος με βάση το συνολικό βάρος των attack paths. Σχεδιάστηκε με σκοπό να εκτιμά τα Commercial Off the Shelf-COTS συστήματα. Σημαντικό μειονέκτημα της συγκεκριμένης μεθόδου είναι ότι δεν λαμβάνει υπόψη της άλλες ευπάθειες του συστήματος, πέραν αυτών που σχετίζονται με το λογισμικό COTS.

2.2.6 STRIDE

Τέλος, η μέθοδος STRIDE αποτελεί ακόμη έναν τρόπο για την ανάλυση των απειλών/επιθέσεων σε ένα σύστημα. Οι απειλές στη συγκεκριμένη μέθοδο είναι το αντίθετο των ιδιοτήτων που θα θέλαμε να έχει ένα σύστημα: αυθεντικότητα (authenticity), ακεραιότητα (integrity), αποποίηση ευθύνης (non-repudiation), εμπιστευτικότητα (confidentiality), διαθεσιμότητα (availability) και εξουσιοδότηση (authorization). Πιο συγκεκριμένα, το ακρωνύμιο STRIDE αναφέρεται σε έξι απειλές που δύναται να εμφανιστούν σε ένα σύστημα οι οποίες είναι: Spoofing (προσποίηση), Tampering (αλλοίωση), Repudiation (αποποίηση ευθύνης), Denial of Service (άρνηση υπηρεσιών) και Elevation of privilege (αναβάθμιση προνομίων). Βασική προϋπόθεση για την εφαρμογή της μεθόδου είναι ο ακριβής προσδιορισμός του συστήματος και των δεδομένων που ανταλλάσσονται, ώστε να είναι εφικτό στη συνέχεια να προσδιοριστεί η κάθε μία από τις έξι απειλές στο εκάστοτε σύστημα και υποσύστημα. Η STRIDE είναι μία ακόμη ταξινόμηση όπως η CIA (Confidentiality, Integrity and Availability), με τη διαφορά ότι είναι περισσότερο ολοκληρωμένη. Σημαντικό πλεονέκτημα της μεθόδου είναι ότι δεν λειτουργεί σε απομονωμένο περιβάλλον και προσφέρει τη δυνατότητα συνδυαστικής εφαρμογής με τις μεθόδους SDL, DFD και άλλες. [22]



Εικόνα 1. Είδη απειλών

Για την ανάλυση των απειλών στη παρούσα εργασία ακολουθήθηκε η μέθοδος STRIDE, την οποία συζητάμε σε λεπτομέρεια στην επόμενη ενότητα. Όταν στόχος ενός προβλήματος είναι ο καθορισμός των απειλών, είναι χρήσιμο να τίθενται ερωτήματα όπως:

- Με ποιο τρόπο ένας επιτιθέμενος μπορεί να αλλάξει τα δεδομένα αυθεντικοποίησης;
- Ποιος είναι ο αντίκτυπος στην περίπτωση που ο επιτιθέμενος μπορέσει και διαβάσει ευαίσθητα δεδομένα;
- Τι συμβαίνει όταν απορρίπτεται η είσοδος σε ένα σύστημα ενός νόμιμου χρήστη;

Είναι σημαντικό λοιπόν για την αναγνώριση απειλών στα συστήματα και τα υποσυστήματα του cyber-enabled πλοίου να απαντηθούν παρόμοια ερωτήματα, τα οποία είναι χαρακτηριστικό της μεθόδου STRIDE. Η STRIDE συνδυάζει και συγκεντρώνει τα αποτελέσματα ενεργητικών και παθητικών απειλών, όπως φαίνεται στο σχήμα 1. Αυτό αποτελεί ακόμα ένα κριτήριο επιλογής για το συγκεκριμένο πεδίο εφαρμογής, καθώς τα συστήματα του πλοίου είναι cyber-physical συστήματα τα οποία αλληλοεπιδρούν μεταξύ τους καθιστώντας τη συνδυαστική μέθοδο STRIDE μία απλή λογική ανάλυσης απειλών και

ανάπτυξης επιθέσεων συγκριτικά με την μέθοδο των Attack trees. Τέλος, οι περισσότερες μέθοδοι της βιβλιογραφίας απαιτούν, για την ορθή εφαρμογή τους, τη λεπτομερή ανάλυση των συστημάτων, των διεργασιών και των αλληλοεπιδράσεων μεταξύ των συστημάτων, γεγονός που τις καθιστά μη αποδεκτές για την αρχιτεκτονική του cyber-enabled πλοίου, καθώς η τόσο λεπτομερής πληροφορία για τη λειτουργία του δεν είναι ακόμα διαθέσιμη.

2.3 Η μέθοδος STRIDE

Όπως αναφέρθηκε και προηγουμένως, STRIDE είναι το ακρωνύμιο των: Spoofing, Tampering, Repudiation, Denial of Service και Elevation of privilege. Η συγκεκριμένη μέθοδος αναπτύχθηκε από τους Loren Kohnfelder και Praerit Garg το 1999, με σκοπό να αναγνωρίζονται ευκολότερα οι επιθέσεις που δύναται να εκμεταλλευτούν ευπάθειες λογισμικού [23].

ΑΠΕΙΛΕΣ	ΠΑΡΑΒΙΑΣΕΙΣ
Προσποίηση ταυτότητας (Spoofing)	Αυθεντικοποίηση
Αλλοίωση δεδομένων (Tampering)	Ακεραιότητα
Αποποίηση ευθύνης (Repudiation)	Non-Repudiation
Διαρροή πληροφορίας (Information Disclosure)	Εμπιστευτικότητα
Άρνηση Υπηρεσίας (Denial of Service)	Διαθεσιμότητα
Αναβάθμιση προνομίων (Elevation of Privilege)	Εξουσιοδότηση

Πίνακας 2. Απειλές και παραβιάσεις

Η απειλή Προσποίηση ταυτότητας (Spoofing) αναφέρεται στη δυνατότητα του επιτιθέμενου να προσποιηθεί ότι είναι κάτι ή κάποιος άλλος.

- Προσποίηση Διεργασίας: ο επιτιθέμενος μπορεί να επέμβει σε μία διεργασία είτε δημιουργώντας αρχείο είτε ανακατευθύνοντας το ήδη υπάρχον.
- Προσποίηση Μηχανήματος: ο επιτιθέμενος μπορεί να προσποιηθεί ένα μηχάνημα σε πολλά επίπεδα του δικτύου όπως είναι οι IP διευθύνσεις, DNS και ARP.
- Προσποίηση Ατόμου: αυτό επιτυγχάνεται μέσω κοινωνικής μηχανικής.

Η απειλή αλλοίωσης/τροποποίησης (Tampering) αφορά τη τροποποίηση/αλλοίωση στοιχείων του δίσκου, του δικτύου ή και της μνήμης του συστήματος και στοχεύει συνήθως αποθήκες δεδομένων και διεργασίες. Η αλλοίωση των δεδομένων ενός αρχείου, η τροποποίηση των πακέτων σε ένα δίκτυο και η προσθήκη δεδομένων σε μία βάση αποτελούν παραδείγματα της συγκεκριμένης απειλής.

- Αλλοίωση αρχείου: ο επιτιθέμενος μπορεί να τροποποιήσει κάποιο αρχείο και να αλλοιώσει τα δεδομένα του.
- Αλλοίωση μνήμης.
- Αλλοίωση δικτύου: συνήθως στόχος του επιτιθέμενου είναι να διαβάσει τα δεδομένα τα οποία ανταλλάσσονται σε ένα δίκτυο και στη συνέχεια να τα τροποποιήσει προς όφελός του.

Η αποποίηση της ευθύνης (repudiation) είναι η άρνηση εκτέλεσης μίας ενέργειας ή η αποποίηση της ευθύνης. Η συγκεκριμένη απειλή διαφέρει συγκριτικά με άλλες, καθώς συνήθως εμφανίζεται στο επιχειρησιακό επίπεδο, το οποίο βρίσκεται πάνω από τα επίπεδα δικτύου και εφαρμογής.

- Αποποίηση ευθύνης προσώπου ή μηχανής: ο επιτιθέμενος μπορεί να ισχυριστεί ότι δεν πραγματοποίησε κάποια πράξη ή να εισέλθει στον λογαριασμό κάποιου άλλου χρήστη.
- Αποποίηση ευθύνης διεργασίας: η συγκεκριμένη επίθεση στοχεύει κυρίως τα αρχεία καταγραφής (logs) από τα οποία ο επιτιθέμενος μπορεί να αντλήσει χρήσιμες πληροφορίες σχετικά με διεργασίες που εκτελούνται, καθώς επίσης και προσωπικά δεδομένα.

Η διαρροή πληροφοριών αποτελεί μία σημαντική απειλή, καθώς μη εξουσιοδοτημένα άτομα έχουν πρόσβαση σε πληροφορίες του συστήματος.

- Διαρροή πληροφοριών βάσεων δεδομένων: η λάθος παραμετροποίηση των βάσεων δεδομένων και η ελλιπής χρήση μηχανισμών ασφάλειας (κρυπτογράφηση) μπορεί να οδηγήσει στη διαρροή των δεδομένων της βάσης.
- Διαρροή δεδομένων διεργασιών: οι πληροφορίες που ανταλλάσσονται κατά τη διάρκεια εκτέλεσης των διεργασιών πολλές φορές είναι ευαίσθητες και ο επιτιθέμενος εκμεταλλευόμενος τις ευπάθειές τους μπορεί να διαβάσει αυτές τις πληροφορίες.

Ακόμη μία σημαντική απειλή είναι η άρνηση υπηρεσιών (Denial of Service) κατά την οποία ο επιτιθέμενος απορροφά όλους τους πόρους καθιστώντας αδύνατη τη διεκπεραίωση των λειτουργιών του συστήματος.

- Άρνηση υπηρεσίας σε μία διεργασία: απορροφά του πόρους από την CPU ή τη RAM.
- Άρνηση υπηρεσίας σε βάση δεδομένων: γέμισμα της βάσης με εγγραφές ή δημιουργία πολλών ερωτημάτων με στόχο την αργή ανταπόκριση της βάσης.
- Άρνηση υπηρεσίας σε data flow: απορροφά όλους του πόρους του δικτύου.

Τέλος, η απειλή αναβάθμισης προνομίων (elevation of privilege) επιτρέπει στο άτομο που θα την εκμεταλλευτεί να πραγματοποιήσει ενέργειες τις οποίες δεν είναι εξουσιοδοτημένο να εκτελέσει. Παράδειγμα της συγκεκριμένης απειλής είναι να επιτραπεί σε έναν απλό χρήστη να εκτελέσει μία ενέργεια διαχειριστή.

- Αναβάθμιση προνομίων σε διαδικασίες: ο επιτιθέμενος, εκμεταλλευόμενος την ευπάθεια του λειτουργικού συστήματος ή κάποιας διεργασίας, αποκτά δικαιώματα διαχειριστή.

2.4 Ανάλυση κινδύνων

Ο International Maritime Organization (IMO), έχει δημοσιεύσει αρκετές οδηγίες [24], αναγνωρίζοντας τα θέματα ασφάλειας πληροφοριών και φυσικής ασφάλειας με τα οποία έρχεται αντιμέτωπο ένα σύγχρονο πλοίο. Τα σύγχρονα πλοίο είναι εφοδιασμένα με πολλά συστήματα, τα οποία είναι ευπαθή σύμφωνα με τον IMO. Ο IMO μάλιστα επισημαίνει τη σημασία της ασφάλειας στα συστήματα γέφυρας, συστήματα διαχείρισης φορτίου, συστήματα πρόωσης και μηχανικής διαχείρισης, συστήματα διαχείρισης ενέργειας, συστήματα ελέγχου εισόδου και διαχείρισης προσωπικού, δημόσια δίκτυα εξυπηρέτησης πελατών και

στα συστήματα επικοινωνίας. Επίσης, ο IMO [24] πραγματοποιεί μία διάκριση των συστημάτων σε συστήματα πληροφοριών και σε λειτουργικά συστήματα. Τα πρώτα απλά δέχονται τα δεδομένα σαν πληροφορία και τα δεύτερα χρησιμοποιούν τα δεδομένα για τον έλεγχο και την επίβλεψη άλλων συστημάτων [8]. Σύμφωνα με την ίδια δημοσίευση [24] ο IMO αναφέρει πως ο κίνδυνος προκύπτει από ευπάθειες οι οποίες προκαλούνται από λάθος χειρισμό, συντήρηση και σχεδιασμό τον cyber-enabled συστημάτων, καθώς και από παγκόσμιες κυβερνοεπιθέσεις. Πολλοί ερευνητές [25] [26] και η International Electrotechnical Commission (IEC) έχουν επισημάνει την ανάγκη για τη κατάλληλη λήψη μέτρων ασφάλειας στις πληροφορικές υποδομές των συμβατικών και μη πλοίων. Λαμβάνοντας λοιπόν υπόψη μας ότι τα αυτόνομα πλοία αποτελούνται από τα παραπάνω συστήματα ενός συμβατικού πλοίου, τα οποία συμπληρώνονται με ορισμένα σύγχρονα, είναι φανερό ότι αποτελεί ζωτικής σημασίας η σωστή και εις βάθος ανάλυση κινδύνου που αντιμετωπίζουν τα τηλεχειριζόμενα και τα αυτόνομα πλοία.

Η ανάλυση κινδύνων πραγματοποιείται συγκρίνοντας τη πιθανότητα πραγματοποίησης μίας πιθανής επίθεσης με τις συνέπειες που θα επιφέρει αυτή. Για το σύστημά μας θα χρησιμοποιήσουμε τη μήτρα αποτίμησης κινδύνου της εικόνας 4, λαμβάνοντας υπόψη τα αντίστοιχα κριτήρια. Το μέγεθος των συνεπειών και των πιθανοτήτων εκδήλωσης των επιθέσεων υπολογίζεται λαμβάνοντας υπόψη τα κριτήρια που καταγράφονται στους παρακάτω πίνακες [16].

2.4.1 Κριτήρια αποτίμησης συνεπειών

HIGH

- Απειλές που μπορούν να προκαλέσουν απώλεια ανθρώπινης ζωής.
- Απειλές που μπορούν να προκαλέσουν σημαντικά εκτεταμένες απώλειες ενέργειας.
- Απειλές που μπορούν να προκαλέσουν ζημιές/καταστροφές στην υποδομή.
- Απειλές που μπορούν να προκαλέσουν απώλεια των προσωπικών δεδομένων.
- Απειλές που μπορούν να προκαλέσουν σημαντικές οικονομικές καταστροφές και απώλεια πελατών.
- Απειλές οι οποίες μπορούν να προκαλέσουν δυσλειτουργία ολόκληρου του συστήματος.

MEDIUM

- Απειλές που μπορούν να προκαλέσουν αποτυχία κάποιας διεργασίας ελέγχου σε πραγματικό χρόνο.
- Απειλές που μπορούν να προκαλέσουν ανεπιθύμητους υπολογισμούς οι οποίοι επηρεάζουν την λειτουργία των συστημάτων.
- Απειλές που μπορούν να προκαλέσουν την δυσαρέσκεια των πελατών καθώς και να βλάψει την φήμη της εταιρίας.
- Απειλές που μπορούν να προκαλέσουν την διαρροή καταγεγραμμένων πληροφοριών που υπάρχουν στα συστήματα .
- Απειλές που μπορούν να επηρεάσουν την ακεραιότητα των συστημάτων.
- Απειλές που μπορούν να επηρεάσουν την διαθεσιμότητα των συστημάτων.
- Απειλές οι οποίες μπορούν να προκαλέσουν διαρροή πληροφοριών του δικτύου και της διασύνδεσης των υποσυστημάτων.
- Απειλές οι οποίες μπορούν να προκαλέσου νομικές κυρώσεις στην επιχείρηση/οργανισμό και στην ανάγκη καταβολής προστίμων.

LOW

- Απειλές που μπορούν να προκαλέσουν καθυστέρηση λειτουργίας ή αποτυχία λειτουργίας σε μη κρίσιμες διεργασίες.
- Απειλές που μπορούν να διαρροή μη ευαίσθητων πληροφοριών.

Εικόνα 2. Κριτήρια αποτίμησης συνεπειών

2.4.2 Κριτήρια αποτίμησης πιθανοτήτων

Very Likely	• Ο επιτιθέμενος είναι υψηλά υποκινούμενος και ικανός, και τα αντίμετρα που υπάρχουν στο σύστημα για την συγκεκριμένη ευπάθεια δεν επαρκούν. • Η ύπαρξη ενός ευρέως γνωστού exploit το οποίο μπορεί να εκτελεστεί οποιαδήποτε στιγμή στο δίκτυο. • Όταν υπάρχει μεγάλη έκθεση των υποσυστημάτων σε εξωτερικά συστήματα.
Moderate	• Ο επιτιθέμενος είναι υψηλά υποκινούμενος και ικανός, αλλά τα αντίμετρα για την ευπάθεια υπάρχουν αλλά δεν είναι επαρκή. • Η ευπάθεια του συστήματος είναι ευρέως γνωστή αλλά ο επιτιθέμενος για να δράσει χρειάζεται άμεση πρόσβαση με τα συστήματα. • Δεν υπάρχει άμεση έκθεση σε εξωτερικά συστήματα.
Rare	• Ο επιτιθέμενος δεν είναι υψηλά υποκινούμενος ή δεν έχει τις επαρκής γνώσεις για να πραγματοποιήσει την επίθεση ή τα αντίμετρα για την ευπάθεια είναι αρκετά για να προστατέψουν το σύστημα. • Ο κακόβουλος χρήστης χρειάζεται να έχει δικαιώματα διαχειριστή για να πραγματοποιήσει την επίθεση. • Δεν διασυνδέονται με κάποιο εξωτερικό δίκτυο ή σύστημα.

Εικόνα 3. Κριτήρια αποτίμησης πιθανοτήτων

Στη συνέχεια πραγματοποιείται η αποτίμηση του κινδύνου με βάση την παρακάτω μήτρα:

ΠΙΘΑΝΟΤΗΤΑ \ ΑΝΤΙΚΤΥΠΟΣ	HIGH	MEDIUM	LOW
VERY LIKELY	HIGH	HIGH	MEDIUM
MODERATE	HIGH	MEDIUM	LOW
RARE	MEDIUM	LOW	LOW

Εικόνα 4. Μήτρα αποτίμησης κινδύνου

Ο παρακάτω πίνακας 3 αναλύει τους βαθμούς κινδύνου όπως προκύπτουν από την παραπάνω μήτρα. Παρόμοια διαβάθμιση ακολουθείται από το NIST στο [27], στο οποίο προτείνονται και τα απαραίτητα αντίμετρα με βάση τα αποτελέσματα της αποτίμησης κινδύνου.

Κίνδυνος	**Περιγραφή**
High	• Μία παρατήρηση χαρακτηρίζεται ως υψηλού κινδύνου όταν μπορεί να προκαλέσει καταστροφικές συνέπειες στις διεργασίες του οργανισμού, στα αγαθά του, σε ανθρώπους και σε συνεργαζόμενους οργανισμούς.
Medium	• Μία παρατήρηση χαρακτηρίζεται ως μετρίου κινδύνου όταν είναι πιθανό να έχει σοβαρές συνέπειες στις λειτουργίες, στα αγαθά και σε ανθρώπους του οργανισμού.
Low	• Μία παρατήρηση χαρακτηρίζεται ως χαμηλού κινδύνου όταν έχει περιορισμένες έως και μηδαμινές συνέπειες στις λειτουργίες, στα αγαθά και σε ανθρώπους του οργανισμού.

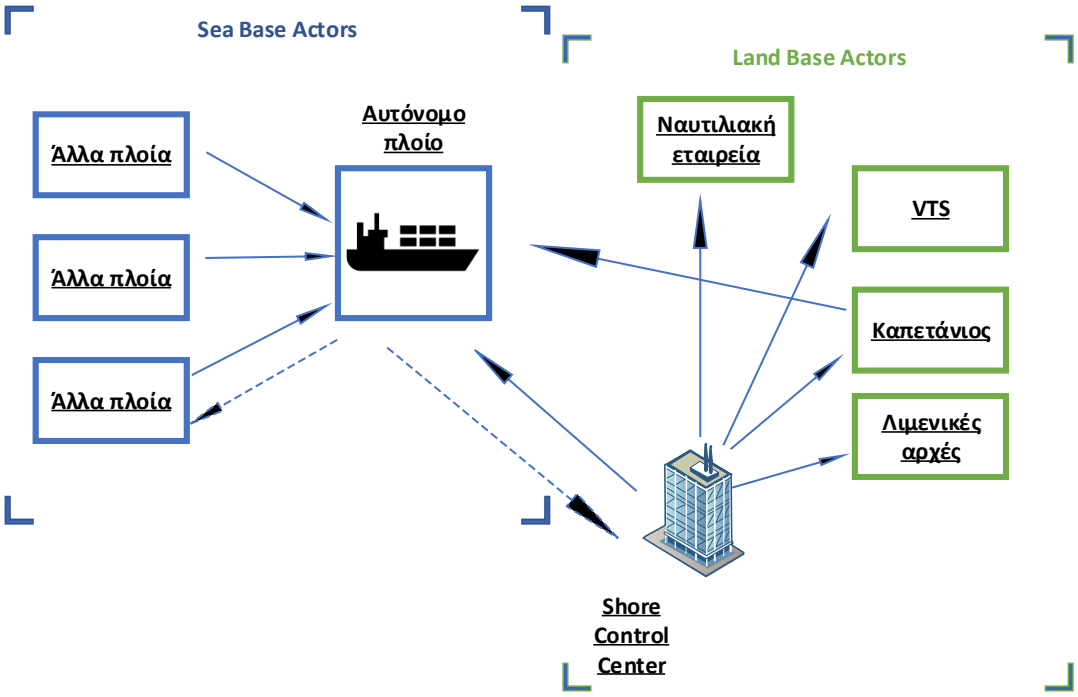
Πίνακας 3. Βαθμοί Κινδύνου

Κεφάλαιο 3

3.1 Αρχιτεκτονική

Αρχικός στόχος της παρούσας διπλωματικής εργασίας είναι η μελέτη και ανάλυση της αρχιτεκτονικής του cyber-enabled πλοίου. Είναι σημαντικό να αναφερθεί ότι στην αντίστοιχη βιβλιογραφία δεν υπάρχει σαφής προσδιορισμός της συνολικής αρχιτεκτονικής των συστημάτων και των υποσυστημάτων που υπάρχουν σε ένα πλοίο. Αυτό αποτελεί ένα εμπόδιο στον πλήρη προσδιορισμό τους και την καταγραφή των αλληλεπιδράσεών τους, οι οποίες αποτελούν σημαντικό μέρος της ανάλυσης, καθώς πρόκειται για cyber-physical systems.

Στην Εικόνα 5 παρουσιάζεται μια συνοπτική παρουσίαση των οντοτήτων της αρχιτεκτονικής του cyber-enabled πλοίου καθώς και των αλληλοεπιδράσεων των συστημάτων τους. Όπως παρατηρείται, οι ρόλοι έχουν διακριθεί σε δύο ομάδες: αυτούς της ξηράς και της θάλασσας αντίστοιχα. Στη πρώτη ομάδα βρίσκεται το κέντρο ελέγχου του πλοίου, η ναυτιλιακή εταιρεία καθώς επίσης και τα μέρη που τις συγκροτούν και στη δεύτερη ομάδα βρίσκονται το cyber-enabled πλοίο και τα υπόλοιπα πλοία που δύναται να πλέουν και να επικοινωνούν μαζί του.



Εικόνα 5. Αλληλοεπιδράσεις του πλοίου με τις υπόλοιπες οντότητες.

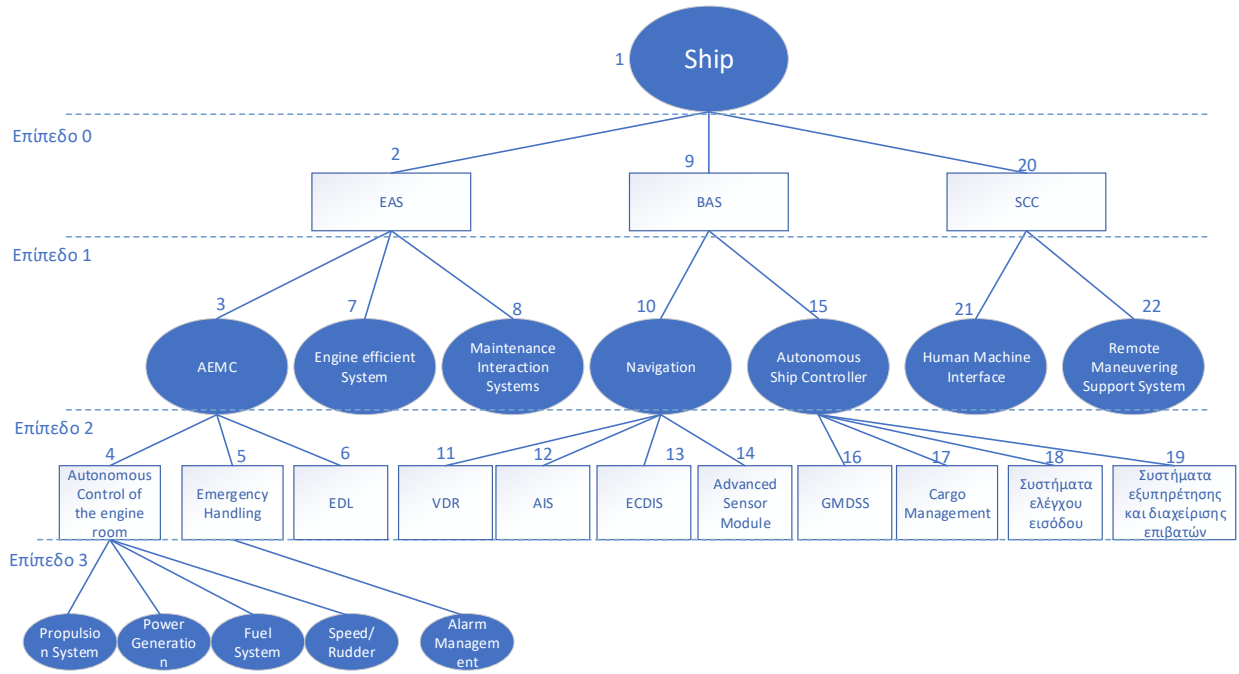
Η αρχιτεκτονική του cyber-enabled πλοίου ακολουθεί μία δενδρική αναπαράσταση των συστημάτων όπως αυτά περιγράφονται στο ευρωπαϊκό έργο MUNIN [28] και στην αντίστοιχη αναφορά της BIMCO: The Guidelines on Cyber Security Onboard Ships Version 2.0 [8]. Η παρούσα αρχιτεκτονική ανάλυση επικεντρώνεται στην αρχιτεκτονική του MUNIN για τον λόγο ότι αυτή της BIMCO [8] συμπληρώνει αυτή του MUNIN. Επίσης, τα συστήματα τα οποία αναφέρονται στο [8] είναι συστήματα τα οποία δεν

παρέχουν όλα τις ίδιες αυτοματοποιημένες διεργασίες τις οποίες έχει ανάγκη για να λειτουργήσει ένα cyber-enabled πλοίο. Τέλος, σημαντικό πλεονέκτημα της αρχιτεκτονικής MUNIN είναι ότι έχει προχωρήσει σε μια γενική κατηγοριοποίηση των συστημάτων, γεγονός που ωφελεί την ανάλυση των υποσυστημάτων σε μετέπειτα στάδιο με στόχο την αποτίμηση κινδύνου και την ανάλυση απειλών σε αυτά. Αφού το πλοίο αποτελεί ένα σύστημα συστημάτων τα οποία αλληλοεπιδρούν μεταξύ τους, η δενδρική αναπαράσταση καθιστά ευκολότερη τη κατανόηση των λειτουργιών τους και τον τρόπο με τον οποίο αυτά αλληλοεπιδρούν και διασυνδέονται.

Τα cyber-physical συστήματα του πλοίου δύναται να διακριθούν στις εξής τέσσερις κατηγορίες:

- Βιομηχανικά: Κλιματισμός, συναγερμοί, κλπ.
- Πρόωσης: τα συστήματα πρόωσης συμβάλλουν στη μετακίνηση του πλοίου και είναι τα συστήματα μηχανών, προπελών, πηδαλίων. Το σύστημα πρόωσης μπορεί να είναι κλασικής διάταξης με αξονικό σύστημα, με υδροπρόωση ή με ειδικά χαρακτηριστικά.
- Πλοήγησης: τα συστήματα πλοήγησης διαδραματίζουν σημαντικό ρόλο στη λειτουργία/μετακίνηση του πλοίου. Οι γυροσκοπικές πυξίδες, τα Radar, το AIS, το Electronic Chart Display and Information System (ECDIS) και το Voyage Data Recorder (VDR) είναι μερικά παραδείγματα αυτών των συστημάτων.
- Επικοινωνίας: στη συγκεκριμένη κατηγορία ανήκουν όλα τα συστήματα τα οποία συνδράμουν στην επικοινωνία μεταξύ των πλοίων αλλά και στην επικοινωνία του πλοίου με το κέντρο ελέγχου ξηράς (Shore Control Center). Παραδείγματα τέτοιων συστημάτων είναι το GMDSS, Satellite και το Digital Selective Calling-DSC.

Λαμβάνοντας υπόψη τον διαχωρισμό των τεσσάρων κατηγοριών, πραγματοποιήθηκε η αντίστοιχη ταξινόμηση των συστημάτων στα 3 επίπεδα του δέντρου. Στο επίπεδο 0 βρίσκεται το πλοίο, το οποίο αποτελεί ρίζα του δέντρου, αφού είναι η οντότητα που εμπεριέχει όλα τα επιμέρους συστήματα. Στη συνέχεια, στο επίπεδο 1, βρίσκονται οι απόγονοι της ρίζας, τα συστήματα της γέφυρας (Bridge Automation System - BAS), τα συστήματα ελέγχου μηχανών (Engine Automation System) και τα συστήματα τα οποία είναι υπεύθυνα για τον απομακρυσμένο έλεγχο του πλοίου (Shore Control Center - SCC). Στο επίπεδο 2, υπάρχουν τα αντίστοιχα υποσυστήματα των συστημάτων του επιπέδου 1. Αναλυτικότερα, στο σύστημα EAS αντιστοιχούν τα υποσυστήματα αυτόματου ελέγχου και παρακολούθησης μηχανών (Autonomous Engine Monitoring and Control System-AEMC), βελτίωσης μηχανών (Engine Efficient System) και τα συστήματα συντήρησης (Maintenance Interaction System). Στο BAS αντιστοιχούν τα υποσυστήματα της πλοήγησης και του αυτόματου ελέγχου του πλοίου (Autonomous ship Controller-ASC.) Τέλος, στο SCC υπάγονται τα συστήματα απομακρυσμένου ελέγχου και υποστήριξης του πλοίου (Remote Maneuvering Support System) και το σύστημα διεπαφής του πλοίου με τη ξηρά (Human Machine Interface). Συνεχίζοντας, στο επίπεδο 3 του δέντρου βρίσκονται τα υποσυστήματα του AEMC τα οποία είναι το σύστημα καταγραφής συμβάντων μηχανής (Engine Data Logger - EDL), το σύστημα αυτόνομου ελέγχου του μηχανοστασίου (Autonomous Control of the Engine Room) και το σύστημα διαχείρισης έκτακτων περιστατικών. Στο ίδιο επίπεδο είναι και τα υποσυστήματα τη πλοήγησης, δηλαδή το VDR, το AIS, το ECDIS, το GPS και το Advanced Sensor Module. Τέλος, στο επίπεδο 3 βρίσκονται και τα υποσυστήματα του Autonomous Ship Controller, τα οποία είναι τα GMDSS, τα συστήματα διαχείρισης φορτίου, τα συστήματα ελέγχου εισόδου και τα συστήματα επιβατών.



Εικόνα 6. Αρχιτεκτονική cyber-enabled πλοίου

3.2 Συστήματα cyber-enabled Πλοίου

3.2.1 Αυτόματα συστήματα μηχανών (Engine Automation System – EAS)

Το EAS συμπεριλαμβάνει όλα εκείνα τα συστήματα τα οποία είναι υπεύθυνα για τη παραγωγή και διαχείριση της ενέργειας του πλοίου καθώς επίσης και τα συστήματα πρόωσης. Αναλυτικότερα, τα υποσυστήματα του συγκεκριμένου συστήματος είναι υπεύθυνα για τη διαχείριση και συντήρηση των μηχανών του πλοίου. Τα μέρη που συντελούν το EAS είναι το AEMC, οι κύριες μηχανές με τα συστήματα υποστήριξής τους, οι βοηθητικές μηχανές, τα συστήματα πρόωσης και καθοδήγησης, τα συστήματα ελέγχου των δεξαμενών και τέλος κάποια από τα συστήματα συναγερμού σε περίπτωση πυρκαγιάς ή βλάβης. Συστήματα υποστήριξης των μηχανών είναι όλα τα υποσυστήματα τα οποία είναι υπεύθυνα για τη σωστή λίπανση των μηχανών, τον έλεγχο της στάθμης των καυσίμων και της σωστής ψύξης αυτών.

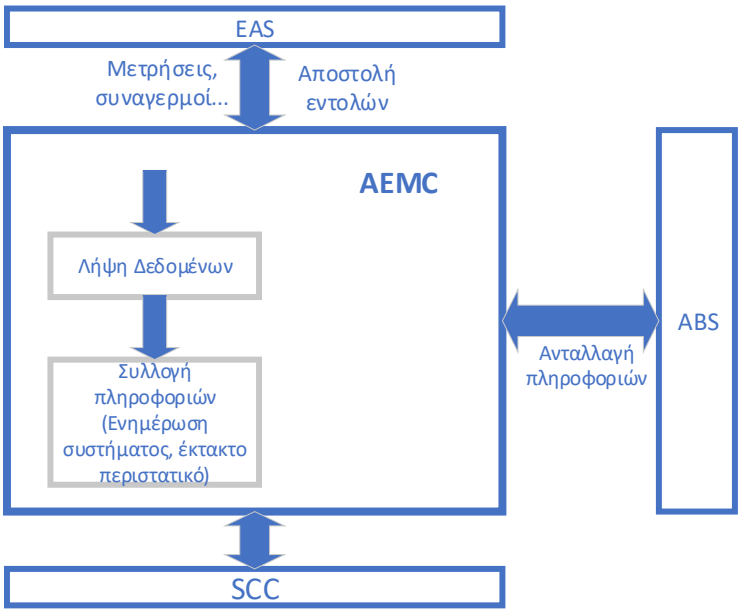
3.2.2 Σύστημα αυτόματου ελέγχου και παρακολούθησης μηχανών (Autonomous Engine Monitoring and Control-AEMC)

Το συγκεκριμένο υποσύστημα είναι άμεσα συνδεδεμένο με τα μηχανικά μέρη του πλοίου. Χρησιμοποιείται για τον έλεγχο και τη διαχείριση των μηχανών και επίσης είναι το μέσο διαχείρισης όλων των αυτοματοποιημένων διαδικασιών και συστημάτων που εκτελούνται στο πλοίο. Αυτό σημαίνει ότι συνδέεται άρρηκτα με το BAS και το SCC, καθώς όλες οι εντολές από και προς τα μηχανικά μέρη διέρχονται μέσω αυτού.

Σημαντικές διεργασίες του συγκεκριμένου υποσυστήματος είναι ακόμη ο έλεγχος που πραγματοποιείται μέσω του AEMC για τη σωστή λίπανση και ψύξη των κινητήρων. Ακόμη, το σύστημα πρόωσης,

παραγωγής και διαχείρισης ενέργειας, το σύστημα στήριξης και εξάτμισης και το σύστημα καυσίμων βρίσκεται υπό τον έλεγχο του AEMC. Επίσης μία λειτουργία του συστήματος είναι να παρακολουθεί όλες τις διεργασίες και να τις αναμεταδίδει στο SCC, καθώς και να ειδοποιεί άμεσα σε περίπτωση έκτακτου περιστατικού. Τέλος, το AEMC διασυνδέεται άμεσα με το Engine Efficiency System καθώς δέχεται πληροφορίες από αυτό για τον χειρισμό πολλών αυτοματοποιημένων διεργασιών.

Πολλά είναι τα υποσυστήματα με τα οποία διασυνδέεται πλήρως το AEMC αλλά και πολλά είναι αυτά με τα οποία απλά υπάρχει μία ανταλλαγή πληροφορίας λειτουργώντας ως απλός διαμεσολαβητής της πληροφορίας. Πιο αναλυτικά, το AEMC συνδέεται με το υποσύστημα διαχείρισης συναγερμών αλλά μόνο για τους συναγερμούς που είναι υπεύθυνοι για τα μηχανικά μέρη. Επίσης, η διασύνδεσή του με το σύστημα έρματος είναι μόνο για τη παροχή πληροφοριών στο SCC, δηλαδή πληροφορίες για τη στάθμη του νερού στις δεξαμενές έρματος.



Εικόνα 7. Δομή του AEMC [24]

3.2.3 Σύστημα καταγραφής συμβάντων των μηχανών (Engine Data Logger – EDL)

Το συγκεκριμένο σύστημα είναι επιφορτισμένο με τη καταγραφή όλων των λειτουργιών και της κατάστασης των μηχανών του πλοίου. Έχει τη δυνατότητα να συλλέγει δεδομένα όλο το εικοσιτετράωρο σχετικά με τις μετρήσεις παραμέτρων των μηχανών, τον έλεγχο των θερμοκρασιών σε αυτές καθώς και ό,τι συμβαίνει στο περιβάλλον τους. Αυτό συμβάλλει στη καλύτερη και πληρέστερη κατανόηση των συμβάντων των σχετικών με τις μηχανές και την αποτροπή ενδεχομένων δυσλειτουργιών. Αποτελεί μία παραλλαγή του VDR καθώς ο ρόλος και των δύο είναι η καταγραφή συμβάντων και πληροφοριών, μόνο που ο σκοπός του EDL περιορίζεται στο πεδίο των μηχανών.

3.2.4 Σύστημα αυτόματου ελέγχου μηχανών (Autonomous Control of the Engine Room)

Το υποσύστημα αυτό του AEMC είναι υπεύθυνο για τη λειτουργία όλων των μηχανικών συστημάτων και των υποστηρικτικών τους. Στόχος του είναι η ορθή και ομαλή λειτουργία των μηχανών του πλοίου. Για την επίτευξη του στόχου του αλληλοεπιδρά με άλλα συστήματα τα οποία είναι:

- Συστήματα πρόωσης
- Συστήματα παραγωγής ενέργειας
- Συστήματα καυσίμων
- Συστήματα λίπανσης των κινητήρων
- Συστήματα πηδαλίου
- Συστήματα εκπομπής καυσίμων

3.2.5 Σύστημα διαχείρισης εκτάκτων περιστατικών (Emergency Handling)

Το συγκεκριμένο σύστημα συμβάλλει στην αναγνώριση τυχόν σφάλματος στα υπόλοιπα συστήματα του πλοίου, παρακολουθώντας βασικές παραμέτρους, λαμβάνοντας πληροφορίες από το EAS καθώς επίσης και από το σύστημα των αισθητήρων. Συνεπώς, η διαχείριση εκτάκτων περιστατικών έχει σκοπό την εφαρμογή των κατάλληλων αντιμέτρων για την αποφυγή ζημιών στην υποδομή. Υποσυστήματα τα οποίο συγκροτούν το σύστημα διαχείρισης εκτάκτων περιστατικών είναι:

- Συστήματα γενικού συναγερμού
- Συναγερμός πυρκαγιάς
- Συναγερμός ότι κάποιος άνθρωπος βρίσκεται στη θάλασσα
- Συναγερμός ακυβέρνητου πλοίου
- Συναγερμός ανίχνευσης διοξειδίου του άνθρακα
- Πλημμύρα του δωματίου μηχανών
- Πλημμύρα του χώρου φορτίων
- Κίνδυνος μόλυνσης

3.2.6 Σύστημα βελτιστοποίησης απόδοσης μηχανών (Engine Efficient System)

Το συγκεκριμένο σύστημα είναι ζωτικής σημασίας για την ορθή λειτουργία του πλοίου, καθώς είναι το σύστημα μέσω του οποίου πραγματοποιείται η απαραίτητη συντήρηση όπου και όποτε χρειάζεται λαμβάνοντας υπόψη τους αντίστοιχους KPIs (Key Performance Indicators). Η λειτουργία του είναι αδιάκοπη και ελέγχει συνεχώς για τυχόν σφάλματα που μπορεί να υπάρξουν στο υλικό ή και στο λογισμικό. Μία από τις κύριες λειτουργίες του είναι η διασφάλιση ότι τα μηχανήματα παραγωγής ενέργειας λειτουργούν κανονικά καθώς επίσης και η πραγματοποίηση ελέγχων της κατανάλωσης καυσίμων και ενέργειας με στόχο τη μείωση της εκπομπής καυσαερίων.

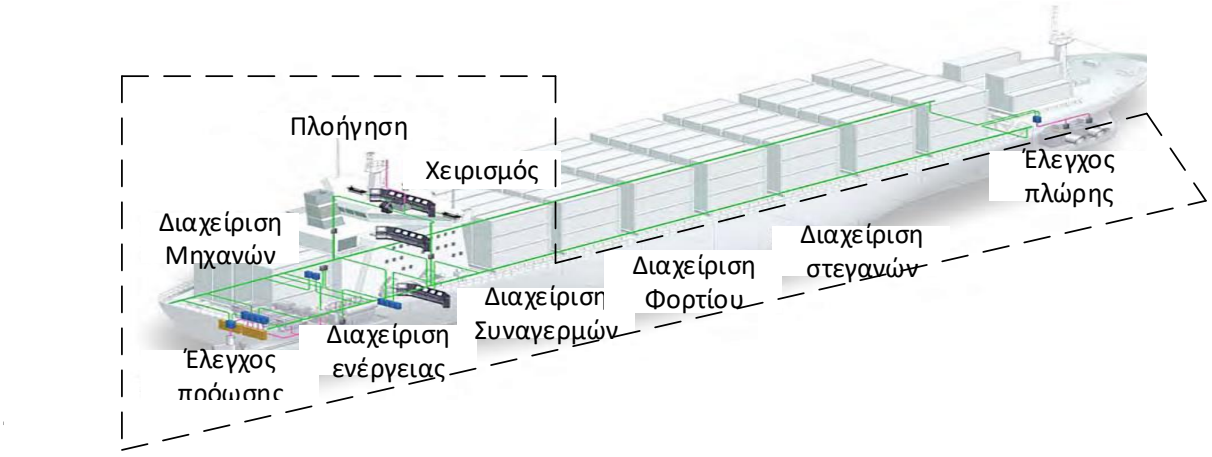
3.2.7 Σύστημα συντήρησης (Maintenance Interaction System)

Η κύρια λειτουργία του συγκεκριμένου υποσυστήματος είναι να παρέχει την απαραίτητη συντήρηση στο μηχανοστάσιο ενός cyber-enabled πλοίου. Όλες οι δραστηριότητες που στοχεύουν στην ομαλή συντήρηση αποτελούν συνδυασμό τεχνικών, διοικητικών και διαχειριστικών ενεργειών καθ' όλη τη διάρκεια ζωής των μηχανών, για να είναι σε θέση να διεκπεραιώνουν όλες τις ενέργειες που τους

ανατίθενται. Στη πραγματικότητα τα συστήματα αυτά παρέχουν ένα Key Performance Indicator (KPI), ο οποίος αποτελεί είσοδο σε άλλα υποσυστήματα, όπως το Engine Efficient System.

3.3 Σύστημα αυτοματοποίησης γέφυρας (Bridge Automation System – BAS)

Στόχος του αυτόνομου πλοίου είναι να εκτελούνται οι διεργασίες με τη λιγότερη δυνατή ανθρώπινη παρέμβαση. Τα συστήματα και τα υποσυστήματα που βρίσκονται στη γέφυρα του πλοίου είναι ζωτικής σημασίας, αφού η μέχρι τώρα λειτουργία και ο χειρισμός του πραγματοποιούταν μέσω αυτών. Πολλά είναι τα συστήματα στη γέφυρα των πλοίων τα οποία λειτουργούν ήδη με αυτοματοποιημένες διαδικασίες, όπως π.χ. το AIS, χωρίς ωστόσο να είναι σε θέση να λειτουργήσουν χωρίς καθόλου ανθρώπινη παρέμβαση. Το σύστημα BAS αποτελείται από όλα τα υποσυστήματα που υπάρχουν στη γέφυρα του πλοίου και τον αντίστοιχο εξοπλισμό τους. Σημαντικά υποσυστήματα του BAS είναι τα συστήματα πλοήγησης και τα συστήματα διαχείρισης του πλοίου [29].



Εικόνα 8. Συστήματα γέφυρας (by Kongsberg)

3.3.1 Συστήματα Πλοήγησης (Navigation)

Τα συστήματα πλοήγησης είναι καθοριστικά για την ορθή και αποτελεσματική λειτουργία των πλοίων. Αυτά καθορίζουν τη διαδρομή που ακολουθεί το κάθε πλοίο και την τυχόν παρέκκλισή τους από αυτή, που μπορεί να προκληθεί από καιρικά φαινόμενα ή από περιστατικά έκτακτης ανάγκης όπως η συνάντηση με ένα άλλο πλοίο. Πιο αναλυτικά, το σύστημα πλοήγησης πραγματοποιεί τις εξής διεργασίες:

1) Καθορίζει την πορεία και τις κινήσεις του πλοίου σύμφωνα με τις υποχρεώσεις που ορίζουν οι κανονισμοί COLREG (International Regulations for Preventing Collisions at Sea 1972).

2) Καθορίζει τα δρομολόγια των πλοίων σύμφωνα με τα εκάστοτε προγνωστικά για τον καιρό.
3) Είναι υπεύθυνο για την ομαλή και ασφαλή πλοήγηση του πλοίου σε καταστάσεις με έντονα καιρικά φαινόμενα, σύμφωνα με τα κριτήρια που ορίζει ο IMO.

Σκοπός λοιπόν του συστήματος πλοήγησης είναι να κατευθύνει το πλοίο με ασφάλεια από το σημείο αναχώρησης στο σημείο προορισμού. Για να επιτευχθεί αυτό, το σύστημα είναι άμεσα συνδεδεμένο με όλα τα υποσυστήματα του BAS, τα οποία το υποβοηθούν για τη συγκέντρωση πληροφοριών για τις καιρικές συνθήκες, για τις δυναμικές του πλοίου, την αποφυγή συγκρούσεων και την έναρξη συναγερμών [29].

3.3.2 Σύστημα καταγραφής δεδομένων ταξιδιού (Voyage Data Recorder – VDR)

Το συγκεκριμένο υποσύστημα συγκεντρώνει και αποθηκεύει όλες τις διαθέσιμες πληροφορίες σχετικά με την κατάσταση του πλοίου, τη θέση του, την κίνησή του, ακόμη και ηχογραφήσεις από τα συστήματα μηχανών και ασυρμάτου. Τα καταγεγραμμένα δεδομένα τουλάχιστον δώδεκα ωρών παραμένουν αποθηκευμένα στο σύστημα για την ανάγκη τυχόν διερεύνησης μελλοντικού ατυχήματος ή μηχανικού προβλήματος. Για τον λόγο αυτό, τα δεδομένα θα πρέπει να είναι επαρκώς ασφαλισμένα, ώστε να μην μπορούν να αλλοιωθούν. Σημαντικό είναι ότι το VDR θα πρέπει να είναι εφοδιασμένο με την αντίστοιχη γεννήτρια, η οποία σε περίπτωση ατυχήματος ή διακοπής της παροχής ρεύματος να είναι σε θέση να διατηρήσει τα δεδομένα για τουλάχιστον δύο ώρες.

Αναλυτικότερα τα στοιχεία που πρέπει να εμπεριέχει συνήθως το VDR συνοψίζονται στα εξής:

- Ημέρα και ώρα (SVDR)
- Τοποθεσία του πλοίου (SVDR)
- Ταχύτητα και προορισμός (SVDR)
- Ηχογραφήσεις στη γέφυρα (SVDR)
- Ηχογραφήσεις επικοινωνιών (SVDR)
- Δεδομένα του Radar (SVDR)
- Δεδομένα του ECDIS (SVDR)
- Συναγερμοί
- Κινήσεις του πηδαλίου
- Καταγραφή των ανοιχτών πορτών
- Υδατοστεγείς πόρτες και πόρτες πυρκαγιάς
- Επιτάχυνση
- Πιέσεις
- Ταχύτητα και κατεύθυνση ανέμου

3.3.3 Σύστημα Αυτόματης Ταυτοποίησης – AIS

Το AIS έχει ως στόχο τον εντοπισμό και την παρακολούθηση των κινήσεων των πλοίων από τις ναυτικές αρχές αλλά και από τα άλλα πλοία. Ο εντοπισμός πραγματοποιείται μέσω εκπομπής σήματος στις συχνότητες VHF. Το συγκεκριμένο σύστημα, σε συνδυασμό με το σύστημα ηλεκτρονικών χαρτών (ECDIS), παρέχει πληροφορίες όπως είναι η ακριβής θέση του πλοίου, η πορεία του, η ταχύτητα που κινείται, οι διαστάσεις του και το όνομά του.

Τα πρώτα συστήματα AIS εμφανίστηκαν το 2002 και έκτοτε η εξέλιξη τους συνεχίζεται. Το συγκεκριμένο σύστημα είναι υποχρεωτικό σε όλα τα πλοία, αφού κύριος σκοπός του είναι η βελτίωση της ασφάλειας στη ναυσιπλοΐα. Σημαντική είναι η συνεισφορά του συστήματος στη μείωση των συγκρούσεων των πλοίων και στη καλύτερη διαχείριση της θαλάσσιας κυκλοφορίας. Το μειονέκτημά του είναι ότι τις περισσότερες φορές, η ακρίβεια και η αξιοπιστία των δεδομένων δεν μπορεί να εκτιμηθεί. Για τον λόγο αυτό, η συνηθέστερη χρήση του είναι ως βοηθητικό σύστημα πλοήγησης.

Οι πληροφορίες τις οποίες διαχειρίζεται το σύστημα AIS θα μπορούσαν να κατηγοριοποιηθούν σε 1) στατικές, 2) δυναμικές και 3) πληροφορίες ναυσιπλοΐας.

1) Στατικές είναι οι πληροφορίες οι οποίες διατηρούνται αμετάβλητες.
   - Αριθμός αναγνώρισης οργανισμού IMO
   - Διεθνές διακριτικό σήμα και όνομα
   - Διαστάσεις του πλοίου
   - Αριθμός Ταυτοποίησης Κινητών Θαλάσσιων Υπηρεσιών (MMSI)
2) Δυναμικές είναι οι πληροφορίες οι οποίες μεταβάλλονται με τη πάροδο του χρόνου.
   - Πραγματική θέση του πλοίου
   - Συντονισμένη παγκόσμια ώρα (UTC)
   - Πορεία που ακολουθεί το πλοίο
   - Ταχύτητα
3) Οι πληροφορίες ναυσιπλοΐας αφορούν αποκλειστικά το ταξίδι που εκτελεί το πλοίο.
   - Ώρα άφιξης στον εκάστοτε προορισμό
   - Λιμάνι προορισμού
   - Μέγεθος και βύθισμα του πλοίου
   - Αριθμός πληρώματος
   - Σημεία διέλευσης
   - Γενικές γεωγραφικές πληροφορίες για τα λιμάνια και για άλλες περιοχές

3.3.4 Σύστημα Ηλεκτρονικής Απεικόνισης Χαρτών και Πληροφοριών – ECDIS

Το σύστημα ECDIS, όπως υποδηλώνει και η ονομασία του, είναι ένα σύστημα ηλεκτρονικής απεικόνισης χαρτών πλοήγησης και αποτελεί ένα υποχρεωτικό σύστημα για τα περισσότερα πλοία. Υπάρχει μία πληθώρα κανονισμών για τη σωστή εφαρμογή και λειτουργία του και είναι υποχρεωτικό σε όλα τα πλοία να υπάρχει και εφεδρική μονάδα, προκειμένου να επιτευχθεί ασφαλέστερη και αποδοτικότερη πλοήγηση. Το συγκεκριμένο σύστημα, όπως και το AIS, αναμεταδίδει πολλές και χρήσιμες πληροφορίες και αλληλοεπιδρά σε σημαντικό βαθμό με τα υπόλοιπα συστήματα πλοήγησης, όπως το AIS, το GNSS, το NAVTEX και τα Radar/ARPA. Οι πληροφορίες οι οποίες αναμεταδίδει συνήθως αναφέρονται στα στοιχεία της ακριβούς θέσης του πλοίου με τη χρήση του GPS, στα Radar, καθώς επίσης και στο AIS που αναφέραμε προηγουμένως. Καθοριστική είναι η λειτουργία του συστήματος για τη διαχείριση εκτάκτων περιστατικών, καθώς είναι υπεύθυνο για την παροχή οπτικοακουστικών προειδοποιήσεων για πιθανούς επικείμενους κινδύνους, προσθέτοντας ακόμα μία προσφερόμενη υπηρεσία, αυτή της διαχείρισης συναγερμών πλοήγησης [30].

Οι δυνατότητές του ποικίλλουν ανάλογα με τον κατασκευαστή, αλλά θα πρέπει να είναι σε θέση να αντικαθιστά πλήρως τους παραδοσιακούς χάρτες στη γέφυρα ενός πλοίου. Η είσοδος των δεδομένων προέρχεται πάντα από μία προκαθορισμένη πηγή και δεν υπάρχουν περιθώρια λάθους, ενισχύοντας με αυτόν τον τρόπο την αξιοπιστία του.

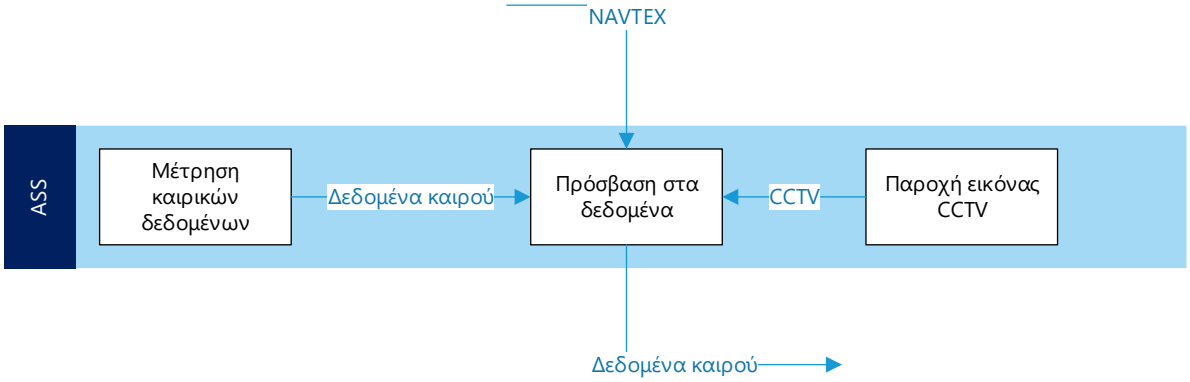
Αν και το συγκεκριμένο σύστημα είναι ένα από τα πιο αξιόπιστα και εύχρηστα συστήματα στη ναυσιπλοΐα, υπάρχουν σημαντικές προτάσεις βελτίωσης, με στόχο την ενσωμάτωσή του και στις αυτοματοποιημένες λειτουργίες ενός αυτόνομου πλοίου. Το ευρωπαϊκό έργο MUNIN προτείνει την ανάπτυξη ενός πρόσθετου συστήματος πλοήγησης στο ECDIS, το οποίο ονομάζεται Integrated Navigation System (INS). Αυτό είναι υπεύθυνο για την ενίσχυση της φυσικής ασφάλειας της πλοήγησης, συγκεντρώνοντας όλη τη διαθέσιμη πληροφορία της πλοήγησης σε ένα ενιαίο σύστημα και παρακολουθώντας όλη τη ροή των δεδομένων και των διαδικασιών από και προς το σύστημα. Στην περίπτωση που υπάρχουν πολλές πηγές από τις οποίες μπορεί να προέρχεται μία πληροφορία, οι σχετικές πληροφορίες θα υφίστανται κατάλληλη επεξεργασία, με σκοπό την επιλογή της επικρατέστερης τιμής, η οποία και θα διανέμεται στο υπόλοιπο σύστημα. Με αυτόν τον τρόπο θα διασφαλίζεται η ποιότητα της πληροφορίας που ανταλλάσσεται. Επιπροσθέτως, το INS θα είναι σε θέση να συγκρίνει τις δραστηριότητες, τις λειτουργίες, τους αισθητήρες και τα συστήματα της γέφυρας του πλοίου και να επιτρέπει τη πρόσβαση σε αυτά μέσω μίας ενιαίας πλατφόρμας. [31]

Στο κεντρικό σύστημα του ECDIS είναι συνδεδεμένα, όπως προαναφέραμε, ορισμένα όργανα που υπάρχουν στη γέφυρα του πλοίου και είναι σημαντικά για την ασφαλή πλοήγησή του [30].

- Δρομόμετρο: Το συγκεκριμένο όργανο είναι υπεύθυνο για την ενημέρωση σχετικά με την ταχύτητα του πλοίου.
- Βαθύμετρο: Μέσω του συγκεκριμένου οργάνου δίνονται στο σύστημα πληροφορίες σχετικά με το βάθος της θάλασσας όπου πλέει το πλοίο και ελέγχεται συγκριτικά με αυτά τα στοιχεία η ακρίβεια των στοιχείων του ηλεκτρονικού χάρτη στη συγκεκριμένη περιοχή.
- Γυροσκοπική πυξίδα: Το όργανο αυτό είναι υπεύθυνο για την ενημέρωση της ακριβούς πορείας του πλοίου, καθώς επίσης και για τις κατευθύνσεις/θέσεις των παραπλεόντων πλοίων και των ακτογραμμών.
- Ανεμόμετρο: Το όργανο αυτό παρέχει πληροφορίες σχετικά με την ένταση του ανέμου και τη συσχέτισή του ως προς το πλοίο.
- Radar και ARPA: Οι συσκευές αυτές είναι υπεύθυνες για την παροχή πληροφοριών θέσης και διόπτευσης των στόχων του Radar. Με αυτόν τον τρόπο οι στόχοι εμφανίζονται στην οθόνη του συστήματος ECDIS, συμβάλλοντας στον τρόπο που αξιολογούνται οι πορείες των πλοίων και εκτιμάται ο κίνδυνος στην περίπτωση που δύο πλοία έχουν την ίδια πορεία ή πλησιάζουν μεταξύ τους.
- Δείκτης GPS: Το συγκεκριμένο όργανο εκπέμπει το στίγμα του πλοίου το οποίο επίσης εμφανίζεται στη κονσόλα του ECDIS.
- Συστήματα αυτόματης πλοήγησης και κίνησης πηδαλίων: Η σύνδεση με το συγκεκριμένο όργανο παρέχει τη δυνατότητα στο ECDIS να μπορεί να εκτελεί άμεσους και γρήγορους χειρισμούς του πλοίου.

3.3.5 Συστήματα προηγμένων αισθητήρων (Advanced Sensor Systems - ASS)

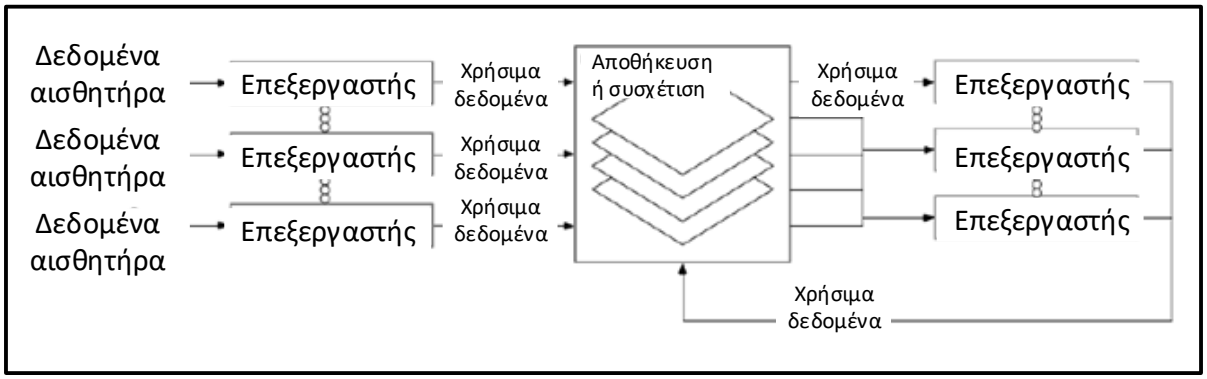
Το ASS έχει ως στόχο τη παραγωγή αξιόπιστης πληροφορίας σχετικά με την κατάσταση που βρίσκεται το πλοίο. Το υποσύστημα περιλαμβάνει τα ραντάρ του πλοίου, τις κάμερες ασφάλειας και παρακολούθησης και γενικότερα τα συστήματα τα οποία συμβάλλουν στην παρατήρηση και παρακολούθηση του περιβάλλοντος του πλοίου. Η λειτουργία του έχει ως στόχο τη διατήρηση μίας συνεχούς και αυτόματης διαδικασίας παρακολούθησης της θαλάσσιας κίνησης και των πιθανών εμποδίων, είτε φυσικών είτε τεχνικών, που το πλοίο μπορεί να συναντήσει κατά τη διάρκεια του ταξιδιού του. Αυτό αποσκοπεί στη συμμόρφωση με τον πέμπτο κανόνα του COLREG, ο οποίος απαιτεί τη συνεχή "maintain a proper look-out […] by all available means to make a full appraisal of the situation and the risk of collision". Επομένως, το ASS ανιχνεύει και ταξινομεί αυτόματα ο,τιδήποτε υπάρχει ή δύναται να εμφανιστεί στο πλοίο και τη περιοχή γύρω του και εξάγει τις απαραίτητες πληροφορίες συγκρίνοντας όλες τις εισόδους των αισθητήρων οι οποίοι είναι άρρηκτα συνδεδεμένοι με συστήματα όπως είναι το AIS, τα Radar και οι κάμερες παρακολούθησης.



Εικόνα 9. Διεργασία αισθητήρων καιρού [31]

Το συγκεκριμένο σύστημα εμπεριέχει έναν αριθμό από αισθητήρες οι οποίοι μπορούν να ταξινομηθούν λαμβάνοντας υπόψη τα αντίστοιχα χαρακτηριστικά τους. Υπάρχουν αισθητήρες οι οποίοι συγκεντρώνουν πληροφορίες από το εσωτερικό του πλοίου, καθώς επίσης και εκείνοι που συγκεντρώνουν από το εξωτερικό περιβάλλον. Επίσης, ένας αισθητήρας μπορεί να είναι ενεργητικός ή παθητικός. Ο ενεργητικός αισθητήρας είναι εκείνος που εκπέμπει ενέργεια για να πραγματοποιήσει κάποια μέτρηση ενώ ο παθητικός μετρά την ενέργεια που αντιλαμβάνεται στην αντίστοιχη εμβέλειά του. Μερικά ακόμη χαρακτηριστικά των αισθητήρων θα μπορούσαν να είναι το πεδίο ορατότητας, η εμβέλεια, η ακρίβεια και η ανάλυση. [32]

Η Εικόνα 10 παρουσιάζει τη ροή εργασιών που πραγματοποιούνται στο σύστημα ASS. Η διαδικασία είναι χωρισμένη σε τρία γενικά μέρη. Στο πρώτο βήμα οι αισθητήρες που σχετίζονται με την πλοήγηση συγκεντρώνουν μεγάλες ποσότητες δεδομένων. Στη συνέχεια, αυτά τα δεδομένα υφίστανται επεξεργασία με σκοπό τον διαχωρισμό των χρήσιμων πληροφοριών. Το επόμενο βήμα είναι να συσχετισθούν τα δεδομένα που έχουν διαχωριστεί. Στο τέλος, τα δεδομένα μπορεί να ξαναχρησιμοποιηθούν με την ίδια διαδικασία σε μία συνεχή διαδικασία συσχέτισης των δεδομένων.

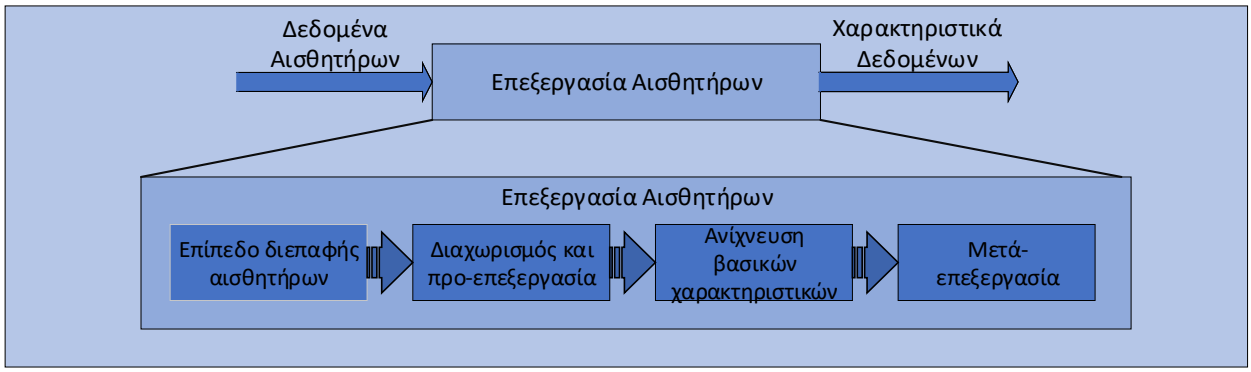


Εικόνα 10. Ροή εργασιών ASS [32]

Η αρχιτεκτονική του ASS [32], η οποία έχει προταθεί στο MUNIN, περιλαμβάνει τέσσερα στάδια διεργασιών:

1. Επίπεδο διεπαφής αισθητήρων: αυτή η διεργασία έχει ως αποτέλεσμα την παροχή όλων των πληροφοριών που παρέχουν οι αισθητήρες για εκτενέστερη επεξεργασία.
2. Διαχωρισμός και προ-επεξεργασία: στο στάδιο αυτό τα βασικά δεδομένα υφίστανται επεξεργασία. Λαμβάνοντας υπόψη τα χαρακτηριστικά των δεδομένων, πραγματοποιείται η πρώτη επεξεργασία από την οποία επιτυγχάνεται η μείωση θορύβου στο σύστημα, στατιστικές αναλύσεις, βελτίωση της εικόνας.
3. Ανίχνευση βασικών χαρακτηριστικών: Από τις ήδη διαχωρισμένες δομές δεδομένων, εξάγονται και αναλύονται τα βασικά χαρακτηριστικά.
4. Μετα - επεξεργασία: Τελικώς, τα προηγούμενα βασικά χαρακτηριστικά, τα οποία έχουν διαχωριστεί, εμπλουτίζονται με ορισμένα παραπάνω στοιχεία που βοηθούν την ανάλυση.

Το παρακάτω σχήμα συνοψίζει τις παραπάνω διεργασίες του ASS:



Εικόνα 11. Σειριακή λειτουργία αισθητήρα [32]

3.3.6 Σύστημα αυτόματου ελέγχου πλοίου (Autonomous Ship Controller)

Το Autonomous Ship Controller – ASC, πραγματοποιεί μία αξιολόγηση των δεδομένων τα οποία έχουν συλλεχθεί από τους αισθητήρες του πλοίου και των δεδομένων που έχουν προέλθει από το SCC και στη συνέχεια πραγματοποιούν τις αντίστοιχες ενέργειες στα υπόλοιπα αυτοματοποιημένα συστήματα του πλοίου. Αποτελεί έναν επιπρόσθετο έλεγχο και μία παραπάνω παρακολούθηση στις λειτουργίες του πλοίου οι οποίες επιτρέπουν την αυτόματη λειτουργία του. Το ASC είναι άρρηκτα συνδεδεμένο με άλλα συστήματα, όπως είναι το AEMC, τα συστήματα πλοήγησης, καθώς επίσης και με όλα τα συστήματα διαχείρισης των επικοινωνιών μεταξύ του πλοίου και του SCC.

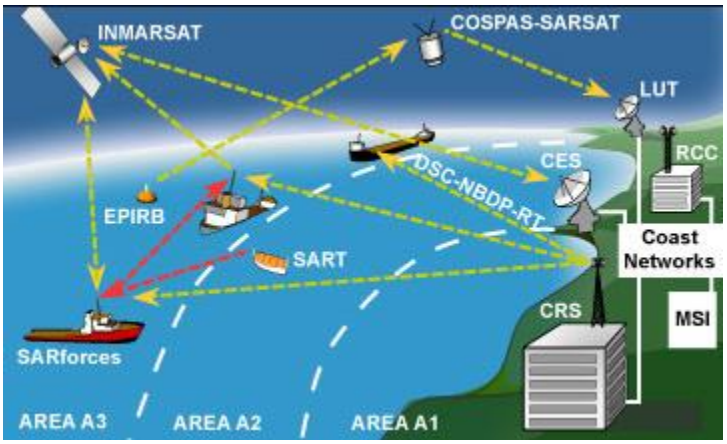
3.3.7 Σύστημα Ναυτιλιακού Κινδύνου Ασφάλειας - GMDSS

Η εισαγωγή του συγκεκριμένου συστήματος στη ναυτιλία πραγματοποιήθηκε πριν περίπου δύο δεκαετίες. Το GMDSS αποτελεί ένα σύνολο διαδικασιών ασφάλειας, τύπων εξοπλισμού και πρωτοκόλλων επικοινωνίας. Σημαντική είναι η προσφορά του στη διάσωση σκαφών που βρίσκονται σε κίνδυνο και στη γενικότερη αύξηση της ασφάλειας, αφού είναι σε θέση να αποστέλλει σήμα κινδύνου και στη ξηρά αλλά και στη θάλασσα, συμβάλλοντας στην αποτελεσματικότερη αντιμετώπιση τέτοιου είδους επεισοδίων.

Για τη διασφάλιση και την αποτελεσματική λειτουργία του συγκεκριμένου συστήματος απαιτείται η εκτέλεση συγκεκριμένων διαδικασιών. Το GMDSS είναι σε θέση να αποστέλλει κλήση για βοήθεια σε άλλα σκάφη, να καθορίζει τον χρόνο και τον τόπο επιφυλακής των κοντινών σκαφών και του κέντρου Έρευνας και Διάσωσης, καθώς επίσης και να προσδιορίζει άμεσα τη θέση ενός σκάφους το οποίο βρίσκεται σε κατάστασης έκτακτης ανάγκης. Επίσης, μέσω του συστήματος GMDSS εκπέμπονται πληροφορίες οι οποίες αφορούν την ασφαλή ναυσιπλοΐα και πληροφορίες οι οποίες εξυπηρετούν την επικοινωνία μεταξύ σκάφους με ξηρά αλλά και μεταξύ δύο σκαφών. Τέλος, μέσω του GMDSS παρέχονται εφεδρικά μέσα για την αντιμετώπιση περιστάσεων έκτακτης ανάγκης.

Όπως το πλοίο αποτελεί ένα σύστημα συστημάτων, έτσι και τα επιμέρους συστήματά του αποτελούν συστήματα συστημάτων. Το GMDSS είναι ένα σύστημα που και αυτό με τη σειρά του αποτελείται από άλλα υποσυστήματα, επικοινωνιακά ως επί των πλείστον, επίγεια ή μη. Χαρακτηριστικά μπορούμε να πούμ ότι αποτελείται από τα εξής πέντε υποσυστήματα:

1. Συστήματα επικοινωνίας στις ζώνες Πολύ Υψηλών Συχνοτήτων – VHF, Υψηλών Συχνοτήτων – HF και Μετρίων Συχνοτήτων – MF
2. Σύστημα NAVTEX
3. Δορυφορικό σύστημα COSPAS-SARSAT
4. Δορυφορικό σύστημα INMARSAT
5. Πομποί SART και ραδιοφάροι EPIRB



Εικόνα 12. Συστήματα του GMDSS

Τα εμπορικά πλοία βάρους άνω των 300 τόνων τα οποία πραγματοποιούν παγκόσμια δρομολόγια είναι υποχρεωμένα να έχουν εγκατεστημένο το σύστημα GMDSS. Η ανταλλαγή πληροφοριών πραγματοποιείται συνήθως μέσω ραδιοκυμάτων ή δορυφορικών επικοινωνιών, χρησιμοποιώντας τα παραπάνω συστήματα. Η πληροφορία που ανταλλάσσεται εμπεριέχει πάντα το MMSI του πλοίου και συνήθως τη θέση του. Επίσης, η φύση της μεταδιδόμενης πληροφορίας μπορεί να καθοριστεί χειροκίνητα εκ των προτέρων και να είναι συναγερμός για πυρκαγιά, πλημμύρα, σύγκρουση, προσάραξη σε ξέρα, κίνδυνος ανατροπής, κίνηση πάνω στο πλοίο, πειρατεία ή ακυβέρνητο πλοίο. Οι πομποί SART από την άλλη, δεν είναι ικανοί να μεταφέρουν τέτοιου είδους πληροφορία αφού ανταποκρίνονται αποκλειστικά σε ραδιοκύματα και χρησιμοποιούνται για την αναμετάδοση θέσεων συνήθως [31].

Συνοψίζοντας λοιπόν για το GMDSS, τα οφέλη που προσφέρει στα πλοία και γενικότερα στον χώρο της ναυτιλίας είναι πολλά. Αρχικά, παρέχει συντονισμένη βοήθεια στην επιχείρηση διάσωσης αφού είναι σχεδόν ταυτόχρονη η ενημέρωση των αρχών έρευνας ξηράς με την ενημέρωση των κοντινών πλοίων. Σημαντικό πλεονέκτημα του συστήματος είναι η ταχύτατη αποστολή πληροφοριών κινδύνου όπως η ταυτότητα του πλοίου, η θέση του και η φύση του κινδύνου στον οποίο βρίσκεται. Τέλος, αποτελεί μία αυτοματοποιημένη διαδικασία διαχείρισης περιστατικών, εφόσον πλέον η συγκέντρωση και η αποστολή των πληροφοριών γίνεται από το ίδιο το σύστημα. Αυτό αποτελεί σημαντικό παράγοντα για την ένταξή του στα αυτοματοποιημένα συστήματα του αυτόνομου πλοίου.

3.3.8 Σύστημα διαχείρισης φορτίου (Cargo Management / Cargo Control Room - CCR)

Το συγκεκριμένο σύστημα εμπεριέχει όλες τις λειτουργίες που πρέπει να εκτελέσει ένα πλοίο για τη διαχείριση και τον έλεγχο του φορτίου του, στο οποίο μπορεί να συγκαταλέγεται και επικίνδυνο υλικό. Σημαντική είναι η αλληλεπίδρασή του με πολλά συστήματα του πλοίου όπως είναι το ASS και το CCTV, αλλά και με υποσυστήματα τα οποία βρίσκονται στο SCC. Τα συστήματα αυτά είναι υπεύθυνα για τη διεκπεραίωση λειτουργιών που συμβάλλουν στην ορθή και αποτελεσματική διαχείριση του φορτίου, όπως η παρακολούθηση της πορείας του πλοίου, η εύρεση της θέσης του και ο έλεγχος του περιβάλλοντός του μέσω του διαδικτύου. Το Cargo management system είναι επίσης υπεύθυνο για την επικοινωνία και τον συντονισμό των γερανών φόρτωσης/εκφόρτωσης οι οποίοι υπάρχουν και στο πλοίο αλλά και στα λιμάνια (AGVs), καθώς επίσης και για λεπτομέρειες του φορτίου οι οποίες επηρεάζουν

άμεσα το πλοίο, όπως είναι η κατάλληλη τοποθέτησή του στο αντίστοιχο μέρος προς αποφυγή απώλειας ισορροπίας ή καταστροφής της υποδομής.

Αναλυτικότερα, μερικά από τα συστήματα τα οποία βρίσκονται στο CCR είναι [8]:

- Συστήματα ελέγχου/ένδειξης επιπέδου: τα συστήματα αυτά ανιχνεύουν το επίπεδο υγρών αλλά και στερεών υλικών τα οποία βρίσκονται στους αποθηκευτικούς χώρους του πλοίου. Η λειτουργία τους είναι ζωτικής σημασίας, ιδιαίτερα όταν το φορτίο δεν είναι συσκευασμένο.
- Συστήματα απομακρυσμένου ελέγχου βαλβίδων - Valve Remote Control System (VRCS) : τα συγκεκριμένα συστήματα χρησιμοποιούνται για τη φόρτωση και εκφόρτωση όλων των ειδών τάνκερ. Το σύστημα VRCS προσφέρει το δικό του περιβάλλον αλληλεπίδρασης για τον ευκολότερο έλεγχο της θερμοκρασίας και της πίεσης.
- Σύστημα έρματος: το σύστημα αυτό επιτρέπει την εισχώρηση και εκχώρηση υδάτων στο πλοίο με στόχο την καλύτερη εξισορρόπησή του κατά τη διάρκεια φορτώσεων και εκφορτώσεων ή δυσμενών καιρικών συνθηκών.
- Σύστημα συναγερμού για εισροή υδάτων - Water Intrusion Detection System - WIDS: το συγκεκριμένο σύστημα έχει σχεδιαστεί για να ανιχνεύει το νερό στα αμπάρια του πλοίου. Συνδέεται κατευθείαν με το κεντρικό σύστημα συναγερμού του πλοίου και συμβάλει στη βελτίωση της φυσικής ασφάλειας.

3.3.9 Συστήματα ελέγχου εισόδου

Σημαντικά υποσυστήματα του BAS αποτελούν αυτά που είναι υπεύθυνα για τον έλεγχο εισόδου στο πλοίο είτε φυσικά είτε απομακρυσμένα. Η ενίσχυση της ασφάλειας στα αυτόνομα πλοία αποτελεί ζωτικής σημασίας, καθώς η εκάστοτε εταιρεία είναι υπεύθυνη για τα φορτία που μεταφέρει ή για τις ανθρώπινες ζωές που μπορεί να βρίσκονται πάνω στο πλοίο, η εφαρμογή λοιπόν κατάλληλων μέτρων ελέγχου εισόδου είναι σημαντική. Τα υποσυστήματα που συμβάλλουν σε αυτή τη διαδικασία είναι τα εξής:

- Συστήματα παρακολούθησης CCTV: Τα συγκεκριμένα συστήματα είναι ικανά να λειτουργούν ακόμα και σε δυσμενείς καταστάσεις (χαμηλή ορατότητα, μηδενικό φως) και να παρέχουν συνεχή παρακολούθηση του ευρύτερου περιβάλλοντος του πλοίου.
- Bridge Navigational Watch Alarm System (BNWAS): Σκοπός του συστήματος είναι να ειδοποιεί το SCC στην περίπτωση που αντιληφθεί ότι το πλοίο είναι ακυβέρνητο. Αυτό επιτυγχάνεται ηχώντας ένα συγκεκριμένο σύνολο συναγερμών και ειδοποιήσεων που επισημαίνουν την ύπαρξη προβλήματος.
- Shipboard Security Alarm Systems (SSAS): Το SSAS αποτελεί ένα μέτρο ενίσχυσης της ασφάλειας του πλοίου και της καταστολής της πειρατείας και της τρομοκρατίας ενάντια σε αυτό. Η λειτουργία του εστιάζεται στην αποστολή ενός σήματος εντοπισμού (beacon) όταν υπάρξει κίνδυνος στο πλοίο. Το beacon μεταδίδει έναν συγκεκριμένο κωδικό χώρας τον οποίο μόλις λάβουν οι αρχές πραγματοποιούν τις αντίστοιχες ενέργειες.
- Electronic Personnel on Board – POB Systems: Πρόκειται για συστήματα τα οποία συλλέγουν πληροφορία για τα άτομα που βρίσκονται στο πλοίο και στα μέρη που δραστηριοποιούνται.

Αποτελούν επίσης ένα συμπληρωματικό σύστημα ελέγχου εισόδου καθώς πολλές λειτουργίες τους αφορούν τον έλεγχο εισόδου στους επιμέρους χώρους του πλοίου.

3.3.10 Συστήματα εξυπηρέτησης και διαχείρισης επιβατών - PSMS

Τα συστήματα που υπάρχουν και αλληλοεπιδρούν στη συγκεκριμένη κατηγορία συστημάτων αποσκοπούν στην εφαρμογή όλων των απαραίτητων λειτουργιών με σκοπό την εξυπηρέτηση των πελατών - επιβατών. Σκοπός τους είναι η σωστή διαχείριση ιδιοκτησίας, επιβίβασης και ελέγχου εισόδου. Έξυπνες συσκευές όπως είναι τα tablets και οι σαρωτές αποτελούν από μόνες τους σημεία επίθεσης, αφού διαρκώς συλλέγουν δεδομένα και τα αποστέλλουν σε άλλα συστήματα του πλοίου. Αυτά τα συστήματα εξυπηρέτησης και διαχείρισης συνήθως αναφέρονται σε πλοία τα οποία θα μεταφέρουν και επιβάτες. Για τον λόγο αυτό οι περισσότερες λειτουργίες των συστημάτων αυτών αφορούν τη καλύτερη οργάνωση και εξυπηρέτησή τους. Υπάρχουν πέντε υποσυστήματα τα οποία αλληλοσυνδέονται για την επίτευξη των παραπάνω στόχων.

- Property Management System – PMS: Το PMS είναι υπεύθυνο για τη διαχείριση και τον συντονισμό των κρατήσεων, των στοιχείων των επιβατών και του ταξιδιού. Επίσης, είναι αρμόδιο για τον συντονισμό του λογιστηρίου και τη συνολική διαχείριση του ταξιδιού των επιβατών (αποσκευές, συναλλάγματα, πληρωμές)
- Medical Records: Το σύστημα αυτό είναι υπεύθυνο για τη διαχείριση ευαίσθητων πληροφοριών οι οποίες αφορούν πιθανά ιατρικά δεδομένα των επιβατών.
- Ship passenger/seafarer boarding access systems.
- Συστήματα υποστήριξης της συνολικής υποδομής: Αυτά τα συστήματα είναι υπεύθυνα για να συμπληρώσουν τις λειτουργίες ελέγχου εισόδου των προηγούμενων υποσυστημάτων. Παράδειγμα τέτοιας λειτουργίας είναι η λήψη DNS και η αυθεντικοποίηση του χρήστη σε υπάρχοντα συστήματα του πλοίου.

3.4 Κέντρο ελέγχου ξηράς (Shore Control Center – SCC)

Το SCC αποτελεί μία νέα οντότητα που εισάγεται στη ναυσιπλοΐα. Το SCC είναι σε θέση να ελέγχει και να καθοδηγεί ένα ή και περισσότερα πλοία, ανάλογα με την υποδομή και σε αυτό μπορούν να απασχοληθούν από τον οικονομικό διευθυντή και τον ιδιοκτήτη της επιχείρησης έως τον πλοίαρχο και του μηχανικούς. Το SCC παρέχει τη δυνατότητα πλέον στο πλοίο να υπάρχει περιορισμένο ή και καθόλου πλήρωμα για την εκτέλεση των λειτουργιών του. Ο χειρισμός και η παρακολούθηση του πλοίου μπορεί να πραγματοποιείται είτε συνεχώς καθ' όλη τη διάρκεια του ταξιδιού είτε μερικώς, σε περιπτώσεις δηλαδή όπου υπάρχει ανάγκη. Το SCC αποτελεί ένα κοινωνικοτεχνικό σύστημα με τις επιμέρους οντότητες να επικοινωνούν και να αλληλοεπιδρούν μεταξύ τους.

Επιγραμματικά, οι διεργασίες που εκτελεί το SCC συνοψίζονται στις εξής [29]:

1) Παρακολούθηση του πλοίου
2) Διασφάλιση της ασφαλούς λειτουργίας
3) Αναγνώριση καταστάσεων
4) Εκτέλεση άμεσων ενεργειών στο πλοίο

3.4.1 Συστήματα διεπαφής πλοίου με τη ξηρά (Human Machine Interface – HMI)

Το συγκεκριμένο υποσύστημα πρέπει να είναι σχεδιασμένο ώστε να είναι σε θέση να παίρνει αποφάσεις σύμφωνα πάντα με τη καθοδήγηση του ανθρώπινου παράγοντα. Μέσω του συγκεκριμένου συστήματος διεπαφής, ο ανθρώπινος παράγοντας είναι σε θέση να παρέμβει στη λειτουργία του αυτόνομου ή τηλεχειριζόμενου πλοίου και να πραγματοποιεί τις ανάλογες ενέργειες. Ένα HMI σύστημα μπορεί να εμπεριέχει επικοινωνιακές λειτουργίες, λειτουργίες πλοήγησης και πλήρη αποτύπωση της εικόνας του EAS και του BAS.

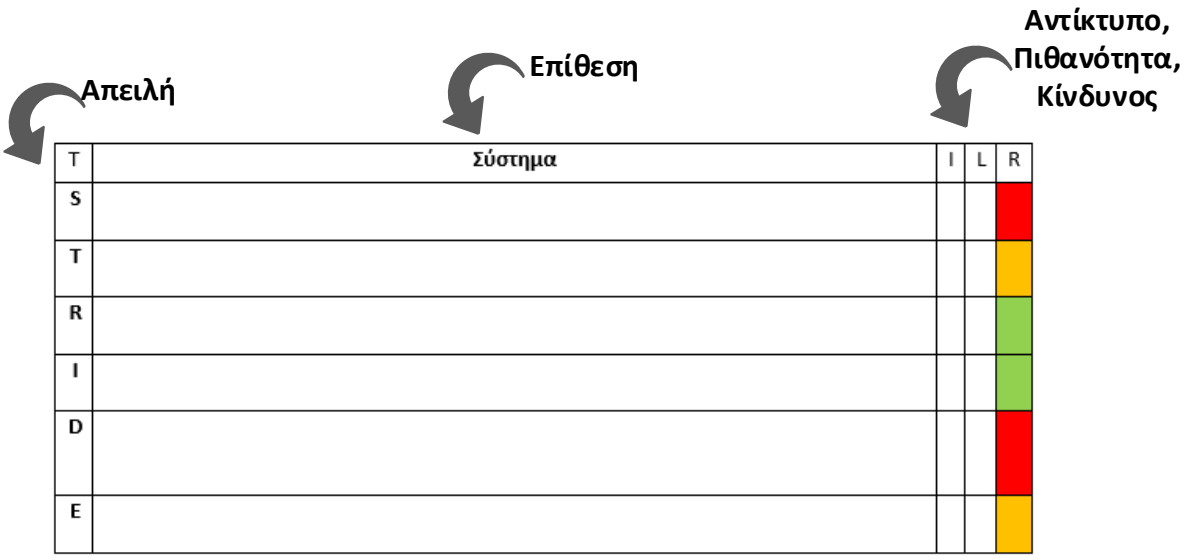
3.4.2 Σύστημα απομακρυσμένου ελέγχου και υποστήριξης πλοίου (Remote Maneuvering Support System – RMSS)

Το RMSS αποτελεί ένα πληροφοριακό σύστημα το οποίο επιτρέπει τη διεκπεραίωση ασφαλών αυτόνομων διεργασιών των πλοίων και ελέγχεται πλήρως από το SCC. Είναι σε θέση να παρέχει αποτελεσματικές προβλέψεις της θέσης του πλοίου, να υπολογίζει πιθανούς περιορισμούς των ελιγμών που πρέπει να εκτελέσει το πλοίο και να υποβοηθά στον απομακρυσμένο έλεγχο του πλοίου από το SCC.

Κεφάλαιο 4

4.1 Στόχος

Στόχος μας στο συγκεκριμένο κεφάλαιο είναι, με τη βοήθεια της μεθόδου STRIDE, να πραγματοποιήσουμε μία ανάλυση απειλών στα συστήματα και υποσυστήματα του πλοίου, λαμβάνοντας υπόψη τα έξι είδη επιθέσεων τα οποία ορίζει η μέθοδος. Στη συνέχεια, αφού αναγνωρίσουμε τις απειλές, πραγματοποιούμε την αποτίμηση κινδύνου και εξάγουμε τα αντίστοιχα αποτελέσματα για τα συστήματα.



Πίνακας 13. Υπόδειγμα πίνακα STRIDE

4.2 Εφαρμογή STRIDE

Οι παρακάτω πίνακες παρουσιάζουν τα αποτελέσματα της ανάλυσης απειλών που πραγματοποιήθηκε στα συστήματα και τα υποσυστήματα του cyber-enabled πλοίου, όπως αυτά αναλύθηκαν στο Κεφάλαιο 3, με τη χρήση της μεθόδου STRIDE. Αναλυτικότερα, η εφαρμογή της μεθόδου STRIDE εφαρμόστηκε μέχρι το επίπεδο 3 του δέντρου αναπαράστασης της αρχιτεκτονικής του πλοίου όπως φαίνεται στην εικόνα 6 του κεφαλαίου 3, αφού τα συστήματα στα χαμηλότερα επίπεδα συμπεριλαμβάνονται επαρκώς μέχρι το επίπεδο 3 χωρίς να επηρεάζουν την εξαγωγή αποτελεσμάτων των Threat και Risk Analysis. Η διάσχιση του δέντρου για την ανάλυση είναι προδιατεταγμένη, ξεκινώντας από τη ρίζα (που είναι το πλοίο).

Στη συνέχεια, ο αντίκτυπος (I) του κάθε συστήματος και υποσυστήματος εκτιμήθηκε σε τρία επίπεδα: High (H), Medium (M) και Low (L) λαμβάνοντας υπόψη την εικόνα 2 του κεφαλαίου 2. Επίσης, η πιθανότητα εμφάνισης (L) της κάθε απειλής υπολογίστηκε λαμβάνοντας υπόψη την εικόνα 3 του δεύτερου κεφαλαίου, σε τρία επίπεδα: Very Likely (V), Moderate (M) και Rare (R). Τέλος, όπως παρουσιάζεται στη τελευταία στήλη των παρακάτω πινάκων, πραγματοποιήθηκε η αποτίμηση κινδύνου

(R) για κάθε σύστημα και υποσύστημα όπως παρουσιάζεται στη μήτρα αποτίμησης κινδύνου της εικόνας 4 του δεύτερου κεφαλαίου.

Likelihood/Impact	HIGH	MEDIUM	LOW
Very Likely	H	H	M
Moderate	H	M	L
Rare	M	L	L

Πίνακας 4. Μήτρα αποτίμησης κινδύνων

T	Αυτόματα συστήματα μηχανών (Engine Automation System – EAS)	I	L	R
S	Στην περίπτωση που ο επιτιθέμενος προσποιηθεί ότι το σύστημα λίπανσης κινητήρα δεν αποδίδει όπως θα έπρεπε, θα μπορεί να προκαλέσει ακόμα και τη καταστροφή του κινητήρα.	**H**	**M**	**H**
T	Η αλλοίωση κάποιας εντολής διαχείρισης των μηχανών θα μπορούσε να οδηγήσει σε καταστροφή του πλοίου και σε απώλεια ανθρώπινης ζωής.	**H**	**R**	**M**
R	Οι περισσότερες λειτουργίες στο συγκεκριμένο υποσύστημα είναι σημαντικές για τη σωστή λειτουργία ολόκληρου του πλοίου. Η μη αποδοχή της εκτέλεσης συγκεκριμένων ενεργειών είναι ανεπίτρεπτη.	**M**	**R**	**L**
I	Η διαρροή πληροφοριών για το συγκεκριμένο υποσύστημα δεν θα μπορούσε να επιφέρει σημαντικά προβλήματα στη λειτουργία ολόκληρου του συστήματος.	**L**	**R**	**L**
D	Η διαθεσιμότητα του συγκεκριμένου υποσυστήματος είναι πολύ σημαντική, καθώς η διακοπή της λειτουργίας του σημαίνει την ακινητοποίηση ολόκληρου του συστήματος.	**H**	**M**	**H**
E	Στην περίπτωση που ένας επιτιθέμενος αποκτήσει πρόσβαση με δικαιώματα διαχειριστή, ενδέχεται να πραγματοποιηθούν ανεπιθύμητες ενέργειες, οι οποίες μπορούν να κοστίσουν σημαντικά σε ολόκληρη την υποδομή.	**H**	**R**	**M**

Πίνακας 5. STRIDE - Αυτόματα συστήματα μηχανών

T	Σύστημα αυτόματου ελέγχου και παρακολούθησης μηχανών (Autonomous Engine Monitoring and Control – AEMC)	I	L	R
S	Στην περίπτωση που το συγκεκριμένο υποσύστημα παραβιαστεί από κακόβουλο χρήστη προσποιούμενο το σύστημα παραγωγής ενέργειας, υπάρχει κίνδυνος διακοπής λειτουργίας των συστημάτων των μηχανών, παραβίασης της ακεραιότητας του υποσυστήματος και άλλων ενεργειών οι οποίες μπορούν να προκαλέσουν σημαντικές καταστροφές στην υποδομή.	**H**	**R**	**M**
T	Η αλλοίωση των δεδομένων του AEMC θα μπορούσε να οδηγήσει σε καταστροφή της υποδομής καθώς είναι υπεύθυνο για διεργασίες όπως η διακοπή λειτουργίας των μηχανών ή ο λάθος χειρισμός του πηδαλίου.	**H**	**M**	**H**
R	Η αποποίηση της εκτέλεσης των διεργασιών του υποσυστήματος αποτελεί σοβαρό πρόβλημα καθώς αυτές οι διεργασίες μπορεί να προκαλέσουν οικονομική καταστροφή καθώς και απώλεια ανθρώπινης ζωής.	**H**	**R**	**M**

I	Η διαρροή πληροφοριών του υποσυστήματος δεν θα προκαλούσε δυσλειτουργία στο σύστημα.	**L**	**M**	**L**
D	Η διακοπή της λειτουργίας του υποσυστήματος θα μπορούσε να προκαλέσει σημαντικές συνέπειες για ολόκληρη την υποδομή, καθώς αποτελεί κύριο σύστημα ελέγχου άλλων συστημάτων όπως τα συστήματα μηχανών, ταχύτητας και παραγωγής ενέργειας.	**H**	**M**	**H**
E	Η παράνομη απόκτηση δικαιωμάτων διαχειριστή στο AEMC θα μπορούσε να προκαλέσει τη δημιουργία ανεπιθύμητων ή μη έγκυρων περιστατικών, προσβάλλοντας τον εξοπλισμό του πλοίου.	**H**	**R**	**M**

Πίνακας 6. STRIDE - Σύστημα αυτόματου ελέγχου και παρακολούθησης μηχανών

T	**Σύστημα καταγραφής συμβάντων των μηχανών (Engine Data Logger – EDL)**	I	L	R
S	Η σύνδεση ενός κακόβουλου χρήστη με τα διαπιστευτήρια κάποιου νόμιμου, του παρέχει τη δυνατότητα ανάγνωσης και τροποποίησης των δεδομένων που αφορούν τη λειτουργία των μηχανών. Μπορεί με αυτόν τον τρόπο να προκληθεί βλάβη στο υποσύστημα και στη συνέχεια στην υποδομή.	**H**	**M**	**H**
T	Παραβιάζοντας την ακεραιότητα των δεδομένων του υποσυστήματος μπορεί να προκληθεί μηχανική βλάβη και απώλεια ανθρώπινης ζωής.	**H**	**M**	**H**
R	Η σύνδεση στο υποσύστημα πραγματοποιείται από συγκεκριμένα άτομα με αποτέλεσμα η μη αποδοχή εκτέλεσης κάποιας ενέργειας να μην είναι αποδεκτή.	**H**	**R**	**M**
I	Η αποκάλυψη πληροφοριών που βρίσκονται στο συγκεκριμένο υποσύστημα δεν μπορεί να βλάψει σοβαρά την υποδομή.	**L**	**M**	**L**
D	Η μη διαθεσιμότητα του υποσυστήματος δύναται να οδηγήσει σε μηχανική βλάβη και σε απώλεια ανθρώπινης ζωής.	**H**	**M**	**H**
E	Η σύνδεση στο σύστημα με δικαιώματα διαχειριστή μπορεί να βλάψει την ακεραιότητα και τη διαθεσιμότητα των δεδομένων, δημιουργώντας σοβαρά προβλήματα σε ολόκληρη την υποδομή.	**H**	**R**	**M**

Πίνακας 7. STRIDE - Σύστημα καταγραφής συμβάντων των μηχανών

T	**Σύστημα αυτόματου ελέγχου μηχανών (Autonomous Control of the Engine Room)**	I	L	R
S	Η δυνατότητα του επιτιθέμενου να προσποιηθεί ότι είναι το σύστημα καυσίμων και να στέλνει μήνυμα ότι είναι άδειο θα οδηγούσε σε αλλοίωση του δρομολογίου του πλοίου, ακόμη και σε απώλεια του φορτίου του ή της υποδομής.	**H**	**M**	**H**
T	Η αλλοίωση/τροποποίηση του δικτύου του συστήματος θα μπορούσε να οδηγήσει στην καταστροφή των μηχανών ή στη διακοπή λειτουργίας τους.	**M**	**M**	**M**

R	Οι ενέργειες στα συστήματα ελέγχου μηχανών είναι ανατεθειμένες στους αντίστοιχους ρόλους, επομένως η αποποίηση ευθύνης για την εκτέλεση μίας πράξης είναι ανεπίτρεπτη.	**M**	**R**	**L**
I	Η παραβίαση της εμπιστευτικότητας του συστήματος δεν θα προκαλούσε σημαντικές βλάβες, καθώς οι πληροφορίες που ανταλλάσσονται δεν είναι ευαίσθητες.	**L**	**M**	**L**
D	Η μη διαθεσιμότητα του συστήματος θα προκαλούσε την ακινησία του πλοίου ή ακόμα και βλάβες στα επιμέρους υποσυστήματα.	**M**	**M**	**M**
E	Η απόκτηση δικαιωμάτων διαχειριστή στο συγκεκριμένο σύστημα θα οδηγούσε στην απόκτηση του ελέγχου του πλοίου, γεγονός που θα επέφερε οικονομικές απώλειες και δυσφήμιση στον οργανισμό.	**H**	**R**	**M**

Πίνακας 8.STRIDE - Σύστημα αυτόματου ελέγχου μηχανών

T	**Σύστημα διαχείρισης έκτακτων περιστατικών (Emergency Handling)**	I	L	R
S	Στην περίπτωση που ένας κακόβουλος χρήστης προσποιηθεί ότι είναι το σύστημα αισθητήρων πυρόσβεσης, θα είναι σε θέση να ενεργοποιήσει τον συναγερμό πυρόσβεσης και να καταστρέψει μέρη της υποδομής.	**M**	**M**	**M**
T	Η τροποποίηση των δεδομένων του συγκεκριμένου συστήματος θα μπορούσε να οδηγήσει σε έναρξη εσφαλμένου συναγερμού πυρόσβεσης και να πλημμυρίσει το πλοίο, προκαλώντας βλάβη στην υποδομή.	**M**	**M**	**M**
R	Η αποποίηση της ευθύνης ότι ο χρήστης πάτησε το κόκκινο κουμπί και σήμανε τον συναγερμό ότι το πλοίο βυθίζεται, είναι ανεπίτρεπτη, καθώς οι ρόλοι είναι πλήρως καθορισμένοι.	**M**	**R**	**L**
I	Η βλάβη της εμπιστευτικότητας του συστήματος δεν θα δημιουργούσε σοβαρές επιπτώσεις στη λειτουργία του πλοίου και γενικότερα σε ολόκληρη την υποδομή.	**M**	**R**	**L**
D	Στην περίπτωση που ο επιτιθέμενος προσβάλει τη διαθεσιμότητα του συστήματος, θα θέσει σε κίνδυνο ολόκληρη την υποδομή και το φορτίο αυτής, καθώς αν παραστεί ανάγκη δεν θα ειδοποιηθεί το SCC.	**H**	**M**	**H**
E	Η απόκτηση δικαιωμάτων διαχειριστή στο σύστημα θα επέφερε σημαντικές αλλαγές στην λειτουργία του, αφού θα μπορούσε να απενεργοποιήσει όλους τους συναγερμούς στο πλοίο.	**H**	**R**	**M**

Πίνακας 9. STRIDE - Σύστημα διαχείρισης έκτακτων περιστατικών

T	**Σύστημα βελτιστοποίησης απόδοσης μηχανών (Engine Efficient System)**	I	L	R
S	Στην περίπτωση που ο επιτιθέμενος προσποιηθεί ότι είναι το σύστημα μηχανής και η κατανάλωση καυσίμων έχει αυξηθεί ανεξήγητα, θα μπορούσε να προκληθεί βλάβη στο σύστημα μηχανών και καθυστέρηση των διεργασιών του πλοίου.	**H**	**R**	**M**

T	Η προσβολή της ακεραιότητας του συστήματος θα έθετε σε κίνδυνο ολόκληρη την υποδομή καθώς σε περίπτωση σφάλματος ή συντήρησης δε θα ήταν εφικτό για το σύστημα να δράσει.	**H**	**M**	**H**
R	Η αποποίηση της ευθύνης εκτέλεσης μίας ενέργειας είναι ανεπίτρεπτη καθώς οι ρόλοι του συστήματος είναι επαρκώς προσδιορισμένοι.	**M**	**M**	**M**
I	Η διαρροή πληροφοριών του συστήματος δεν θα προκαλούσε κάποιο σημαντικό αντίκτυπο στο πλοίο και στην εταιρεία.	**L**	**M**	**L**
D	Η διακοπή της λειτουργίας του συστήματος ελέγχου θα προκαλούσε δυσλειτουργία των συστημάτων μηχανής του πλοίου, χωρίς να προκαλέσει κάποια μεγαλύτερη βλάβη.	**M**	**M**	**M**
E	Στην περίπτωση που ο επιτιθέμενος αποκτήσει δικαιώματα διαχειριστή, θα είναι σε θέση να παρεμποδίσει τη λειτουργία συστημάτων του πλοίου και να αλλοιώσει τα ποσοστά βελτιστοποίησης των συστημάτων επηρεάζοντας την εικόνα του πλοίου στο SCC.	**M**	**M**	**M**

Πίνακας 10.STRIDE - Σύστημα βελτιστοποίησης απόδοσης μηχανών

T	**Συστήματα συντήρησης (Maintenance Interaction Systems)**	I	L	R
S	Στην περίπτωση που ο επιτιθέμενος καταφέρει και προσποιηθεί κάποιον μηχανικό από το SCC, θα αποκτήσει πρόσβαση στο σύστημα και θα είναι σε θέση να παρεμποδίσει το σύστημα από μία αναγκαία λειτουργία συντήρησης.	**H**	**R**	**M**
T	Αλλοιώνοντας τις τιμές του Key Performance Indicator το σύστημα μπορεί να στείλει λανθασμένο μήνυμα για συντήρηση ή μη, οποιουδήποτε συστήματος στο πλοίο.	**H**	**M**	**H**
R	Η αποποίηση της ευθύνης για την εκτέλεση μίας ενέργειας του υποσυστήματος είναι ανεπίτρεπτη, αφού η επικοινωνία με το SCC είναι συνεχής και οι ρόλοι πλήρως καθορισμένοι.	**M**	**R**	**L**
I	Η λειτουργία και η διαχείριση του συγκεκριμένου συστήματος δεν περιλαμβάνει επεξεργασία ευαίσθητων πληροφοριών, επομένως μία διαρροή πληροφορίας δε θα επηρέαζε άμεσα την λειτουργία του.	**L**	**R**	**L**
D	Η διαθεσιμότητα του συγκεκριμένου συστήματος είναι αναγκαία και μία επίθεση που θα διέκοπτε την λειτουργία του για αρκετό χρονικό διάστημα θα μπορούσε να προκαλέσει βλάβη στην υποδομή και οικονομική απώλεια.	**H**	**M**	**H**
E	Η απόκτηση δικαιωμάτων διαχειριστή από έναν κακόβουλο χρήστη θα μπορούσε να προκαλέσει οικονομική ζημία και δυσφήμιση στην επιχείρηση.	**H**	**R**	**M**

Πίνακας 11. STRIDE - Συστήματα συντήρησης

T	**Συστήματα αυτοματοποίησης γέφυρας (Bridge Automation Systems – BAS)**	I	L	R
S	Η περίπτωση που το σύστημα εκτεθεί σε κάποιο malware το οποίο αναγκάζει το σύστημα να αναγνωρίσει τον επιτιθέμενο ως πλοίαρχο, είναι πολύ επικίνδυνη για	**H**	**M**	**H**

	ολόκληρη την υποδομή αλλά και για τον άνθρωπο, καθώς ο επιτιθέμενος θα είναι σε θέση να χειριστεί μηχανήματα και υποσυστήματα του πλοίου ακριβώς όπως ο πλοίαρχος.			
T	Η αλλοίωση των δεδομένων του συγκεκριμένου συστήματος μπορεί να επηρεάσει την ορθή λειτουργία σημαντικών διεργασιών του συστήματος, όπως είναι το σύστημα πλοήγησης, θέτοντας σε κίνδυνο το εμπόρευμα που δύναται να βρίσκεται στο πλοίο ή ακόμα και ολόκληρη την υποδομή.	**H**	**R**	**M**
R	Όπως και στο ASS, η αποποίηση της ευθύνης της εκτέλεσης μίας ενέργειας είναι ανεπίτρεπτη καθώς πρόκειται για κρίσιμη υποδομή, και οι ενέργειές της μπορεί να επηρεάσουν ακόμα και ανθρώπινες ζωές.	**H**	**R**	**M**
I	Η παραβίαση της εμπιστευτικότητας του συγκεκριμένου υποσυστήματος μπορεί να θέσει σοβαρούς κίνδυνους για την ασφάλεια του φορτίου και γενικότερα της υποδομής.	**M**	**M**	**M**
D	Σε συστήματα τα οποία έχουν άμεση σύνδεση με τη σωστή και ασφαλή εκτέλεση των διεργασιών, μία καθυστέρηση των δεδομένων ή απώλεια αυτών είναι ανεπίτρεπτη. Η παραβίαση της διαθεσιμότητας του συγκεκριμένου υποσυστήματος μπορεί να επιφέρει καταστροφικές συνέπειες όπως την απώλεια του φορτίου ή ακόμα και ολόκληρου του πλοίου.	**H**	**M**	**H**
E	Στην περίπτωση που ένας κακόβουλος χρήστης αποκτήσει δικαιώματα διαχειριστή στο συγκεκριμένο υποσύστημα, ταυτόχρονα αποκτά και τον πλήρη έλεγχο ολόκληρου το πλοίου.	**H**	**R**	**M**

Πίνακας 12. STRIDE – Συστήματα αυτοματοποίησης γέφυρας

T	**Συστήματα Πλοήγησης (Navigation Systems)**	I	L	R
S	Ένας κακόβουλος χρήστης μπορεί να προκαλέσει σημαντικές βλάβες στην υποδομή, υποδυόμενος την ταυτότητα κάποιου διαχειριστή του υποσυστήματος. Μπορεί να οδηγήσει το πλοίο στη λήψη λάθος αποφάσεων ή στον υπολογισμό διαφορετικής διαδρομής, προκαλώντας οικονομικές καταστροφές στην επιχείρηση και βλάβες στην υποδομή.	**H**	**M**	**H**
T	Η παραβίαση της ακεραιότητας των πληροφοριών των συστημάτων πλοήγησης μπορεί να προκαλέσει την απώλεια του φορτίου και την καταστροφή ολόκληρης της υποδομής.	**H**	**M**	**H**
R	Η συγκεκριμένη επίθεση είναι ανεπίτρεπτη, καθώς τα άτομα που διαχειρίζονται το συγκεκριμένο σύστημα θα πρέπει να είναι γνωστά.	**H**	**R**	**M**
I	Η αποκάλυψη των πληροφοριών των συστημάτων πλοήγησης θα μπορούσε να οδηγήσει σε κλοπή του εμπορεύματος καθώς και σε καταστροφή της υποδομής. Επίσης, σε αυτή την περίπτωση η εταιρεία θα βρεθεί αντιμέτωπη με τις αντίστοιχες νομικές συνέπειες.	**H**	**M**	**H**
D	Η μη διαθεσιμότητα του υποσυστήματος θα προκαλούσε τη δυσλειτουργία ολόκληρου του πλοίου καθώς θα καθιστούσε ανέφικτη την μετακίνησή του.	**H**	**M**	**H**

E	Εάν ο επιτιθέμενος αποκτήσει πρόσβαση με δικαιώματα διαχειριστή, θα είναι σε θέση να αλλάξει την πορεία του πλοίου και να εκτελέσει ανεπιθύμητες ενέργειες που θα έβλαπταν την ακεραιότητα του φορτίου.	**H**	**R**	**M**

Πίνακας 13. STRIDE - Συστήματα Πλοήγησης

T	**Σύστημα καταγραφής δεδομένων ταξιδιού (Voyage Data Recorder – VDR)**	I	L	R
S	Ένας κακόβουλος χρήστης μπορεί να προκαλέσει παραβίαση της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας του υποσυστήματος. Μπορεί να προκαλέσει νομικές κυρώσεις στην πλοιοκτήτρια εταιρεία, θίγοντας την οικονομική της κατάσταση αλλά και τη φήμη της.	**M**	**M**	**M**
T	Αν υπάρξει αλλοίωση των αποθηκευμένων δεδομένων, μπορεί να υπάρξει οικονομική ζημία και νομικές κυρώσεις.	**M**	**M**	**M**
R	Η άρνηση εκτέλεσης συγκεκριμένων ενεργειών στο συγκεκριμένο σύστημα δεν είναι εφικτή, καθώς η συλλογή των δεδομένων και η αποθήκευσή τους γίνεται με τη βοήθεια των υπόλοιπων υποσυστημάτων που παρέχουν τις συγκεκριμένες πληροφορίες.	**L**	**R**	**L**
I	Τα δεδομένα στο υποσύστημα παρέχουν σημαντικές πληροφορίες για την κατάσταση του εξοπλισμού καθώς και για πολλές διεργασίες οι οποίες εκτελούνται στο πλοίο. Αυτές οι πληροφορίες αποτελούν ευαίσθητα δεδομένα και η αποκάλυψή τους θα μπορούσε να δημιουργήσει προβλήματα στο φορτίο του πλοίου αλλά και σε ολόκληρη την υποδομή.	**H**	**M**	**H**
D	Η μη διαθεσιμότητα του υποσυστήματος δεν θα επιτρέπει την εγγραφή και την αποθήκευση των δεδομένων στη βάση, με αποτέλεσμα, όπως αναφέρθηκε και στην παραβίαση της ακεραιότητας, να προκληθούν νομικές και οικονομικές κυρώσεις.	**M**	**M**	**M**
E	Στην περίπτωση που ο επιτιθέμενος συνδεθεί στο VDR με δικαιώματα διαχειριστή θα είναι σε θέση να τροποποιήσει αλλά και να διαγράψει δεδομένα. Όπως και οι προηγούμενες απειλές, μπορεί να προκαλέσει οικονομική ζημία καθώς και νομικές κυρώσεις.	**H**	**R**	**M**

Πίνακας 14. STRIDE - Σύστημα καταγραφής δεδομένων ταξιδιού

T	**Σύστημα αυτόματης ταυτοποίησης (Automatic Identification System – AIS)**	I	L	R
S	Ο επιτιθέμενος, χρησιμοποιώντας τα κατάλληλα τεχνολογικά μέσα, μπορεί να υποδυθεί την ταυτότητα του ίδιου ή άλλου πλοίου και με αυτό τον τρόπο να λάβει τις πληροφορίες που επιθυμεί.	**M**	**V**	**M**
T	Με την επίθεση αυτή, ο κακόβουλος χρήστης του υποσυστήματος μπορεί να τροποποιήσει ευαίσθητες πληροφορίες που βρίσκονται σε αυτό, όπως είναι η θέση του πλοίου, ο προορισμός του και το φορτίο του, και να αλλοιώσει με αυτό τον τρόπο τη λειτουργία της υποδομής.	**H**	**M**	**H**
R	Επειδή το AIS είναι ένα αυτοματοποιημένο σύστημα και οι εκτέλεση των αντίστοιχων ενεργειών είναι καλά καθορισμένη, μία άρνηση εκτέλεσης κάποιας εντολής είναι	**H**	**V**	**H**

	ανεπίτρεπτη καθώς μπορεί να προκαλέσει απώλεια ανθρώπινης ζωής και οικονομική ζημία.			
I	Όπως τονίστηκε και προηγουμένως, το AIS περιέχει πληροφορίες οι οποίες είναι ευαίσθητες, όπως για παράδειγμα το είδος του φορτίου και ο προορισμός του. Επομένως, η παραβίαση της εμπιστευτικότητας θα μπορούσε να προκαλέσει σημαντικά προβλήματα στην υποδομή.	**H**	**M**	**H**
D	Η μη διαθεσιμότητα του συγκεκριμένου υποσυστήματος θα ήταν καταστροφική για το πλοίο, καθώς το σύστημα είναι υπεύθυνο για την ανταλλαγή και την προβολή πληροφοριών ναυσιπλοΐας, καθώς και άλλων στατικών και δυναμικών πληροφοριών.	**H**	**R**	**M**
E	Στην περίπτωση που ο κακόβουλος χρήστης αποκτήσει δικαιώματα διαχειριστή στο συγκεκριμένο υποσύστημα, θα είναι σε θέση να εκτελέσει μη αναγκαίες ή μη επιθυμητές ενέργειες, όπως είναι η αλλαγή των πληροφοριών ναυσιπλοΐας.	**H**	**M**	**H**

Πίνακας 15. STRIDE - Σύστημα αυτόματης ταυτοποίησης

T	**Σύστημα ηλεκτρονικής απεικόνισης χαρτών και πληροφοριών (Electronic Chart Display and Information System – ECDIS)**	I	L	R
S	Ο κακόβουλος χρήστης, χρησιμοποιώντας τα συνθηματικά του νόμιμου χρήστη μπορεί να προκαλέσει σοβαρά προβλήματα στο συγκεκριμένο υποσύστημα. Μία λάθος εντολή ή η καταστροφή ενός εκ των οργάνων που είναι συνδεδεμένα σε αυτό, θα μπορούσαν να είναι ολέθρια. Αποτελεί πύλη εξόδου στο διαδίκτυο.	**H**	**M**	**H**
T	Η τροποποίηση των δεδομένων του συγκεκριμένου υποσυστήματος επίσης μπορεί να οδηγήσει σε καταστροφικές συνέπειες, όπως η μεταβολή της πορείας του, τροποποιώντας τους αντίστοιχους χάρτες.	**M**	**M**	**M**
R	Οι ενέργειες που εκτελούνται στο συγκεκριμένο υποσύστημα θα πρέπει να είναι ορθά κατανεμημένες σε συγκεκριμένα και γνωστά πρόσωπα. Η αποποίηση της ευθύνης εκτέλεσης οποιαδήποτε ενέργειας είναι ανεπίτρεπτη.	**M**	**M**	**M**
I	Λόγω της διασύνδεσής του με πολλά άλλα υποσυστήματα του πλοίου, περιέχει πληροφορίες σημαντικές για το φορτίο αλλά και για τον πλοιοκτήτη, όπως είναι η ακριβής τοποθεσία του και η διαδρομή που θα εκτελέσει. Η διαρροή λοιπόν πληροφοριών από το συγκεκριμένο υποσύστημα θα μπορούσε να επιφέρει καταστροφικές συνέπειες.	**H**	**M**	**H**
D	Η παραβίαση της διαθεσιμότητας του υποσυστήματος είναι ανεπίτρεπτη, καθώς καθιστά το πλοίο αδύνατον να πλεύσει.	**H**	**M**	**H**
E	Η απόκτηση δικαιωμάτων διαχειριστή του υποσυστήματος θα μπορούσε να προκαλέσει την εκτέλεση ανεπιθύμητων εντολών, όπως την τροποποίηση των χαρτών πλεύσης, που έχει ως αποτέλεσμα οικονομικό κόστος αλλά και απώλεια φήμης.	**M**	**R**	**L**

Πίνακας 16. STRIDE - Σύστημα ηλεκτρονικής απεικόνισης χαρτών και πληροφοριών

T	Συστήματα προηγμένων αισθητήρων (Advanced Sensor System – ASS)	I	L	R
S	Αν ο επιτιθέμενος αποκτήσει πρόσβαση στο συγκεκριμένο σύστημα μέσω ενός malware το οποίο θα αναγκάζει το σύστημα να τον αναγνωρίζει σαν διαχειριστή, θα είναι πολύ εύκολο να παρακάμψει τους συναγερμούς προειδοποίησης και να προκαλέσει καταστροφές στις υποδομές καθώς και οικονομικό κόστος.	**H**	**M**	**H**
T	Αν τα δεδομένα αλλοιωθούν μπορεί να προκληθεί δυσλειτουργία στο σύστημα, η οποία θα έχει ενδεχομένως ως αποτέλεσμα την σύγκρουση με άλλο πλοίο ή ακόμα και την απώλεια ανθρώπινης ζωής.	**H**	**R**	**M**
R	Η απόρριψη της δημιουργίας μη έγκυρων συμβάντων είναι σημαντικό πρόβλημα, καθώς μπορεί να κοστίσει ανθρώπινες ζωές και οικονομική ζημία. Το συγκεκριμένο υποσύστημα δεν είναι πάντα εκτεθειμένο στο διαδίκτυο και ο επιτιθέμενος θα πρέπει να έχει κίνητρο.	**H**	**R**	**M**
I	Η γνώση της αρχιτεκτονικής των αισθητήρων και των δεδομένων τους θα μπορούσε να δημιουργήσει προβλήματα στην ομαλή λειτουργία του πλοίου, καθώς σημαντικό βήμα πριν από κάποια επίθεση, είναι η μελέτη της αρχιτεκτονικής με στόχο την εύρεση ευπαθειών σε αυτή.	**M**	**M**	**M**
D	Η διακοπή της λειτουργίας του συστήματος είναι καταστροφική για το πλοίο, καθώς με μία DoS επίθεση δε θα είναι σε θέση να ελέγχει το περιβάλλον του και τις διεργασίες που πραγματοποιούνται, προκαλώντας οικονομική ζημία και βλάβη στην υποδομή.	**H**	**M**	**H**
E	Στην περίπτωση που ο επιτιθέμενος αποκτήσει πρόσβαση με δικαιώματα διαχειριστή στο ASS, θα μπορούσε να καταστρέψει όλο το σύστημα.	**H**	**R**	**M**

Πίνακας 17. STRIDE - Συστήματα προηγμένων αισθητήρων (ASS)

T	Σύστημα αυτόματου ελέγχου πλοίου (Autonomous Ship Controller – ASC)	I	L	R
S	Η προσβολή του συγκεκριμένου υποσυστήματος από κάποιο malware θα μπορούσε να οδηγήσει σε βλάβη στα συστήματα διαχείρισης φορτίου ή στο GMDSS, επηρεάζοντας τις επικοινωνίες του.	**H**	**M**	**H**
T	Η τροποποίηση αρχείων και δεδομένων που επηρεάζουν τη διεκπεραίωση των διεργασιών του συγκεκριμένου συστήματος θα ήταν καταστροφική για την υποδομή, διότι μία μικρή αλλαγή στις τιμές των μηχανών του πλοίου θα μπορούσε να του αλλάξει πορεία ή ακόμα και να το βυθίσει.	**H**	**R**	**M**
R	Το συγκεκριμένο υποσύστημα διαχειρίζεται ζωτικής σημασίας υποσυστήματα. Για τον λόγο αυτό όλες οι ενέργειες που πραγματοποιούνται θα πρέπει να ανατίθενται σε ένα άτομο, καθώς η μη αποδοχή της εκτέλεσής τους είναι ανεπίτρεπτη.	**M**	**R**	**L**
I	Η παραβίαση της αρχής της εμπιστευτικότητας μπορεί να προκαλέσει σοβαρά προβλήματα, καθώς πληροφορίες όπως ο προορισμός του πλοίου μπορεί να είναι ευαίσθητες και έτσι να τεθεί σε κίνδυνο το φορτίο.	**M**	**R**	**L**
D	Από τα προηγούμενα είναι κατανοητό ότι η μη διαθεσιμότητα του συγκεκριμένου υποσυστήματος είναι ανεπίτρεπτη, εφόσον χωρίς αυτό το πλοίο δεν θα είναι σε θέση να κινηθεί.	**H**	**M**	**H**

E	Στην περίπτωση που κάποιος κακόβουλος χρήστης αποκτήσει δικαιώματα διαχειριστή στο συγκεκριμένο υποσύστημα, θα μπορέσει να ρυθμίσει πολλές παραμέτρους του συστήματος, οι οποίες επηρεάζουν ολόκληρη την λειτουργία του. Μία τέτοια ενέργεια είναι ανεπίτρεπτη καθώς θα μπορούσε να επιφέρει ολέθριες συνέπειες για ολόκληρη την υποδομή.	**H**	**R**	**M**

Πίνακας 18. STRIDE - Σύστημα αυτόματου ελέγχου πλοίου

T	**Σύστημα Ναυτιλιακού Κινδύνου Ασφάλειας (Global Maritime Distress and Safety System – GMDSS)**	I	L	R
S	Ο επιτιθέμενος δύναται να προσποιηθεί ότι είναι ένα άλλο πλοίο το οποίο εκπέμπει συναγερμό, με στόχο την προσέλκυση του πλοίου-στόχου. Κάτι τέτοιο μπορεί να θέσει σε κίνδυνο το πλοίο και το φορτίο του και να επιφέρει οικονομικές καταστροφές και ανθρώπινες απώλειες.	**H**	**M**	**H**
T	Η παραβίαση της ακεραιότητας των δεδομένων του υποσυστήματος είναι εξίσου σημαντική, καθώς δεδομένα όπως είναι οι καιρικές συνθήκες ή οι θέσεις άλλων πλοίων επηρεάζουν άμεσα τις λειτουργίες του πλοίου και μπορούν να προκαλέσουν οικονομικές καταστροφές και απώλεια ανθρώπινης ζωής.	**H**	**M**	**H**
R	Η εκτέλεση πολλών από τις εντολές του συγκεκριμένου υποσυστήματος μπορεί να βλάψει το ίδιο το πλοίο αλλά και το περιβάλλον του. Πρέπει λοιπόν να υπάρχει σαφής διαχωρισμός των εκτελούντων τις διεργασίες.	**M**	**M**	**M**
I	Το υποσύστημα είναι υπεύθυνο για τη μετάδοση πληροφοριών ασφάλειας μεταξύ των πλοίων και των σταθμών ελέγχου ξηράς. Μία παραβίαση της εμπιστευτικότητας αυτών θα μπορούσε να προκαλέσει σοβαρά προβλήματα σε ολόκληρη την υποδομή.	**H**	**M**	**H**
D	Η διακοπή της λειτουργίας του GMDSS θα έθετε σε κίνδυνο ολόκληρη την υποδομή, καθώς μέσω αυτού πραγματοποιούνται οι επικοινωνίες μεταξύ των οντοτήτων με τις οποίες αλληλεπιδρά το πλοίο σε μία κατάσταση ανάγκης.	**H**	**R**	**M**
E	Στην περίπτωση που ο επιτιθέμενος αποκτήσει υψηλά δικαιώματα στο GMDSS, θα είναι σε θέση να ενεργοποιεί και να απενεργοποιεί τους συναγερμούς αλλά και τις επικοινωνίες εντός και εκτός του πλοίου.	**H**	**R**	**M**

Πίνακας 19. STRIDE - Σύστημα Ναυτιλιακού Κινδύνου Ασφάλειας

T	**Συστήματα διαχείρισης φορτίου (Cargo Management Systems - CCR)**	I	L	R
S	Ο κακόβουλος χρήστης, προσποιούμενος την ταυτότητα του πλοιοκτήτη, μπορεί να παρακολουθήσει το εμπόρευμα και να αντλήσει ευαίσθητα δεδομένα όπως το είδος, την τοποθεσία και την ποσότητα αυτού.	**H**	**R**	**M**
T	Μία αλλοίωση στην κάμερα μπορεί να προκαλέσει απώλεια του φορτίου και να οδηγήσει σε οικονομική καταστροφή.	**M**	**M**	**M**
R	Η μη αποδοχή εκτέλεσης συγκεκριμένων εντολών του υποσυστήματος δεν είναι επιτρεπτή, καθώς συγκεκριμένη ομάδα ατόμων είναι υπεύθυνη για την επίβλεψη και τη χρήση του υποσυστήματος.	**H**	**R**	**M**

I	Η παραβίαση της εμπιστευτικότητας του υποσυστήματος μπορεί να οδηγήσει σε νομικές και οικονομικές κυρώσεις καθώς πρόκειται για ευαίσθητα δεδομένα.	**M**	**R**	**M**
D	Η μη διαθεσιμότητα του υποσυστήματος είναι μη επιτρεπτή, καθώς μπορεί να οδηγήσει σε απώλεια του φορτίου και συνεπώς σε οικονομικές και νομικές κυρώσεις.	**H**	**M**	**H**
E	Στην περίπτωση που ο επιτιθέμενος συνδεθεί στο σύστημα με υψηλά δικαιώματα, θα είναι σε θέση να χειριστεί της κάμερες και το υλικό δημιουργώντας σοβαρό πρόβλημα στην υποδομή και στον πλοιοκτήτη.	**H**	**R**	**M**

Πίνακας 20. STRIDE - Συστήματα διαχείρισης φορτίου

T	**Συστήματα ελέγχου εισόδου (Access control)**	I	L	R
S	Ο επιτιθέμενος θα μπορούσε να προσποιηθεί ότι είναι το σύστημα BNWAS και να στέλνει μήνυμα στο SCC ότι το πλοίο δεν είναι ακυβέρνητο, οδηγώντας το με αυτό τον τρόπο εκτός πορείας. Αυτό θα έβλαπτε οικονομικά αλλά και ηθικά τον οργανισμό.	**M**	**R**	**L**
T	Στην περίπτωση που χαθεί η ακεραιότητα του συστήματος, το SCC δύναται να χάσει εικόνα από το πλοίο αφού θα έχουν αλλοιωθεί συστήματα όπως CCTV και BNWAS.	**M**	**M**	**M**
R	Μία επίθεση στα log αρχεία του συστήματος διαγράφοντας όλες τις εισαγωγές θα δημιουργούσε σοβαρό πρόβλημα ελέγχου του πλοίου, προκαλώντας οικονομικές ζημιές και βλάβες στην υποδομή.	**M**	**M**	**M**
I	Η διαρροή πληροφοριών από το σύστημα CCTV θα έθετε σε κίνδυνο τα στοιχεία των πελατών και ευαίσθητα δεδομένα, κάτι που θα προκαλούσε δυσφήμιση στην επιχείρηση αλλά και νομικές κυρώσεις.	**H**	**M**	**H**
D	Η μη διαθεσιμότητα του συστήματος ελέγχου εισόδου θα προκαλούσε οικονομική ζημία, ακόμα και απώλεια φορτίου και της υποδομής.	**M**	**M**	**M**
E	Εκμεταλλευόμενος ο επιτιθέμενος κάποια ευπάθεια αυθεντικοποίησης και αποκτώντας δικαιώματα διαχειριστή, θα είναι σε θέση να καταστρέψει την υποδομή και να φέρει την εταιρεία έναντι νομικών κυρώσεων.	**H**	**M**	**H**

Πίνακας 21. STRIDE - Συστήματα ελέγχου εισόδου

T	**Συστήματα εξυπηρέτησης και διαχείρισης επιβατών (Passenger Servicing and Management Systems- PSMS)**	I	L	R
S	Ο επιτιθέμενος μπορεί να προσποιηθεί ότι είναι επιβάτης του πλοίου και να αποκτήσει φυσική πρόσβαση σε πολλά συστήματα του πλοίου.	**M**	**M**	**M**
T	Η αλλοίωση των δεδομένων του συστήματος θα δημιουργούσε οργανωτικά προβλήματα προκαλώντας βλάβη στην υποδομή.	**M**	**M**	**M**

R	Η αποποίηση της ευθύνης εκτέλεσης μίας λειτουργίας του συστήματος είναι ανεπίτρεπτη και θα έθετε σε κίνδυνο την υποδομή και τις λειτουργίες της.	**L**	**R**	**L**
I	Η διαρροή πληροφοριών θα δημιουργούσε σημαντικές νομικές κυρώσεις στην εταιρεία, καθώς τα δεδομένα που ανταλλάσσονται στο σύστημα είναι ευαίσθητα.	**H**	**M**	**H**
D	Η διακοπή της λειτουργίας των συστημάτων θα προκαλούσε καθυστερήσεις στις λειτουργίες του πλοίου και θα επηρέαζε τα δεδομένα που συγκεντρώνει και αποστέλλει στο SCC.	**L**	**M**	**L**
E	Στην περίπτωση όπου ο επιτιθέμενος αποκτήσει πρόσβαση με υψηλά δικαιώματα, θα έχει πρόσβαση σε όλα τα στοιχεία των επιβατών και των πελατών, προκαλώντας δυσφήμιση στην εταιρεία αλλά και νομικές κυρώσεις.	**H**	**R**	**M**

Πίνακας 22. STRIDE - Συστήματα εξυπηρέτησης και διαχείρισης επιβατών

T	**Κέντρο ελέγχου ξηράς (Shore Control Center – SCC)**	I	L	R
S	Στην περίπτωση που ένας κακόβουλος χρήστης αποκτήσει τα συνθηματικά ενός νόμιμου χρήστη του συστήματος θα είναι σε θέση να εκτελέσει οποιαδήποτε εντολή απομακρυσμένα και να ελέγξει το πλοίο. Αυτό θα ήταν καταστροφικό για το φορτίο, το πλοίο, και θα έθετε σε κίνδυνο ακόμα και ανθρώπινες ζωές.	**H**	**M**	**H**
T	Η αλλοίωση των δεδομένων που προέρχονται από το συγκεκριμένο υποσύστημα είναι επίσης σημαντικό πρόβλημα και θα μπορούσε να προκαλέσει την κατάρρευση ολόκληρου του συστήματος. Η αλλαγή των δεδομένων πλοήγησης, για παράδειγμα, θα είχε ως αποτέλεσμα την μεταβάσή του πλοίου σε διαφορετική τοποθεσία από τον αρχικό προορισμό.	**H**	**R**	**M**
R	Οι συνέπειες που μπορεί να επιφέρει η αποποίηση της ευθύνης για την εκτέλεση των διεργασιών του συγκεκριμένου υποσυστήματος είναι ανεπίτρεπτες, καθώς το άτομο που είναι υπεύθυνο για αυτές θα πρέπει να είναι γνωστό.	**H**	**R**	**M**
I	Τα δεδομένα που διαχειρίζεται το SCC είναι εξίσου σημαντικά με αυτά του BAS και η παραβίαση της εμπιστευτικότητάς τους θα μπορούσε να θέσει σε κίνδυνο το φορτίο του πλοίου και να επιφέρει οικονομική καταστροφή.	**H**	**M**	**H**
D	Η παραβίαση της διαθεσιμότητας μπορεί να προκαλέσει απώλεια της επίβλεψης του πλοίου καθώς και σημαντικών μετρήσεών του που συμβάλλουν στην ορθή λειτουργία του. Το συγκεκριμένο υποσύστημα λειτουργεί σε πραγματικό χρόνο και έτσι οι καταστροφές που μπορούν να προκληθούν από τη μη διαθεσιμότητα είναι σοβαρές.	**H**	**R**	**M**
E	Αυτή η απειλή μπορεί να προκαλέσει παραβίαση της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας του συγκεκριμένου υποσυστήματος.	**H**	**R**	**M**

Πίνακας 23. STRIDE - Κέντρο ελέγχου ξηράς

T	**Σύστημα διεπαφής πλοίου με ξηρά (Human Machine Interface – HMI)**	I	L	R
S	Χρησιμοποιώντας τους κωδικούς ενός νόμιμου χρήστη, ο επιτιθέμενος μπορεί να εισέλθει στο σύστημα και να τροποποιήσει τους χάρτες πλοήγησης με σκοπό να κατευθύνει το πλοίο σε άλλο προορισμό. Με αυτό τον τρόπο θα έθετε σε κίνδυνο την υποδομή, θα προκαλούσε δυσφήμιση στην εταιρεία και πιθανά νομικές κυρώσεις.	**H**	**M**	**H**
T	Η αλλοίωση των δεδομένων στο σύστημα θα ήταν καταστροφική για την υποδομή, καθώς μέσω του συστήματος ενημερώνεται ο ανθρώπινος παράγοντας για την κατάσταση του πλοίου, για να εκτελέσει στην συνέχεια τις απαραίτητες εντολές.	**H**	**M**	**H**
R	Η αποποίηση εκτέλεσης συγκεκριμένης ενέργειας στο σύστημα είναι ανεπίτρεπτη, καθώς είναι σαφώς καθορισμένη να λαμβάνει εντολές από συγκεκριμένα συστήματα.	**M**	**R**	**L**
I	Η αποκάλυψη των πληροφοριών που ενδέχεται να εμπεριέχει το σύστημα θα έθετε σε κίνδυνο το πλοίο και θα προκαλούσε δυσλειτουργία σε όλα τα συστήματά του, καθώς μέσω του συστήματος αυτού ανταλλάσσονται όλες οι πληροφορίες πλοήγησης και διαχείρισης της υποδομής.	**H**	**M**	**H**
D	Η μη διαθεσιμότητα του συστήματος θα ήταν ολέθρια για την υποδομή και θα προκαλούσε δυσφήμιση στην πλοιοκτήτρια εταιρεία.	**H**	**M**	**H**
E	Εάν ο επιτιθέμενος αποκτήσει πρόσβαση με αυξημένα δικαιώματα, θα είναι σε θέση να διαβάσει όλες τις ευαίσθητες πληροφορίες για την κατάσταση του πλοίου καθώς και στοιχεία πελατών. Μία κατάσταση σαν αυτή θα επέφερε νομικές κυρώσεις στην εταιρεία.	**H**	**M**	**H**

Πίνακας 24. STRIDE - Σύστημα διεπαφής πλοίου με ξηρά

T	**Σύστημα απομακρυσμένου ελέγχου και υποστήριξης πλοίου (Remote Maneuvering Support System – RMSS)**	I	L	R
S	Ο επιτιθέμενος δύναται να προσποιηθεί, μέσω ενός malware, ότι είναι το σύστημα ελέγχου μηχανών και να αποστέλλει λανθασμένα στοιχεία στο SCC και να επηρεάζει τον χειρισμό του πλοίου. Αυτό θα προκαλούσε δυσλειτουργία σε αρκετά υποσυστήματα του πλοίου.	**M**	**M**	**M**
T	Η αλλοίωση των δεδομένων που ανταλλάσσονται μέσω του συστήματος είναι ιδιαίτερα σοβαρή καθώς τα δεδομένα αυτά επηρεάζουν απόλυτα τον χειρισμό των μηχανών του πλοίου. Η αποστολή αλλοιωμένων δεδομένων θα προκαλούσε βλάβη σε υποσυστήματα της υποδομής.	**M**	**M**	**M**
R	Η εκτέλεση των αντίστοιχων ενεργειών είναι εξίσου σημαντική και είναι ανεπίτρεπτο να αποποιηθεί οποιοσδήποτε την ευθύνη για την εκτέλεσή τους, καθώς είναι πλήρως καθορισμένοι οι ρόλοι που συμμετέχουν σε αυτό το αυτοματοποιημένο σύστημα.	**M**	**R**	**L**
I	Η διαρροή πληροφοριών των εντολών πλοήγησης θα αποκάλυπτε τον προορισμό του πλοίου, αλλά δεν θα προκαλούσε δυσλειτουργία στα συστήματά του.	**H**	**M**	**H**

D	Η επίθεση με στόχο τη διαθεσιμότητα του συστήματος θα επηρέαζε άμεσα την υποδομή και θα προκαλούσε καθυστέρηση στην εκτέλεση πολλών διεργασιών στο καράβι.	**M**	**M**	**M**
E	Η σύνδεση στο σύστημα με αυξημένα δικαιώματα θα προκαλούσε σημαντικά προβλήματα στην υποδομή, καθώς ο επιτιθέμενος θα είναι σε θέση να δώσει κρίσιμες εντολές στο σύστημα μηχανών, επηρεάζοντας άμεσα τη λειτουργία του.	**H**	**R**	**M**

Πίνακας 25. STRIDE - Σύστημα απομακρυσμένου ελέγχου και υποστήριξης πλοίου

4.3 Εξαγωγή αποτελεσμάτων

Στη συγκεκριμένη εργασία επικεντρωθήκαμε στη λεπτομερή ανάλυση των έξι απειλών που προτείνει η μέθοδος STRIDE για κάθε ένα από τα υποσυστήματα του πλοίου. Στη συνέχεια, υπολογίσαμε τον αντίκτυπο και τη πιθανότητα της εκάστοτε απειλής για να καταφέρουμε στο τέλος να πραγματοποιήσουμε την εκτίμηση κινδύνου. Ακολουθώντας τα επίπεδα του δέντρου της αρχιτεκτονικής όπως παρατηρείται στην εικόνα 6 του δεύτερου κεφαλαίου, από το χαμηλότερο (επίπεδο 3) στο υψηλότερο (επίπεδο 1) καταλήξαμε στα παρακάτω αποτελέσματα.

Στο επίπεδο τρία του δέντρου παρατηρείται μια αυξημένη επικινδυνότητα στα επιμέρους υποσυστήματα. Αρχικά, τα υποσυστήματα αυτόνομου χειρισμού και ελέγχου των μηχανών (AEMC) παρουσίασαν ποικιλομορφία στα αποτελέσματα των πινάκων, με το σύστημα καταγραφής των μηχανών (EDL) να εμφανίζει τον υψηλότερο κίνδυνο. Αναλυτικότερα, το σύστημα EDL εμφανίζει υψηλή επικινδυνότητα σε τρεις απειλές της μεθόδου STRIDE οι οποίες είναι η προσποίηση ταυτότητας (S), η αλλοίωση των δεδομένων (T) και η άρνηση υπηρεσίας (D). Μέτριας επικινδυνότητας για το σύστημα αποτελούν οι απειλές της αποποίησης της ευθύνης για την εκτέλεση μίας ενέργειας (R) και της αναβάθμισης προνομίων (E), ενώ χαμηλής επικινδυνότητας είναι η απειλή της διαρροής πληροφορίας (I). Συνεχίζοντας στο σύστημα αυτόματου ελέγχου των μηχανών (ACER), τα αποτελέσματα παρουσίασαν παρόμοια κατανομή, με υψηλού κινδύνου να αποτελεί η απειλή προσποίησης ταυτότητας (S), δημιουργώντας σοβαρές βλάβες στην υποδομή στην περίπτωση εμφάνισης της επίθεσης σύμφωνα με τον πίνακα 8. Μέτρια επικινδυνότητα εμφανίζουν οι απειλές αλλοίωσης των δεδομένων (T), άρνησης υπηρεσίας (D) και αναβάθμισης προνομίων (E) και ως χαμηλού επιπέδου χαρακτηρίστηκαν οι απειλές αποποίησης ευθύνης (R) και διαρροή πληροφοριών (I), αφού το σύστημα δεν διαχειρίζεται ευαίσθητες πληροφορίες. Το σύστημα διαχείρισης εκτάκτων περιστατικών παρουσίασε μία απειλή υψηλού κινδύνου, αυτή της άρνησης υπηρεσιών (D), καθώς η διακοπή της λειτουργίας του θα καθιστούσε αδύνατη την αντιμετώπιση κάποιου έκτακτου περιστατικού που θα έθετε σε κίνδυνο ολόκληρη την υποδομή. Το ίδιο σύστημα εμφάνισε τρείς απειλές μέτριου κινδύνου και δύο χαμηλού, με αυτές να είναι η προσποίηση ταυτότητας (S), η αναβάθμιση προνομίων (E), η αποποίηση ευθύνης για την εκτέλεση μία ενέργειας (R) και η διαρροή πληροφοριών (I) αντίστοιχα.

Συνεχίζοντας στο ίδιο επίπεδο, ενδιαφέροντα αποτελέσματα παράχθηκαν για τα υποσυστήματα της πλοήγησης, με το σύστημα αυτόματης αναγνώρισης (AIS) να παρουσιάζει τη μεγαλύτερη επικινδυνότητα. Το σύστημα καταγραφής δεδομένων ταξιδιού (VDR) φαίνεται να παρουσιάζει μία απειλή υψηλού κινδύνου, αυτή της διαρροής πληροφοριών (I) και οι απειλές προσποίησης ταυτότητας (S), αλλοίωσης δεδομένων (T), άρνησης υπηρεσιών (D) και αναβάθμισης προνομίων (E) να εμφανίζουν

μέτριο επίπεδο κινδύνου. Η απειλή της αποποίησης ευθύνης (R) αναγνωρίστηκε ως χαμηλού κινδύνου, αφού το συγκεκριμένο σύστημα δεν εκτελεί πολλές διεργασίες πέραν της καταγραφής δεδομένων. Το σύστημα αυτόματης αναγνώρισης (AIS) από την άλλη παρουσίασε ενδιαφέροντα αποτελέσματα αφού εμφάνισε υψηλή επικινδυνότητα σε τέσσερις απειλές της STRIDE. Πιο αναλυτικά, οι απειλές αλλοίωσης δεδομένων (T), αποποίησης ευθύνης (R), διαρροής πληροφοριών (I), και αναβάθμισης προνομίων (E) χαρακτηρίστηκαν ως υψηλού κινδύνου λαμβάνοντας υπόψιν τις αντίστοιχες επιθέσεις του πίνακα 15 και οι απειλές προσποίησης ταυτότητας (S) και άρνησης υπηρεσιών (D) ως μέτριας επικινδυνότητας. Επιπλέον, για το σύστημα ηλεκτρονικής απεικόνισης χαρτών και πληροφοριών (ECDIS), τρείς απειλές χαρακτηρίστηκαν ως υψηλού κινδύνου, αυτές της προσποίησης ταυτότητας (S), διαρροής πληροφοριών (I), και άρνησης υπηρεσιών (D), δύο ως μέτριου κινδύνου, αυτές της αλλοίωσης δεδομένων (T) και αποποίησης ευθύνης (R) και μία χαμηλού, η οποία αφορούσε την απειλή της αναβάθμισης προνομίων (E) που σύμφωνα με την επίθεση που περιγράφεται στον πίνακα 16 δεν προκαλεί σημαντικό αντίκτυπο στην υποδομή. Το σύστημα προηγμένων αισθητήρων (ASS), το οποίο είναι ένα νέο σύστημα, χαρακτηριστικό της αρχιτεκτονικής του MUNIN [32], παρουσίασε δύο απειλές υψηλού κινδύνου, αυτή της προσποίησης ταυτότητας (S) και αυτή της άρνησης υπηρεσιών (D). Σημαντικές είναι και οι απειλές του συστήματος για τις οποίες ο κίνδυνος υπολογίστηκε ως μέτριου επιπέδου: η επίθεση αλλοίωσης δεδομένων (T), αποποίησης της ευθύνης (R), αναβάθμισης προνομίων (E), και της διαρροής πληροφοριών (I).

Στο ίδιο επίπεδο με τα προηγούμενα συστήματα είναι τοποθετημένα και τα υποσυστήματα του Αυτόνομου ελέγχου του πλοίου (ASC). Αναλύοντας το Σύστημα Ναυτιλιακού Κινδύνου και Ασφάλειας (GMDSS), το οποίο αποτελεί ένα διαχρονικό σύστημα πλοίων, παρουσιάστηκαν τρείς απειλές υψηλού κινδύνου: η προσποίηση της ταυτότητας (S), η αλλοίωση των δεδομένων (T) και η διαρροή πληροφοριών (I). Λαμβάνοντας υπόψη τις επιθέσεις του πίνακα 19, ως μέτριας επικινδυνότητας χαρακτηρίστηκαν οι απειλές αποποίησης της ευθύνης (R), άρνησης υπηρεσιών (D) και αναβάθμιση προνομίων (E). Σημαντικό υποσύστημα αποτελεί αυτό της διαχείρισης φορτίου, το οποίο παρουσίασε μία μόνο επίθεση υψηλού κινδύνου και πέντε μέτριου: η άρνηση υπηρεσιών (D) και η προσποίηση ταυτότητας (S), η αλλοίωση δεδομένων (T), η αποποίηση ευθύνης (R), η διαρροή πληροφοριών (I), και η αναβάθμιση προνομίων (E) αντίστοιχα. Το σύστημα ελέγχου εισόδου, το οποίο αποτελεί σημαντικό παράγοντα για την ενίσχυση της ασφάλειας του πλοίου, παρουσίασε δύο απειλές υψηλού κινδύνου σύμφωνα με τη μέθοδο STRIDE, αυτές της διαρροής πληροφοριών (I) και της αναβάθμισης προνομίων (E). Επίσης, σύμφωνα με τον αντίστοιχο πίνακα, τρείς απειλές χαρακτηρίστηκαν ως μέτριου κινδύνου: η αλλοίωση δεδομένων (T), η αποποίηση ευθύνης (R) και η άρνηση υπηρεσίας (D), και μία ως χαμηλού: η προσποίηση ταυτότητας (S). Το τελευταίο υποσύστημα του επιπέδου τρία είναι το σύστημα εξυπηρέτησης και διαχείρισης επιβατών. Αυτό παρουσίασε, σύμφωνα με τον πίνακα 22, μία απειλή υψηλού κινδύνου, αυτή της διαρροής πληροφοριών (I) καθώς είναι ένα σύστημα το οποίο εμπεριέχει ευαίσθητα δεδομένα. Επίσης, οι απειλές προσποίησης ταυτότητας (S), αλλοίωσης δεδομένων (T) και αναβάθμισης προνομίων (E) χαρακτηρίστηκαν ως μέτριου κινδύνου. Τέλος, οι απειλές αποποίησης εκτέλεσης μίας ενέργειας (R) και η άρνηση υπηρεσιών (D) υπολογίστηκαν ως χαμηλής επικινδυνότητας.

Στο δεύτερο επίπεδο του δέντρου της αρχιτεκτονικής του σχήματος 6 στο δεύτερο κεφάλαιο, η ανάλυση έδειξε μία διασπορά των επιπέδων του κινδύνου, με τα περισσότερο ευάλωτα στις απειλές της STRIDE συστήματα να βρίσκονται στο σύστημα αλληλεπίδρασης με το κέντρο ελέγχου (HMI). Στα συστήματα

του EAS, το υποσύστημα του αυτόματου ελέγχου και παρακολούθησης των μηχανών (AEMC) παρουσιάζονται δύο απειλές υψηλού κινδύνου: η αλλοίωση δεδομένων (T) και η άρνηση υπηρεσιών (D). Συνεχίζοντας στο ίδιο υποσύστημα, οι απειλές προσποίησης ταυτότητας (S), αποποίησης ευθύνης (R) και αναβάθμισης προνομίων (E), υπολογίστηκαν ως μέτριου κινδύνου και η απειλή της διαρροής πληροφοριών (I) όπως παρουσιάζεται και στον πίνακα 6, υπολογίστηκε ως χαμηλού κινδύνου. Το σύστημα βελτιστοποίησης μηχανών (Engine efficient system) παρουσίασε μία απειλή υψηλού κινδύνου την αλλοίωση δεδομένων (T). Οι απειλές προσποίησης ταυτότητας (S), αποποίησης ευθύνης (R), άρνησης υπηρεσιών (D) και αναβάθμισης προνομίων (E) αναγνωρίστηκαν ως μέτριου κινδύνου, ενώ η απειλή της διαρροής πληροφοριών (I) ως χαμηλού, αφού σύμφωνα με τον πίνακα 10, η επίθεση δεν προκάλεσε σημαντικές βλάβες στην υποδομή. Αναλύοντας τον επόμενο κόμβο του δέντρου, ο οποίος είναι το σύστημα συντήρησης (Maintenance Interaction), παρουσιάστηκαν δύο απειλές υψηλού κινδύνου σύμφωνα με τη μεθοδολογία της STRIDE στον πίνακα 11, οι οποίες είναι η αλλοίωση δεδομένων (T) και η άρνηση υπηρεσιών (D). Οι απειλές της προσποίησης ταυτότητας (S) και της απόκτησης αναβαθμισμένων προνομίων (E) χαρακτηρίστηκαν ως μέτριου κινδύνου ενώ οι απειλές αποποίησης ευθύνης (R) και διαρροής πληροφοριών (I) χαρακτηρίστηκαν χαμηλής επικινδυνότητας.

Στα υποσυστήματα των συστημάτων της γέφυρας του πλοίου (BAS), το υποσύστημα της πλοήγησης παρουσίασε τη μεγαλύτερη επικινδυνότητα. Αναλυτικότερα, το σύστημα πλοήγησης (Navigation) παρουσίασε σε τέσσερις απειλές της μεθοδολογίας υψηλή επικινδυνότητα. Η προσποίηση της ταυτότητας (S), η αλλοίωση των δεδομένων (T), η διαρροή των πληροφοριών (I) και η άρνηση υπηρεσίας χαρακτηρίστηκαν ως οι περισσότερο επικίνδυνες σύμφωνα με τον πίνακα 13. Οι απειλές της αποποίησης ευθύνης (R) και της αναβάθμισης προνομίων (E) χαρακτηρίστηκαν ως χαμηλής επικινδυνότητας. Σε αντίθεση με την επικινδυνότητα του συστήματος πλοήγησης, το σύστημα αυτόματου ελέγχου του πλοίου (ASC) παρουσίασε μία περισσότερο κατανεμημένη μορφή επικινδυνότητας καθώς, από τον πίνακα 18 διαφαίνονται δύο απειλές υψηλού κινδύνου, δύο μετρίου και δύο χαμηλού. Πιο αναλυτικά, οι απειλές προσποίησης της ταυτότητας (S) και άρνησης υπηρεσίας χαρακτηρίστηκαν ως υψηλού κινδύνου, οι απειλές αλλοίωσης δεδομένων (T) και αναβάθμισής προνομίων ως μέτριου και οι απειλές αποποίησης της ευθύνης (R) και διαρροή πληροφοριών (I) ως χαμηλού.

Συνεχίζοντας την ανάλυση στο ίδιο επίπεδο, ενδιαφέρον παρουσιάζουν τα αποτελέσματα των πινάκων 24,25 των υποσυστημάτων του κέντρου ελέγχου του πλοίου (SCC). Πιο συγκεκριμένα, το σύστημα διεπαφής του πλοίου με τη ξηρά (HMI) εμφανίζει μεγάλη επικινδυνότητα στις απειλές προσποίησης ταυτότητας (S), αλλοίωσης δεδομένων (T), διαρροής πληροφοριών (I) και άρνησης υπηρεσίας (D). Η λειτουργία του είναι ιδιαίτερα κρίσιμη για την ασφάλεια της υποδομής. Χαμηλού κινδύνου χαρακτηρίστηκε η απειλή της αποποίησης ευθυνών (R) καθώς σύμφωνα με τον πίνακα 24 ο επιτιθέμενος είναι σπάνιο να εφαρμόσει τη συγκεκριμένη επίθεση λόγω έλλειψης γνώσεων των ρόλων της υποδομής. Το τελευταίο σύστημα του συγκεκριμένου επιπέδου είναι το σύστημα απομακρυσμένου ελέγχου και υποστήριξης του πλοίου (RMSS). Σύμφωνα με τη μεθοδολογία STRIDE, αναγνωρίστηκαν μία απειλή υψηλού κινδύνου, τέσσερις μέτριου και μία χαμηλού. Αναλυτικότερα, η διαρροή πληροφοριών (I) αποτελεί μία άκρως επικίνδυνη απειλή για το πλοίο, η προσποίηση ταυτότητας (S), η αλλοίωση δεδομένων (T), η άρνηση υπηρεσιών (D) και η αναβάθμιση προνομίων (E) αποτελούν μέτριας επικινδυνότητας απειλές για την υποδομή και τέλος η άρνηση της ευθύνης εκτέλεσης μία ενέργειας χαρακτηρίστηκε ως χαμηλού κινδύνου, όπως παρατηρείται και στον πίνακα 25.

Στο επίπεδο ένα της αρχιτεκτονικής έχουν ταξινομηθεί τα αυτόματα συστήματα μηχανών (EAS), τα αυτόματα συστήματα της γέφυρας (BAS) καθώς επίσης και τα συστήματα του κέντρου ελέγχου ξηράς (SCC), τα οποία αποτελούν υποσυστήματα της ρίζας του δέντρου (πλοίου). Πιο αναλυτικά, στα αυτόματα συστήματα μηχανών (EAS) όπως αναλύονται στον πίνακα 5, έχουν αναγνωριστεί δύο επιθέσεις υψηλού κινδύνου, δύο μέτριου και δύο χαμηλού. Ως υψηλού κινδύνου, η ανάλυση χαρακτήρισε τις απειλές προσποίησης ταυτότητας (S) και άρνησης υπηρεσιών (D), ως μέτριου κινδύνου τις απειλές αλλοίωσης δεδομένων (T) και αναβάθμισης προνομίων (E) και ως χαμηλής επικινδυνότητας τις απειλές αποποίησης ευθύνης (R) και διαρροής πληροφοριών (I). Συνεχίζοντας στον επόμενο κόμβο του πρώτου επιπέδου ο οποίος είναι τα αυτόματα συστήματα γέφυρας (BAS), μέσω της μεθόδου STRIDE αναγνωρίστηκαν δύο απειλές υψηλού κινδύνου και τέσσερις μέτριου. Οι πρώτες αφορούν τις απειλές προσποίησης ταυτότητας (S) και άρνησης υπηρεσιών (D) της STRIDE και οι επόμενες της αλλοίωσης δεδομένων (T), αποποίησης ευθύνης (R), διαρροής πληροφοριών (I) και αναβάθμισης προνομίων (E). Τελευταία συστήματα του επιπέδου αποτελούν τα συστήματα ελέγχου ξηράς (SCC) για τα οποία η μεθοδολογία STRIDE συγκέντρωσε πανομοιότυπα αποτελέσματα με αυτά των συστημάτων γέφυρας (BAS) καθώς και στα συγκεκριμένα, σύμφωνα με τις επιθέσεις του πίνακα 12 χαρακτηρίστηκαν δύο επιθέσεις υψηλού κινδύνου και τέσσερις μέτριου. Αναλυτικότερα, οι απειλές προσποίησης ταυτότητας (S) και διαρροής πληροφοριών (I) χαρακτηρίστηκαν υψηλής επικινδυνότητας και οι απειλές αλλοίωσης δεδομένων (T), αποποίησης ευθύνης (R), άρνησης υπηρεσίας (D) και αναβάθμισης προνομίων (E) χαρακτηρίστηκαν μέτριας επικινδυνότητας.

Κεφάλαιο 5

5.1 Συμπεράσματα

Οι τεχνολογίες για την ανάπτυξη του τηλεχειριζόμενων και αυτόνομων οχημάτων υπάρχουν και γίνονται ολοένα και πιο δημοφιλείς στον κλάδο της ναυτιλίας. Όμως, η τηλεχειριζόμενη και αυτόνομη λειτουργία των πλοίων δημιουργεί αρκετά ερωτήματα σχετικά με την ασφάλειά των ίδιων, αλλά και των οντοτήτων που υπάρχουν στο περιβάλλον τους. Τα αυτόνομα συστήματα πρέπει να συνυπάρχουν με συστήματα τα οποία χειρίζεται ο άνθρωπος και να διενεργούν αυτόνομες διεργασίες σε συνεργασία με αυτά, γεγονός που απαιτεί τη συνεχή παρακολούθησή τους από το Shore Control Center (SCC).

Συνοψίζοντας, η παρούσα εργασία ανέλυσε και επεξήγησε πολλές έννοιες που σχετίζονται με την ιδέα του cyber-enabled πλοίου. Πιο συγκεκριμένα, η συνεισφορά της παρούσας εργασίας συνίσταται στα εξής:

- Προσφέρει το υπόβαθρο για τη κατανόηση των εννοιών του τηλεχειριζόμενου και του αυτόνομου πλοίου.
- Πραγματοποιεί μία λεπτομερή ανάλυση των συστημάτων και των υποσυστημάτων των cyber-enabled πλοίων.
- Σχεδιάζει ένα αφαιρετικό μοντέλο της αρχιτεκτονικής που δύναται να επικρατεί στα cyber-enable πλοία, καθώς στη βιβλιογραφία δεν υπάρχει σαφής προσδιορισμός της.
- Πραγματοποιεί ανάλυση απειλών στα συστήματα και τα υποσυστήματα της παραπάνω αρχιτεκτονικής μέσω της μεθοδολογίας STRIDE.
- Εφαρμόζει μία ανάλυση κινδύνου, λαμβάνοντας υπόψη τα αποτελέσματα της ανάλυσης απειλών.
- Αναλύει τα αποτελέσματα των δύο προηγούμενων.

Άνθρωποι που δεν είναι εξοικειωμένοι με τις αντίστοιχες έννοιες, μπορούν να κατανοήσουν την αρχιτεκτονική και τις λειτουργίες ενός cyber-enabled πλοίου και να συνειδητοποιήσουν, μέσω του υπόβαθρου που προσφέρουν τα εισαγωγικά κεφάλαια, πως αυτά τα συστήματα είναι ιδιαίτερα εκτεθειμένα σε κυβερνοεπιθέσεις.

Επίσης, από την αντίστοιχη ανάλυση απειλών και την ανάλυση κινδύνου που πραγματοποιείται, παρατηρείται μία υψηλή επικινδυνότητα στα συστήματα και στη συνολική λειτουργία του cyber-enabled πλοίου. Εύκολα μπορεί να γίνει αντιληπτό από τους αντίστοιχους πίνακες ότι υπάρχουν συστήματα στο πλοίο τα οποία είναι άμεσα εκτεθειμένα στον κόσμο του διαδικτύου, με αποτέλεσμα να αυξάνεται ο κίνδυνος των απειλών. Χαρακτηριστικά, στο τρίτο επίπεδο της αρχιτεκτονικής, το σύστημα αυτόματου προσδιορισμού θέσης (AIS) εμφάνισε τα υψηλότερα επίπεδα κινδύνου σε τέσσερις από τις έξι απειλές της μεθόδου STRIDE και ακολούθησαν τα συστήματα ηλεκτρονικής απεικόνισης χαρτών και πληροφοριών (ECDIS) και το Σύστημα Ναυτιλιακού Κινδύνου και Ασφάλειας (GMDSS) με τρείς απειλές υψηλού κινδύνου από τις έξι της μεθοδολογίας. Στο δεύτερο επίπεδο, σε ιδιαίτερο κίνδυνο βρίσκονται το σύστημα διεπαφής του πλοίου με τη ξηρά (HMI) και τα συστήματα πλοήγησης (Navigation) συγκεντρώνοντας πέντε και τέσσερις απειλές υψηλού κινδύνου από τις έξι που προτείνει η μέθοδος. Αξίζει να σημειωθεί σε αυτό το σημείο, ότι τα συστήματα του τρίτου επιπέδου με τον υψηλότερο κίνδυνο είναι υποσυστήματα των συστημάτων του δεύτερου επιπέδου που παρουσίασαν τον υψηλότερο κίνδυνο. Τέλος στο πρώτο επίπεδο τα συστήματα της γέφυρας (BAS) και τα συστήματα ελέγχου ξηράς

(SCC) παρουσίασαν τον μεγαλύτερο κίνδυνο, λαμβάνοντας υπόψη και τις απειλές που χαρακτηρίστηκαν ως μέτριου κινδύνου. Τα παραπάνω αποτελέσματα της ανάλυσης απειλών και κινδύνων οδηγούν ένα βήμα πιο κοντά στη δημιουργία μιας μεθόδου η οποία θα εξετάζει συστήματα συστημάτων και θα εξάγει ενιαία αποτέλεσμα για αυτά.

5.2 Μελλοντική δουλειά

Για μελλοντική δουλειά, θα μπορούσε να πραγματοποιηθεί η επέκταση των αυτόματων συστημάτων του cyber-enabled πλοίου, καθώς ορισμένα από αυτά που αναφέρονται στην υπάρχουσα εργασία δεν έχουν υλοποιηθεί ακόμα.

Σημαντικό επίσης μέρος αποτελεί η ανάλυση απειλών και κινδύνων και με ποιο τρόπο αυτά τα δύο μπορούν να συνδυαστούν σε μία ενιαία μεθοδολογία για εφαρμογή σε αντίστοιχες υποδομές (Systems of systems) λαμβάνοντας υπόψη και τη φυσική ασφάλεια, καθώς υποδομές σαν αυτή του πλοίου συνδέονται στενά με τον ανθρώπινο παράγοντα.

Βιβλιογραφικές Πηγές

[1] E. Jokioinem, «Remote and Autonomous Ship - The next steps,» *Rolls-Royce,* p. 88.

[2] S. K. Katsikas, «Cyber Security of the Autonomous Ship,» *CPSS'17, Abu Dhabi, United Arab Emirates,* 02 April 2017.

[3] «Βικιλεξικό,» [Ηλεκτρονικό]. Available: https://el.wiktionary.org/wiki/%CE%B1%E1%BD%90%CF%84%CF%8C%CE%BD%CE%BF%CE%BC%CE%BF%CF%82.

[4] T. B. Sheridan, Telerobotics, Automation, and Human Supervisory Control, 1992.

[5] R. Parasuraman, T. Sheridan και C. Wickens, «A model for types and levels of human interaction with automation,» *IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS, PART A: SYSTEMS AND HUMANS, VOL. 30, NO. 3,,* 2000.

[6] G. Dorais, D. Kortenkamp, N. Johnson, S. Center και G. A. Dorais, «Designing Human -Centered Centered Autonomous Agents.».

[7] R.-R. A. P. Paper, «Remote and Autonomous Ship - The next steps,» England, 2016.

[8] BIMCO, «The Guidelines on Cyber Security Onboard Ships Version 2.0,» 2016.

[9] «Maritime Unmanned Navigation through Intelligence in Networks-MUNIN,» June 2016. [Ηλεκτρονικό]. Available: http://www.unmanned-ship.org/munin/.

[10] «Wikipedia,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Huginn_and_Muninn. [Πρόσβαση 15 January 2018].

[11] Ø. J. Rødseth, Å. Tjora και P. Baltzersen, «MUNIN, D4.5 Architecture Specification,» 2013.

[12] R. Parasuraman, T. Sheridan και C. Wickens, «A model for types and levels of human interaction with automation,» *IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A: SYSTEMS AND HUMANS, VOL. 30, NO. 3,* p. 12, MAY 2000.

[13] «e-Navigation – it's all about the data».

[14] ENISA, «Glossary Published under Risk Management,» ENISA, [Ηλεκτρονικό]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary. [Πρόσβαση 15 January 2018].

[15] NIST, «Glossary of Key Information Security Terms,» May 2013.

[16] B. Jelacic, D. Rosic, I. Lendak, M. Stanojevic και S. Stoja, «STRIDE to a secure Smart Grid in a hybrid cloud,» *CyberICPS 2017, SECPRE 2017: Computer Security,* pp. pp 77-90, Septemper 2017.

[17] Ø. Rødseth και H. Burmeister, «Risk Assessment for an Unmanned Merchant Ship,» *the International Journal on Marine Navigation and Safety of Sea Transportation,* September 2015.

[18] E. Byres, M. Franz και . D. Miller, «The Use of Attack Trees in Assessing Vulnerabilities in SCADA System,» *International Infrastructure Survivability Workshop (IISW'04),* 2004.

[19] M. Howard και S. Lipner, «The Threat-Modeling Process,» σε *The Security Development Lifecycle*, Microsoft Press, 2006, pp. 105-124.

[20] H. N. J. Havinga και O. D. T. Sessink, «Risk Reduction Overview A Visualization Method for Risk Management,» *IFIP International Federation for Information Processing,* pp. 239-249, 2014.

[21] H. Havinga και . O. Sessink, «Risk Reduction Overview Manual,» September 7 2014.

[22] A. Shostack, Threat Modeling Designing for Security, John Wiley & Sons, Inc., 2014.

[23] «The STRIDE Threat Model,» Microsoft, [Ηλεκτρονικό]. Available: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx. [Πρόσβαση 2017].

[24] IMO, «INTERIM GUIDELINES ON MARITIME CYBER RISK MANAGEMENT MSC.1/Circ.1526,» 1 June 2016.

[25] O. Fitton, D. Prince, B. Germond και M. Lacy, «The Future of Maritime Cyber Security,» 2015.

[26] M. Song και K. Lee , «Design Challenges and Implementation of a Shipborne Gateway for Safe and Secure Navigational Networks,» *Advanced Multimedia and Ubiquitous Engineering: Future Information Technology Volume 2, J. J. (Jong H. Park, H.-C. Chao, H. Arabnia, and N. Y. Yen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg,* p. pp. 129–135, 2016.

[27] N. S. P. 800-30, «Guide for Conducting Risk Assessments,» September 2012.

[28] Ø. J. Rødseth, Å. Tjora και P. Baltzersen, «MUNIN, D4.5 Architecture Specification,» 2013.

[29] H.-C. Burmeister, W. Bruhn, L. Walther, J. A. Moræus και B. Sage-Fuller, «MUNIN D8.6: Final Report: Autonomous Bridge,» 2015.

[30] Δ. Χ. Κόκοτος, Ν. Β. Νικητάκος, Δ. Σ. Λιναρδάτος και Ε. Σ. Τζανάτος, Τεχνολογίες πληροφορικής και επικοινωνιών στη ναυτιλία, Σταμούλη Α.Ε., 2011.

[31] W. Bruhn, H. Burmeister, L. Walther, J. Moræus, M. Long, M. Schaub και E. Fentzahn, «MUNIN D5.2: Process map for autonomous navigation,» 2013.

[32] W. C. Bruhn, H.-C. Burmeister, M. T. Long και J. A. Moræus, «Conducting look-out on an unmanned vessel: Introduction to the advanced sensor module for MUNIN's autonomous dry bulk carrier,» σε *The 10th International Symposium ISIS 2014 „Integrated Ship's Information Systems"Related ISIS Topics: "Sensors and Components: AIS, LRIT, AtoN, Radar"*, 2014.

[33] C. Möckel και A. E. Abdallah, «THREAT MODELING APPROACHES AND TOOLS FOR SECURING ARCHITECTURAL DESIGNS OF AN E-BANKING APPLICATION,» *Sixth International Conference on Information Assurance and Security,* 2010.

[34] Y. Chen, B. Boehm και L. Sheppard, «Value Driven Security Threat Modeling Based on Attack Path Analysis,» *HICSS '07 Proceedings of the 40th Annual Hawaii International Conference on System Sciences,* 2007 .

[35] «Maritime Unmanned Navigation through Intelligence in Networks,» EU, 2016. [Ηλεκτρονικό]. Available: http://www.unmanned-ship.org/munin/.

[36] M. Schmidt, E. Fentzahn, G. F. Atlason και H. Rødseth, «8.7 Final Report Autonomous Engine Room,» 2015.