



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

«Πτυχιακή Εργασία»

Τίτλος Πτυχιακής Εργασίας	Ελληνικά: "Διαχείριση Κινδύνου Ασφάλειας Λιμενικών Εγκαταστάσεων Πληροφορικής" Αγγλικά: "Cyber Risk Management of Port Facilities"
Ονοματεπώνυμο Φοιτητή	Αθανάσιος Ρηγόπουλος
Πατρώνυμο	Γεώργιος
Αριθμός Μητρώου	Π22148
Επιβλέπουσα:	Δέσποινα Πολέμη, Καθηγήτρια.

Ημερομηνία Παράδοσης: Σεπτέμβριος 2026

Copyright ©

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν αποκλειστικά τον συγγραφέα και δεν αντιπροσωπεύουν τις επίσημες θέσεις του Πανεπιστημίου Πειραιώς.

Ως συγγραφέας της παρούσας εργασίας δηλώνω πως η παρούσα εργασία δεν αποτελεί προϊόν λογοκλοπής και δεν περιέχει υλικό από μη αναφερόμενες πηγές.

Ευχαριστίες

Θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες στην επιβλέπουσα καθηγήτρια κ. Δέσποινα Πολέμη, για την καθοδήγηση, τις εύστοχες παρατηρήσεις και τη συνεχή υποστήριξη καθ' όλη τη διάρκεια εκπόνησης της παρούσας πτυχιακής εργασίας.

Ευχαριστώ επίσης το Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς για τις γνώσεις και τις δεξιότητες που απέκτησα κατά τη διάρκεια των σπουδών μου, οι οποίες αποτέλεσαν το θεμέλιο για την εκπόνηση αυτής της εργασίας.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου] για την υπομονή και τη στήριξή τους καθ' όλη τη διάρκεια των σπουδών μου.

Περίληψη

Η ραγδαία ψηφιοποίηση και η σύγκλιση Πληροφοριακών Συστημάτων (IT) και Επιχειρησιακών Τεχνολογιών (OT) στις σύγχρονες λιμενικές υποδομές έχει διευρύνει σημαντικά την επιφάνεια κυβερνοεπίθεσης, καθιστώντας την παραδοσιακή, αποσπασματική διαχείριση ασφάλειας ανεπαρκή. Η παρούσα πτυχιακή εργασία αναπτύσσει και εφαρμόζει πρακτικά μια ολοκληρωμένη μεθοδολογία ανάλυσης κυβερνοκινδύνου για λιμενικές εγκαταστάσεις, υιοθετώντας μια ρητή Διπλή Προσέγγιση (Dual Approach) που εξετάζει ταυτόχρονα το πληροφοριακό και το βιομηχανικό περιβάλλον ως ενιαίο, αλληλεξαρτώμενο σύστημα.

Μεθοδολογικά, η εργασία συνδυάζει το διεθνές πρότυπο ISO/IEC 27005, τη σειρά προτύπων IEC 62443 και κατευθύνσεις του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA), εφαρμοσμένα πρακτικά μέσω του λογισμικού ανοιχτού κώδικα MONARC σε έναν υποθετικό Τερματικό Σταθμό Εμπορευματοκιβωτίων. Μετά τη θεωρητική χαρτογράφηση αγαθών, απειλών και ευπαθειών, αξιολογήθηκαν ποσοτικά οκτώ στοχευμένα σενάρια επίθεσης. Τα αποτελέσματα επιβεβαίωσαν εμπειρικά τη διαφοροποίηση προτεραιοτήτων ασφάλειας μεταξύ IT (μοντέλο CIA, μέγιστος αντίκτυπος 3) και OT (μοντέλο AIC/Safety, μέγιστος αντίκτυπος 4, με ρητά σενάρια κινδύνου ανθρώπινης ζωής). Η εφαρμογή οκτώ στοχευμένων μέτρων αντιμετώπισης, βασισμένων στα ISO/IEC 27002 και IEC 62443, οδήγησε σε μέση μείωση του κινδύνου κατά περίπου 70%. Η μελέτη ολοκληρώνεται με τη θεσμοθέτηση πολιτικών ασφαλείας, επιχειρησιακών διαδικασιών και Σχεδίου Επιχειρησιακής Συνέχειας, με δείκτες ανάκαμψης παραγόμενους απευθείας από τα δεδομένα αξιολόγησης κινδύνου. Η εργασία συνεισφέρει μια αναπαραγώγιμη μεθοδολογία που απαντά στο κενό τυποποίησης που έχει επισημάνει ο ENISA για τους ευρωπαϊκούς λιμένες.

Επιστημονική Περιοχή: Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων

Λέξεις Κλειδιά: Κυβερνοασφάλεια Λιμένων, Ανάλυση Κινδύνου (ISO/IEC 27005), Σύγκλιση IT/OT, MONARC, Προστασία Κρίσιμων Υποδομών

Abstract

The rapid digitalization and convergence of Information Technology (IT) and Operational Technology (OT) in modern port infrastructures has significantly expanded the cyber-attack surface, rendering traditional, fragmented security management insufficient. This thesis develops and practically applies a comprehensive cyber risk analysis methodology for port facilities, adopting an explicit Dual Approach that examines both the information and industrial environments as a single, interdependent system.

Methodologically, the study combines the international standard ISO/IEC 27005, the IEC 62443 series, and guidance from the European Union Agency for Cybersecurity (ENISA), applied in practice through the open-source software MONARC on a hypothetical Container Terminal. Following theoretical mapping of assets, threats, and vulnerabilities, eight targeted attack scenarios were quantitatively assessed. Results empirically confirmed the differentiation of security priorities between IT (CIA model, maximum impact level 3) and OT (AIC/Safety model, maximum impact level 4, reflecting explicit human-life risk scenarios). Implementation of eight targeted countermeasures, based on ISO/IEC 27002 and IEC 62443, achieved an average risk reduction of approximately 70%. The study concludes with the establishment of security policies, operational procedures, and a Business Continuity Plan, with recovery indicators derived directly and traceably from the risk assessment data. The work contributes a reproducible methodology that addresses the standardization gap identified by ENISA for European ports.

Scientific Area: Information Systems and Network Security

Keywords: Port Cybersecurity, Risk Assessment (ISO/IEC 27005), IT/OT Convergence, MONARC, Critical Infrastructure Protection

Πίνακας Περιεχομένων

Copyright ©	i
Ευχαριστίες	ii
Περίληψη	iii
Πίνακας Περιεχομένων	iv
Κατάλογος Εικόνων	vi
Κατάλογος Πινάκων	vii
Εισαγωγή	1
1.1 Περιγραφή του Προβλήματος και Σημασία της Κυβερνοασφάλειας	1
1.2 Σκοπός και Αντικείμενο Μελέτης	1
1.3 Δομή της Εργασίας	2
1 Πρότυπα, Μεθοδολογίες και Εργαλεία Ανάλυσης Επικινδυνότητας	3
1.1 Το Διεθνές και Ευρωπαϊκό Ναυτιλιακό Πλαίσιο: Ανάλυση των Κανονιστικών και Νομικών Απαιτήσεων	3
1.1.1 Η Θεσμική Θεμελίωση από τον IMO και η Μετάβαση του Κώδικα ISPS	3
1.1.2 Βέλτιστες Πρακτικές της Βιομηχανίας και Απαιτήσεις Νηογνωμόνων (BIMCO & IACS)	4
1.1.3 Σύγχρονες Ευρωπαϊκές & Διεθνείς Ρυθμίσεις: NIS2, N. 5160/2024 και USCG Final Rule	5
1.2 Μεθοδολογικές Προσεγγίσεις Διαχείρισης Κινδύνου IT και OT: Τα Πρότυπα ISO 27005, IEC 62443 και οι Οδηγίες του ENISA	6
1.2.1 Το Πρότυπο ISO/IEC 27005: Μεθοδολογική Θεμελίωση Διαχείρισης Κινδύνων IT	6
1.2.2 Η Ιδιαιτερότητα του OT: Τα Πρότυπα IEC 62443 και NIST SP 800-82 Rev. 3	6
1.2.3 Κατευθυντήριες Οδηγίες ENISA για Λιμένες και η Σύγκλιση IT/OT	7
1.3 Εισαγωγή στα Εργαλεία και τις Μεθοδολογίες Αξιολόγησης Κινδύνων: Κατηγοριοποίηση, Σύγχρονα Πλαίσια και η Επιλογή του MONARC	7
1.3.1 Κατηγοριοποίηση Μεθοδολογιών και το Ελεγκτικό Πρίσμα του EMSA	7
1.3.2 Σύγχρονα Διεθνή Πλαίσια και Εργαλεία: NIST CSF 2.0, CSET, FAIR και EBIOS RM ..	8
1.3.3 Η Στρατηγική Επιλογή του Ανοιχτού Λογισμικού MONARC ως Κεντρικού Εργαλείου ..	9
2 Αρχιτεκτονική Λιμενικών Υποδομών και Αποτίμηση Κινδύνου	10
2.1 Χαρτογράφηση του Λιμενικού Οικοσυστήματος: Ζώνες IT/OT/Ναυσιπλοΐας και Ανθρώπινος Παράγοντας	10
2.1.1 Λειτουργική Ομαδοποίηση Δευτερευόντων Αγαθών σε Τέσσερις Ζώνες και Εγκάρσιους Αγωγούς (IEC 62443)	11
2.1.2 Χαρτογράφηση του Ανθρώπινου Παράγοντα: Οι Πέντε Κρίσιμοι Ρόλοι	12
2.2 Μοντέλο Αγαθών (Asset Model) και Δίκτυο Εξαρτήσεων (Ai)	13
2.2.1 Ορισμός Πρωτευόντων Αγαθών (Dual Approach)	13
2.2.2 Το Δέντρο Εξαρτήσεων και η Σύγκλιση IT/OT	13
2.2.3 Οπτική και Μαθηματική Αναπαράσταση (DAG & DSM)	14
2.3 Αποτίμηση Απειλών (Threat Assessment) στο Ναυτιλιακό Οικοσύστημα: Αντιστοίχιση των Αγαθών με Ψηφιακές, Φυσικές και Ανθρώπινες Απειλές	16
2.3.1 Ψηφιακές και Κυβερνο-Φυσικές Απειλές (Cyber & Cyber-Physical Threats)	16
2.3.2 Φυσικές και Περιβαλλοντικές Απειλές (Physical & Environmental Threats)	16
2.3.3 Ανθρώπινες Απειλές και Κίνδυνοι Εφοδιαστικής Αλυσίδας (Human & Supply Chain Threats)	17
2.4 Αποτίμηση Αδυναμιών (Vulnerability Assessment): Εντοπισμός Ευπαθειών ανά Ζώνη Λιμενικής Υποδομής	17
2.4.1 Ευπάθειες στη Ζώνη 1 (IT Domain) & Ζώνη 2 (Bridging Zone / TOS)	17

2.4.2 Ευπάθειες στη Ζώνη 3 (OT / Βιομηχανικό Περιβάλλον)	18
2.4.3 Ευπάθειες στη Ζώνη 4 (Ναυσιπλοΐα και Επικοινωνίες)	18
3 Πρακτική Εφαρμογή της Ανάλυσης Κινδύνου στο Λογισμικό MONARC.....	19
3.1 Τεχνική Ανάπτυξη και Περιβάλλον Λειτουργίας του Λογισμικού MONARC	19
3.2 Εισαγωγή Δεδομένων και Παραμετροποίηση Στοχευμένου Σεναρίου	20
3.2.1 Ορισμός Παραμέτρων Έργου και Στοχευμένου Σεναρίου.....	20
3.2.2 Ορισμός Κλιμάκων Αξιολόγησης και Κριτηρίων Κινδύνου	20
3.2.3 Εισαγωγή των Πρωτευόντων Αγαθών και Κατηγοριοποίηση σε Ζώνες	21
3.3 Εκτίμηση Αντικτύπου και Αξιολόγηση Κινδύνων	22
3.3.1 Εμπειρική Επιβεβαίωση της Διχοτομίας IT/OT	22
3.3.2 Υπολογισμός Τρέχοντος Κινδύνου ανά Ζώνη.....	23
3.3.3 Ποσοτικές Στρεβλώσεις και τα Όρια των Γενικών Προτύπων	24
3.4 Εξαγωγή Αποτελεσμάτων: Παραγωγή Γραφημάτων και Μαθηματική Επιβεβαίωση.....	25
3.4.1 Συγκριτική Ανάλυση Απειλών ανά Περιβάλλον (IT vs OT)	25
3.4.2 Οπτική Επαλήθευση του Μαθηματικού Τύπου (Risk Cartography).....	25
3.4.3 Συγκεντρωτική Ιεράρχηση Κινδύνων (Top Risks)	26
4 Σχέδιο Αντιμετώπισης Κινδύνων και Οργανωτικές Δομές Ασφάλειας	27
4.1 Προτεινόμενα Μέτρα Προστασίας (Τεχνικά και Μη-Τεχνικά)	27
4.1.1 Μέτρα για το Πληροφοριακό Σύστημα (PCS - Ζώνη 1)	27
4.1.2 Μέτρα για τον Βιομηχανικό Εξοπλισμό (Physical Crane - Ζώνη 3)	28
4.2 Εφαρμογή της Θεραπείας Κινδύνου στο MONARC και Υπολογισμός Υπολειπόμενου Κινδύνου	29
4.2.1 Μεθοδολογία Βαθμολόγησης Υπολειπόμενης Ευπάθειας	29
4.2.2 Οπτικοποίηση και Μαθηματική Επαλήθευση.....	29
4.2.3 Στρατηγική και Χρονοδιάγραμμα Υλοποίησης	31
4.3 Κατανομή Οργανωτικών Δομών και Αρμοδιοτήτων	31
4.3.1 Ορισμός Ρόλων και Διαχωρισμός Αρμοδιοτήτων (Segregation of Duties).....	32
4.3.2 Επιχειρησιακή Εφαρμογή μέσω Μήτρας RACI.....	32
5 Βασικές Πολιτικές, Διαδικασίες και Επιχειρησιακή Συνέχεια	33
5.1 Βασικές Πολιτικές Ασφάλειας	33
5.1.1 Πολιτική Ελέγχου Πρόσβασης (Access Control Policy)	33
5.1.2 Πολιτική Κωδικών και Πιστοποίησης (Password & Authentication Policy).....	33
5.1.3 Πολιτική Καταγραφής και Ελέγχου (Logging & Audit Policy).....	34
5.1.4 Πολιτική Αντιγράφων Ασφαλείας (Backup Policy).....	34
5.2 Βασικές Διαδικασίες (Procedures).....	35
5.2.1 Διαδικασία Αντιμετώπισης Περιστατικών Κυβερνοασφάλειας.....	35
5.2.2 Διαδικασία Δημιουργίας και Επαναφοράς Αντιγράφων (Backup & Restore)	35
5.2.3 Διαδικασία Διαχείρισης Χρηστών (JML Lifecycle).....	36
5.3 Σχέδιο Επιχειρησιακής Συνέχειας (Business Continuity Plan).....	36
5.3.1 Ανάλυση Επιχειρησιακών Επιπτώσεων και Παραγωγή Δεικτών (RTO & RPO).....	36
5.3.2 Στρατηγική Ανάκαμψης από Ολική Καταστροφή (Total Disaster Strategy).....	37
Συμπεράσματα	37
Πίνακας Ορολογίας	39
Πίνακας συντμήσεων-αρτικόλεξων-ακρονύμων	44
Βιβλιογραφία	47

Κατάλογος Εικόνων

Εικόνα 2.1: Κατευθυνόμενος Άκυκλος Γράφος (DAG) Εξαρτήσεων Αγαθών — Απεικόνιση της Σύγκλισης IT/OT μέσω του TOS. Πηγή: Ιδία επεξεργασία.	15
Εικόνα 3.1: Το περιβάλλον διεπαφής του λογισμικού MONARC v. 2.13.3 κατά την αρχική εκκίνηση.	20
Εικόνα 3.2: Πίνακας αξιολογημένων κινδύνων για το Πληροφοριακό Σύστημα (IT/PCS) στο περιβάλλον του MONARC. (NC3, 2025)	23
Εικόνα 3.3: Πίνακας αξιολογημένων κινδύνων για τη Διαδικασία Εκφόρτωσης (OT/Γερανός) στο περιβάλλον του MONARC. (NC3, 2025)	24
Εικόνα 3.4: Συγκριτική κατανομή επιπέδων κινδύνου διαχωρισμένη ανά Πρωτεύον Αγαθό (Continuous Container Unloading Process έναντι PCS & Customs Data). (NC3, 2025)	25
Εικόνα 3.5: Χαρτογράφηση Κινδύνων (Cartography). Οπτική επιβεβαίωση της συνάρτησης Αντικτύπου (Y) και του γινομένου Πιθανότητας/Ευπάθειας (X). (NC3, 2025)	26
Εικόνα 3.6: Συνολική ιεράρχηση των εξεταζόμενων απειλών βάσει του μέγιστου συσχετιζόμενου επιπέδου κινδύνου. (NC3, 2025)	27
Εικόνα 4.1: Συγκριτική κατανομή (Current vs Residual risks). Εμφανής η ολική εξάλειψη των κρίσιμων (High) κινδύνων. (NC3, 2025)	30
Εικόνα 4.2: Αναλυτική πτώση του επιπέδου κινδύνου, διαχωρισμένη ανά περιβάλλον (IT έναντι OT). (NC3, 2025)	30
Εικόνα 4.3: Χαρτογράφηση Κινδύνων (Cartography). Αριστερά οι αρχικοί κίνδυνοι και δεξιά η μετατόπισή τους σε ασφαλείς ζώνες μετά τη θεραπεία. (NC3, 2025)	31

Κατάλογος Πινάκων

Πίνακας 1.1: Συγκριτική Αξιολόγηση Πλαισίων και Εργαλείων Διαχείρισης Κινδύνου για Λιμενικές Υποδομές. Πηγή: Ιδία επεξεργασία.	9
Πίνακας 2.1: Μήτρα Εξαρτήσεων (DSM) Αγαθών Λιμενικής Εγκατάστασης (Το Χ" δηλώνει ότι το Στοιχείο Γραμμής εξαρτάται άμεσα από το Στοιχείο Στήλης) Πηγή: Ιδία επεξεργασία.	14
Πίνακας 3.1: Αξιολόγηση Κινδύνων IT (Port Community System - PA2). Πηγή: Ιδία επεξεργασία.	23
Πίνακας 3.2: Αξιολόγηση Κινδύνων OT (Physical Crane - PA1). Πηγή: Ιδία επεξεργασία.	24
Πίνακας 4.1: Μήτρα κατανομής αρμοδιοτήτων RACI (R=Υπεύθυνος εκτέλεσης, A=Υπόλογος/Εγκρίνων, C=Σύμβουλος/Ερωτώμενος, I=Ενημερούμενος). Πηγή: Ιδία επεξεργασία	32
Πίνακας 5.1: Δείκτες Ανάκαμψης ανά Πρωτεύον Αγαθό (IT και OT). Πηγή: Ιδία επεξεργασία	37

Εισαγωγή

1.1 Περιγραφή του Προβλήματος και Σημασία της Κυβερνοασφάλειας

Ο ναυτιλιακός τομέας διανύει μια περίοδο ταχύτατου ψηφιακού μετασχηματισμού, στον οποίο η αδιάλειπτη λειτουργία των παγκόσμιων εφοδιαστικών αλυσίδων εξαρτάται άμεσα από την αξιοπιστία των τεχνολογικών υποδομών. Παραδοσιακά, τα πλοία και οι λιμενικές εγκαταστάσεις λειτουργούσαν ως μηχανικά, απομονωμένα συστήματα, στα οποία η φυσική ασφάλεια επαρκούσε για την αποτροπή εξωτερικών απειλών. Ωστόσο, η σύγχρονη πραγματικότητα επιβάλλει την πλήρη σύγκλιση των Πληροφοριακών Συστημάτων (Information Technology - IT) με τις Επιχειρησιακές Τεχνολογίες (Operational Technology - OT). Η διασύνδεση των λιμενικών συστημάτων διαχείρισης, όπως τα Port Community Systems (PCS), με κρίσιμα συστήματα ναυσιπλοΐας και ελέγχου κυκλοφορίας, όπως το Automatic Identification System (AIS), έχει καταργήσει την παραδοσιακή "ψηφιακή απομόνωση" (air-gap) των ναυτιλιακών υποδομών (BIMCO et al., 2020). Η εξέλιξη αυτή, αν και βελτιστοποιεί την επιχειρησιακή απόδοση, δημιουργεί μια εκτεταμένη επιφάνεια επίθεσης (attack surface), καθιστώντας τις υποδομές ευάλωτες σε κακόβουλες ενέργειες στον κυβερνοχώρο.

Το μέγεθος του προβλήματος γίνεται αντιληπτό αν αναλογιστεί κανείς ότι η ναυτιλία διακινεί περίπου το 90% του παγκόσμιου εμπορίου, γεγονός που την καθιστά πρωταρχικό στόχο για εξειδικευμένες κυβερνοεπιθέσεις, οικονομικό εκβιασμό (Ransomware), αλλά και γεωπολιτικές παρεμβάσεις από κρατικά υποστηριζόμενες ομάδες (ENISA, 2019). Ορόσημο στην ανάδειξη της κρισιμότητας αυτών των απειλών αποτέλεσε η ιστορική επίθεση με το κακόβουλο λογισμικό NotPetya το 2017, η οποία έπληξε τον ναυτιλιακό κολοσσό A.P. Møller-Maersk. Η διακοπή λειτουργίας των συστημάτων IT της εταιρείας οδήγησε σε γενικευμένη παράλυση 76 τερματικών σταθμών εμπορευματοκιβωτίων παγκοσμίως, αποδεικνύοντας ότι ένα κενό ασφαλείας στα διοικητικά δίκτυα μπορεί να προκαλέσει άμεση κατάρρευση των φυσικών λιμενικών λειτουργιών και ανυπολόγιστες οικονομικές ζημιές (ENISA, 2019).

Η ραγδαία αυτή αύξηση της επικινδυνότητας έχει μεταβάλλει ριζικά το δόγμα ασφαλείας στον ναυτιλιακό χώρο. Η παραδοσιακή έννοια της ασφαλείας στη θάλασσα (Safety), που αφορά την προστασία της ανθρώπινης ζωής, του πλοίου και του περιβάλλοντος από ατυχήματα, είναι πλέον άρρηκτα συνδεδεμένη με την ψηφιακή ασφάλεια (Cyber Security). Μια επιτυχής επίθεση πλαστογράφησης στίγματος (spoofing) στο σύστημα AIS ή η παράνομη διείσδυση στα δίκτυα ελέγχου μιας λιμενικής εγκατάστασης δεν συνιστά απλώς μια απώλεια δεδομένων, αλλά μια άμεση απειλή με καταστροφικές φυσικές συνέπειες, όπως συγκρούσεις σκαφών ή θαλάσσια ρύπανση. Κατά συνέπεια, η αντιμετώπιση του προβλήματος δεν μπορεί να περιορίζεται σε αποσπασματικά τεχνικά μέτρα ή σε παθητική αντίδραση μετά το περιστατικό. Αναδεικνύεται ως επιτακτική ανάγκη η υιοθέτηση μιας δομημένης και προληπτικής μεθοδολογίας Ανάλυσης και Διαχείρισης Κινδύνων (Risk Assessment), η οποία θα χαρτογραφεί τα κρίσιμα αγαθά, θα ποσοτικοποιεί τις απειλές και θα θωρακίζει οργανωτικά και τεχνικά το ναυτιλιακό οικοσύστημα.

1.2 Σκοπός και Αντικείμενο Μελέτης

Πρωταρχικός σκοπός της παρούσας πτυχιακής εργασίας είναι η μετάβαση από τη θεωρητική και κανονιστική προσέγγιση της κυβερνοασφάλειας στην πρακτική, μεθοδική και ποσοτικοποιημένη αποτίμηση του κυβερνοκινδύνου (Cyber Risk Assessment) στον ναυτιλιακό τομέα. Η μελέτη επιδιώκει να γεφυρώσει τις σύγχρονες κανονιστικές επιταγές του Διεθνούς Ναυτιλιακού Οργανισμού για την ενσωμάτωση της διαχείρισης κυβερνοκινδύνων στα Συστήματα Ασφάλειας και Διαχείρισης (IMO, 2017) με τα διεθνώς αναγνωρισμένα πρότυπα ασφαλείας πληροφοριών. Ειδικότερα, κεντρικός στόχος είναι η πρακτική εφαρμογή ενός μαθηματικού μοντέλου επικινδυνότητας, το οποίο συνδυάζει την πιθανότητα εκδήλωσης απειλής, τη σοβαρότητα ευπάθειας και τον αντίκτυπο στο αγαθό, μέσω του εξειδικευμένου λογισμικού ανοιχτού κώδικα MONARC. Μέσω αυτής της διαδικασίας, επιδιώκεται η εξαγωγή ενός ρεαλιστικού Σχεδίου

Αντιμετώπισης Κινδύνων (Risk Treatment Plan) που θα θωρακίζει αποτελεσματικά τις σύγχρονες λιμενικές υποδομές.

Για την επίτευξη του ανωτέρω σκοπού και προκειμένου να καταστεί εφικτή η πρακτική προσομοίωση στο λογισμικό MONARC, ως αντικείμενο μελέτης ορίζεται ένας υποθετικός, μεσαίας προς μεγάλης κλίμακας Λιμενικός Φορέας Διαχείρισης Εμπορευματοκιβωτίων (Hypothetical Container Terminal Port Facility). Ο συγκεκριμένος οργανισμός διαθέτει μια πλήρως ψηφιοποιημένη οργανωτική και επιχειρησιακή δομή, η οποία χωρίζεται σε δύο διακριτούς αλλά στενά διασυνδεδεμένους πυλώνες: το Διοικητικό και Εμπορικό Κέντρο, που φιλοξενεί τις υποδομές εξυπηρετητών (servers), τα δίκτυα LAN/WAN και τις υπηρεσίες υπολογιστικού νέφους (cloud), και το Επιχειρησιακό Τμήμα (Terminal Operations), το οποίο ελέγχει τη θαλάσσια κυκλοφορία στη λιμενολεκάνη, την αυτοματοποιημένη διαχείριση των πυλών (automated gates) και την ασφαλή φορτοεκφόρτωση των πλοίων από τους γερανούς απόθεσης.

Η ακτινογραφία του υποθετικού λιμένα εστιάζει κατά προτεραιότητα σε δύο κρίσιμα υποσυστήματα που αποτελούν τη σπονδυλική στήλη της λειτουργίας του: το Port Community System (PCS) και το Automatic Identification System (AIS). Το PCS λειτουργεί ως η κεντρική ψηφιακή πλατφόρμα Πληροφοριακών Συστημάτων (IT), μέσω της οποίας ανταλλάσσονται εμπιστευτικά εμπορικά, τελωνειακά και εφοδιαστικά δεδομένα σε πραγματικό χρόνο μεταξύ της λιμενικής αρχής, των ναυτιλιακών εταιρειών και των κρατικών φορέων. Μια διακοπή της λειτουργίας του PCS ισοδυναμεί με άμεση εμπορική παράλυση του λιμένα και κατάρρευση της εφοδιαστικής αλυσίδας. Αντίστοιχα, το AIS αποτελεί ένα ζωτικής σημασίας Επιχειρησιακό Σύστημα (OT), το οποίο παρακολουθεί αδιάλειπτα το ακριβές στίγμα, την ταυτότητα και την πορεία των καταπλεόντων και αποπλεόντων πλοίων. Ενδεχόμενη παραβίαση ή αλλοίωση των δεδομένων του AIS θέτει σε άμεσο κίνδυνο την ασφάλεια ναυσιπλοΐας (Safety), δημιουργώντας κίνδυνο θαλάσσιων ατυχημάτων και περιβαλλοντικής καταστροφής (ENISA, 2019). Η μοντελοποίηση της αλληλεξάρτησης αυτών των δύο συστημάτων αποτελεί τον πυρήνα της ανάλυσης κινδύνου στα επόμενα κεφάλαια της εργασίας.

1.3 Δομή της Εργασίας

Η παρούσα πτυχιακή εργασία αναπτύσσεται μέσα από μια λογική, κλιμακωτή μετάβαση από το γενικό στο ειδικό, διαρθρωμένη σε έξι διακριτά αλλά αλληλένδετα κεφάλαια, το καθένα εκ των οποίων οικοδομείται πάνω στα συμπεράσματα του προηγούμενου. Στο Κεφάλαιο 1 τίθεται το θεωρητικό, κανονιστικό και μεθοδολογικό θεμέλιο της μελέτης. Αρχικά αναλύεται το διεθνές ναυτιλιακό πλαίσιο, εξετάζοντας τις σύγχρονες οδηγίες και βέλτιστες πρακτικές των οργανισμών IMO και BIMCO, καθώς και τις απαιτήσεις του Κώδικα ISPS. Στη συνέχεια, θεμελιώνεται η μεθοδολογία της εργασίας πάνω στο διεθνές πρότυπο ISO 27005 και στις ειδικές αναφορές του οργανισμού ENISA για την ασφάλεια των λιμένων. Το κεφάλαιο ολοκληρώνεται με μια κριτική παρουσίαση των σύγχρονων εργαλείων αξιολόγησης κινδύνων (Risk Assessment Tools), συμπεριλαμβανομένης μιας αναφοράς στη μεθοδολογία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια στη Θάλασσα (EMSA).

Ο κεντρικός πυρήνας της πρακτικής μοντελοποίησης και ανάλυσης αναπτύσσεται στα Κεφάλαια 2 και 3. Το Κεφάλαιο 2 εστιάζει στη χαρτογράφηση της ναυτιλιακής υποδομής, προσδιορίζοντας τις κρίσιμες τεχνολογίες —όπως το σύστημα AIS και τα Port Community Systems (PCS)— και καταγράφοντας τα αγαθά και τους χρήστες του συστήματος. Μέσω της δημιουργίας ενός μοντέλου αγαθών (Asset Model) και του αντίστοιχου δικτύου εξαρτήσεων, αποτυπώνεται ο τρόπος με τον οποίο η αστοχία ενός υποσυστήματος επηρεάζει ολόκληρη την αλυσίδα, προετοιμάζοντας το έδαφος για την αναλυτική αποτίμηση των φυσικών, ψηφιακών και ανθρώπινων απειλών (Threat Assessment) και την ανίχνευση των ευπαθειών (Vulnerability Assessment). Αυτή η θεωρητική χαρτογράφηση τροφοδοτεί άμεσα το Κεφάλαιο 3, όπου πραγματοποιείται η πρακτική εφαρμογή της ανάλυσης κινδύνου στο εξειδικευμένο λογισμικό ανοιχτού κώδικα MONARC. Στο κεφάλαιο αυτό περιγράφεται η αιτιολόγηση επιλογής του εργαλείου, εισάγονται και παραμετροποιούνται τα πραγματικά δεδομένα του σεναρίου, αξιολογούνται οι επιπτώσεις (Impact Assessment) και εξάγονται τα τελικά γραφήματα και οι αναφορές, επαληθεύοντας μαθηματικά το επίπεδο του διαλειπόμενου ρίσκου.

Η εργασία ολοκληρώνεται με τον σχεδιασμό της θωράκισης, τη θεσμοθέτηση διαδικασιών και την εξαγωγή των τελικών συμπερασμάτων στα Κεφάλαια 4, 5 και 6. Το Κεφάλαιο 4 προτείνει ένα ολοκληρωμένο Σχέδιο Αντιμετώπισης Κινδύνων (Risk Treatment Plan), καταγράφοντας τα απαραίτητα τεχνικά και μη τεχνικά μέτρα προστασίας, ενώ παράλληλα καθορίζει την κατανομή των οργανωτικών ρόλων ασφάλειας (όπως ο ρόλος του Υπεύθυνου Ασφάλειας Πληροφοριών - CISO). Στο Κεφάλαιο 5 διαμορφώνεται το επιχειρησιακό πλαίσιο, μέσω της συγγραφής βασικών πολιτικών (όπως ο έλεγχος πρόσβασης και η διαχείριση κωδικών), της καταγραφής βήμα-προςβήμα διαδικασιών για την αντιμετώπιση περιστατικών, καθώς και της ανάπτυξης ενός Σχεδίου Επιχειρησιακής Συνέχειας (Business Continuity Plan) για την ανάκαμψη των λειτουργιών σε περίπτωση κρίσης. Τέλος, το Κεφάλαιο 6 ανακεφαλαιώνει τα ευρήματα της μελέτης, αναδεικνύοντας την αδιαμφισβήτητη αξία της συστηματικής ανάλυσης κινδύνου και της χρήσης εργαλείων όπως το MONARC στη σύγχρονη ναυτιλιακή βιομηχανία.

1 Πρότυπα, Μεθοδολογίες και Εργαλεία Ανάλυσης Επικινδυνότητας

1.1 Το Διεθνές και Ευρωπαϊκό Ναυτιλιακό Πλαίσιο: Ανάλυση των Κανονιστικών και Νομικών Απαιτήσεων

Η ραγδαία ψηφιοποίηση της παγκόσμιας ναυτιλίας και η αυξανόμενη αλληλεξάρτηση μεταξύ των συστημάτων πληροφορικής (Information Technology - IT) και των επιχειρησιακών τεχνολογιών (Operational Technology - OT) κατέστησαν επιβεβλημένη τη θέσπιση ενός αυστηρού κανονιστικού και νομικού πλαισίου. Το σύγχρονο θαλάσσιο οικοσύστημα δεν περιορίζεται πλέον στη φυσική ασφάλεια των πλοίων και των λιμένων, αλλά απαιτεί την ολιστική θωράκιση των ψηφιακών υποδομών και των δικτύων επικοινωνίας από κακόβουλες ενέργειες. Στο πλαίσιο αυτό, διεθνείς οργανισμοί, ρυθμιστικές αρχές και νηογνώμονες έχουν αναπτύξει ένα πολυεπίπεδο σύστημα οδηγιών, κανονισμών και βέλτιστων πρακτικών (Best Practices), το οποίο καθορίζει τις ελάχιστες απαιτήσεις κυβερνοανθεκτικότητας για τη διεπαφή πλοίου-λιμένα (Ship-to-Shore interface).

1.1.1 Η Θεσμική Θεμελίωση από τον IMO και η Μετάβαση του Κώδικα ISPS

Η θεμελιώδης στροφή προς την υποχρεωτική διαχείριση των κυβερνοκινδύνων σε διεθνές επίπεδο πραγματοποιήθηκε από τον Διεθνή Ναυτιλιακό Οργανισμό (International Maritime Organization - IMO). Με την έκδοση της εγκυκλίου *MSC-FAL.1/Circ.3*, ο IMO παρείχε τις πρώτες υψηλού επιπέδου κατευθυντήριες γραμμές για την προστασία των ναυτιλιακών υποδομών —ένα ζωντανό έγγραφο το οποίο έχει αναθεωρηθεί επανειλημμένα, φτάνοντας στην 3η αναθεώρησή του (Rev.3), ώστε να ανταποκρίνεται στο μεταβαλλόμενο τοπίο των απειλών (IMO, 2025). Μάλιστα, η συγκεκριμένη αναθεώρηση εναρμονίζει τα λειτουργικά της στοιχεία με το ανανεωμένο πρότυπο NIST Cybersecurity Framework 2.0, ενσωματώνοντας για πρώτη φορά την κρίσιμη λειτουργία της «Διακυβέρνησης» (Govern) δίπλα στους πέντε παραδοσιακούς πυλώνες (Identify, Protect, Detect, Respond, Recover). Ωστόσο, το καθοριστικό κανονιστικό βήμα επιτελέστηκε με την υιοθέτηση της Απόφασης *Resolution MSC.428(98)* τον Ιούνιο του 2017, η οποία κατέστησε νομικά δεσμευτική την ενσωμάτωση της διαχείρισης των κυβερνοκινδύνων (Maritime Cyber Risk Management) στα Συστήματα Διαχείρισης Ασφάλειας (Safety Management Systems - SMS) των ναυτιλιακών εταιρειών, στο πλαίσιο του Διεθνούς Κώδικα Ασφαλούς Διαχείρισης (ISM Code), με καταληκτική ημερομηνία εφαρμογής την 1η Ιανουαρίου 2021 (IMO, 2017). Η απόφαση αυτή μετέβαλε ριζικά το κλίμα συμμόρφωσης, μετατρέποντας την κυβερνοασφάλεια από προαιρετική καλή πρακτική σε προϋπόθεση για την αξιοπιστία και την εμπορική λειτουργία του πλοίου.

Παράλληλα, καθοριστικός είναι ο ρόλος του Διεθνούς Κώδικα για την Ασφάλεια Πλοίων και Λιμενικών Εγκαταστάσεων (International Ship and Port Facility Security Code - ISPS Code), ο οποίος υιοθετήθηκε τυπικά τον Δεκέμβριο του 2002 ως τροποποίηση της σύμβασης SOLAS και

τέθηκε σε πλήρη ισχύ την 1η Ιουλίου 2004, ως απόκριση στις συμβατικές απειλές φυσικής τρομοκρατίας (IMO, 2004). Στη σύγχρονη εποχή, το πεδίο εφαρμογής του Κώδικα ISPS έχει διευρυνθεί, αναγνωρίζοντας ότι η παράλυση μιας λιμενικής εγκατάστασης μέσω ψηφιακής επίθεσης επιφέρει ισοδύναμες ή και σοβαρότερες επιπτώσεις από μια φυσική δολιοφθορά. Σε ευρωπαϊκό επίπεδο, η νομική ενσωμάτωση του Κώδικα ISPS υλοποιήθηκε μέσω του *Κανονισμού (ΕΚ) 725/2004*, ο οποίος αφορά την ενίσχυση της ασφάλειας των πλοίων και των λιμενικών εγκαταστάσεων, και συμπληρώθηκε με την *Οδηγία 2005/65/ΕΚ*, που επεκτείνει τα μέτρα ασφάλειας σε ολόκληρη τη λιμενική ζώνη (European Parliament and Council, 2004; 2005). Είναι αξιοσημείωτο ότι ο Κανονισμός 725/2004 προβλέπει ρητά πως οι Εκτιμήσεις Ασφάλειας Λιμενικής Εγκατάστασης (Port Facility Security Assessments - PFSA) οφείλουν να συνεκτιμούν την ακεραιότητα των υπολογιστικών συστημάτων και των δικτύων επικοινωνίας. Εντούτοις, λόγω του αρχικού προσανατολισμού στη φυσική ασφάλεια, η Ευρωπαϊκή Επιτροπή, μέσα από πρόσφατη έκθεσή της, αναγνώρισε την επιτακτική ανάγκη ανάπτυξης εξειδικευμένης καθοδήγησης που θα αποσαφηνίζει τις νομοθετικές απαιτήσεις του πλαισίου ISPS όσον αφορά την ασφάλεια των συστημάτων πληροφοριών στα λιμάνια, προετοιμάζοντας το έδαφος για τη σύγκλιση με το νεότερο αυστηρό δίκαιο κυβερνοασφάλειας (European Commission, 2024).

1.1.2 Βέλτιστες Πρακτικές της Βιομηχανίας και Απαιτήσεις Νηογνωμόνων (BIMCO & IACS)

Ενώ ο IMO και η ΕΕ θέτουν το γενικό νομικό περίγραμμα, η εξειδίκευση των τεχνικών και επιχειρησιακών μέτρων προστασίας καθοδηγείται από τις πρωτοβουλίες της διεθνούς ναυτιλιακής βιομηχανίας. Ο Διεθνής Ναυτιλιακός Οργανισμός BIMCO, σε συνεργασία με κορυφαίους φορείς του κλάδου (όπως οι DCSA, ICS, INTERCARGO, INTERTANKO, OCIMF και IUMI), εκδίδει και ανανεώνει διαρκώς τον οδηγό *The Guidelines on Cyber Security Onboard Ships*, με την 5η και πιο πρόσφατη έκδοση (Version 5) να δημοσιεύεται στις **14 Νοεμβρίου 2024** (BIMCO et al., 2024). Ο εν λόγω οδηγός αποτελεί το απόλυτα επικαιροποιημένο πρότυπο αναφοράς για την εφαρμογή βέλτιστων πρακτικών, εστιάζοντας στην προστασία τόσο των συστημάτων IT (email, ναυτιλιακά λογισμικά) όσο και των κρίσιμων συστημάτων OT (ECDIS, συστήματα πρόωσης, διαχείριση φορτίου). Η μεθοδολογία της BIMCO δίνει ιδιαίτερη βαρύτητα στη διαχείριση του ανθρώπινου παράγοντα, στην ασφάλεια της εφοδιαστικής αλυσίδας (Supply Chain Security) και στη διασφάλιση της διεπαφής κατά τη σύνδεση του πλοίου με τα λιμενικά πληροφοριακά συστήματα (Port Community Systems - PCS).

Σε τεχνικό επίπεδο, η μετάβαση από τις εθελοντικές βέλτιστες πρακτικές στις υποχρεωτικές προδιαγραφές κατασκευής και επιθεώρησης υλοποιήθηκε από τη Διεθνή Ένωση Νηογνωμόνων (International Association of Classification Societies - IACS). Το 2022 η IACS υιοθέτησε τις αρχικές προδιαγραφές για την κυβερνοασφάλεια, οι οποίες όμως αναθεωρήθηκαν ουσιαστικά μέσα στο 2023 έπειτα από εκτενή ανατροφοδότηση της βιομηχανίας (με τις αρχικές να αποσύρονται). Οι τελικές, αναθεωρημένες Ενιαίες Απαιτήσεις *UR E26* («Cyber resilience of ships») και *UR E27* («Cyber resilience of on-board systems and equipment») κατέστησαν υποχρεωτικές για όλα τα νέα συμβασιοποιούμενα πλοία από την **1η Ιουλίου 2024** (IACS, 2023a; 2023b). Η απαίτηση *UR E26* στοχεύει στην ασφαλή ενσωμάτωση των συστημάτων OT και IT στο δίκτυο του πλοίου, καλύπτοντας πέντε πυλώνες: αναγνώριση εξοπλισμού, προστασία, ανίχνευση, απόκριση και ανάκαμψη. Αντίστοιχα, η *UR E27* επιβάλλει αυστηρούς ελέγχους ακεραιότητας στους προμηθευτές ναυτιλιακού εξοπλισμού τρίτων (Third-party equipment suppliers). Για να εφαρμόσουν αυτές τις απαιτήσεις στην πράξη, κορυφαίοι νηογνώμονες ανέπτυξαν εξειδικευμένες σημάνσεις κλάσης (Class Notations). Χαρακτηριστικό παράδειγμα αποτελεί ο νηογνώμονας DNV με την υποχρεωτική σήμανση **DNV Cyber Secure (Essential)**, η οποία πιστοποιεί ότι το πλοίο και τα διασυνδεδεμένα συστήματά του συμμορφώνονται πλήρως με τις προδιαγραφές των *UR E26* και *E27*, μετατρέποντας τη θεωρητική ανθεκτικότητα σε ελεγχόμενο αντικείμενο επιθεώρησης (DNV, 2024).

1.1.3 Σύγχρονες Ευρωπαϊκές & Διεθνείς Ρυθμίσεις: NIS2, N. 5160/2024 και USCG Final Rule

Η ολοκλήρωση του σύγχρονου κανονιστικού ψηφιδωτού για τις λιμενικές υποδομές πραγματοποιείται μέσα από τη σύγκλιση του Ευρωπαϊκού και του Αμερικανικού δικαίου, που θέτουν στο επίκεντρο τις κρίσιμες υποδομές. Στον ευρωπαϊκό χώρο, το σημείο καμπής αποτελεί η Οδηγία (ΕΕ) 2022/2555, γνωστή ως **NIS2 Directive**, η οποία αντικατέστησε την παλαιότερη Οδηγία NIS, στοχεύοντας στην επίτευξη υψηλού, κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση (European Parliament and Council, 2022). Η Οδηγία NIS2 εντάσσει ρητά τον τομέα των θαλάσσιων και λιμενικών μεταφορών στις «**Ουσιώδεις Οντότητες**» (**Essential Entities**) υψηλής κρίσιμότητας. Στην Ελληνική έννομη τάξη, η ενσωμάτωση της NIS2 ολοκληρώθηκε με τη ψήφιση του **Νόμου 5160/2024** τον Νοέμβριο του 2024 (Εφημερίδα της Κυβερνήσεως, 2024). Ο ελληνικός νόμος επιβάλλει στους φορείς διαχείρισης λιμένων (π.χ. Οργανισμοί Λιμένων, Terminal Operators) την υποχρεωτική εφαρμογή μέτρων διαχείρισης κινδύνου για συστήματα IT και OT και τη συνεχή παρακολούθηση της εφοδιαστικής αλυσίδας. Ιδιαίτερης αυστηρότητας είναι το **τριστάδιο χρονοδιάγραμμα αναφοράς** περιστατικών που προβλέπει (Άρθρο 23 της NIS2): απαιτείται έγκαιρη προειδοποίηση (early warning) εντός 24 ωρών, επίσημη ειδοποίηση περιστατικού εντός 72 ωρών και υποβολή τελικής αναφοράς εντός ενός μηνός στην Εθνική Αρχή Κυβερνοασφάλειας. Παράλληλα, θεσπίζει βαρύτατες οικονομικές κυρώσεις και άμεση διοικητική ευθύνη για τα ανώτατα διοικητικά στελέχη σε περίπτωση μη συμμόρφωσης.

Η παγκόσμια σύγκλιση προς αυτή την αυστηρή ρυθμιστική κατεύθυνση επιβεβαιώνεται από τις πρόσφατες εξελίξεις στις Ηνωμένες Πολιτείες. Στις **17 Ιανουαρίου 2025**, η Αμερικανική Ακτοφυλακή (U.S. Coast Guard - USCG) δημοσίευσε τον οριστικό κανονισμό (Final Rule) με τίτλο «*Cybersecurity in the Marine Transportation System*», ο οποίος τίθεται σε πλήρη ισχύ την 16η Ιουλίου 2025 (USCG, 2025). Ο κανονισμός θεσπίζει υποχρεωτικές ελάχιστες απαιτήσεις κυβερνοασφάλειας όχι μόνο για τα πλοία αμερικανικής σημαίας, αλλά και για τις χερσαίες και λιμενικές εγκαταστάσεις που υπάγονται στο Νόμο περί Ασφάλειας Θαλάσσιων Μεταφορών (MTSA), καθιστώντας υποχρεωτική την αναφορά περιστατικών στο Εθνικό Κέντρο Απόκρισης (National Response Center).

Ιδιαίτερης σημασίας για τη μοντελοποίηση κινδύνου σε τερματικούς σταθμούς εμπορευματοκιβωτίων (Container Terminals) αποτελεί η έκδοση της οδηγίας **MARSEC Directive 105-4**. Η συγκεκριμένη οδηγία εστιάζει ρητά και αποκλειστικά στον κυβερνοκίνδυνο που προέρχεται από γερανογέφυρες ξηράς-πλοίου (Ship-to-Shore / STS Cranes) **κατασκευασμένες από εταιρείες της Λαϊκής Δημοκρατίας της Κίνας (PRC)**. Δεδομένου ότι οι κινεζικής κατασκευής γερανογέφυρες αντιπροσωπεύουν σχεδόν το 80% της παγκόσμιας αγοράς, οι αρμόδιες αρχές αναγνώρισαν τον κρίσιμο γεωπολιτικό κίνδυνο της εφοδιαστικής αλυσίδας και την ύπαρξη ευπαθειών που σχετίζονται με δυνατότητες απομακρυσμένου ελέγχου και προγραμματισμού τους. Καθώς το πλήρες κείμενο της οδηγίας περιέχει διαβαθμισμένο υλικό ασφάλειας (Sensitive Security Information - SSI) και δεν διατίθεται στο δημόσιο, η επιβολή των μέτρων γνωστοποιήθηκε μέσω επίσημης ανακοίνωσης στο Ομοσπονδιακό Μητρώο των ΗΠΑ (USCG, 2024a). Μάλιστα, τον Νοέμβριο του 2024, η Ακτοφυλακή εξέδωσε τη συμπληρωματική οδηγία **MARSEC Directive 105-5**, εντείνοντας περαιτέρω τις απαιτήσεις θωράκισης για τον λιμενικό εξοπλισμό OT (USCG, 2024b).

Συνοψίζοντας, το σύγχρονο διεθνές ναυτιλιακό πλαίσιο διαμορφώνει ένα αυστηρό, αλληλοσυμπληρούμενο περιβάλλον όπου οι οδηγίες του IMO και της BIMCO συνδυάζονται με τους τεχνικούς ελέγχους των νηογνωμόνων (IACS UR E26/E27) και τις δεσμευτικές επιταγές εθνικών και περιφερειακών νόμων (NIS2 / N. 5160/2024, USCG Final Rule). Η γνώση και η συμμόρφωση με το πλαίσιο αυτό αποτελεί το απαραίτητο πρώτο βήμα για τη συστηματική αξιολόγηση και θωράκιση κάθε σύγχρονης λιμενικής υποδομής.

1.2 Μεθοδολογικές Προσεγγίσεις Διαχείρισης Κινδύνου IT και OT: Τα Πρότυπα ISO 27005, IEC 62443 και οι Οδηγίες του ENISA

Η αποτελεσματική θωράκιση μιας σύγχρονης λιμενικής υποδομής απαιτεί την υιοθέτηση μιας δομημένης μεθοδολογίας διαχείρισης κινδύνου, ικανής να γεφυρώσει το χάσμα μεταξύ των κλασικών συστημάτων πληροφορικής (Information Technology - IT) και των επιχειρησιακών τεχνολογιών ελέγχου (Operational Technology - OT). Η εγγενής πολυπλοκότητα των τερματικών σταθμών εμπορευματοκιβωτίων καθιστά ανεπαρκή τη χρήση μιας μονοδιάστατης προσέγγισης. Ως εκ τούτου, η παρούσα μελέτη στηρίζεται σε ένα τριγωνικό μεθοδολογικό πλαίσιο, το οποίο συνθέτει το διεθνές πρότυπο ISO/IEC 27005 για την ασφάλεια πληροφοριών, τη σειρά προτύπων IEC 62443 και NIST SP 800-82 Rev. 3 για τα βιομηχανικά συστήματα και τις εξειδικευμένες κατευθυντήριες οδηγίες του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA) για το ναυτιλιακό και λιμενικό οικοσύστημα.

1.2.1 Το Πρότυπο ISO/IEC 27005: Μεθοδολογική Θεμελίωση Διαχείρισης Κινδύνων IT

Ο θεμέλιος λίθος της μεθοδολογικής μας διαδρομής αντλείται από το διεθνές πρότυπο *ISO/IEC 27005:2022*, το οποίο παρέχει κατευθυντήριες οδηγίες για τη διαχείριση κινδύνων ασφάλειας πληροφοριών, εναρμονισμένες με τις απαιτήσεις του ISO/IEC 27001 (ISO/IEC 27005, 2022). Η μεθοδολογία του ISO 27005 δεν επιβάλλει μια άκαμπτη διαδικασία, αλλά ορίζει ένα διαδραστικό, κυκλικό μοντέλο που απαρτίζεται από διακριτά στάδια: τον Προσδιορισμό του Πλαισίου (Context Establishment), την Εκτίμηση Κινδύνου (Risk Assessment) —η οποία υποδιαιρείται στην Αναγνώριση (Identification), την Ανάλυση (Analysis) και την Αξιολόγηση (Evaluation) του ρίσκου— και, τέλος, την Αντιμετώπιση του Κινδύνου (Risk Treatment). Η τελευταία αναθεώρηση του προτύπου (έκδοση 2022) εισάγει παράλληλα με την παραδοσιακή προσέγγιση που βασίζεται στα αγαθά (asset-based approach) και την προσέγγιση που βασίζεται σε γεγονότα (event-based approach), επιτρέποντας την ευέλικτη μοντελοποίηση σύνθετων σεναρίων επίθεσης.

Η επιλογή του ISO 27005 ως κεντρικού άξονα της παρούσας εργασίας κάθε άλλο παρά τυχαία είναι. Το εν λόγω πρότυπο αποτελεί την αλγοριθμική και λογική ραχοκοκαλιά του ανοιχτού κώδικα λογισμικού **MONARC**, το οποίο αποτελεί το κεντρικό εργαλείο μοντελοποίησης στα επόμενα κεφάλαια της πτυχιικής. Μέσω της αυστηρής ονοματολογίας του ISO 27005, τα κρίσιμα περιουσιακά στοιχεία (πρωτεύοντα και δευτερεύοντα αγαθά) ενός λιμένα συσχετίζονται με συγκεκριμένες απειλές και ευπάθειες, επιτρέποντας τον ακριβή υπολογισμό του διαλειπόμενου κινδύνου. Ωστόσο, ενώ το ISO 27005 υπερέχει στην ανάλυση του διοικητικού και διακομιστικού περιβάλλοντος IT (όπως οι βάσεις δεδομένων, τα συστήματα ERP και το εταιρικό δίκτυο), η αμιγής εφαρμογή του σε περιβάλλοντα βιομηχανικού αυτοματισμού παρουσιάζει δομικούς περιορισμούς, καθιστώντας αναγκαία την ενσωμάτωση προτύπων ειδικού σκοπού για το OT.

1.2.2 Η Ιδιαιτερότητα του OT: Τα Πρότυπα IEC 62443 και NIST SP 800-82 Rev. 3

Η θεμελιώδης διαφοροποίηση μεταξύ των περιβαλλόντων IT και OT έγκειται στην αντιστροφή των προτεραιοτήτων ασφάλειας. Στο κλασικό IT, η ιεράρχηση διέπεται από την παραδοσιακή τριάδα CIA, με απόλυτη προτεραιότητα στην Εμπιστευτικότητα (Confidentiality), ακολουθούμενη από την Ακεραιότητα (Integrity) και τη Διαθεσιμότητα (Availability). Αντιθέτως, στις Επιχειρησιακές Τεχνολογίες ενός λιμένα (όπως οι γερανογέφυρες STS και RTG, τα προγραμματιζόμενα λογικά ρελέ - PLCs και τα συστήματα SCADA), η τριάδα αντιστρέφεται σε **AIC/Safety**. Η απόλυτη και αδιαπραγμάτευτη προτεραιότητα είναι η Διαθεσιμότητα και η Ασφάλεια της ανθρώπινης ζωής και του εξοπλισμού (Safety), καθώς μια ενδεχόμενη κυβερνοεπίθεση που διακόπτει τη λειτουργία ενός βιομηχανικού ελεγκτή επιφέρει άμεσες φυσικές και καταστροφικές συνέπειες.

Για την αποτελεσματική διαχείριση αυτών των ιδιαιτεροτήτων, η μεθοδολογία μας συμπληρώνεται από τη σειρά προτύπων *IEC 62443*, η οποία αποτελεί το διεθνές de facto πλαίσιο για την ασφάλεια Βιομηχανικών Συστημάτων Αυτοματισμού και Ελέγχου (IACS). Ειδικότερα, το μέρος *IEC 62443-3-2* εισάγει τις κρίσιμες έννοιες των «**Ζωνών και Αγωγών**» (**Zones and Conduits**), επιτρέποντας τη λογική τμηματοποίηση του λιμενικού δικτύου σε αυτόνομες ζώνες με βάση την κρίσιμότητα των λειτουργιών τους (IEC, 2020). Παράλληλα, καθορίζει τα Επίπεδα Ασφάλειας (Security Levels - SL 0 έως 4), τα οποία ορίζουν τον βαθμό θωράκισης έναντι διαφορετικών προφίλ επιτιθέμενων. Την αρχιτεκτονική αυτή έρχεται να ενισχύσει η

επικαιροποιημένη οδηγία *NIST SP 800-82 Rev. 3* («Guide to Operational Technology Security»), η οποία δημοσιεύτηκε τον Σεπτέμβριο του 2023 (NIST, 2023). Το πρότυπο του NIST αναγνωρίζει ρητά το φαινόμενο της σύγκλισης IT/OT (IT/OT Convergence) στα σύγχρονα λιμάνια, όπου τα παραδοσιακά απομονωμένα δίκτυα διασυνδέονται πλέον με το Cloud. Για την αντιμετώπιση του ρίσκου, προτείνει μια κατηγοριοποίηση κινδύνου βάσει συνεπειών (consequence-based risk assessment), η οποία αξιολογεί τον αντίκτυπο στη φυσική διαδικασία και στο περιβάλλον, συμπληρώνοντας αρμονικά την ποσοτική και ποιοτική ανάλυση του ISO 27005.

1.2.3 Κατευθυντήριες Οδηγίες ENISA για Λιμένες και η Σύγκλιση IT/OT

Ο τρίτος πυλώνας της θεμελίωσής μας μεταφέρει τις παραπάνω μεθοδολογίες από το γενικό θεωρητικό επίπεδο στην πραγματικότητα του θαλάσσιου τομέα, αντλώντας καθοδήγηση από τις εκθέσεις του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA). Η αφετηρία δίνεται με τη θεμελιώδη έκθεση «*Port Cybersecurity*», η οποία χαρτογραφεί το λιμενικό οικοσύστημα, ταυτοποιώντας τις κρίσιμες διεπαφές και τα συστήματα που αποτελούν πιθανούς στόχους, με έμφαση στα Λιμενικά Πληροφοριακά Συστήματα (Port Community Systems - PCS) (ENISA, 2019). Ωστόσο, καθοριστικής σημασίας για την παρούσα πτυχιακή εργασία αποτελεί η εξειδικευμένη έκθεση «*Cyber Risk Management for Ports*» (ENISA, 2020). Στο έγγραφο αυτό, ο ENISA προβαίνει σε μια κρίσιμη διαπίστωση: **δεν υπάρχει μία ενιαία, τυποποιημένη ή υποχρεωτική μεθοδολογία** για την αξιολόγηση του κυβερνοκινδύνου που να εφαρμόζεται καθολικά από τους λιμενικούς φορείς της Ευρωπαϊκής Ένωσης.

Αυτή η επίσημη διαπίστωση του ευρωπαϊκού οργάνου αναδεικνύει το υφιστάμενο μεθοδολογικό κενό και προσδίδει άμεση ακαδημαϊκή και πρακτική αξία στον σκοπό της εργασίας μας. Η υιοθέτηση και προσαρμογή της μεθοδολογίας ISO 27005 μέσω του εργαλείου MONARC, σε συνδυασμό με τις αρχές του IEC 62443 για το βιομηχανικό OT, έρχεται να προτείνει ένα δομημένο, επαναληψίμο και τυποποιημένο μοντέλο ανάλυσης κινδύνου για τα Container Terminals, απαντώντας ρητά στην ανάγκη που εντόπισε ο ENISA. Η επιτακτικότητα αυτής της ολοκληρωμένης προσέγγισης υπογραμμίζεται από τα πιο πρόσφατα ερευνητικά δεδομένα του *ENISA Threat Landscape*, σύμφωνα με τα οποία οι επιθέσεις που στοχεύουν ή επηρεάζουν άμεσα την Επιχειρησιακή Τεχνολογία (OT) αντιπροσωπεύουν πλέον περισσότερο από το 18% των καταγεγραμμένων περιστατικών σε κρίσιμες υποδομές (ENISA, 2025). Η διαπίστωση αυτή επιβεβαιώνει ότι η ασφάλεια των λιμένων δεν μπορεί να επιτευχθεί με μεμονωμένα μέτρα IT, αλλά απαιτεί την ολιστική, μεθοδολογική σύγκλιση όλων των διασυνδεδεμένων ψηφιακών και βιομηχανικών αγαθών του οργανισμού.

1.3 Εισαγωγή στα Εργαλεία και τις Μεθοδολογίες Αξιολόγησης Κινδύνων: Κατηγοριοποίηση, Σύγχρονα Πλαίσια και η Επιλογή του MONARC

Η μετάβαση από το θεωρητικό και ρυθμιστικό πλαίσιο στην πρακτική διαχείριση της κυβερνοασφάλειας προϋποθέτει την αξιοποίηση εξειδικευμένων εργαλείων και μεθοδολογιών αξιολόγησης κινδύνων (Risk Assessment Tools). Στο σύγχρονο θαλάσσιο και λιμενικό περιβάλλον, όπου ο όγκος των δεδομένων και η πολυπλοκότητα της διασύνδεσης IT και OT αυξάνονται εκθετικά, η χειροκίνητη εκτίμηση καθίσταται αναξιόπιστη. Η διεθνής κοινότητα έχει αναπτύξει πληθώρα προτύπων και λογισμικών, το καθένα από τα οποία προσεγγίζει τη μοντελοποίηση των απειλών από διαφορετική οπτική γωνία. Η κριτική ανάλυση αυτών των εργαλείων και η σωστή κατηγοριοποίησή τους αποτελούν το θεμέλιο για την επιλογή του καταλληλότερου μοντέλου εφαρμογής στις κρίσιμες λιμενικές υποδομές.

1.3.1 Κατηγοριοποίηση Μεθοδολογιών και το Ελεγκτικό Πρίσμα του EMSA

Τα εργαλεία και οι μεθοδολογίες εκτίμησης κινδύνου κατατάσσονται ευρέως σε τρεις βασικές κατηγορίες, ανάλογα με τον τρόπο επεξεργασίας των δεδομένων και την εξαγωγή των αποτελεσμάτων:

- **Ποιοτικές Μεθοδολογίες (Qualitative Approaches):** Βασίζονται στην περιγραφική αξιολόγηση της πιθανότητας εκδήλωσης μιας απειλής και της αναμενόμενης επίπτωσής της, χρησιμοποιώντας κλίμακες ταξινόμησης (π.χ. Χαμηλή, Μέση, Υψηλή, Κρίσιμη). Πλεονεκτούν στην ταχύτητα εφαρμογής και στην ευκολία κατανόησης από τη διοίκηση, αλλά υστερούν σε μαθηματική ακρίβεια.
- **Ποσοτικές Μεθοδολογίες (Quantitative Approaches):** Αξιοποιούν μαθηματικά, στατιστικά μοντέλα και χρηματοοικονομικούς δείκτες για να αποδώσουν ακριβείς αριθμητικές ή νομισματικές τιμές στον κίνδυνο (π.χ. υπολογισμός Ετήσιας Αναμενόμενης Ζημίας - ALE). Παρότι προσφέρουν αντικειμενικότητα, απαιτούν τεράστιο όγκο ιστορικών δεδομένων, τα οποία συχνά απουσιάζουν στον νεοσύστατο τομέα των ναυτιλιακών κυβερνοεπιθέσεων.
- **Υβριδικές / Ημι-ποσοτικές Μεθοδολογίες (Hybrid / Semi-quantitative Approaches):** Συνδυάζουν την ευελιξία της ποιοτικής προσέγγισης με σταθμισμένες αριθμητικές κλίμακες και αλγορίθμους προτεραιοποίησης. Η προσεγγιστική αυτή ιεράρχηση επιτρέπει τη ρεαλιστική μοντελοποίηση σύνθετων συστημάτων χωρίς την ανάγκη απόλυτων στατιστικών καταγραφών.

Στο ναυτιλιακό πεδίο, ο Ευρωπαϊκός Οργανισμός Για την Ασφάλεια στη Θάλασσα (**EMSA**) καθορίζει τις απαιτήσεις που πρέπει να πληρούν τα συστήματα διαχείρισης κινδύνου μέσα από το ελεγκτικό και επιθεωρητικό του πλαίσιο. Με την έκδοση της επίσημης οδηγίας *Doc. 9209* τον Νοέμβριο του 2023, ο EMSA παρέχει κατευθύνσεις για το πώς πρέπει να ελέγχεται η κυβερνοασφάλεια κατά τη διάρκεια των επιθεωρήσεων (audits, controls, verifications and inspections) (EMSA, 2023). Μέσα από αυτό το ελεγκτικό πρίσμα, ο Οργανισμός υπογραμμίζει ότι οποιοδήποτε εργαλείο αξιολόγησης κινδύνου επιλεγεί, δεν επιτρέπεται να περιορίζεται στον τεχνολογικό εξοπλισμό, αλλά οφείλει να ενσωματώνει πλήρως τον **ανθρώπινο παράγοντα (Human Element)**, τις διαδικασίες εκπαίδευσης και την ετοιμότητα μέσω τακτικών ασκήσεων (drills). Επιπλέον, καθιστά σαφές ότι η εκτίμηση κινδύνου πρέπει να είναι οργανικά δεμένη με το Σύστημα Διαχείρισης Ασφάλειας (SMS), διασφαλίζοντας ότι η θωράκιση του IT και του OT ελέγχεται με γνώμονα τη διατήρηση της επιχειρησιακής συνέχειας και της ασφάλειας στη θάλασσα.

1.3.2 Σύγχρονα Διεθνή Πλαίσια και Εργαλεία: NIST CSF 2.0, CSET, FAIR και EBIOS RM

Στο διεθνές στερέωμα, ξεχωρίζουν τέσσερις κορυφαίες μεθοδολογίες και εργαλεία, τα οποία αντιπροσωπεύουν τις σύγχρονες τάσεις της βιομηχανίας:

1. **NIST Cybersecurity Framework (CSF) 2.0:** Η αναθεωρημένη έκδοση του αμερικανικού πλαισίου (NIST CSWP 29), η οποία δημοσιεύτηκε στις **26 Φεβρουαρίου 2024**, αποτελεί το πλέον αναγνωρίσιμο ταξινομικό μοντέλο υψηλού επιπέδου παγκοσμίως (NIST, 2024). Το **NIST CSF 2.0** διεύρυνε το πεδίο εφαρμογής του σε όλους τους κλάδους και εισήγαγε τη θεμελιώδη λειτουργία της **«Διακυβέρνησης» (Govern)** δίπλα στις πέντε παραδοσιακές λειτουργίες (Identify, Protect, Detect, Respond, Recover), αναδεικνύοντας τη διαχείριση κινδύνου σε στρατηγικό εταιρικό ζήτημα.
2. **CSET (Cyber Security Evaluation Tool):** Ανεπτυγμένο από την Υπηρεσία Κυβερνοασφάλειας και Ασφάλειας Υποδομών των ΗΠΑ (CISA), το CSET είναι ένα επιτραπέζιο εργαλείο λογισμικού που εστιάζει στην αξιολόγηση βιομηχανικών συστημάτων ελέγχου (ICS/SCADA) και OT υποδομών (CISA, 2024). Λειτουργεί βάσει δομημένων ερωτηματολογίων συμμόρφωσης με πρότυπα όπως το IEC 62443 και το NIST SP 800-82, προσφέροντας άμεση απεικόνιση των κενών ασφάλειας ενός βιομηχανικού δικτύου.
3. **FAIR (Factor Analysis of Information Risk):** Αποτελεί το κορυφαίο διεθνές πρότυπο για την **ποσοτική χρηματοοικονομική ανάλυση** του κυβερνοκινδύνου (FAIR Institute, 2023). Η μεθοδολογία FAIR αποδομεί τον κίνδυνο σε συγκεκριμένους παράγοντες συχνότητας συμβάντων και πιθανού νομισματικού κόστους, επιτρέποντας στους οργανισμούς να υπολογίσουν με ακρίβεια το Return on Security Investment (ROSI).
4. **EBIOS Risk Manager (EBIOS RM):** Η επίσημη μεθοδολογία της Εθνικής Υπηρεσίας Ασφάλειας Πληροφοριακών Συστημάτων της Γαλλίας (ANSSI). Το EBIOS RM υιοθετεί μια καινοτόμο προσέγγιση βασισμένη σε σενάρια απειλών (scenario-based) και στο οικοσύστημα

του οργανισμού, εστιάζοντας στον εντοπισμό στοχευμένων επιθέσεων από προηγμένους δρώντες (Advanced Persistent Threats - APTs). Ιδιαίτερης σημασίας αποτελεί η επικαιροποίηση της μεθοδολογίας τον Μάρτιο του 2024, η οποία πραγματοποιήθηκε με σκοπό την πλήρη ευθυγράμμισή της με το νέο πρότυπο *ISO/IEC 27005:2022* (ANSSI, 2024). Το εύρημα αυτό αποδεικνύει την παγκόσμια τάση σύγκλισης των σύγχρονων εργαλείων γύρω από τη μεθοδολογική ραχοκοκαλιά του ISO 27005.

1.3.3 Η Στρατηγική Επιλογή του Ανοιχτού Λογισμικού MONARC ως Κεντρικού Εργαλείου

Παρά την αδιαμφισβήτητη αξία των προαναφερθέντων εργαλείων, η εφαρμογή τους σε μια σύνθετη λιμενική εγκατάσταση εμπορευματοκιβωτίων (Container Terminal) με διασυνδεδεμένα Πληροφοριακά Συστήματα Λιμένα (PCS), αυτοματοποιημένες γερανογέφυρες και δίκτυα SCADA, παρουσιάζει πρακτικούς και μεθοδολογικούς περιορισμούς. Το μεν CSET λειτουργεί πρωτίστως ως λίστα ελέγχου συμμόρφωσης (compliance checklist) χωρίς δυνατότητα δυναμικής συσχέτισης εξαρτήσεων μεταξύ αγαθών, το δε FAIR απαιτεί πλούσια ιστορικά οικονομικά δεδομένα για λιμενικά κυβερνοπεριστατικά, τα οποία είναι ανύπαρκτα στον κλάδο, ενώ εμπορικά εργαλεία επιβάλλουν υπέρογκα κόστη αδειοδότησης και «κλειστούς» αλγόριθμους.

Για την οπτική κωδικοποίηση και τη συγκριτική αξιολόγηση των χαρακτηριστικών τους έναντι των απαιτήσεων της παρούσας έρευνας, παρατίθεται ο **Πίνακας 1.1**, ο οποίος αναδεικνύει σαφώς την ανάγκη για ένα ανοιχτό, υβριδικό εργαλείο μοντελοποίησης.

Πίνακας 1.1: Συγκριτική Αξιολόγηση Πλαισίων και Εργαλείων Διαχείρισης Κινδύνου για Λιμενικές Υποδομές. Πηγή: Ιδία επεξεργασία.

Πλαίσιο / Εργαλείο	Τύπος Μεθοδολογίας	Κύριο Πεδίο Εφαρμογής	Απαιτήσεις Δεδομένων	Άδεια & Κόστος	Κρίσιμος Περιορισμός για Container Terminals
NIST CSF 2.0	Ποιοτικό / Ταξινομικό	Γενικό (IT / OT / Corporate)	Χαμηλές (περιγραφική στοχοθέτηση)	Ανοιχτό / Δωρεάν (πρότυπο αναφοράς)	Πλαίσιο διακυβέρνησης υψηλού επιπέδου — δεν παρέχει αλγόριθμο υπολογισμού διαλειπόμενου ρίσκου
CISA CSET	Ποιοτικό / Compliance	OT / ICS / SCADA (με στοιχεία IT)	Μέτριες (δομημένα ερωτηματολόγια)	Ανοιχτό / Δωρεάν (λογισμικό ΗΠΑ)	Λειτουργεί πρωτίστως ως checklist συμμόρφωσης — απουσία δυναμικής, δενδρικής συσχέτισης κινδύνων
FAIR	Ποσοτικό / Οικονομικό	IT / Financial Risk	Εξαιρετικά υψηλές (ιστορικά στατιστικά δεδομένα)	Ανοιχτό πρότυπο (Open FAIR) / εμπορικά εργαλεία υλοποίησης (π.χ. RiskLens)	Ανύπαρκτα ιστορικά δεδομένα νομισματικού κόστους για εξειδικευμένες επιθέσεις σε λιμενικό OT εξοπλισμό

EBIOS RM (ANSSI)	Scenariobased / Ημιποιοτικό	Γενικό (IT / OT / Supply Chain)	Μέτριες έως υψηλές (ανάλυση APT/απειλών)	Ανοιχτή μεθοδολογία / εμπορικά εργαλεία υλοποίησης	Εξαιρετικό για στοχευμένες επιθέσεις, απαιτεί όμως υψηλή εξειδίκευση και πολύπλοκη υλοποίηση
MONARC (NC3)	Υβριδικό (Ποιοτικό & Ποσοτικό)	Ενιαίο (σύγκλιση IT & OT)	Μέτριες (γνώση εμπειρογνομώνων + πρότυπα)	Ανοιχτού κώδικα (GNU GPL) / Δωρεάν	Απαιτεί αρχική χειροκίνητη παραμετροποίηση δέντρων αγαθών — προσφέρει όμως πλήρη προσαρμογή στο λιμενικό σενάριο

Όπως καθίσταται αυτονόητο από τη συγκριτική σύνθεση του Πίνακα 1.1, η παρούσα διπλωματική εργασία επιλέγει ως κεντρικό εργαλείο μοντελοποίησης και αξιολόγησης κινδύνου το ανοιχτού κώδικα λογισμικό MONARC (Method for an Optimised aNalysis of Risks by CASES) (NC3, 2025). Η επιλογή αυτή τεκμηριώνεται στη βάση τεσσάρων στρατηγικών πλεονεκτημάτων:

1. **Εγγενής Ευθυγράμμιση με το ISO/IEC 27005:** Το MONARC έχει δομηθεί αλγοριθμικά πάνω στα στάδια του ISO 27005:2022. Η ακρίβεια αυτής της επιλογής επιβεβαιώνεται από το γεγονός ότι ακόμη και κορυφαία εθνικά πρότυπα, όπως το EBIOS RM της ΕΕ, αναθεωρήθηκαν πρόσφατα για να συγκλίνουν στο ίδιο ακριβώς διεθνές πρότυπο.
2. **Δενδρική Μοντελοποίηση Αγαθών και Κινδύνων (Asset-to-Risk Trees):** Το λογισμικό επιτρέπει την πλήρη χαρτογράφηση της εξάρτησης μεταξύ πρωτευόντων επιχειρησιακών αγαθών (π.χ. συνεχής εκφόρτωση εμπορευματοκιβωτίων, ακεραιότητα δεδομένων PCS) και δευτερευόντων υποστηρικτικών στοιχείων (π.χ. PLCs γερανογεφυρών, διακομιστές βάσεων δεδομένων, δίκτυα οπτικών ινών).
3. **Υβριδική / Επαναληπτική Αξιολόγηση:** Επιτρέπει τον συνδυασμό ποιοτικών εκτιμήσεων εμπειρογνομώνων με σταθμισμένες κλίμακες επιπτώσεων (Ακεραιότητα, Διαθεσιμότητα, Εμπιστευτικότητα), υπολογίζοντας αυτόματα τον διαλειπόμενο κίνδυνο (residual risk) μετά την εφαρμογή προτεινόμενων μέτρων ελέγχου (security controls).
4. **Ανοιχτή Αρχιτεκτονική και Προσαρμοστικότητα (Open-Source & Flexibility):** Ως λογισμικό ανοιχτού κώδικα (GNU GPL), προσφέρει πλήρη διαφάνεια στον τρόπο υπολογισμού των κινδύνων και επιτρέπει την εισαγωγή προσαρμοσμένων βιβλιοθηκών απειλών (custom threat libraries), προσαρμοσμένων ακριβώς στο υβριδικό IT/OT περιβάλλον ενός σύγχρονου λιμένα εμπορευματοκιβωτίων.

Η ολοκλήρωση της θεωρητικής, θεσμικής και μεθοδολογικής ανασκόπησης στο Κεφάλαιο 1 προετοιμάζει το έδαφος για την πρακτική εφαρμογή. Στα επόμενα κεφάλαια, η αρχιτεκτονική του MONARC θα τεθεί σε λειτουργία για την εκτέλεση ενός ρεαλιστικού σεναρίου ανάλυσης κινδύνου σε τερματικό σταθμό εμπορευματοκιβωτίων, αποδεικνύοντας στην πράξη την αξία της μεθοδολογικής σύνθεσης που καθιερώθηκε.

2 Αρχιτεκτονική Λιμενικών Υποδομών και Αποτίμηση Κινδύνου

2.1 Χαρτογράφηση του Λιμενικού Οικοσυστήματος: Ζώνες IT/OT/Ναυσιπλοΐας και Ανθρώπινος Παράγοντας

Η συστηματική αξιολόγηση των κυβερνοκινδύνων σε μια σύγχρονη ναυτιλιακή και λιμενική εγκατάσταση προϋποθέτει την ακριβή χαρτογράφηση του ψηφιακού και βιομηχανικού της οικοσυστήματος. Η παρούσα μελέτη εστιάζει σε έναν υποθετικό, υψηλής αυτοματοποίησης τερματικό σταθμό εμπορευματοκιβωτίων (Smart Container Terminal Port Facility), ο οποίος λειτουργεί ως κόμβος διατροφικών μεταφορών. Η μοντελοποίηση της συγκεκριμένης υποδομής ακολουθεί αυστηρά τη μεθοδολογική ονοματολογία του διεθνούς προτύπου ISO/IEC 27005 και του λογισμικού MONARC, διαχωρίζοντας τα υπό εξέταση στοιχεία σε **Πρωτεύοντα Αγαθά (Primary Assets)** —τα οποία αντιπροσωπεύουν τις επιχειρησιακές διαδικασίες διακίνησης φορτίου και την εμπιστευτικότητα των πληροφοριών— και σε **Δευτερεύοντα Αγαθά (Secondary Assets)**, δηλαδή τον τεχνολογικό εξοπλισμό, τα δίκτυα, το λογισμικό και το ανθρώπινο δυναμικό που υποστηρίζουν την επιχειρησιακή συνέχεια.

2.1.1 Λειτουργική Ομαδοποίηση Δευτερευόντων Αγαθών σε Τέσσερις Ζώνες και Εγκάρσιους Αγωγούς (IEC 62443)

Ενώ η δενδρική λογική Πρωτευόντων και Δευτερευόντων Αγαθών ακολουθεί πιστά το μοντέλο του ISO 27005, τα Δευτερεύοντα Αγαθά ομαδοποιούνται περαιτέρω σε τέσσερις διακριτούς λειτουργικούς τομείς. Η ταξινόμηση αυτή υιοθετεί την αρχιτεκτονική των **«Ζωνών και Αγωγών» (Zones and Conduits)** του προτύπου IEC 62443-3-2, όπου ως Ζώνες ορίζονται τα αυτόνομα υποσυστήματα με κοινές απαιτήσεις ασφάλειας και ως Αγωγοί τα αυτόνομα δίκτυα επικοινωνίας που τα διασυνδέουν (IEC, 2020):

- **Ζώνη 1 – Πληροφοριακό Περιβάλλον (IT Domain):** Περιλαμβάνει τις κλασικές υπολογιστικές υποδομές διοίκησης και εμπορικής διαχείρισης. Κυρίαρχο στοιχείο αποτελεί το Λιμενικό Πληροφοριακό Σύστημα (**Port Community System – PCS**), μια ηλεκτρονική πλατφόρμα που συνδέει σε πραγματικό χρόνο τις τελωνειακές αρχές, τις ναυτιλιακές εταιρείες, τους εκτελωνιστές και τη διοίκηση του λιμένα (ENISA, 2019). Στη ζώνη αυτή εντάσσονται επίσης τα Ενδοεπιχειρησιακά Συστήματα Διαχείρισης Πόρων (ERP), οι διακομιστές βάσεων δεδομένων (SQL Servers), τα εταιρικά τοπικά δίκτυα (Corporate LAN) και οι υποδομές Cloud.
- **Ζώνη 2 – Η Γέφυρα Σύγκλισης (The Bridging Zone / TOS):** Στο σημείο τομής μεταξύ Πληροφοριακής (IT) και Επιχειρησιακής Τεχνολογίας (OT) τοποθετείται το Λειτουργικό Σύστημα Τερματικού Σταθμού (**Terminal Operating System – TOS**). Το TOS (π.χ. συστήματα τύπου Navis N4 ή TOPX) λειτουργεί ως ο «εγκέφαλος» του λιμένα: παραλαμβάνει τα εμπορικά δεδομένα φορτίου από το PCS (IT) και μεταφράζει τον σχεδιασμό στοιβασίας σε άμεσες εντολές πραγματικού χρόνου προς τον βιομηχανικό εξοπλισμό (OT). Η ψηφιοποίηση και ο αυτοματισμός που επιβάλλουν συστήματα όπως το TOS, αν και βελτιστοποιούν την εφοδιαστική αλυσίδα, αυξάνουν δραματικά την επιφάνεια κυβερνοεπιθέσεων, καθιστώντας τον λιμένα ευάλωτο σε στοχευμένες ψηφιακές διακοπές (UNCTAD, 2025). Ο κρίσιμος, γεφυρωτικός ρόλος του TOS επιβεβαιώθηκε ιστορικά κατά την επίθεση του κακόβουλου λογισμικού *NotPetya* (2017), όπου η παράλυση των συστημάτων TOS της Maersk/APM Terminals οδήγησε στην απόλυτη παύση των αυτοματοποιημένων λιμενικών λειτουργιών παγκοσμίως, επιβάλλοντας την επιστροφή σε χειροκίνητες διαδικασίες (ENISA, 2019).
- **Ζώνη 3 – Βιομηχανικό Περιβάλλον (OT / Industrial Domain):** Απαρτίζεται από τις επιχειρησιακές υποδομές διαχείρισης φορτίου, όπου η προτεραιότητα εστιάζει αδιαπραγμάτευτα στη Διαθεσιμότητα και την Ασφάλεια ζωής (AIC/Safety). Περιλαμβάνει τις Γερανογέφυρες Εκφόρτωσης Ξηράς-Πλοίου (Ship-to-Shore – STS Cranes), τις Γερανογέφυρες Στοιβασίας με Ελαστικά Επίσωτρα (RTG), καθώς και τους Προγραμματιζόμενους Λογικούς Ελεγκτές (PLCs) και τα Συστήματα Εποπτικού Ελέγχου και Συλλογής Δεδομένων (SCADA) που ρυθμίζουν την κίνηση των μηχανημάτων (NIST, 2023). Στη ζώνη αυτή εντάσσονται επίσης οι βιομηχανικοί αισθητήρες IoT που παρακολουθούν τη θερμοκρασία και την κατάσταση των εμπορευματοκιβωτίων ψυγείων (Reefer Containers).
- **Ζώνη 4 – Περιβάλλον Ναυσιπλοΐας και Επικοινωνιών (Navigation & Communication Domain):** Καλύπτει τις τεχνολογίες που διασφαλίζουν την ασφαλή προσέγγιση των πλοίων και την επιτήρηση του θαλάσσιου χώρου ευθύνης του λιμένα. Κεντρικό στοιχείο αποτελεί το Αυτόματο Σύστημα Αναγνώρισης πλοίων (**AIS – Automatic Identification System**), το οποίο

μεταδίδει το στίγμα, την ταυτότητα και τα στοιχεία του φορτίου, λειτουργώντας σε άμεση και συνεχή διασύνδεση με το ραντάρ επιφανείας και τις υποδομές των Υπηρεσιών Κυκλοφορίας Πλοίων (VTS – Vessel Traffic Services) (ENISA, 2019).

Η διασύνδεση των τεσσάρων προαναφερθέντων αυτόνομων Ζωνών επιτυγχάνεται μέσω ενός εγκάρσιου δικτυακού στρώματος **Αγωγών (Conduits)**. Το στρώμα αυτό δεν ανήκει σε συγκεκριμένη ζώνη, αλλά υλοποιείται με την ανάπτυξη ενός ικριώματος ιδιωτικού δικτύου 5G (Private 5G) και εφεδρικών δικτύων οπτικών ινών υψηλής ταχύτητας (NIST, 2023). Μέσω αυτών των Αγωγών διασφαλίζεται η αδιάλειπτη και ασφαλής μεταφορά των εντολών πραγματικού χρόνου από το TOS (Ζώνη 2) προς τον βιομηχανικό εξοπλισμό της Ζώνης 3, καθώς και η ροή τηλεμετρίας από τα συστήματα ναυσιπλοΐας της Ζώνης 4 προς το κέντρο ελέγχου.

2.1.2 Χαρτογράφηση του Ανθρώπινου Παράγοντα: Οι Πέντε Κρίσιμοι Ρόλοι

Η ολιστική μοντελοποίηση ενός τερματικού σταθμού επιβάλλει την ισότιμη ένταξη του Ανθρώπινου Παράγοντα (Human Element) στο οικοσύστημα των Δευτερευόντων Αγαθών. Οι χρήστες και διαχειριστές του λιμένα αποτελούν ταυτόχρονα την πρώτη γραμμή άμυνας αλλά και τον συχνότερο φορέα ευπαθειών. Για την απόλυτη συμμετρία με τις τέσσερις τεχνολογικές ζώνες και τη διασφάλιση ότι κανένα κρίσιμο σύστημα δεν παραμένει χωρίς ορισμένη διοικητική ευθύνη, το ανθρώπινο δυναμικό ταξινομείται σε πέντε διακριτούς ρόλους:

1. **Διεύθυνση Ασφάλειας και Διαχειριστές Συστημάτων (CISO & IT/OT System Administrators):** Τα ανώτατα στελέχη και οι μηχανικοί που φέρουν τη συνολική ευθύνη για τη διαμόρφωση των πολιτικών ασφάλειας, τη διαχείριση των διακομιστών, τη διατήρηση των δικλειδών ελέγχου (firewalls) και την επιτήρηση της δικτυακής κίνησης στη Ζώνη 1 και στη Γέφυρα του TOS.
2. **Χειριστές Λιμενικών Συστημάτων (Terminal Operators / Logistics Planners):** Το διοικητικό και επιχειρησιακό προσωπικό που αλληλεπιδρά καθημερινά με το Λιμενικό Πληροφοριακό Σύστημα (PCS) και το Λειτουργικό Σύστημα (TOS). Είναι υπεύθυνοι για την εισαγωγή δεδομένων φορτίου, τον προγραμματισμό αφίξεων και τη διαχείριση εγγράφων τελωνείου.
3. **Χειριστές Βιομηχανικού Εξοπλισμού και Τεχνικοί Πεδίου (Crane Operators & Field Technicians):** Το εξειδικευμένο προσωπικό της Ζώνης 3, το οποίο ελέγχει φυσικά ή απομακρυσμένα τις γερανογέφυρες STS και RTG και εκτελεί τις εργασίες συντήρησης των PLCs, των αισθητήρων και του ηλεκτρομηχανολογικού εξοπλισμού.
4. **Αξιωματικοί Λιμένος και Χειριστές Ναυσιπλοΐας (Port Officers / VTS & AIS Operators):** Το θεσμικό και επιχειρησιακό προσωπικό που επιτηρεί τη Ζώνη 4. Είναι υπεύθυνοι για την παρακολούθηση της θαλάσσιας κυκλοφορίας, την επιβεβαίωση των δεδομένων AIS και την επικοινωνία με τα προσεγγίζοντα πλοία μέσω του κέντρου ελέγχου VTS.
5. **Εξωτερικοί Προμηθευτές και Συντηρητές Εφοδιαστικής Αλυσίδας (External Vendors / Supply Chain Maintainers):** Τρίτες εταιρείες (όπως κατασκευαστές λογισμικού TOS ή κατασκευαστές βιομηχανικών γερανογεφυρών) που διαθέτουν δικαιώματα απομακρυσμένης πρόσβασης (Remote Maintenance Access) για την αναβάθμιση και διαγνωστική υποστήριξη των συστημάτων. Ο συγκεκριμένος ρόλος ενέχει εξαιρετικά υψηλή κρισιμότητα, καθότι μια παραβίαση των συστημάτων του προμηθευτή δύναται να χρησιμοποιηθεί ως «δούρειος ίππος» για την παράκαμψη των εσωτερικών ελέγχων του λιμένα, επιβεβαιώνοντας τις αυστηρές κανονιστικές απαιτήσεις θωράκισης της εφοδιαστικής αλυσίδας που επιβάλλουν οδηγίες όπως η MARSEC Directive 105-4.

Η χαρτογράφηση αυτή διαμορφώνει ένα πλήρες, δομημένο και αλληλεξαρτώμενο μητρώο τεχνολογικών και ανθρώπινων πόρων. Στο επόμενο υποκεφάλαιο, οι πόροι αυτοί θα οργανωθούν σε ιεραρχικά δέντρα, αναδεικνύοντας τις ακριβείς αλυσίδες αιτιότητας και εξάρτησης που διέπουν τη λειτουργία του τερματικού σταθμού.

2.2 Μοντέλο Αγαθών (Asset Model) και Δίκτυο Εξαρτήσεων (A_i)

Η μεθοδολογία αξιολόγησης κινδύνου που βασίζεται στο διεθνές πρότυπο ISO/IEC 27005 (ISO/IEC 27005, 2022) και εφαρμόζεται πρακτικά μέσω του λογισμικού MONARC (NC3, 2025), απαιτεί τη μετάφραση της τεχνολογικής χαρτογράφησης του προηγούμενου υποκεφαλαίου σε ένα αυστηρά ιεραρχικό μοντέλο. Ο πυρήνας αυτού του μοντέλου είναι ο προσδιορισμός των εξαρτήσεων μεταξύ των αγαθών: η κατανόηση, δηλαδή, του τρόπου με τον οποίο η αστοχία ενός υποστηρικτικού (Δευτερεύοντος) αγαθού προκαλεί αλυσιδωτές επιπτώσεις (cascading effects) στα κρίσιμα (Πρωτεύοντα) επιχειρησιακά αγαθά του τερματικού σταθμού.

2.2.1 Ορισμός Πρωτευόντων Αγαθών (Dual Approach)

Για την αποτύπωση της πολυπλοκότητας ενός σύγχρονου λιμένα, κρίνεται αναγκαία η υιοθέτηση μιας «διπλής προσέγγισης» (Dual Approach) που θα ενσωματώνει τόσο τον κόσμο της Επιχειρησιακής Τεχνολογίας (OT) όσο και τον κόσμο της Πληροφορικής (IT). Κατόπιν τούτου, ορίζονται δύο Πρωτεύοντα Αγαθά (Primary Assets), τα οποία αποτελούν τον τελικό στόχο προστασίας:

- **Πρωτεύον Αγαθό 1 (OT/Process - Διαδικασία):** «Αδιάλειπτη Διαδικασία Εκφόρτωσης / Φόρτωσης Εμπορευματοκιβωτίων». Το συγκεκριμένο αγαθό αντιπροσωπεύει τον πυρήνα της λιμενικής λειτουργίας. Σύμφωνα με την προσέγγιση AIC (Availability, Integrity, Confidentiality) για τα βιομηχανικά συστήματα, η απόλυτη προτεραιότητα προστασίας εδώ είναι η Διαθεσιμότητα (Availability) της διαδικασίας και η Ασφάλεια ζωής/εξοπλισμού (Safety).
- **Πρωτεύον Αγαθό 2 (IT/Information - Πληροφορία):** «Ακεραιότητα και Εμπιστευτικότητα Δεδομένων (PCS / Τελωνείου)». Αντιπροσωπεύει το πληροφοριακό φορτίο του λιμένα (δηλωτικά, τελωνειακά έγγραφα, σχέδια στοιβασίας). Εδώ, εφαρμόζεται η κλασική τριάδα CIA (Confidentiality, Integrity, Availability), με έμφαση στην αποτροπή μη εξουσιοδοτημένης πρόσβασης και αλλοίωσης εμπορικών δεδομένων.

2.2.2 Το Δέντρο Εξαρτήσεων και η Σύγκλιση IT/OT

Βάσει της μεθοδολογίας MONARC, η μοντελοποίηση ακολουθεί τη λογική «το Πρωτεύον εξαρτάται από το Δευτερεύον» (A depends on B). Για να επιτευχθεί ολιστική αναπαράσταση, αναπτύσσονται δύο παράλληλες αλυσίδες εξάρτησης, οι οποίες όμως, σε ένα σύγχρονο Smart Container Terminal, συγκλίνουν στρατηγικά:

Η πρώτη αλυσίδα (**OT/Διαδικασία**) διαμορφώνεται ως εξής:

Η αδιάλειπτη *Διαδικασία Εκφόρτωσης (Πρωτεύον 1)* εξαρτάται άμεσα από τη λειτουργία του *Φυσικού Γερανού (STS/RTG)*. Ο Γερανός εξαρτάται από τον βιομηχανικό ελεγκτή *PLC (Ζώνη 3)* και τον Γερανοδηγό για την εκτέλεση της κίνησης. Το PLC, για να λάβει τις οδηγίες στοιβασίας, εξαρτάται από το ασύρματο *Δίκτυο 5G (Αγωγή)*. Το Δίκτυο, με τη σειρά του, εξαρτάται από την πηγή των εντολών, δηλαδή το λειτουργικό σύστημα *TOS (Ζώνη 2)*, το οποίο υποστηρίζεται από τους κεντρικούς *Διακομιστές (Servers - Ζώνη 1)*.

Παράλληλα, η δεύτερη αλυσίδα (**IT/Πληροφορία**) διαμορφώνεται ως εξής:

Τα *Δεδομένα Τελωνείου (Πρωτεύον 2)* εξαρτώνται από την πλατφόρμα *PCS (Ζώνη 1)* που τα φιλοξενεί. Το PCS εξαρτάται από τον *SQL Server* για την αποθήκευσή τους. Ο διακομιστής υποστηρίζεται από το *Εταιρικό Δίκτυο (Corporate LAN)* και διαχειρίζεται από τον *IT Administrator*.

Το κρίσιμότερο, ωστόσο, σημείο της αρχιτεκτονικής είναι η **σύγκλιση των δύο αλυσίδων**. Στην πραγματικότητα, το σύστημα TOS δεν λειτουργεί απομονωμένα, αλλά προκειμένου να σχεδιάσει τις εντολές προς τους γερανούς, τροφοδοτείται με πληροφορίες (manifests) από το PCS. Συνεπώς, προστίθεται μια θεμελιώδης διαγώνια εξάρτηση: *Το TOS (Ζώνη 2) εξαρτάται από το PCS (Ζώνη 1)*. Αυτό το σημείο επαφής αποδεικνύει εμπράκτως την έννοια του **IT/OT Convergence**, μετατρέποντας τα δύο μεμονωμένα δέντρα σε έναν ενιαίο, διασυνδεδεμένο οργανισμό, όπου ένα συμβάν ασφαλείας στο IT μπορεί να παραλύσει το OT (cascade effect).

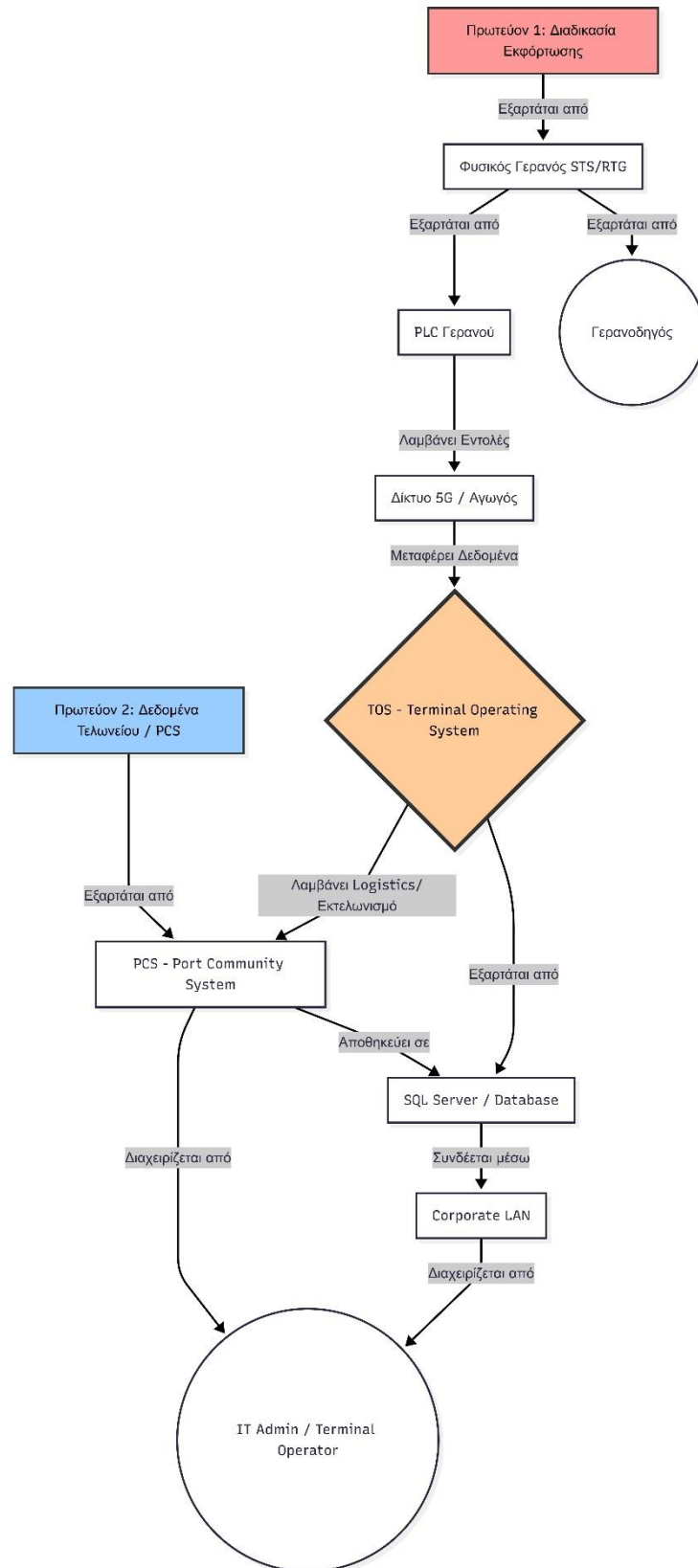
2.2.3 Οπτική και Μαθηματική Αναπαράσταση (DAG & DSM)

Για την ακαδημαϊκή και μαθηματική αποτύπωση των ανωτέρω εξαρτήσεων, αξιοποιούνται δύο εργαλεία αναπαράστασης. Το πρώτο είναι ο **Κατευθυνόμενος Άκυκλος Γράφος (Directed Acyclic Graph - DAG)**. Ο γράφος (Σχήμα 2.1) επιτρέπει την οπτικοποίηση της δομής, με τους κόμβους (nodes) να αναπαριστούν τα αγαθά και τις ακμές (edges) τη φορά της εξάρτησης. Για να διατηρηθεί η μαθηματική αυστηρότητα της "ακυκλικότητας" (acyclic) που επιβάλλει η θεωρία γράφων, πρέπει να σημειωθεί ότι το μοντέλο εστιάζει αποκλειστικά στην κατεύθυνση εντολής/ελέγχου (command & control). Τυχόν αμφίδρομη τηλεμετρία ή ανατροφοδότηση κατάστασης (status feedback) από τα PLCs προς το TOS, αν και υπαρκτή τεχνολογικά, παραλείπεται σκόπιμα από τον γράφο, προκειμένου να μην δημιουργηθούν λογικοί κύκλοι (loops) που θα καθιστούσαν αδύνατο τον υπολογισμό του διαλειπόμενου ρίσκου από το λογισμικό MONARC. Σημειώνεται ότι, κατά την υλοποίηση μιας κυβερνοεπίθεσης, η διάδοση της αστοχίας (impact propagation) ακολουθεί την αντίστροφη κατεύθυνση των απεικονιζόμενων ακμών εξάρτησης.

Συμπληρωματικά, το δίκτυο εξαρτήσεων κωδικοποιείται ψηφιακά μέσω μιας **Μήτρας Εξαρτήσεων (Design Structure Matrix - DSM)** (Πίνακας 2.1). Η μήτρα απεικονίζει σε μορφή πίνακα το κατά πόσον ένα στοιχείο της γραμμής (*i*) εξαρτάται άμεσα από ένα στοιχείο της στήλης (*j*). Η αναπαράσταση αυτή αποτελεί το τελικό μεταβατικό στάδιο, καθώς αντιστοιχεί ακριβώς στη δομή δεδομένων (data array) με την οποία θα τροφοδοτηθεί ο αλγόριθμος του εργαλείου αξιολόγησης στο Κεφάλαιο 3.

Πίνακας 2.1: Μήτρα Εξαρτήσεων (DSM) Αγαθών Λιμενικής Εγκατάστασης (Το Χ" δηλώνει ότι το Στοιχείο Γραμμής εξαρτάται άμεσα από το Στοιχείο Στήλης) Πηγή: Ιδία επεξεργασία.

Αγαθά (Assets)	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
(1) Πρωτεύον: Διαδικασία Εκφόρτωσης	-					X		
(2) Πρωτεύον: Δεδομένα PCS		-			X			
(3) TOS (Bridging Zone)			-	X	X			
(4) IT Servers & Database				-				X
(5) PCS (Λιμενικό Σύστημα)				X	-			X
(6) Φυσικός Γερανός (STS/RTG)						-	X	X
(7) PLC Γερανού			X				-	
(8) Ανθρώπινος Παράγοντας								-



Εικόνα 2.1: Κατευθυνόμενος Άκυκλος Γράφος (DAG) Εξαρτήσεων Αγαθών — Απεικόνιση της

Σύγκλιση IT/OT μέσω του TOS. Πηγή: Ιδία επεξεργασία.

2.3 Αποτίμηση Απειλών (Threat Assessment) στο Ναυτιλιακό Οικοσύστημα: Αντιστοίχιση των Αγαθών με Ψηφιακές, Φυσικές και Ανθρώπινες Απειλές

Με την ολοκλήρωση της δενδρικής χαρτογράφησης των αγαθών και τον καθορισμό των εξαρτήσεών τους, το επόμενο κρίσιμο βήμα στη μεθοδολογία ανάλυσης κινδύνου είναι ο προσδιορισμός των Απειλών (Threats - T). Στο πλαίσιο λειτουργίας του λογισμικού MONARC, οι απειλές αντλούνται από τυποποιημένους καταλόγους (Threat Catalogs) που βασίζονται στα διεθνή πρότυπα ISO/IEC 27005 και BSI IT-Grundschutz. Οι κατάλογοι αυτοί ταξινομούν τους κινδύνους σε θεμελιώδεις κατηγορίες, όπως η «Απώλεια Βασικών Υπηρεσιών» (Loss of essential services), οι «Τεχνικές Αστοχίες» (Technical failures), η «Φυσική Καταστροφή» (Physical damage) και οι «Μη Εξουσιοδοτημένες Ενέργειες» (Unauthorized actions) (ISO/IEC 27005, 2022). Για την εννοιολογική σαφήνεια και την ομαλή αφηγηματική μετάβαση προς το πρακτικό Κεφάλαιο 3, οι απειλές αυτές ομαδοποιούνται στην παρούσα θεωρητική ανάλυση σε τρεις μακρο-πυλώνες: Ψηφιακές, Φυσικές και Ανθρώπινες Απειλές, οι οποίες αντιστοιχίζονται στοχευμένα με τα αγαθά του λιμενικού οικοσυστήματος.

2.3.1 Ψηφιακές και Κυβερνο-Φυσικές Απειλές (Cyber & Cyber-Physical Threats)

Ο πρώτος πυλώνας περιλαμβάνει τις σκόπιμες κακόβουλες ενέργειες που στοχεύουν τα λογισμικά, τα δίκτυα και τα συστήματα ελέγχου των τεσσάρων Ζωνών:

- **Κακόβουλο Λογισμικό Εκβιασμού (Ransomware):** Στοχεύει κατά κύριο λόγο τους διακομιστές (IT Servers) της Ζώνης 1 και το σύστημα TOS της Ζώνης 2. Σκοπός είναι η κρυπτογράφηση των εμπορικών δεδομένων και των σχεδίων στοιβασίας, οδηγώντας σε απώλεια διαθεσιμότητας και απόλυτη παράλυση της εφοδιαστικής αλυσίδας, σε ευθυγράμμιση με το ιστορικό πρότυπο της επίθεσης *NotPetya* (ENISA, 2019).
- **Κατανεμημένη Επίθεση Άρνησης Εξυπηρέτησης (Distributed Denial of Service - DDoS):** Στοχεύει ευθέως το Λιμενικό Πληροφοριακό Σύστημα (PCS). Κατακλύζοντας τον διακομιστή με ψευδή αιτήματα σύνδεσης, οι επιτιθέμενοι καθιστούν το σύστημα μη διαθέσιμο, διακόπτοντας την κρίσιμη επικοινωνία του λιμένα με τα τελωνεία και τις ναυτιλιακές εταιρείες.
- **Απομακρυσμένη Κατάληψη και Έγχυση Εντολών (Remote Takeover & Command Injection):** Απειλή υψίστης κρισιμότητας που στοχεύει αποκλειστικά το OT (Ζώνη 3). Μέσω της παραβίασης των PLCs, ο επιτιθέμενος αποκτά τον έλεγχο των γερανογεφυρών STS. Η συγκεκριμένη απειλή ενσωματώνει ρεαλιστικούς γεωπολιτικούς κινδύνους, αποτελώντας την αιτία έκδοσης της αμερικανικής οδηγίας *MARSEC Directive 105-4* (USCG, 2024a).
- **Παραμβολή Σημάτων και Παραπλάνηση (GNSS/GPS Jamming & AIS Spoofing):** Μια διττή κυβερνο-φυσική απειλή. Αφενός στοχεύει τη Ζώνη 4 (Ναυσιπλοΐα), εκπέμποντας ψευδή στίγματα που τυφλώνουν ή παραπλανούν το VTS. Επιπλέον, η παρεμβολή σήματος GPS (Jamming) επηρεάζει άμεσα και τη Ζώνη 3, προκαλώντας την παύση των αυτοματοποιημένων γερανογεφυρών (RTGs) που στηρίζονται στη δορυφορική τηλεμετρία για την αυτόματη πλοήγησή τους (auto-steering) εντός της αυλής των εμπορευματοκιβωτίων.

2.3.2 Φυσικές και Περιβαλλοντικές Απειλές (Physical & Environmental Threats)

Ο δεύτερος πυλώνας αντιστοιχεί στις επίσημες κατηγορίες "Physical damage" και "Loss of essential services" του BSI IT-Grundschutz, πλήττοντας κυρίως τις φυσικές υποδομές και τους δικτυακούς αγωγούς (Conduits):

- **Φυσική Δολιοφθορά (Sabotage / Vandalism):** Αφορά τη σκόπιμη φυσική καταστροφή κρίσιμου εξοπλισμού, όπως η κοπή των υπογείων καλωδίων οπτικών ινών ή η καταστροφή των κεραιών του ιδιωτικού δικτύου 5G. Η ενέργεια αυτή αποκόπτει τους Αγωγούς, καθιστώντας αδύνατη τη μετάδοση εντολών από το TOS προς τα PLCs.
- **Ακραία Περιβαλλοντικά Φαινόμενα και Φυσικές Καταστροφές:** Περιλαμβάνει κινδύνους όπως πλημμύρες, πυρκαγιές ή σεισμούς που στοχεύουν τα Κέντρα Δεδομένων (Data Centers

- Ζώνη 1), προκαλώντας καταστροφή του υλικού εξοπλισμού (Hardware) και μη αναστρέψιμη απώλεια δεδομένων (εφόσον δεν λειτουργήσει το Σχέδιο Επιχειρησιακής Συνέχειας).
- **Απώλεια Βασικών Υπηρεσιών (Power Blackout):** Η εκτεταμένη και παρατεταμένη διακοπή ηλεκτροδότησης αποτελεί έναν από τους συχνότερους κινδύνους διαθεσιμότητας, παραλύοντας ταυτόχρονα και τις 4 Ζώνες του λιμένα, εάν τα συστήματα αδιάλειπτης παροχής ενέργειας (UPS) και οι γεννήτριες αποτύχουν.

2.3.3 Ανθρώπινες Απειλές και Κίνδυνοι Εφοδιαστικής Αλυσίδας (Human & Supply Chain Threats)

Ο τρίτος πυλώνας εστιάζει στον «Αδύναμο Κρίκο» της κυβερνοασφάλειας, αντιστοιχίζοντας τους 5 ρόλους που ορίστηκαν στο Υποκεφάλαιο 2.1 με τις αντίστοιχες "Μη εξουσιοδοτημένες ενέργειες" και τα ανθρώπινα σφάλματα:

- **Στοχευμένη Κοινωνική Μηχανική (Targeted Phishing / Social Engineering):** Στοχεύει πρωτίστως τους *Terminal Operators* και τους *IT Admins*. Μέσω παραπλανητικών μηνυμάτων ηλεκτρονικού ταχυδρομείου (π.χ. πλαστά τελωνειακά έγγραφα), οι επιτιθέμενοι αποσπούν διαπιστευτήρια (credentials) για την πρόσβαση στο PCS.
- **Εσωτερική Απειλή και Ανθρώπινο Λάθος (Insider Threat & Human Error):** Αφορά ενέργειες που προέρχονται εκ των έσω. Είτε πρόκειται για το εσκεμμένο ψηφιακό σαρπηδόρα από έναν δυσαρεστημένο διαχειριστή (Malicious Insider), είτε για το ακούσιο, κρίσιμο σφάλμα διαμόρφωσης (misconfiguration) ενός δικτύου από τον *OT Technician*, η εσωτερική απειλή παρακάμπτει σχεδόν όλες τις περιμετρικές άμυνες του οργανισμού.
- **Παραβίαση Εξωτερικού Προμηθευτή (Supply Chain Compromise):** Μια από τις πλέον σύγχρονες και καταστροφικές απειλές. Στοχεύει τον *External Vendor*, αξιοποιώντας το Εικονικό Ιδιωτικό Δίκτυο (VPN) που διατηρεί ο προμηθευτής για την Απομακρυσμένη Πρόσβαση Συντήρησης (Remote Maintenance Access) στον λιμένα. Ο επιτιθέμενος μολύνει πρώτα τον (συχνά λιγότερο προστατευμένο) προμηθευτή και, μέσω αυτού, εισχωρεί βαθιά στο OT δίκτυο (Ζώνη 3) και στο TOS (Ζώνη 2), χωρίς να ενεργοποιήσει τους συναγερμούς της Ζώνης 1.

Μέσω αυτής της αυστηρής αντιστοίχισης (Threat-to-Asset Mapping), το λιμενικό οικοσύστημα προετοιμάζεται πλήρως για τον μαθηματικό υπολογισμό του κινδύνου. Το τελευταίο στοιχείο που απαιτείται για την ολοκλήρωση της εξίσωσης, είναι ο εντοπισμός των τεχνολογικών και οργανωτικών Ευπαθειών (Vulnerabilities - V) που επιτρέπουν στις ανωτέρω Απειλές να υλοποιηθούν.

2.4 Αποτίμηση Αδυναμιών (Vulnerability Assessment): Εντοπισμός Ευπαθειών ανά Ζώνη Λιμενικής Υποδομής

Για να μετουσιωθεί μια θεωρητική απειλή σε πραγματικό περιστατικό ασφάλειας, απαιτείται η ύπαρξη μιας δομικής ή οργανωτικής αδυναμίας. Στη μεθοδολογία του ISO/IEC 27005 και του λογισμικού MONARC, η Ευπάθεια (Vulnerability - V) αποτελεί την "ανοιχτή θύρα" που επιτρέπει στην Απειλή (T) να εκμεταλλευτεί ένα Αγαθό (A), λειτουργώντας ως ο βασικός καταλύτης που θα καθορίσει τον τελικό υπολογισμό του διαλειπόμενου ρίσκου στο επόμενο πρακτικό κεφάλαιο. Διατηρώντας την αρχιτεκτονική συνέπεια της παρούσας μελέτης, οι ευπάθειες του τερματικού σταθμού εμπορευματοκιβωτίων εντοπίζονται και κατηγοριοποιούνται συμμετρικά βάσει των τεσσάρων λειτουργικών Ζωνών που ορίστηκαν στο Υποκεφάλαιο 2.1.

2.4.1 Ευπάθειες στη Ζώνη 1 (IT Domain) & Ζώνη 2 (Bridging Zone / TOS)

Στο πληροφοριακό και γεφυροποιό επίπεδο της εγκατάστασης, όπου η διασύνδεση με τον εξωτερικό κόσμο (Διαδίκτυο, Τελωνεία, Προμηθευτές) είναι συνεχής, οι κρίσιμες αδυναμίες εντοπίζονται στην αρχιτεκτονική του δικτύου και τη διαχείριση προσβάσεων:

Απουσία Ελέγχου Ταυτότητας Πολλαπλών Παραγόντων (Lack of MFA): Η αποκλειστική χρήση απλών κωδικών πρόσβασης (single-factor authentication) για την απομακρυσμένη πρόσβαση

των εξωτερικών προμηθευτών (Vendor Remote Access) στο PCS και το TOS, δημιουργεί την ιδανική ευπάθεια για την υλοποίηση επιθέσεων εφοδιαστικής αλυσίδας (Supply Chain Compromise) και κοινωνικής μηχανικής.

Μοναδικό Σημείο Αστοχίας (Single Point of Failure - SPOF): Η ύπαρξη ενός μοναδικού, μη εφεδρικού τείχους προστασίας (Single Firewall) στο όριο διασύνδεσης IT και OT. Εάν το συγκεκριμένο σημείο παρακαμφθεί ή καταρρεύσει, ο επιτιθέμενος αποκτά ανεμπόδιστη πλευρική κίνηση (lateral movement) από το εταιρικό LAN προς το λειτουργικό σύστημα του TOS.

2.4.2 Ευπάθειες στη Ζώνη 3 (OT / Βιομηχανικό Περιβάλλον)

Το βιομηχανικό περιβάλλον διαχείρισης φορτίου συγκεντρώνει τις πλέον χαρακτηριστικές (textbook) αδυναμίες του κλάδου, λόγω της ιστορικής προτεραιοποίησης της λειτουργικότητας έναντι της ψηφιακής ασφάλειας:

- **Ανασφαλή Βιομηχανικά Πρωτόκολλα (Insecure by Design Protocols):** Η χρήση πρωτοκόλλων όπως το Modbus/TCP ή το PROFINET για την επικοινωνία των PLCs. Τα πρωτόκολλα αυτά σχεδιάστηκαν χωρίς εγγενείς μηχανισμούς κρυπτογράφησης ή αυθεντικοποίησης, επιτρέποντας την ευχερή έγχυση κακόβουλων εντολών (Command Injection) εφόσον ο επιτιθέμενος αποκτήσει πρόσβαση στο τοπικό δίκτυο.
- **Ανασφαλής Ασύρματη Ζεύξη Ελέγχου (Insecure RF Control Link):** Η απουσία ισχυρής κρυπτογράφησης στο ασύρματο κανάλι επικοινωνίας (Radio Frequency) μεταξύ του Απομακρυσμένου Σταθμού Χειρισμού (Remote Operation Station) και της αυτοματοποιημένης γερανογέφυρας. Η ευπάθεια αυτή επιτρέπει την υποκλοπή ή παρεμβολή του σήματος ελέγχου, αποτελώντας το τεχνικό υπόβαθρο που καθιστά εφικτό το σενάριο της απομακρυσμένης κατάληψης (Remote Takeover) κινεζικών γερανών, το οποίο περιγράφεται στην οδηγία *MARSEC Directive 105-4* (USCG, 2024a).
- **Παρωχημένα Λειτουργικά Συστήματα (Legacy Systems):** Η ευρεία χρήση μη υποστηριζόμενων λειτουργικών συστημάτων (π.χ. Windows XP/7) στους σταθμούς διεπαφής ανθρώπου-μηχανής (HMI) εντός των καμπινών ελέγχου. Επειδή τα συστήματα αυτά δεν επιδέχονται πλέον ενημερώσεις ασφαλείας (unpatchable), είναι εξαιρετικά ευάλωτα σε γνωστές αδυναμίες. Είναι χαρακτηριστικό ότι η ίδια ακριβώς κατηγορία ευπάθειας στο πρωτόκολλο SMB (exploit *EternalBlue*) αποτέλεσε την κερκόπορτα που εκμεταλλεύτηκε ιστορικά το *NotPetya* για να παραλύσει τα συστήματα TOS.
- **Προεπιλεγμένα Διαπιστευτήρια (Default/Weak Credentials):** Η αποτυχία αλλαγής των εργοστασιακών κωδικών πρόσβασης στους ελεγκτές PLCs και τα HMI panels, μια αδυναμία που συχνά καθιστά τον βιομηχανικό εξοπλισμό άμεσα ανιχνεύσιμο και προσβάσιμο μέσω μηχανών αναζήτησης ανοιχτού κώδικα (όπως το Shodan).
- **Επίπεδα Δίκτυα (Flat Networks):** Η απουσία εσωτερικού λογικού διαχωρισμού (Network Segmentation / VLANs) εντός της αυλής των εμπορευματοκιβωτίων, γεγονός που επιτρέπει σε ένα μολυσμένο υποσύστημα να μεταδώσει ταχύτητα κακόβουλο λογισμικό σε ολόκληρο τον βιομηχανικό εξοπλισμό.

2.4.3 Ευπάθειες στη Ζώνη 4 (Ναυσιπλοΐα και Επικοινωνίες)

Στο επίπεδο της τηλεμετρίας και του ελέγχου της θαλάσσιας κυκλοφορίας, η αδυναμία εντοπίζεται στη φύση των ναυτιλιακών ραδιοεπικοινωνιών:

- **Μη Κρυπτογραφημένες Εκπομπές (Unencrypted Cleartext Broadcasts):** Η εγγενής ευπάθεια του πρωτοκόλλου AIS, το οποίο βασίζεται στην ανοιχτή (cleartext) ραδιοεκπομπή (VHF). Η παντελής απουσία μηχανισμών επαλήθευσης ταυτότητας (authentication mechanism) ή κρυπτογραφικής υπογραφής, επιτρέπει σε οποιονδήποτε διαθέτει έναν απλό πομποδέκτη Software-Defined Radio (SDR) να εκπέμψει πλαστά δεδομένα (Spoofing), παραπλανώντας τα ραντάρ VTS του λιμένα.

Με την ολοκλήρωση του εντοπισμού των Ευπαθειών (*V*), ολοκληρώνεται πλήρως η θεωρητική μοντελοποίηση του σεναρίου. Οι τρεις παράμετροι —Αγαθά (*A*), Απειλές (*T*) και

Ευπάθειες (V)— έχουν πλέον χαρτογραφηθεί αυστηρά, εξασφαλίζοντας ένα συμπαγές, αλληλένδετο οικοδόμημα. Το σύνολο αυτών των δεδομένων αποτελεί την αρχιτεκτονική βάση η οποία, στο επόμενο κεφάλαιο, θα εισαχθεί στο ψηφιακό περιβάλλον του λογισμικού MONARC για την πρακτική, μαθηματική αποτίμηση του λιμενικού κυβερνοκινδύνου.

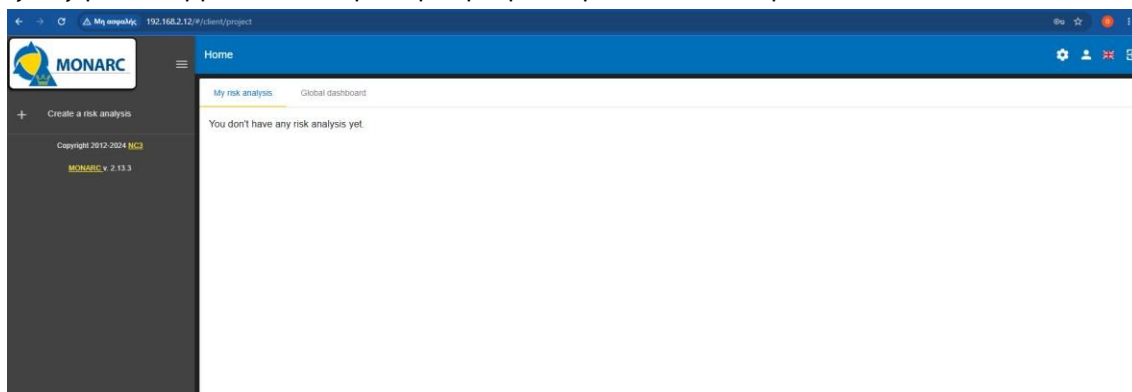
3 Πρακτική Εφαρμογή της Ανάλυσης Κινδύνου στο Λογισμικό MONARC

3.1 Τεχνική Ανάπτυξη και Περιβάλλον Λειτουργίας του Λογισμικού MONARC

Η θεωρητική και συγκριτική τεκμηρίωση της επιλογής του λογισμικού MONARC ως του καταλληλότερου εργαλείου για τη διενέργεια ανάλυσης κινδύνου σε λιμενικές υποδομές, αναλύθηκε εκτενώς στο Υποκεφάλαιο 1.3.3. Κατόπιν τούτου, το παρόν υποκεφάλαιο εστιάζει αποκλειστικά στην πρακτική, τεχνική ανάπτυξη (deployment) του εργαλείου, καθορίζοντας το ψηφιακό περιβάλλον της μελέτης με γνώμονα τη διασφάλιση της επιστημονικής αναπαραγωγιμότητας (scientific reproducibility) των τελικών αποτελεσμάτων.

Προκειμένου να αποφευχθούν διενέξεις με το τοπικό λειτουργικό σύστημα και να απομονωθεί πλήρως το περιβάλλον της δοκιμής, επιλέχθηκε η χρήση της επίσημης Εικονικής Μηχανής (Virtual Machine Appliance) που παρέχει η ομάδα ανάπτυξης του MONARC. Ως λογισμικό εικονικοποίησης (hypervisor) χρησιμοποιήθηκε το Oracle VM VirtualBox, έκδοση 7.2.14 (Oracle, 2026). Η εικονική μηχανή διαμορφώθηκε με επαρκείς υπολογιστικούς πόρους για την ομαλή εκτέλεση της βάσης δεδομένων και των υπολογιστικών αλγορίθμων του συστήματος, δεσμεύοντας τέσσερις (4) πυρήνες επεξεργαστή (CPUs) και 4096 MB μνήμης τυχαίας προσπέλασης (RAM). Η πρόσβαση στο γραφικό περιβάλλον του συστήματος δεν απαιτεί την εγκατάσταση πρόσθετου λογισμικού, καθώς η διεπαφή φιλοξενείται τοπικά και είναι προσβάσιμη μέσω οποιουδήποτε σύγχρονου προγράμματος περιήγησης ιστού (web browser), στη διεύθυνση IP που αποδίδεται δυναμικά στην εικονική μηχανή από το τοπικό δίκτυο μέσω προσαρμογέα γέφυρας (Bridged Networking).

Η έκδοση του λογισμικού που αξιοποιείται για την παρούσα ανάλυση είναι η MONARC v. 2.13.3 (NC3, 2025). Κατά την πρώτη επιτυχή σύνδεση στο σύστημα, ο διαχειριστής οδηγείται στην αρχική οθόνη (Home), υπό την ενεργή καρτέλα «My risk analysis». Όπως αποτυπώνεται στην Εικόνα 3.1, το γραφικό περιβάλλον (User Interface) διακρίνεται για τη μινιμαλιστική και χρηστική του προσέγγιση. Η οργάνωση των δεδομένων στο MONARC ακολουθεί ιεραρχική δομή πελάτη/έργου (Client/Project), επιτρέποντας στον διαχειριστή να διατηρεί πολλαπλές αναλύσεις κινδύνου ταυτόχρονα. Το σημείο εκκίνησης για τη μεταφορά του θεωρητικού μοντέλου (Αγαθά, Απειλές, Ευπάθειες) που αναπτύχθηκε στο Κεφάλαιο 2, αποτελεί η επιλογή «Δημιουργία Ανάλυσης Κινδύνου» (Create a risk analysis). Μέσω αυτής της λειτουργίας, το σύστημα προετοιμάζει την κενή βάση δεδομένων που θα υποδεχθεί τα λειτουργικά χαρακτηριστικά του εξεταζόμενου τερματικού σταθμού εμπορευματοκιβωτίων στα επόμενα στάδια.



Εικόνα 3.1: Το περιβάλλον διεπαφής του λογισμικού MONARC v. 2.13.3 κατά την αρχική εκκίνηση.

3.2 Εισαγωγή Δεδομένων και Παραμετροποίηση Στοιχευμένου Σεναρίου

3.2.1 Ορισμός Παραμέτρων Έργου και Στοιχευμένου Σεναρίου

Το πρώτο στάδιο της πρακτικής εφαρμογής αφορά τη δημιουργία του ψηφιακού "κελύφους" της μελέτης εντός του λογισμικού MONARC. Δεδομένου ότι η αρχιτεκτονική του εργαλείου σε αυτόνομες εγκαταστάσεις (single-tenant deployments) δεν απαιτεί τη δημιουργία ξεχωριστής οντότητας "Πελάτη" (Client), ο οργανισμός-στόχος, ήτοι ο υποθετικός Τερματικός Σταθμός Εμπορευματοκιβωτίων, ενσωματώθηκε άμεσα στα υπερδεδομένα (metadata) της ίδιας της ανάλυσης κινδύνου.

Ως βάση εκκίνησης επιλέχθηκε η χρήση ενός κενού μοντέλου («Blank model») έναντι των προκαθορισμένων προτύπων του εργαλείου. Η στρατηγική αυτή επιλογή κρίθηκε επιβεβλημένη, προκειμένου να διασφαλιστεί ότι το περιβάλλον της ανάλυσης θα παραμείνει "καθαρό" από προεγκατεστημένα, γενικά (generic) αγαθά τα οποία δεν συνάδουν με τον εξειδικευμένο λιμενικό κλάδο. Κατ' αυτόν τον τρόπο, η ανάλυση ονομάστηκε "Cyber Risk Analysis - Smart Container Terminal" και παραμετροποιήθηκε στην αγγλική γλώσσα, ώστε να διατηρηθεί η εννοιολογική ευθυγράμμιση με τους καταλόγους και την ορολογία του προτύπου ISO/IEC 27005 που υιοθετήθηκαν στο Κεφάλαιο 2. Στο πεδίο της περιγραφής του έργου, ορίστηκε ρητά η εστίαση της αξιολόγησης στα κρίσιμα συστήματα PCS, TOS και AIS.

3.2.2 Ορισμός Κλιμάκων Αξιολόγησης και Κριτηρίων Κινδύνου

Το στάδιο παραμετροποίησης των κλιμάκων ανέδειξε μια θεμελιώδη αρχιτεκτονική σύγκλιση μεταξύ του επιλεγμένου λογισμικού και της θεωρητικής μεθοδολογίας της παρούσας μελέτης. Το εργαλείο διαχωρίζει εγγενώς τους κινδύνους σε δύο διακριτά υπολογιστικά μονοπάτια: τους Πληροφοριακούς (Information risks) και τους Λειτουργικούς/Επιχειρησιακούς (Operational risks). Ο διαχωρισμός αυτός ταυτίζεται απόλυτα με τη Διπλή Προσέγγιση (Dual Approach) IT και OT αγαθών που θεμελιώθηκε στο Υποκεφάλαιο 2.2.

Ειδικότερα, για τους πληροφοριακούς κινδύνους, το σύστημα υπολογίζει το ρίσκο βάσει του τύπου $R = I \times (T \times V)$, αναλύοντας την πιθανότητα σε δύο ανεξάρτητους παράγοντες: την Απειλή (Threat) και την Ευπάθεια (Vulnerability). Αυτό κρίνεται μεθοδολογικά ορθό, καθώς σε μια κυβερνοεπίθεση η πιθανότητα εξαρτάται τόσο από την ικανότητα του επιτιθέμενου όσο και από την έκθεση του συστήματος. Αντίθετα, στους λειτουργικούς κινδύνους (π.χ. φυσική βλάβη εξοπλισμού), το εργαλείο χρησιμοποιεί τον τύπο $R = I \times P$ (NC3, 2025), ενοποιώντας την παράμετρο σε μία ενιαία Πιθανότητα (Probability - P), προσεγγίζοντας έτσι ρεαλιστικότερα τα φυσικά συμβάντα.

Το σύστημα αξιολογεί τις παραμέτρους του ρίσκου σε ασύμμετρες κλίμακες. Συγκεκριμένα, οι επιπτώσεις (Impact) και η πιθανότητα (Likelihood) βαθμολογούνται σε πενταβάθμια κλίμακα [04], ενώ η ευπάθεια βαθμολογείται σε εξαβάθμια κλίμακα [0-5]. Ως προς τα κριτήρια αξιολόγησης, οι πέντε κατηγορίες συνεπειών (Φήμη, Λειτουργία, Νομικά, Οικονομικά, Προσωπικό) είναι κοινές και στα δύο υπολογιστικά μονοπάτια. Η ανάλυση της επίπτωσης στις τρεις θεμελιώδεις διαστάσεις Εμπιστευτικότητας, Ακεραιότητας και Διαθεσιμότητας (C-I-A) εφαρμόζεται όμως αποκλειστικά στους Πληροφοριακούς κινδύνους. Αντιθέτως, οι Λειτουργικοί/Επιχειρησιακοί κίνδυνοι αξιολογούνται με μία ενιαία, μη διασπασμένη κλίμακα επίπτωσης, συνέπεια που ευθυγραμμίζεται πλήρως με την απλούστερη λογική του τύπου $R = I \times P$ που περιγράφηκε παραπάνω.

Κατόπιν μελέτης του ψηφιακού περιβάλλοντος, ελήφθη η ενεργή, τεκμηριωμένη απόφαση να διατηρηθούν πλήρως οι προκαθορισμένες (default) κλίμακες του MONARC, δίχως τη δημιουργία προσαρμοσμένων (custom) κριτηρίων. Η απόφαση αυτή βασίστηκε στο γεγονός ότι οι ενσωματωμένες βαθμίδες συνεπειών καλύπτουν ήδη με απόλυτη σαφήνεια το κριτήριο της Φυσικής Ασφάλειας (Safety). Χαρακτηριστικά, στο ανώτατο επίπεδο 4, η κατηγορία «Reputation» αναφέρει ρητά το σενάριο απώλειας ανθρώπινης ζωής (Death of someone) ως πρωτεύουσα

συνέπεια, ενώ η κατηγορία «Personal» περιλαμβάνει τον θάνατο ως ένα εκ των παραδειγμάτων μη αναστρέψιμων συνεπειών. Η πρόβλεψη αυτή ικανοποιεί απόλυτα τις απαιτήσεις αξιολόγησης του ΟΤ περιβάλλοντος, καθιστώντας τις εργοστασιακές ρυθμίσεις ιδανικές. Τέλος, το τελικό εξαγόμενο ρίσκο αποτυπώνεται οπτικά σε έναν πίνακα αποδοχής (Acceptance thresholds) με χρωματική διαβάθμιση, ο οποίος κατηγοριοποιεί άμεσα την κρισιμότητα των ευρημάτων από το πράσινο έως το κόκκινο χρώμα.

3.2.3 Εισαγωγή των Πρωτευόντων Αγαθών και Κατηγοριοποίηση σε Ζώνες

Μετά τον καθορισμό των παραμέτρων και των κλιμάκων αξιολόγησης, το επόμενο στάδιο της πρακτικής εφαρμογής αφορά τη μεταφορά του θεωρητικού μοντέλου της Διπλής Προσέγγισης (Dual Approach) στο ψηφιακό περιβάλλον του MONARC. Η διαδικασία ξεκίνησε με την εισαγωγή των δύο Πρωτευόντων Αγαθών (Primary Assets) της μελέτης, τα οποία αποτελούν τις "ρίζες" των δέντρων εξάρτησης.

Αρχικά, καταχωρήθηκε το πληροφοριακό πρωτεύον αγαθό με την πλήρη ονομασία (Name) «PCS & Customs Data». Ως αναγνωριστική ετικέτα (Label) ορίστηκε ο σύντομος κωδικός «PA2», εξασφαλίζοντας την καθαρή οπτική αποτύπωση στα γραφήματα του συστήματος. Το αγαθό ταξινομήθηκε στον επίσημο τύπο «INFO - Information», επιβεβαιώνοντας την πληροφοριακή του φύση. Αντίστοιχα, για τον πυρήνα της επιχειρησιακής λειτουργίας, εισήχθη το αγαθό «Continuous Container Unloading/Loading Process» με ετικέτα «PA1». Λόγω της φύσης του ως βιομηχανικής διαδικασίας, ορίστηκε στον τύπο «PROC - Process». Το εύρος (Score) και για τα δύο αγαθά διατηρήθηκε ως Τοπικό (Local), καθώς αφορούν αποκλειστικά τη συγκεκριμένη, αυτόνομη μελέτη περίπτωσης.

Σε αυτό το σημείο, εφαρμόστηκε μια κρίσιμη μεθοδολογική επιλογή προκειμένου να γεφυρωθεί η θεωρητική αρχιτεκτονική του Κεφαλαίου 2.1 με το λογισμικό. Το ελεύθερο πεδίο της Κατηγορίας (Category) δεν χρησιμοποιήθηκε απλώς ως διοικητική ετικέτα, αλλά αξιοποιήθηκε στρατηγικά για να αποτυπώσει το μοντέλο των Ζωνών (IEC 62443). Έτσι, δημιουργήθηκαν εξ υπαρχής οι κατηγορίες «Zone 1 - IT Domain» και «Zone 3 - OT/Industrial Domain», εντός των οποίων τοποθετήθηκαν τα αγαθά PA2 και PA1 αντίστοιχα. Η ενέργεια αυτή επιτρέπει στο εργαλείο να "αντιλαμβάνεται" τη χωρική και λογική τοπολογία του λιμένα. Η ίδια λογική κατηγοριοποίησης θα εφαρμοστεί συνεπώς και κατά την εισαγωγή των Δευτερευόντων Αγαθών στο επόμενο στάδιο, διασφαλίζοντας μια ενιαία και συνεπή αρχιτεκτονική σε ολόκληρο το δέντρο εξάρτησης.

Τέλος, επισημαίνεται ότι, στην τρέχουσα φάση της εισαγωγής, τα ταμπλό του συστήματος καταγράφουν μηδενικούς κινδύνους (0 risks) για αμφότερα τα αγαθά. Αυτό είναι απολύτως αναμενόμενο και μεθοδολογικά ορθό, καθώς η γένεση του ρίσκου στο MONARC προϋποθέτει τον εντοπισμό και τη σύνδεση των αγαθών με συγκεκριμένες Απειλές και Ευπάθειες. Η διαδικασία αυτή, μαζί με την εισαγωγή των Δευτερευόντων Αγαθών που θα "συνθέσουν" τα Πρωτεύοντα, αποτελεί το αντικείμενο των επόμενων σταδίων της ανάλυσης.

Μετά την ολοκλήρωση της εισαγωγής των δύο "ριζών", ακολούθησε η προσθήκη των αντίστοιχων Δευτερευόντων Αγαθών (Secondary Assets), τα οποία συνθέτουν την ιεραρχία του κάθε δέντρου. Σε αντίθεση με τα Πρωτεύοντα, η δημιουργία Δευτερευόντων Αγαθών στο MONARC ακολουθεί μια διαδικασία δύο σταδίων: αρχικά το αγαθό καταχωρείται ανεξάρτητα στη γενική Βιβλιοθήκη (Assets library) με τα πλήρη χαρακτηριστικά του (Name, Label, Asset type, Category), και εν συνεχεία συνδέεται ως εξαρτώμενο στοιχείο (component) του αντίστοιχου Πρωτεύοντος μέσω της λειτουργίας "Composition". Ακολουθώντας πιστά την αλυσίδα που τεκμηριώθηκε στη Μήτρα Εξαρτήσεων (DSM) (βλ. Κεφάλαιο 2, Πίνακας 2.1), εισήχθη αρχικά ο φυσικός γερανός «Physical Crane (STS/RTG)» (ετικέτα: SA1, τύπος: MAT_FIX - Fixed equipment, Κατηγορία: Zone 3) ως άμεσο εξάρτημα της Διαδικασίας (PA1). Αντίστοιχα, το «Port Community System (PCS)» (ετικέτα: SA2, τύπος: LOG_APP - Business application, Κατηγορία: Zone 1) ενσωματώθηκε ως άμεσο εξάρτημα των Πληροφοριακών Δεδομένων (PA2).

Η καταχώρηση των δύο αυτών Δευτερευόντων Αγαθών ανέδειξε μια κρίσιμη λειτουργική ιδιότητα του εργαλείου: κάθε αγαθό, ανάλογα με τον επίσημο τεχνικό του τύπο, ενεργοποιεί αυτόματα έναν προκαθορισμένο κατάλογο πιθανών συνδυασμών Απειλής και Ευπάθειας, ο οποίος αντλείται από την ενσωματωμένη βάση γνώσης του λογισμικού (NC3, 2025). Σημειώνεται

ότι ο ενσωματωμένος κατάλογος απειλών/ευπαθειών του λογισμικού φαίνεται να ακολουθεί τη δομή παλαιότερης έκδοσης του προτύπου (ISO/IEC 27005, 2018), σε αντίθεση με τη μεθοδολογική προσέγγιση της παρούσας εργασίας που βασίζεται στην πλέον πρόσφατη έκδοση (ISO/IEC 27005, 2022) — μια αναμενόμενη χρονική απόκλιση μεταξύ της στιγμιαίας κατάστασης ενός λογισμικού εργαλείου και της τρέχουσας θεωρίας. Συγκεκριμένα, το SA1 (Γερανός) απέδωσε αυτόματα 53 τέτοιους συνδυασμούς, ενώ το SA2 (PCS) απέδωσε 87. Παράλληλα, παρατηρήθηκε ότι η κατηγοριοποίηση σε τεχνικούς κινδύνους ("information risks") εμφανίζεται συστηματικά στη σελίδα κάθε Δευτερεύοντος Αγαθού, ενώ η κατηγορία των επιχειρησιακών κινδύνων ("operational risks") εμφανίζεται αποκλειστικά στη σελίδα κάθε Πρωτεύοντος. Το γεγονός αυτό επιβεβαιώνει πρακτικά ότι ο διαχωρισμός των κινδύνων συνδέεται αυστηρά με το ιεραρχικό επίπεδο του αγαθού (Πρωτεύον έναντι Δευτερεύοντος) και όχι με τη θεματική του φύση (IT έναντι ΟΤ).

Δεδομένου του τεράστιου όγκου των αυτοματοποιημένων συνδυασμών (140 συνολικά κίνδυνοι μόνο για τα δύο πρώτα εξαρτήματα), η πλήρης ανάλυσή τους θα ξέφευγε από τα όρια ενός ρεαλιστικού σεναρίου. Το πλήρες, ακατέργαστο μητρώο αυτών των 140 κινδύνων εξήχθη από το λογισμικό MONARC και παρατίθεται αυτούσιο ως υπολογιστικό φύλλο (βλ. Παράρτημα Ι - Πίνακες Excel Εξαγωγής Κινδύνων) για λόγους ακαδημαϊκής διαφάνειας. Ωστόσο, για τους σκοπούς της παρούσας ανάλυσης κρίθηκε επιβεβλημένη η εφαρμογή μιας μεθοδολογίας φιλτραρίσματος. Στο επόμενο στάδιο (Εκτίμηση Κινδύνου), διατηρούνται προς αξιολόγηση αποκλειστικά οι συνδυασμοί που ταυτίζονται με τις στοχευμένες Απειλές και Ευπάθειες, οι οποίες τεκμηριώθηκαν θεωρητικά στα Υποκεφάλαια 2.3 και 2.4.

3.3 Εκτίμηση Αντικτύπου και Αξιολόγηση Κινδύνων

Η φάση της αξιολόγησης εντός του περιβάλλοντος MONARC πραγματοποιήθηκε με βάση τον μαθηματικό τύπο $R = I \times (T \times V)$, όπου ο Τρέχων Κίνδυνος (Current Risk - R) προκύπτει από το γινόμενο του Αντικτύπου (Impact - I), της Πιθανότητας Απειλής (Threat Probability - T) και της Ποιότητας Ευπάθειας (Vulnerability Qualification - V). Το λογισμικό εφαρμόζει εγγενώς κλίμακα 04 για Πιθανότητα και Αντίκτυπο, και 0-5 για Ευπάθεια (NC3, 2025), όπως ήδη τεκμηριώθηκε στο Υποκεφάλαιο 3.2.2, σε πλήρη συνέπεια με τη γενική μεθοδολογία του προτύπου ISO/IEC 27005:2022 (ISO/IEC 27005, 2022).

3.3.1 Εμπειρική Επιβεβαίωση της Διχοτομίας IT/OT

Κατά τον ορισμό του Αντικτύπου (Impact Assessment) στα Πρωτεύοντα Αγαθά, αποδείχθηκε εμπειρικά η θεωρητική προσέγγιση του Υποκεφαλαίου 2.2, η οποία διαχωρίζει τις προτεραιότητες ασφαλείας του IT (μοντέλο CIA) έναντι του ΟΤ (μοντέλο AIC/Safety).

Στην περίπτωση του Πληροφοριακού Συστήματος PCS (PA2), οι μέγιστες τιμές αντικτύπου διαμορφώθηκαν στο επίπεδο 3 (Υψηλό) για όλες τις διαστάσεις (Εμπιστευτικότητα: 3, Ακεραιότητα: 3, Διαθεσιμότητα: 3). Η απουσία φυσικών κινδύνων για την ανθρώπινη ζωή εμποδίζει την ενεργοποίηση της μέγιστης βαθμολογίας (Καταστροφικό/4) στο περιβάλλον της πληροφορικής.

Αντιθέτως, στη Διαδικασία Εκφόρτωσης (PA1 - ΟΤ), η ανάλυση οδήγησε σε ριζικά διαφορετικό προφίλ: $\text{Max}(C, I, A) = \{1, 4, 4\}$. Η Εμπιστευτικότητα (Confidentiality) υποβαθμίστηκε σκόπιμα στο επίπεδο 1, καθώς η διαρροή δεδομένων τηλεμετρίας δεν προκαλεί άμεση λειτουργική ζημιά. Παράλληλα, η Ακεραιότητα και η Διαθεσιμότητα αξιολογήθηκαν με την ανώτατη βαθμολογία (4) για εντελώς διαφορετικούς λόγους: η Ακεραιότητα έφτασε στο επίπεδο 4 μέσω της στήλης Φήμης (Reputation) σε σενάριο απώλειας ανθρώπινης ζωής ("Death of someone"), ενώ η Διαθεσιμότητα έφτασε στο ίδιο ανώτατο επίπεδο μέσω μιας ανεξάρτητης στήλης, της Επιχειρησιακής Λειτουργίας (Operational), για το σενάριο της πλήρους επιχειρησιακής παράλυσης ("Complete stop of all services"). Αυτή η ποσοτική διαφοροποίηση αποτελεί την έμπρακτη απόδειξη της ένταξης της φυσικής ασφάλειας (Safety) στον πυρήνα των βιομηχανικών ελέγχων.

3.3.2 Υπολογισμός Τρέχοντος Κινδύνου ανά Ζώνη

Με τον Αντίκτυπο να έχει κληρονομηθεί από τα Πρωτεύοντα Αγαθά, πραγματοποιήθηκε η αξιολόγηση των συγκεκριμένων σεναρίων επίθεσης.

Για το περιβάλλον IT (Δίκτυο Ζώνης 1), τα υψηλότερα επίπεδα κινδύνου καταγράφηκαν στις επιθέσεις Phishing και DDoS (Current Risk: 60), γεγονός που αντικατοπτρίζει την υψηλή πιθανότητα εκδήλωσής τους λόγω της ευρείας διαθεσιμότητας εργαλείων και της απουσίας αυστηρών πολιτικών ελέγχου. Η στοχευμένη επίθεση μέσω λογαριασμών προμηθευτών (Vendor MFA) αξιολογήθηκε χαμηλότερα ως προς την πιθανότητα, αλλά διατηρεί κρίσιμη ευπάθεια.

Πίνακας 3.1: Αξιολόγηση Κινδύνων IT (Port Community System - PA2). Πηγή: Ιδία επεξεργασία.

Σενάριο Επίθεσης (Κεφ. 2)	Threat Label (MONARC)	Vulnerability Label (MONARC)	Impact (I)	Prob. (T)	Qualif. (V)	Current Risk (R)
Phishing / Social Engineering	Forging of rights	No audit policy	3	4	5	60
DDoS / Saturation	Saturation of the information system	No filter to protect the system against saturation	3	4	5	60
Ransomware	Malware infection	Possibility of modifying or corrupting the software	3	4	4	48
Vendor MFA / Supply Chain	Illegal processing of data	Software can be used by everyone (no password required)	3	3	5	45

ID	Asset	Impact	Threat	Prob.	Vulnerability	Existing controls	Qualif.	Current risk	Treatment	Residual risk
		C I A	Label		Label			C I A		
38	Port Community System (PCS)	3 3 3	Forging of rights	4	No audit policy		5	60 60 60	Not treated	60
73	Port Community System (PCS)	3 3 3	Saturation of the information system	4	No filter to protect the system against saturation		5	60 60 60	Not treated	60
33	Port Community System (PCS)	3 3 3	Malware infection	4	Possibility of modifying or corrupting the software		4	48 48 48	Not treated	48
23	Port Community System (PCS)	3 3 3	Illegal processing of data	3	Software can be used by everyone (e.g. no password required for remote administration of a workstation)		5	45 45 45	Not treated	45

Εικόνα 3.2: Πίνακας αξιολογημένων κινδύνων για το Πληροφοριακό Σύστημα (IT/PCS) στο περιβάλλον του MONARC. (NC3, 2025)

Στο βιομηχανικό περιβάλλον OT (Ζώνη 3), η κατάληψη συστημάτων και η εκτέλεση κακόβουλων εντολών (Remote Takeover / Command Injection) αναδείχθηκε ως ο απόλυτος κίνδυνος (Current Risk: 60), καθώς επηρεάζει άμεσα την Ακεραιότητα και τη Διαθεσιμότητα του φυσικού εξοπλισμού με ανώτατο αντίκτυπο (I=4).

Πίνακας 3.2: Αξιολόγηση Κινδύνων OT (Physical Crane - PA1). Πηγή: Ιδία επεξεργασία.

Σενάριο Επίθεσης (Κεφ. 2)	Threat Label (MONARC)	Vulnerability Label (MONARC)	Impact (I)	Prob. (T)	Qualif. (V)	Current Risk (R)
Remote Takeover (Command Injection)	Abuse of rights	The system is connected to external networks	4	3	5	60
Power Blackout	Loss of power supply	Equipment sensitive to electrical disturbances	4	3	4	48
Physical Sabotage / Vandalism	Destruction of equipment or supports	Equipment accessible to unauthorized persons	4	2	3	24
GNSS/GPS Jamming & Spoofing	Interception of compromising interference signals	Equipment capable of emitting compromising stray radiation	1 (C)	2	5	10

ID	Asset	Impact	Threat	Prob.	Vulnerability	Existing controls	Qualif.	Current risk	Treatment	Residual risk
		C I A	Label		Label			C I A		
106	Physical Crane (STSRTO)	1 4 4	Abuse of rights	3	The system is connected to external networks		5	15 60 66	Not treated	60
121	Physical Crane (STSRTO)	1 4 4	Loss of power supply	3	Equipment sensitive to electrical disturbances (voltage drops, overvoltages, transient power-cuts)		4	48 48 48	Not treated	48
122	Physical Crane (STSRTO)	1 4 4	Destruction of equipment or supports	2	Equipment accessible to unauthorized persons		3	24 24 24	Not treated	24
132	Physical Crane (STSRTO)	1 4 4	Interception of compromising interference signals	2	Equipment capable of emitting compromising stray radiation		5	10 10 10	Not treated	10

Εικόνα 3.3: Πίνακας αξιολογημένων κινδύνων για τη Διαδικασία Εκφόρτωσης (ΟΤ/Γερανός) στο περιβάλλον του MONARC. (NC3, 2025)

3.3.3 Ποσοτικές Στρεβλώσεις και τα Όρια των Γενικών Προτύπων

Η πρακτική εφαρμογή του εργαλείου MONARC ανέδειξε έναν κρίσιμο περιορισμό των τυποποιημένων καταλόγων απειλών, όπως αυτοί του προτύπου ISO/IEC 27005:2018 (ISO/IEC 27005, 2018), όταν εφαρμόζονται σε εξειδικευμένα ναυτιλιακά περιβάλλοντα.

Η αναγκαστική χρήση της κατηγορίας "Interception of compromising interference signals" (ID 132) για την αναπαράσταση του σεναρίου ενεργητικής παρεμβολής στο δορυφορικό σήμα (GNSS/GPS Jamming) δεν οδήγησε απλώς σε εννοιολογική ανακρίβεια, αλλά και σε ποσοτική υποεκτίμηση του πραγματικού κινδύνου. Καθώς η συγκεκριμένη κατηγορία στο MONARC ενεργοποιεί αποκλειστικά τη διάσταση της Εμπιστευτικότητας (όπου Impact = 1 για το PA1), το υπολογιζόμενο ρίσκο καθελώθηκε μαθηματικά στο 10 ($1 \times 2 \times 5$).

Εάν η ίδια απειλή είχε ορθά ταξινομηθεί ως πλήγμα στη Διαθεσιμότητα (όπου Impact = 4), το θεωρητικό ρίσκο θα ανερχόταν στο 40 ($4 \times 2 \times 5$). Το ζήτημα αυτό αναδεικνύει ξεκάθαρα τα όρια

εφαρμογής ενός γενικού καταλόγου σε εξειδικευμένα σενάρια ναυτιλιακού ΟΤ και την ανάγκη θεωρητικής επέκτασης πέρα από τα έτοιμα εργαλεία πληροφορικής.

3.4 Εξαγωγή Αποτελεσμάτων: Παραγωγή Γραφημάτων και Μαθηματική Επιβεβαίωση

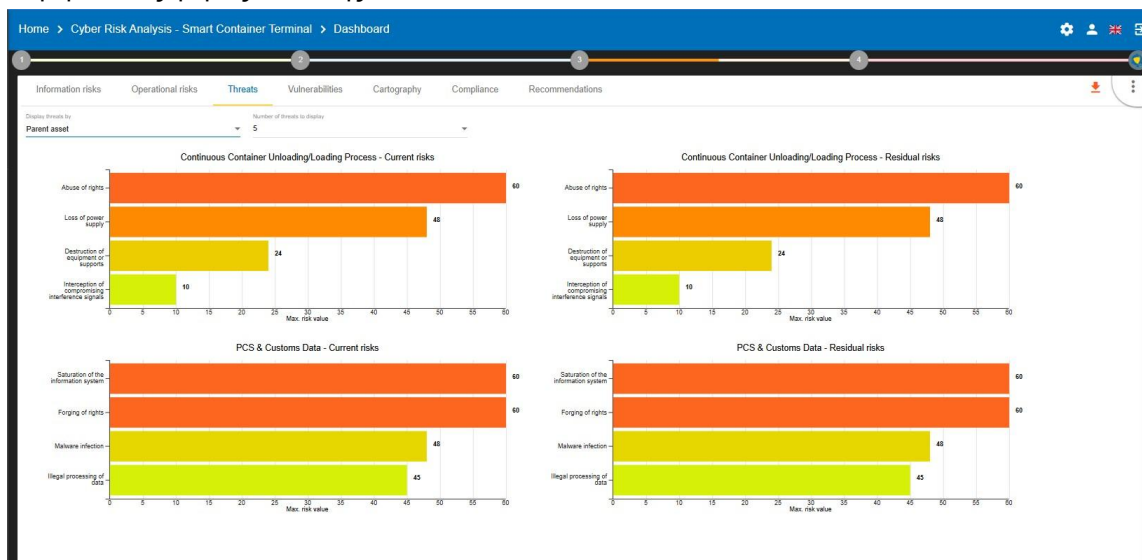
Με την ολοκλήρωση της καταχώρησης των δεδομένων στις αναλυτικές καρτέλες των κινδύνων (Risk Sheets), το εργαλείο MONARC προχώρησε στην αυτόματη συλλογή και οπτικοποίηση των αποτελεσμάτων μέσω του ενσωματωμένου Πίνακα Ελέγχου (Dashboard). Η φάση αυτή είναι κρίσιμη για τη διοικητική αναφορά (management reporting), καθώς μεταφράζει τα τεχνικά δεδομένα σε στρατηγικούς δείκτες απόφασης.

Σημειώνεται ότι παρά την τεκμηρίωση και των δύο υπολογιστικών μονοπατιών του εργαλείου (Information και Operational Risks) στο Υποκεφάλαιο 3.2.2, η πρακτική αξιολόγηση της παρούσας μελέτης επικεντρώθηκε αποκλειστικά στο μονοπάτι των Πληροφοριακών Κινδύνων. Όλα τα στοχευμένα σενάρια απειλής αντιστοιχίστηκαν επιτυχώς σε τεχνικές κατηγορίες αυτού του καταλόγου, γεγονός που εξηγεί την απουσία δεδομένων (No Data Available) στην καρτέλα των γενικών Επιχειρησιακών Κινδύνων (Operational Risks) του Πίνακα Ελέγχου.

3.4.1 Συγκριτική Ανάλυση Απειλών ανά Περιβάλλον (IT vs OT)

Η πρώτη κρίσιμη απεικόνιση αφορά την κατανομή των μέγιστων επιπέδων κινδύνου διαχωρισμένη ανά Πρωτεύον Αγαθό (Parent Asset), επιτρέποντας την άμεση σύγκριση μεταξύ του Πληροφοριακού Συστήματος (PCS) και της Βιομηχανικής Διαδικασίας (Γερανός).

Όπως παρατηρείται στο παραγόμενο γράφημα, το εργαλείο αναπαρήγαγε αυτόματα την ίδια συγκριτική αρχιτεκτονική (IT vs OT) που θεμελιώθηκε θεωρητικά. Και τα δύο περιβάλλοντα παρουσιάζουν ισοδύναμους μέγιστους κινδύνους της τάξης του 60. Επιβεβαιώνεται οπτικά ότι η διαφοροποίηση του αντικτύπου —με το μοντέλο CIA στο IT και το μοντέλο AIC/Safety στο OT οδηγεί σε μαθηματικά συγκρίσιμα επίπεδα κρίσιμου ρίσκου, προερχόμενα ωστόσο από ριζικά διαφορετικούς φορείς επίθεσης.



Εικόνα 3.4: Συγκριτική κατανομή επιπέδων κινδύνου διαχωρισμένη ανά Πρωτεύον Αγαθό (Continuous Container Unloading Process έναντι PCS & Customs Data). (NC3, 2025)

3.4.2 Οπτική Επαλήθευση του Μαθηματικού Τύπου (Risk Cartography)

Η πλέον σημαντική λειτουργία του Dashboard για την επαλήθευση της μεθοδολογίας είναι η παραγωγή της Χαρτογράφησης Κινδύνων (Cartography / Heatmap). Ο συγκεκριμένος πίνακας αποδεικνύει οπτικά και μαθηματικά τη λειτουργία του τύπου $R = I \times (T \times V)$.

Στον παραγόμενο χάρτη, ο κάθετος άξονας (Y) αναπαριστά τον Αντίκτυπο (Impact) σε κλίμακα 0-4. Ο οριζόντιος άξονας (X) ονομάζεται "Likelihood" από το εργαλείο, ωστόσο δεν ταυτίζεται με την απλή Πιθανότητα Απειλής (T, κλίμακα 0-4). Αντιθέτως, αναπαριστά το μαθηματικό γινόμενο της Πιθανότητας Απειλής επί την Ποιότητα Ευπάθειας ($T \times V$). Δεδομένου ότι $T_{max} = 4$ και $V_{max} = 5$, ο άξονας εκτείνεται λογικά έως το 20.

Η πλήρης αντιστοίχιση των 8 σεναρίων ως ζεύγη (Impact, $T \times V$) επιβεβαιώνεται απόλυτα από τα ενεργά κελιά του χάρτη:

Κελί (X=20, Y=3): Δείχνει "2" κινδύνους (Phishing και DDoS), όπου $3 \times (4 \times 5) = 60$.

Κελί (X=16, Y=3): Δείχνει "1" κίνδυνο (Ransomware), όπου $3 \times (4 \times 4) = 48$.

Κελί (X=15, Y=4): Δείχνει "1" κίνδυνο (Remote Takeover), όπου $4 \times (3 \times 5) = 60$.

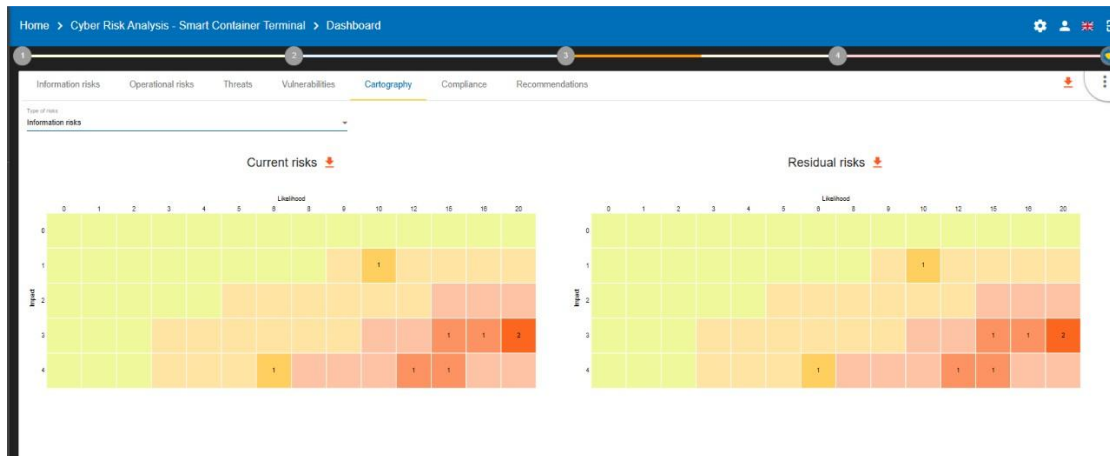
Κελί (X=15, Y=3): Δείχνει "1" κίνδυνο (Vendor MFA), όπου $3 \times (3 \times 5) = 45$.

Κελί (X=12, Y=4): Δείχνει "1" κίνδυνο (Power Blackout), όπου $4 \times (3 \times 4) = 48$.

Κελί (X=10, Y=1): Δείχνει "1" κίνδυνο (GPS Jamming), όπου $1 \times (2 \times 5) = 10$.

Κελί (X=6, Y=4): Δείχνει "1" κίνδυνο (Physical Sabotage), όπου $4 \times (2 \times 3) = 24$.

Η αποτύπωση αυτή αποτελεί την ανεξάρτητη μαθηματική απόδειξη ότι το εργαλείο ακολούθησε με απόλυτη ακρίβεια τη θεωρητική τεκμηρίωση, σύμφωνα με τις προδιαγραφές του (ISO/IEC 27005, 2022).



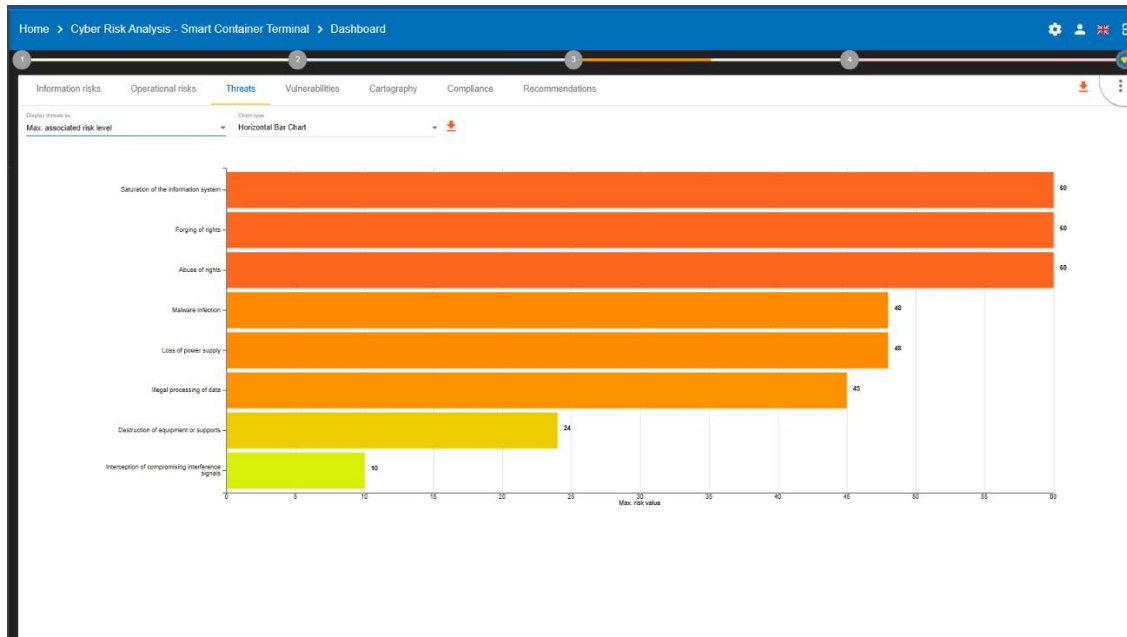
Εικόνα 3.5: Χαρτογράφηση Κινδύνων (Cartography). Οπτική επιβεβαίωση της συνάρτησης Αντικτύπου (Y) και του γινομένου Πιθανότητας/Ευπάθειας (X). (NC3, 2025)

3.4.3 Συγκεντρωτική Ιεράρχηση Κινδύνων (Top Risks)

Η τελική αναφορά επικεντρώνεται στην ολική ιεράρχηση των απειλών, ανεξαρτήτως ζώνης, δημιουργώντας την τελική λίστα προτεραιοτήτων για τη διοίκηση.

Όπως αποτυπώνεται στο παραγόμενο ραβδόγραμμα (Max associated risk level), από τα οκτώ εξεταζόμενα σενάρια, τα έξι κατατάσσονται στην κατηγορία του Υψηλού Κινδύνου (High Risk, σκορ > 27) απαιτώντας άμεση αντιμετώπιση. Στην απόλυτη κορυφή (σκορ 60) βρίσκονται οι επιθέσεις Saturation, Forging of rights και Abuse of rights. Στη μεσαία κλίμακα (Medium Risk, σκορ ≤ 27) κατατάσσονται το Physical Sabotage (24) και το GPS Jamming (10), αποτέλεσμα της ήδη αναλυθείσας στρέβλωσης του γενικού καταλόγου απειλών.

Αυτή η ιεράρχηση αποτελεί τη βάση μετάβασης στο Κεφάλαιο 4, όπου θα οριστούν οι στρατηγικές αντιμετώπισης (Risk Treatment) για τη μείωση αυτών των τιμών σε αποδεκτά επίπεδα υπολειπόμενου κινδύνου (Residual Risk).



Εικόνα 3.6: Συνολική ιεράρχηση των εξεταζόμενων απειλών βάσει του μέγιστου συσχετιζόμενου επιπέδου κινδύνου. (NC3, 2025)

4 Σχέδιο Αντιμετώπισης Κινδύνων και Οργανωτικές Δομές Ασφάλειας

4.1 Προτεινόμενα Μέτρα Προστασίας (Τεχνικά και Μη-Τεχνικά)

Η μετάβαση από την αποτίμηση στην αντιμετώπιση του κινδύνου (Risk Treatment) απαιτεί τη συστηματική επιλογή αντιμέτρων, στοχευμένων ειδικά στις ευπάθειες που εντοπίστηκαν και ποσοτικοποιήθηκαν στο προηγούμενο στάδιο. Ακολουθώντας τη Διπλή Προσέγγιση (Dual Approach) της παρούσας μελέτης, τα μέτρα αντλούνται από διακριτά πρότυπα αναφοράς: το ISO/IEC 27002:2022 για το περιβάλλον της πληροφορικής (IT) (ISO/IEC 27002, 2022) και τη σειρά IEC 62443 για το βιομηχανικό περιβάλλον (OT) (ISA/IEC 62443-3-3, 2013).

Μεθοδολογικά, κάθε προτεινόμενο μέτρο στοχεύει πρωτίστως στη μείωση της παραμέτρου Ποιότητας Ευπάθειας (Vulnerability - V) του μαθηματικού τύπου του MONARC, διατηρώντας σταθερή την Πιθανότητα Απειλής (Threat Probability - T). Η λογική αυτή υπαγορεύεται από το γεγονός ότι η συχνότητα εκδήλωσης μιας απειλής (π.χ. η αποστολή ενός κακόβουλου email) αποτελεί εξωτερικό παράγοντα πέρα από τον έλεγχο του οργανισμού. Αντιθέτως, η εφαρμογή δικλίδων ασφαλείας καθιστά το σύστημα λιγότερο "εκμεταλλεύσιμο" κατά τη στιγμή της επίθεσης, μειώνοντας άμεσα την τιμή της Ευπάθειας (V) και οδηγώντας στη μείωση του συνολικού κινδύνου.

4.1.1 Μέτρα για το Πληροφοριακό Σύστημα (PCS - Ζώνη 1)

Η στρατηγική άμυνας για το Πληροφοριακό Σύστημα Λιμένα (PCS) βασίζεται στους αναθεωρημένους ελέγχους (Controls) του προτύπου ISO/IEC 27002:2022.

- **Phishing / Social Engineering (Ευπάθεια: "No audit policy"):** Η θέσπιση επίσημης πολιτικής ελέγχου και καταγραφής δραστηριοτήτων εξουδετερώνει άμεσα την εντοπισμένη ευπάθεια. Σε τεχνικό επίπεδο, εφαρμόζεται ο Έλεγχος 8.5 (Secure Authentication), ο οποίος επιβάλλει τη χρήση Ελέγχου Ταυτότητας Πολλαπλών Παραγόντων (MFA) για την αποτροπή χρήσης υποκλαπέντων διαπιστευτηρίων. Σε μη-τεχνικό (οργανωτικό) επίπεδο, εφαρμόζεται ο Έλεγχος 6.3 (Information security awareness, education and training) μέσω

επαναλαμβανόμενων προγραμμάτων ευαισθητοποίησης του προσωπικού απέναντι σε τακτικές κοινωνικής μηχανικής.

- **DDoS / Saturation (Ευπάθεια: "No filter against saturation"):** Σύμφωνα με τον Έλεγχο 8.6 (Capacity Management), διασφαλίζεται η επαρκής διαχείριση χωρητικότητας. Το τεχνικό αντίμετρο περιλαμβάνει την εγκατάσταση Τείχους Προστασίας Διαδικτυακών Εφαρμογών (WAF) με μηχανισμούς περιορισμού ρυθμού αιτημάτων (rate limiting), καθώς και τη χρήση εξωτερικής υπηρεσίας μετριασμού (DDoS mitigation cloud scrubbing).
- **Ransomware (Ευπάθεια: "Possibility of modifying/corrupting the software"):** Η αντιμετώπιση επιτυγχάνεται μέσω συνδυασμού των Ελέγχων 8.7 (Protection against malware) και 8.8 (Management of technical vulnerabilities). Τεχνικά, προτείνεται η χρήση συστημάτων EDR (Endpoint Detection and Response) και η αυστηρή πολιτική διαχείρισης ενημερώσεων (patch management). Ως έσχατο οργανωτικό και τεχνικό μέτρο αποκατάστασης, υιοθετείται ο Έλεγχος 8.13 (Information backup) με την τήρηση απομονωμένων και αμετάβλητων αντιγράφων ασφαλείας (offline/immutable backups).
- **Vendor MFA / Supply Chain (Ευπάθεια: "No password required for remote administration"):** Η έκθεση στην αλυσίδα εφοδιασμού (third-party risk) καλύπτεται από τους Ελέγχους 5.19 έως 5.21 (Information security in supplier relationships). Τεχνικά, επιβάλλεται αυστηρός έλεγχος των απομακρυσμένων συνδέσεων συντήρησης με την ανάπτυξη λύσεων PAM (Privileged Access Management) και υποχρεωτικό MFA, τερματίζοντας οριστικά τις ανώνυμες ή κοινόχρηστες προσβάσεις.

4.1.2 Μέτρα για τον Βιομηχανικό Εξοπλισμό (Physical Crane - Ζώνη 3)

Τα μέτρα για τον έλεγχο των PLC, των αισθητήρων και της τροφοδοσίας του Γερανού (ΟΤ) πηγάζουν από τις απαιτήσεις της σειράς προτύπων IEC 62443, δίνοντας έμφαση στη Διαθεσιμότητα και τη Φυσική Ασφάλεια.

- **Command Injection / Remote Takeover (Ευπάθεια: "System is connected to external networks"):** Αντιμετωπίζεται μέσω της τεχνικής απαίτησης SR 5.2 (Zone Boundary Protection) του IEC 62443-3-3. Το πρωτεύον τεχνικό μέτρο είναι η εγκατάσταση εφεδρικού βιομηχανικού τείχους προστασίας (Redundant Industrial Firewall), το οποίο επιβάλλει αυστηρό έλεγχο ροής δεδομένων μεταξύ της Ζώνης 1 και της Ζώνης 3. Η λύση της εφεδρείας (redundancy) επιλύει ταυτόχρονα το Ενιαίο Σημείο Αποτυχίας (Single Point of Failure - SPOF) της δικτυακής αρχιτεκτονικής, το οποίο είχε εντοπιστεί ως θεωρητικό κενό στο Υποκεφάλαιο 2.4. Παράλληλα, οργανωτικά εφαρμόζεται η Αρχή των Ελάχιστων Προνομίων (Least Privilege).
- **Power Blackout (Ευπάθεια: "Equipment sensitive to electrical disturbances"):** Ανταποκρινόμενοι στην απαίτηση SR 7.2 (Resource Management), τοποθετούνται συστήματα αδιάλειπτης παροχής ενέργειας (UPS) βιομηχανικού τύπου, διατάξεις προστασίας από υπερτάσεις (surge protectors) και εφεδρικές γεννήτριες (Τεχνικά Μέτρα). Οργανωτικά, επιβάλλεται ένα αυστηρό πρόγραμμα προληπτικής συντήρησης των ηλεκτρολογικών υποδομών.
- **Physical Sabotage (Ευπάθεια: "Equipment accessible to unauthorized persons"):** Σύμφωνα με τις οργανωτικές απαιτήσεις φυσικής ασφάλειας του προτύπου IEC 62443-2-1 (IEC 62443-2-1, 2024), ο φυσικός εξοπλισμός (καμπίνες PLC, καλωδιώσεις δικτύου) θωρακίζεται μέσω ελεγχόμενης πρόσβασης (βιομετρικά συστήματα ή έξυπνες κάρτες) και συστημάτων παρακολούθησης (CCTV). Οργανωτικά, υιοθετούνται αυστηρές διαδικασίες ταυτοποίησης για τους επισκέπτες και τους εξωτερικούς εργολάβους, καθώς και πρωτόκολλα απομόνωσης ενέργειας (lock-out/tag-out).
- **GNSS/GPS Jamming & Spoofing (Ευπάθεια: "Compromising stray radiation"):** Για την προστασία του αυτοματοποιημένου συστήματος διεύθυνσης, εγκαθίστανται GNSS δέκτες προηγμένης τεχνολογίας με αντικλεπτικές ιδιότητες (anti-jamming/anti-spoofing antennas) ως πρώτο τεχνικό ανάχωμα, ικανοποιώντας την απαίτηση SR 7.1 (Denial of Service Protection). Ωστόσο, το κρίσιμότερο οργανωτικό και τεχνικό αντίμετρο είναι η ύπαρξη διαδικασιών

αδρανειακής πλοήγησης (dead-reckoning) και η δυνατότητα άμεσης, χειροκίνητης παράκαμψης (manual fallback) του ελέγχου από εκπαιδευμένο γερανοδηγό, διασφαλίζοντας τη φυσική ασφάλεια (Safety) σε περίπτωση ολοκληρωτικής απώλειας του δορυφορικού σήματος.

4.2 Εφαρμογή της Θεραπείας Κινδύνου στο MONARC και Υπολογισμός Υπολειπόμενου Κινδύνου

Μετά τον θεωρητικό καθορισμό των προτεινόμενων μέτρων, το επόμενο στάδιο αφορά την πρακτική εισαγωγή τους στο λογισμικό MONARC. Σκοπός είναι ο υπολογισμός του Υπολειπόμενου Κινδύνου (Residual Risk), δηλαδή του ρίσκου που παραμένει ενεργό στο σύστημα μετά την εφαρμογή της θεραπείας (Treatment). Στο περιβάλλον του εργαλείου, επιλέχθηκε η στρατηγική «Μείωσης» (Reduction) (NC3, 2025) για το σύνολο των 8 αξιολογημένων απειλών, στοχεύοντας αποκλειστικά στη μείωση της Ποιότητας Ευπάθειας (V_{new}).

4.2.1 Μεθοδολογία Βαθμολόγησης Υπολειπόμενης Ευπάθειας

Για την αποφυγή αυθαίρετων ποσοτικοποιήσεων, η νέα βαθμολογία της Ευπάθειας (V_{new}) υπάκουσε σε μια αυστηρή, τριμερή φιλοσοφία αξιολόγησης, βασισμένη στην κλίμακα 0-5 του εργαλείου.

Σημειώνεται ότι η κλιμάκωση αυτή περιορίζεται σκόπιμα στο εύρος 1-3, αποκλείοντας τα άκρα της επίσημης κλίμακας του εργαλείου: το επίπεδο 0 θα αντιπροσώπευε μη ρεαλιστική, απόλυτη εξάλειψη κινδύνου, ασύμβατη με τη φιλοσοφία συνεχούς διαχείρισης της παρούσας μελέτης, ενώ τα επίπεδα 4-5 θα υποδήλωναν αναποτελεσματικά μέτρα — αντίθετα με την ίδια την υπόθεση εφαρμογής ουσιαστικών αντιμέτρων σε κάθε σενάριο.

- $V = 1$ (Πολύ χαμηλή ευπάθεια): Αποδόθηκε αποκλειστικά σε μέτρα απόλυτα ώριμα, τα οποία εξουδετερώνουν την απειλή στη ρίζα της, ανεξαρτήτως εξωτερικών παραγόντων.
- $V = 2$ (Χαμηλή ευπάθεια): Αποδόθηκε σε ισχυρά μέτρα προστασίας τα οποία, ωστόσο, διατηρούν εγγενή κενά, κυρίως λόγω του απρόβλεπτου ανθρώπινου παράγοντα ή περιορισμών σε υποκείμενα πρωτόκολλα.
- $V = 3$ (Μέτρια ευπάθεια): Αποδόθηκε συντηρητικά σε περιπτώσεις όπου η σύγχρονη τεχνολογία έχει αποδεδειγμένα όρια έναντι προηγμένων επιθέσεων, λειτουργώντας και ως αναγνώριση των μεθοδολογικών "τυφλών σημείων" του καταλόγου.

Εφαρμόζοντας αυτό το «κλειδί ανάγνωσης» στα 8 σενάρια της μελέτης, προέκυψαν οι εξής προσαρμογές:

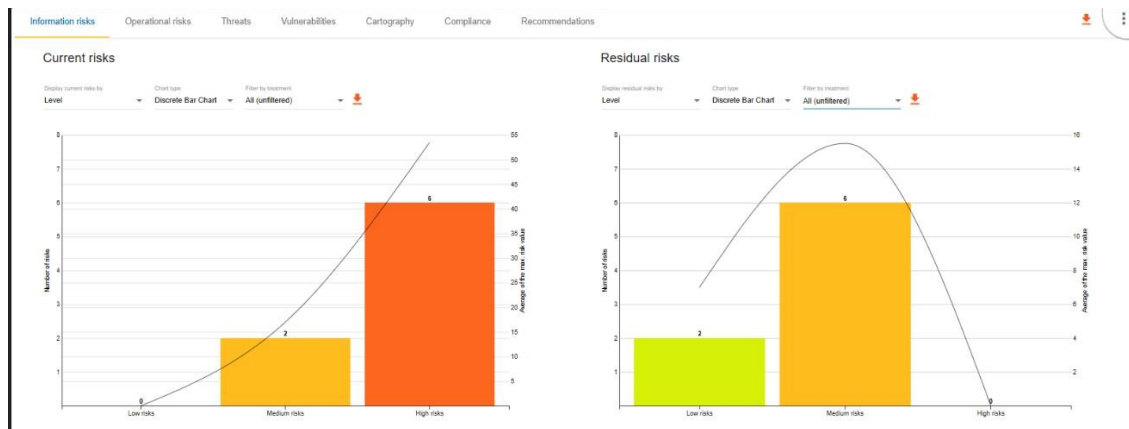
Στο Πληροφοριακό Σύστημα (IT), οι επιθέσεις Ransomware, DDoS και Vendor MFA έλαβαν βαθμολογία $V=1$, καθώς οι προτεινόμενες τεχνικές (Immutable Backups, Cloud Scrubbing, PAM) λειτουργούν ντετερμινιστικά και αποκόπτουν πλήρως την αλυσίδα επίθεσης. Αντιθέτως, η απειλή του Phishing αξιολογήθηκε με $V=2$, διότι η κοινωνική μηχανική και η «κόπωση» ελέγχου ταυτότητας (MFA fatigue) δεν εξαλείφονται ποτέ απόλυτα.

Αντίστοιχα στο Βιομηχανικό Περιβάλλον (OT), το Power Blackout και το Physical Sabotage έλαβαν $V=1$ λόγω της ωριμότητας των μηχανολογικών/φυσικών λύσεων (UPS, Βιομετρικά). Το Command Injection περιορίστηκε στο $V=2$, καθώς τα βιομηχανικά πρωτόκολλα πίσω από το τείχος προστασίας παραμένουν εγγενώς μη κρυπτογραφημένα. Τέλος, το GPS Jamming αξιολογήθηκε συντηρητικά με $V=3$, αποτυπώνοντας τα τεχνολογικά όρια των anti-jamming κεραιών έναντι στρατιωτικού επιπέδου παρεμβολών.

4.2.2 Οπτικοποίηση και Μαθηματική Επαλήθευση

Η καταχώρηση των νέων τιμών (V_{new}) στον Πίνακα Ελέγχου (Dashboard) του MONARC μετέβαλε ριζικά το προφίλ ρίσκου της εγκατάστασης.

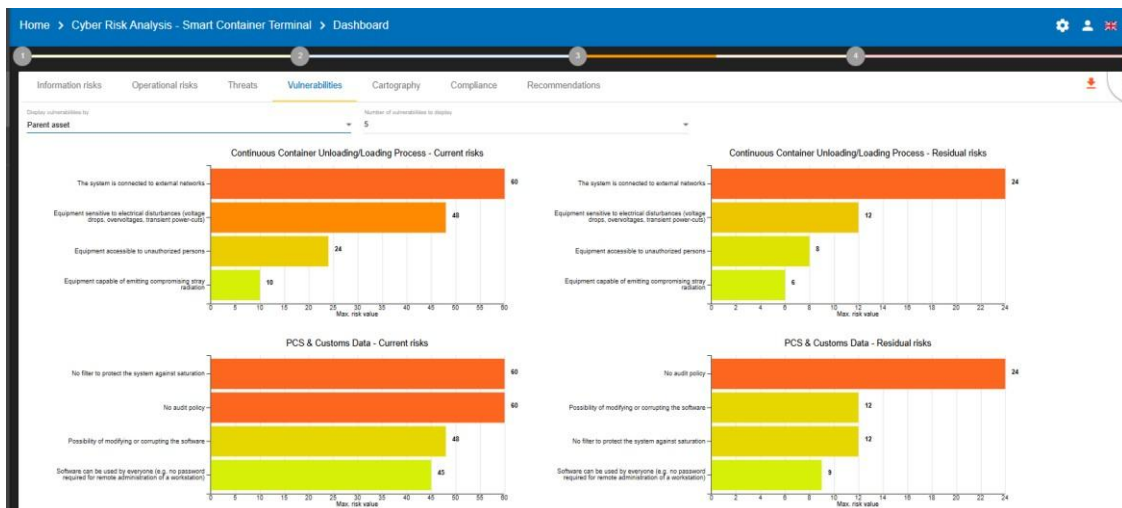
Όπως αποτυπώνεται στο συγκεντρωτικό ραβδόγραμμα (Εικόνα 4.A), η αρχική κατάσταση (Current risks) εμφάνιζε 6 κινδύνους στην κατηγορία High (Κόκκινο, >27) και 2 στην κατηγορία Medium (Πορτοκαλί, ≤27). Μετά τη θεραπεία (Residual risks), η κατηγορία High μηδενίστηκε.



Εικόνα 4.1: Συγκριτική κατανομή (Current vs Residual risks). Εμφανής η ολική εξάλειψη των κρίσιμων (High) κινδύνων. (NC3, 2025)

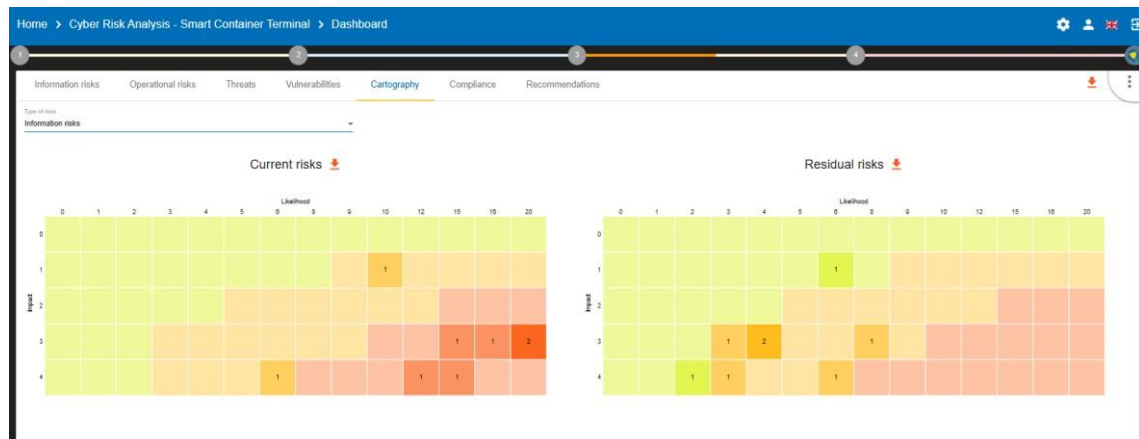
Αξίζει να σημειωθεί ότι 6 από τα 8 ρίσκα προσγειώθηκαν στην κατηγορία Medium, ενώ μόνο 2 (Physical Sabotage και GPS Jamming) έφτασαν στην κατηγορία Low (Πράσινο, ≤8), κυρίως λόγω του αρχικά χαμηλού τους αντικτύπου. Η θεραπεία, συνεπώς, επέφερε ουσιαστική, όχι όμως πλήρη εξάλειψη του κινδύνου. Το αποτέλεσμα αυτό δεν αποτελεί αδυναμία της ανάλυσης, αλλά ρεαλιστική και τίμια αναπαράσταση που συνάδει με τη φύση της κυβερνοασφάλειας ως συνεχούς διαδικασίας διαχείρισης και όχι ως εφάπαξ επίλυσης.

Η αναλυτική πτώση των κινδύνων ανά Πρωτεύον Αγαθό (Εικόνα 4.B) επιβεβαιώνει μαθηματικά τον τύπο $R = I \times (T \times V_{new})$. Χαρακτηριστικά, το Phishing έπεσε από το 60 στο 24 ($3 \times (4 \times 2)$), ενώ το Power Blackout από το 48 στο 12 ($4 \times (3 \times 1)$).



Εικόνα 4.2: Αναλυτική πτώση του επιπέδου κινδύνου, διαχωρισμένη ανά περιβάλλον (IT έναντι OT). (NC3, 2025)

Η συνολική επιτυχία του Σχεδίου Αντιμετώπισης αποδεικνύεται οπτικά μέσω της νέας Χαρτογράφησης Κινδύνων (Εικόνα 4.C). Στο Heatmap του Υπολειπόμενου Κινδύνου, παρατηρείται η μαζική μετατόπιση όλων των τιμών (κουτάκια) προς τα κάτω και αριστερά, απομακρυνόμενες οριστικά από τη θερμή (κόκκινη) ζώνη του διαγράμματος.



Εικόνα 4.3: Χαρτογράφηση Κινδύνων (Cartography). Αριστερά οι αρχικοί κίνδυνοι και δεξιά η μετατόπισή τους σε ασφαλείς ζώνες μετά τη θεραπεία. (NC3, 2025)

4.2.3 Στρατηγική και Χρονοδιάγραμμα Υλοποίησης

Για τη μετάβαση από τη θεωρητική βαθμολόγηση στην πρακτική εφαρμογή από τον οργανισμό λιμένα, η υλοποίηση των μέτρων διακρίνεται σε δύο φάσεις, με κριτήριο το κόστος (CAPEX) και την πολυπλοκότητα:

Άμεση Εφαρμογή (0-3 μήνες): Περιλαμβάνει μέτρα λογισμικού και πολιτικών ασφαλείας που δεν απαιτούν πολύπλοκη προμήθεια υλικού. Εδώ εντάσσονται η ενεργοποίηση MFA, η διαμόρφωση του συστήματος PAM για τους προμηθευτές, η εφαρμογή πολιτικών Audit/Patch Management και η έναρξη του προγράμματος εκπαίδευσης του προσωπικού.

Σταδιακή Εφαρμογή (3-12 μήνες): Αφορά παρεμβάσεις υψηλού κόστους και υλικού εξοπλισμού (hardware). Σε αυτή τη φάση εντάσσεται η εγκατάσταση του Redundant Βιομηχανικού Firewall στη Ζώνη 3, η τοποθέτηση βιομηχανικών UPS, η εγκατάσταση κεραιών anti-jamming στον γερανό, καθώς και η σύναψη εξωτερικών συμβάσεων για Cloud Scrubbing υπηρεσίες.

Συνολικά, η εφαρμογή των 8 στοχευμένων μέτρων προστασίας που προτάθηκαν στην παρούσα μελέτη, επέφερε την πτώση του μέσου όρου ρίσκου (για το σύνολο των σεναρίων) από το 44.4 (Current Risk) στο 13.4 (Residual Risk). Το γεγονός αυτό μεταφράζεται σε μια συνολική, μετρήσιμη μείωση της τάξης του ~70% στο επίπεδο κινδύνου της εγκατάστασης.

4.3 Κατανομή Οργανωτικών Δομών και Αρμοδιοτήτων

Η επιτυχής εφαρμογή των τεχνικών και οργανωτικών αντιμέτρων που αξιολογήθηκαν πρακτικά στο περιβάλλον του MONARC, προϋποθέτει τη μετάβαση από τον τεχνικό σχεδιασμό στην καθιέρωση ενός ισχυρού πλαισίου Διακυβέρνησης Ασφάλειας (Security Governance). Ένα σύστημα διαχείρισης κινδύνου καθίσταται λειτουργικό μόνο όταν συνοδεύεται από σαφή κατανομή αρμοδιοτήτων (Security Roles and Responsibilities) εντός του οργανισμού.

Είναι αξιοσημείωτο ότι τόσο το πρότυπο της πληροφορικής ασφάλειας (ISO/IEC 27002, 2022) μέσω του Ελέγχου 5.2 ("Information security roles and responsibilities"), όσο και το πρότυπο της βιομηχανικής ασφάλειας (IEC 62443-2-1, 2024) μέσω της οργανωτικής απαίτησης ORG 1.3 ("Security roles and responsibilities"), συγκλίνουν ανεξάρτητα στην ίδια ακριβώς θεμελιώδη απαίτηση. Η σύμπτωση αυτή των δύο διαφορετικών επιτροπών τυποποίησης επιβεβαιώνει τη διαχρονική εγκυρότητα της Διπλής Προσέγγισης (Dual Approach) που υιοθετεί η παρούσα μελέτη, όχι μόνο σε επίπεδο τεχνικής ανάλυσης, αλλά και στο κρίσιμο επίπεδο της οργανωσιακής διακυβέρνησης.

4.3.1 Ορισμός Ρόλων και Διαχωρισμός Αρμοδιοτήτων (Segregation of Duties)

Για να διασφαλιστεί η ακεραιότητα της λειτουργίας του Λιμένα, η κατανομή των ρόλων υπακούει ρητά στον Έλεγχο 5.3 (Segregation of Duties) του προτύπου ISO/IEC 27002:2022 (ISO/IEC 27002, 2022), ο οποίος επιβάλλει τον διαχωρισμό συγκρουόμενων αρμοδιοτήτων. Υπό αυτό το πρίσμα, ορίζεται μια κοινή κορυφή λογοδοσίας, αλλά διακριτή, εξειδικευμένη εκτέλεση μεταξύ των ζωνών IT και OT:

1. **Υπεύθυνος Ασφάλειας Πληροφοριών (CISO):** Αποτελεί τον κεντρικό πυρήνα ελέγχου. Δεν εκτελεί τις τεχνικές ρυθμίσεις, αλλά λογοδοτεί (Accountable) στη διοίκηση του λιμένα για τη συνολική στρατηγική, την έγκριση των πολιτικών και την εποπτεία του υπολειπόμενου κινδύνου, διασφαλίζοντας τη σύγκλιση (convergence) μεταξύ IT και OT.
2. **Διαχειριστής Ασφάλειας Συστημάτων IT (IT Security Administrator):** Είναι υπεύθυνος (Responsible) για την τεχνική εφαρμογή των μέτρων στο Πληροφοριακό Σύστημα (Ζώνη 1), όπως η διαχείριση ταυτότητας χρηστών (MFA), το Patch Management και η εποπτεία του WAF.
3. **Μηχανικός Ασφάλειας OT / Υπεύθυνος Εγκατάστασης (OT Security Engineer / Plant Manager):** Αναλαμβάνει την αποκλειστική ευθύνη (Responsible) για τη Ζώνη 3. Διαχειρίζεται το Redundant Firewall, τα βιομηχανικά πρωτόκολλα των PLC και συντηρεί τις μηχανολογικές διατάξεις (UPS, Anti-jamming κεραίες). Ο διαχωρισμός αυτού του ρόλου από τον IT Administrator αποτρέπει τα τυφλά "patching" από μη εξειδικευμένο προσωπικό που θα μπορούσαν να σταματήσουν την παραγωγή.
4. **Τελικοί Χρήστες / Χειριστές Γερανών (End Users / Crane Operators):** Αποτελούν την πρώτη γραμμή άμυνας. Ο ρόλος τους δεν είναι απλώς παθητικός· είναι υπεύθυνοι (Responsible) για την άμεση αναφορά απόπειρων Phishing και για την εκτέλεση διαδικασιών έκτακτης ανάγκης, όπως η Χειροκίνητη Παράκαμψη (Manual Fallback) σε περίπτωση GPS Jamming.

4.3.2 Επιχειρησιακή Εφαρμογή μέσω Μήτρας RACI

Ενώ τα προαναφερθέντα πρότυπα καθορίζουν τι πρέπει να γίνει, η πρακτική εφαρμογή αυτών των απαιτήσεων στην καθημερινή λειτουργία του λιμένα επιτυγχάνεται μέσω της μήτρας RACI (Responsible, Accountable, Consulted, Informed). Η εν λόγω μήτρα δεν αποτελεί εργαλείο τυποποίησης των προτύπων ISO/IEC, αλλά ένα καταξιωμένο, ανεξάρτητο εργαλείο διοίκησης και οργανωσιακής διακυβέρνησης. Μέσω αυτού, αποτυπώνεται οπτικά το πώς αλληλεπιδρούν οι τέσσερις προαναφερθέντες ρόλοι στις κρίσιμες διεργασίες ασφαλείας που προέκυψαν από το Σχέδιο Αντιμετώπισης Κινδύνων (Κεφάλαιο 4.1).

Πίνακας 4.1: Μήτρα κατανομής αρμοδιοτήτων RACI (R=Υπεύθυνος εκτέλεσης, A=Υπόλογος/Εγκρίνων, C=Σύμβουλος/Ερωτώμενος, I=Ενημερούμενος). Πηγή: Ιδία επεξεργασία

Κρίσιμη Διεργασία / Αντίμετρο	CISO	IT Sec Admin	OT Sec Eng	End Users
Σύνταξη, Έγκριση και Αναθεώρηση Πολιτικών Ασφαλείας	R/A	C	C	I
Εκτέλεση Ενημερώσεων Λογισμικού (IT Patch Management)	A	R	I	I
Παραμετροποίηση Βιομηχανικού Τείχους (OT Redundant Firewall)	A	C	R	I
Εκτέλεση Χειροκίνητης Παράκαμψης (Manual Fallback / Jamming)	I	I	A	R
Αναφορά Περιστατικού Κυβερνοασφάλειας (π.χ. Phishing)	A	I	I	R

Μέσω αυτής της οργανωτικής δομής, διασφαλίζεται ότι τα μέτρα που εξομοίωσε το MONARC δεν παραμένουν σε θεωρητικό επίπεδο, αλλά εντάσσονται ομαλά και ελεγχόμενα στις καθημερινές διαδικασίες του ναυτιλιακού οργανισμού.

5 Βασικές Πολιτικές, Διαδικασίες και Επιχειρησιακή Συνέχεια

Έχοντας ολοκληρώσει την αξιολόγηση των κινδύνων (Κεφάλαιο 3) και τον σχεδιασμό των μέτρων και της οργανωτικής δομής (Κεφάλαιο 4), το παρόν κεφάλαιο μεταφράζει τα τεχνικά ευρήματα σε εφαρμόσιμους επιχειρησιακούς κανόνες. Οι πολιτικές και οι διαδικασίες αποτελούν το «Σύνταγμα» και το «Εγχειρίδιο Λειτουργίας» του ναυτιλιακού οργανισμού, διασφαλίζοντας ότι η ασφάλεια ενσωματώνεται στην καθημερινότητα του λιμένα.

5.1 Βασικές Πολιτικές Ασφάλειας

Για τη σύνταξη των Πολιτικών Ασφαλείας επιλέχθηκε η δομημένη προσέγγιση (Σκοπός, Πεδίο Εφαρμογής, Δηλώσεις Πολιτικής, Επιβολή), εναρμονισμένη με τις βέλτιστες πρακτικές σύνταξης εταιρικών εγγράφων (π.χ. πρότυπα SANS Institute).

Είναι εξαιρετικά σημαντικό να τονιστεί ότι η θεμελιώδης αρχή της Διπλής Προσέγγισης (Dual Approach) που διατρέχει την παρούσα μελέτη, επιβεβαιώνεται εκ νέου. Όπως θα φανεί στις παρακάτω πολιτικές, οι απαιτήσεις του προτύπου IT (ISO/IEC 27002, 2022) και του προτύπου OT (ISA/IEC 62443-3-3, 2013) καταλήγουν σε σχεδόν ταυτόσημες, παράλληλες επιταγές, γεφυρώνοντας πλήρως τον κόσμο της Πληροφορικής με τον κόσμο του Βιομηχανικού Ελέγχου.

5.1.1 Πολιτική Ελέγχου Πρόσβασης (Access Control Policy)

- **Πρότυπα Αναφοράς:** ISO/IEC 27002 (Έλεγχος 5.15) & IEC 62443-3-3 (SR 1.1, SR 2.1).
- **Σκοπός:** Η αποτροπή μη εξουσιοδοτημένης πρόσβασης σε κρίσιμα δεδομένα (PCS) και βιομηχανικό εξοπλισμό (PLC), αμβλύνοντας άμεσα τις ευπάθειες τύπου "Command Injection".
- **Πεδίο Εφαρμογής:** Εφαρμόζεται σε όλους τους υπαλλήλους, εργολάβους και συστήματα που αλληλεπιδρούν με τη Ζώνη 1 (IT) και τη Ζώνη 3 (OT).
- **Δηλώσεις Πολιτικής (Κανόνες):**
 - Η πρόσβαση σε όλα τα συστήματα διέπεται αυστηρά από την Αρχή των Ελάχιστων Προνομίων (Least Privilege).
 - Απαγορεύεται ρητά η χρήση κοινόχρηστων λογαριασμών (shared accounts) για την πρόσβαση σε κρίσιμες εφαρμογές του PCS ή σε διεπαφές διαχείρισης των Γερανών.
 - Οποιαδήποτε απομακρυσμένη πρόσβαση από εξωτερικά δίκτυα προς τη Ζώνη 3 (OT) επιτρέπεται μόνο μέσω κρυπτογραφημένης σήραγγας (VPN) και περνώντας υποχρεωτικά από το Redundant Firewall.
 - Αρμοδιότητα Επιβολής: Σύμφωνα με τη Μήτρα RACI (Πίνακας 4.1), η τεχνική επιβολή στη Ζώνη 1 βαρύνει τον IT Security Administrator, ενώ στη Ζώνη 3 τον OT Security Engineer. Ο CISO διατηρεί τον ρόλο του Υπόλογου (Accountable).

5.1.2 Πολιτική Κωδικών και Πιστοποίησης (Password & Authentication Policy)

- **Πρότυπα Αναφοράς:** ISO/IEC 27002 (Έλεγχος 5.17) & IEC 62443-3-3 (SR 1.7). (Σημείωση: Αποτελούν στενά παράλληλες απαιτήσεις της έννοιας "Strength of authentication" σε IT και OT).
- **Σκοπός:** Η αντιμετώπιση του φαινομένου "No password required" για απομακρυσμένη διαχείριση (Vendor MFA risk), η εξάλειψη των εργοστασιακών κωδικών στα PLC (ευπάθεια

που εντοπίστηκε στο Κεφ. 2.4), και η θωράκιση έναντι επιθέσεων κοινωνικής μηχανικής (Phishing).

- **Πεδίο Εφαρμογής:** Όλα τα συστήματα ταυτοποίησης χρηστών στις Ζώνες 1 και 3.
- **Δηλώσεις Πολιτικής (Κανόνες):**
 - Επιβάλλεται υποχρεωτικά η χρήση Ελέγχου Ταυτότητας Πολλαπλών Παραγόντων (MFA) για κάθε απομακρυσμένη σύνδεση, καθώς και για συνδέσεις τρίτων προμηθευτών (Vendors) μέσω συστήματος PAM.
 - Οι κωδικοί πρόσβασης πρέπει να έχουν ελάχιστο μήκος δεκατεσσάρων (14) χαρακτήρων και να συνδυάζουν αλφαριθμητικά σύμβολα.
 - Σε περίπτωση υποψίας παραβίασης (π.χ. αναφορά ύποπτου email από End User), τα διαπιστευτήρια του χρήστη ανακαλούνται και αλλάζουν άμεσα.
 - Αρμοδιότητα Επιβολής: Εκτελεστικός υπεύθυνος (R) ορίζεται ο IT Security Administrator για τη Ζώνη 1, και ο OT Security Engineer για τη Ζώνη 3 (συμπεριλαμβανομένης της αλλαγής διαπιστευτηρίων σε PLCs και HMI panels).

5.1.3 Πολιτική Καταγραφής και Ελέγχου (Logging & Audit Policy)

- **Πρότυπα Αναφοράς:** ISO/IEC 27002 (Έλεγχος 8.15) & IEC 62443-3-3 (SR 2.8, SR 2.9).
- **Σκοπός:** Η εξάλειψη της ευπάθειας "No audit policy" που καταγράφηκε στο MONARC, διασφαλίζοντας την ιχνηλασιμότητα των ενεργειών πριν, κατά τη διάρκεια και μετά από ένα συμβάν ασφαλείας.
- **Πεδίο Εφαρμογής:** Εφαρμόζεται σε διακομιστές, δίκτυα (Firewalls) και κρίσιμους σταθμούς εργασίας της Ζώνης 1 και Ζώνης 3.
- **Δηλώσεις Πολιτικής (Κανόνες):**
 - Τα συστήματα οφείλουν να καταγράφουν (log) όλες τις επιτυχημένες και αποτυχημένες προσπάθειες σύνδεσης, καθώς και τις αλλαγές σε δικαιώματα συστήματος.
 - Τα αρχεία καταγραφής διατηρούνται σε ασφαλή, κεντρικό διακομιστή για ελάχιστο χρονικό διάστημα έξι (6) μηνών.
 - Απαγορεύεται αυστηρά η τροποποίηση ή η διαγραφή των αρχείων καταγραφής από τους διαχειριστές συστημάτων (προστασία έναντι tampering).
 - Αρμοδιότητα Επιβολής: Η υλοποίηση ανήκει στους IT Sec Admin και OT Sec Eng, ενώ η περιοδική ανασκόπηση των αναφορών (audit review) ανήκει στον CISO.

5.1.4 Πολιτική Αντιγράφων Ασφαλείας (Backup Policy)

- **Πρότυπα Αναφοράς:** ISO/IEC 27002 (Έλεγχος 8.13) & IEC 62443-3-3 (SR 7.3).
- **Σκοπός:** Η διασφάλιση της επιχειρησιακής συνέχειας (Availability) και η γρήγορη ανάκαμψη από περιστατικά όπως μόλυνση από Ransomware ή βλάβες υλικού (Power Blackout).
- **Πεδίο Εφαρμογής:** Δεδομένα του συστήματος PCS (Ζώνη 1) και αρχεία παραμετροποίησης (configurations) των PLC του Γερανού (Ζώνη 3).
- **Δηλώσεις Πολιτικής (Κανόνες):**
 - Εφαρμόζεται ρητά ο κανόνας "3-2-1" (3 αντίγραφα, σε 2 διαφορετικά μέσα, 1 εκτός εγκατάστασης).
 - Τα κρίσιμα αντίγραφα ασφαλείας πρέπει να είναι αμετάβλητα (immutable) και αποσυνδεδεμένα από το κύριο δίκτυο (offline) για την προστασία από κακόβουλο λογισμικό κρυπτογράφησης.
 - Απαιτείται η διεξαγωγή δοκιμών επαναφοράς (restoration tests) τουλάχιστον μία φορά το εξάμηνο.
 - Αρμοδιότητα Επιβολής: Η εκτέλεση και συντήρηση των αντιγράφων βαρύνει (R) τους αντίστοιχους διαχειριστές (IT και OT) ανάλογα με τη ζώνη, υπό την τελική έγκριση (A) του CISO.

5.2 Βασικές Διαδικασίες (Procedures)

Ενώ οι Πολιτικές Ασφαλείας (Υποκεφάλαιο 5.1) ορίζουν τους κανόνες και το "τι" πρέπει να γίνει, οι Διαδικασίες αποτελούν τα επιχειρησιακά εγχειρίδια που περιγράφουν το "πώς" εκτελούνται αυτοί οι κανόνες βήμα προς βήμα. Για τη διασφάλιση της ορθής εκτέλεσης, κάθε βήμα ανατίθεται ρητά στους ρόλους που θεσπίστηκαν στη Μήτρα RACI (Κεφάλαιο 4.3).

5.2.1 Διαδικασία Αντιμετώπισης Περιστατικών Κυβερνοασφάλειας

Για τη διαχείριση περιστατικών, η παρούσα μελέτη υιοθετεί τις πλέον πρόσφατες οδηγίες του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας των ΗΠΑ, και συγκεκριμένα το αναθεωρημένο πρότυπο NIST SP 800-61 Rev. 3 (NIST SP 800-61r3, 2025). Η νέα αυτή έκδοση εγκαταλείπει το παρωχημένο μοντέλο τεσσάρων φάσεων και ευθυγραμμίζεται πλήρως με τον πυρήνα του NIST CSF 2.0, γεφυρώνοντας τη διαδικασία με το πλαίσιο που αναλύθηκε στο Κεφάλαιο 1.3.

Η διαδικασία εφαρμόζεται μέσα από το ακόλουθο ρεαλιστικό σενάριο επίθεσης (Worked Example): Μόλυνση του Πληροφοριακού Συστήματος (PCS) από Ransomware.

Παρότι οι λειτουργίες Govern, Identify και Protect του NIST αποτελούν στην πραγματικότητα συνεχείς, διαρκείς δραστηριότητες διαχείρισης κινδύνου (και όχι ένα διακριτό αρχικό στάδιο), στο παρόν σενάριο παρουσιάζονται ακολουθιακά ως «Φάσεις» αποκλειστικά για λόγους αφηγηματικής σαφήνειας στο συγκεκριμένο παράδειγμα.

- **Φάση 1:** Προετοιμασία (Govern, Identify, Protect) ◦ Ενέργεια: Βασίζεται προληπτικά στα ήδη εγκατεστημένα μέτρα προστασίας (όπως τα Redundant Firewalls και η τακτική διαχείριση ενημερώσεων - Patch Management) και στην ισχύουσα Πολιτική Αντιγράφων Ασφαλείας (Κεφ. 5.1.4).
- **Φάση 2:** Ανίχνευση (Detect) ◦ Ενέργεια: Το σύστημα EDR ή τα εργαλεία κεντρικής καταγραφής (Logging) εντοπίζουν μαζική, ανώμαλη κρυπτογράφηση αρχείων στο PCS.
 - Εκτελείται από: IT Security Administrator (ή μέσω αναφοράς End User).
- **Φάση 3:** Απόκριση (Respond) ◦ Βήμα 3.1 - Περιορισμός: Άμεση αποσύνδεση του μολυσμένου διακομιστή PCS από το δίκτυο για να αποτραπεί η πλευρική μετακίνηση (lateral movement) προς το βιομηχανικό δίκτυο (Ζώνη 3).
 - Εκτελείται από: IT Security Administrator (Ενημερώνεται ο OT Security Engineer).

Βήμα 3.2 - Εξάλειψη: Απομόνωση του κακόβουλου λογισμικού και διαγραφή των μολυσμένων αρχείων, χωρίς την καταβολή λύτρων.
- **Φάση 4:** Ανάκαμψη (Recover) ◦ Ενέργεια: Επαναφορά του συστήματος PCS στην προηγούμενη υγιά του κατάσταση μέσω των αμετάβλητων (immutable) αντιγράφων ασφαλείας.
 - Εκτελείται από: IT Security Administrator (Κατόπιν έγκρισης του CISO).
- **Φάση 5:** Βελτίωση (Improve) ◦ Ενέργεια: Καταγραφή των διδαγμάτων (Lessons Learned) και επικαιροποίηση των τιμών της Ευπάθειας στο λογισμικό MONARC (Κεφάλαιο 3) για συνεχή βελτίωση του προφίλ ρίσκου.

5.2.2 Διαδικασία Δημιουργίας και Επαναφοράς Αντιγράφων (Backup & Restore)

Η παρούσα διαδικασία λειτουργικοποιεί τον κανόνα "3-2-1" που θεσπίστηκε στην Πολιτική 5.1.4, εξασφαλίζοντας τη διαθεσιμότητα των δεδομένων του λιμένα.

- **Βήμα 1:** Προγραμματισμένη Λήψη Αντιγράφων ◦ Ενέργεια: Εκτέλεση ημερήσιου αυξητικού (incremental) backup και εβδομαδιαίου πλήρους (full) backup.
 - Εκτελείται από: IT Security Administrator (για το PCS) και OT Security Engineer (για τα configurations των PLC).
- **Βήμα 2:** Απομόνωση (Air-Gapping)
 - Ενέργεια: Μεταφορά του εβδομαδιαίου πλήρους αντιγράφου σε μέσο αποθήκευσης εκτός δικτύου (offline/immutable), καθιστώντας το απρόσβλητο σε επιθέσεις Ransomware.

- ο Εκτελείται από: IT Security Administrator.
- **Βήμα 3:** Εξαμηνιαία Δοκιμή Επαναφοράς (Restore Test) ο Ενέργεια: Δοκιμαστική επαναφορά του συστήματος από τα αντίγραφα σε απομονωμένο περιβάλλον (sandbox), για την επαλήθευση της ακεραιότητάς τους. ο Εκτελείται από: IT Security Administrator / OT Security Engineer (Έγκριση: CISO).

5.2.3 Διαδικασία Διαχείρισης Χρηστών (JML Lifecycle)

Βασιζόμενη στον Έλεγχο 5.18 (Access rights) του ISO/IEC 27002:2022 (ISO/IEC 27002, 2022), η διαδικασία εφαρμόζει την αρχή των Ελάχιστων Προνομίων μέσα από τον καθιερωμένο κύκλο ζωής "JML" (Joiner - Mover - Leaver).

- **Βήμα 1:** Νεοεισερχόμενος (Joiner) ο Ενέργεια: Δημιουργία λογαριασμού για τον νέο υπάλληλο. Αποδίδονται αυστηρά τα ελάχιστα δικαιώματα που απαιτεί ο ρόλος του (Least Privilege) και διαμορφώνεται άμεσα ο Έλεγχος Ταυτότητας Πολλαπλών Παραγόντων (MFA). ο Εκτελείται από: IT Security Administrator.
- **Βήμα 2:** Μετακινούμενος (Mover) ο Ενέργεια: Σε περίπτωση αλλαγής πόστου (π.χ. μετακίνηση από γραφείο σε χειρισμό γερανού), ανακαλούνται άμεσα τα παλαιά δικαιώματα και εκδίδονται τα νέα, αποτρέποντας τη συσσώρευση προνομίων (privilege creep). ο Εκτελείται από: IT Security Administrator (σε συνεννόηση με τον OT Security Engineer).
- **Βήμα 3:** Αποχωρών (Leaver) ο Ενέργεια: Άμεση και οριστική απενεργοποίηση (όχι απλή διαγραφή, ώστε να διατηρούνται τα ίχνη ελέγχου) όλων των λογαριασμών και των δικαιωμάτων VPN/απομακρυσμένης πρόσβασης του υπαλλήλου τη στιγμή της αποχώρησής του. ο Εκτελείται από: IT Security Administrator.

5.3 Σχέδιο Επιχειρησιακής Συνέχειας (Business Continuity Plan)

Η ύπαρξη προληπτικών μέτρων και διαδικασιών αντιμετώπισης δεν αποκλείει το ενδεχόμενο μιας ακραίας, καταστροφικής αστοχίας. Το Σχέδιο Επιχειρησιακής Συνέχειας (Business Continuity Plan - BCP) του λιμένα σχεδιάστηκε με γνώμονα το διεθνές πρότυπο ISO 22301:2019 (ISO 22301, 2019), προκειμένου να διασφαλιστεί η ταχεία ανάκαμψη των κρίσιμων λειτουργιών.

Για την Ανάλυση Επιχειρησιακών Επιπτώσεων (Business Impact Analysis - BIA), η οποία αποτελεί τον πυρήνα του σχεδίου, χρησιμοποιήθηκε ως μεθοδολογικό πλαίσιο το πρότυπο ISO/TS 22317:2021 (ISO/TS 22317, 2021), αξιοποιώντας άμεσα τα δεδομένα που παρήγαγε το λογισμικό MONARC (Κεφάλαιο 3).

5.3.1 Ανάλυση Επιχειρησιακών Επιπτώσεων και Παραγωγή Δεικτών (RTO & RPO)

Σε αντίθεση με τις γενικόλογες βιομηχανικές προσεγγίσεις, οι στόχοι χρόνου και δεδομένων του λιμένα (RTO και RPO) προκύπτουν αυστηρά μέσα από τις παραμέτρους Impact (C, I, A) του MONARC και τις πολιτικές αντιγράφων ασφαλείας του Υποκεφαλαίου 5.1.

Πίνακας 5.1: Δείκτες Ανάκαμψης ανά Πρωτεύον Αγαθό (IT και OT). Πηγή: Ιδία επεξεργασία

Σύστημα (Πρωτεύον Αγαθό)	Στόχος Σημείου Ανάκαμψης (RPO)	Στόχος Χρόνου Ανάκαμψης (RTO)	Αιτιολόγηση βάσει MONARC & Πολιτικών
Πληροφοριακό Σύστημα (PCS / IT)	24 Ώρες	4 έως 8 Ώρες	Το RPO προκύπτει μαθηματικά από την πολιτική ημερήσιων (daily) incremental backups. Το RTO βασίζεται στο MONARC, όπου ο μέγιστος αντίκτυπος αξιολογήθηκε με "3" (Διακοπή τμήματος), όχι "4" (Ολική παράλυση), επιτρέποντας έναν μετρίως σφιχτό, αλλά ρεαλιστικό χρόνο αποκατάστασης ωρών.
Βιομηχανικός Γερανός (PLC / OT)	24 Ώρες (Χαμηλής κρισιμότητας)	Ασφαλείας (Safety): < 5 Λεπτά/Λειτουργικότητας: 24-48 Ώρες	Το RPO παραμένει ίδιο, αν και τα αρχεία διαμόρφωσης (configs) αλλάζουν σπάνια. Το RTO, λόγω Impact "4" (Κίνδυνος ανθρώπινης ζωής), διαχωρίζεται: Ο γερανός τίθεται άμεσα σε ασφαλή κατάσταση μέσω Χειροκίνητης Παράκαμψης (Safety RTO). Ωστόσο, η πλήρης επαναφορά στην αυτοματοποιημένη λειτουργία απαιτεί φυσική επιθεώρηση, αυξάνοντας τον χρόνο (Operational RTO).

5.3.2 Στρατηγική Ανάκαμψης από Ολική Καταστροφή (Total Disaster Strategy)

Το χειρίστο σενάριο (Worst-Case Scenario) προβλέπει την ταυτόχρονη και ολοκληρωτική κατάρρευση τόσο του Πληροφοριακού Συστήματος (PCS) όσο και του αυτοματοποιημένου ελέγχου των Γερανών (OT), εξαιτίας μιας συντονισμένης κυβερνοεπίθεσης ή μιας φυσικής καταστροφής εκτεταμένης κλίμακας.

Σε ένα τέτοιο σενάριο, η στρατηγική του λιμένα υπερβαίνει την ψηφιακή αποκατάσταση. Ενεργοποιείται το Σχέδιο Ολικής Καταστροφής, όπου ο οργανισμός επιστρέφει προσωρινά σε πλήρως χειροκίνητες διαδικασίες και έγχαρτη (paper-based) διαχείριση του φορτίου. Οι γερανοί ελέγχονται αποκλειστικά από φυσικούς χειριστές στις καμπίνες (μέσω του Safety RTO), ενώ τα φορτωτικά έγγραφα και τα τελωνειακά δελτία συμπληρώνονται χειρόγραφα και καταχωρούνται προσωρινά εκτός δικτύου.

Η προσέγγιση αυτή ακολουθεί το ιστορικό προηγούμενο της ναυτιλιακής εταιρείας Maersk κατά τη διάρκεια της καταστροφικής επίθεσης του Ransomware NotPetya (Εισαγωγή· βλ. αναλυτικά Κεφ. 2.1, ENISA 2019). Η ικανότητα επιστροφής σε αναλογικές, παραδοσιακές μεθόδους (manual fallback), έως ότου εξυγιανθεί ο ψηφιακός εξοπλισμός, αποτελεί την έσχατη και πιο αξιόπιστη δικλείδα επιχειρησιακής συνέχειας ενός σύγχρονου λιμένα.

Συμπεράσματα

Η παρούσα πτυχιακή εργασία είχε ως αντικείμενο τη μετάβαση από τη θεωρητική και κανονιστική προσέγγιση της κυβερνοασφάλειας στην πρακτική, ποσοτικοποιημένη αποτίμηση του κυβερνοκινδύνου σε λιμενικές υποδομές. Στηριζόμενη στο διεθνές πλαίσιο του Διεθνούς Ναυτιλιακού Οργανισμού, της BIMCO και των νηογνώμωνων (Κεφάλαιο 1), η μελέτη υιοθέτησε ως μεθοδολογικό άξονα το τριγωνικό σχήμα ISO/IEC 27005, IEC 62443 και κατευθύνσεων ENISA, εφαρμοσμένο πρακτικά μέσω του λογισμικού ανοιχτού κώδικα MONARC σε έναν υποθετικό Smart Container Terminal. Κεντρικός στόχος υπήρξε η ρητή, συστηματική εφαρμογή μιας Διπλής Προσέγγισης (Dual Approach), η ταυτόχρονη δηλαδή εξέταση τόσο του πληροφοριακού (IT) όσο και του επιχειρησιακού/βιομηχανικού (OT) περιβάλλοντος του λιμένα ως ενιαίου, αλληλεξαρτώμενου συστήματος — μια απάντηση στο κενό τυποποιημένης μεθοδολογίας που είχε επισημάνει ο Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας για τους ευρωπαϊκούς λιμένες (ENISA, 2020).

Η συνθετική επισκόπηση των αποτελεσμάτων διατρέχει το σύνολο της πρακτικής εφαρμογής. Στο Κεφάλαιο 2, η χαρτογράφηση του λιμενικού οικοσυστήματος σε τέσσερις λειτουργικές Ζώνες και η μοντελοποίηση των Πρωτευόντων και Δευτερευόντων Αγαθών μέσω Κατευθυνόμενου Άκυκλου Γράφου και Μήτρας Εξαρτήσεων παρήγαγε ένα πλήρες, επαληθεύσιμο δίκτυο δέκα εξαρτήσεων, στο οποίο στηρίχθηκε η στοχευμένη αντιστοίχιση οκτώ απειλών με τις αντίστοιχες τεχνολογικές και ανθρώπινες ευπάθειες. Η μεταφορά αυτού του μοντέλου στο περιβάλλον του MONARC (Κεφάλαιο 3) επιβεβαίωσε εμπειρικά, όχι απλώς θεωρητικά, τη θεμελιώδη διάκριση των δύο περιβαλλόντων: το Πρωτεύον Αγαθό του Πληροφοριακού Συστήματος περιορίστηκε σε μέγιστο αντίκτυπο επιπέδου 3 σε όλες τις διαστάσεις της τριάδας CIA, ενώ το Πρωτεύον Αγαθό της βιομηχανικής διαδικασίας έφτασε στο ανώτατο επίπεδο 4 τόσο ως προς την Ακεραιότητα όσο και ως προς τη Διαθεσιμότητα, αντικατοπτρίζοντας ρητά σενάρια απώλειας ανθρώπινης ζωής και πλήρους επιχειρησιακής παράλυσης. Στο Κεφάλαιο 4, η εφαρμογή οκτώ στοχευμένων μέτρων αντιμετώπισης, βασισμένων στα πρότυπα ISO/IEC 27002 και IEC 62443 και οργανωμένων γύρω από σαφή κατανομή οργανωτικών ρόλων μέσω Μήτρας RACI, οδήγησε σε μέση μείωση του επιπέδου κινδύνου από 44,4 σε 13,4 μονάδες, περίπου 70%, χωρίς ωστόσο πλήρη εξάλειψή του. Τέλος, στο Κεφάλαιο 5, το τεχνικό αυτό αποτέλεσμα θεμελιώθηκε οργανωτικά μέσα από τέσσερις εφαρμόσιμες πολιτικές ασφαλείας, τρεις λεπτομερείς επιχειρησιακές διαδικασίες —με χαρακτηριστικότερη τη διαδικασία απόκρισης σε περιστατικό, ευθυγραμμισμένη με το επικαιροποιημένο πρότυπο NIST SP 800-61 Rev. 3— και ένα πλήρες Σχέδιο Επιχειρησιακής Συνέχειας, όπου οι στόχοι χρόνου ανάκαμψης παρήχθησαν με ιχνηλάσιμο τρόπο απευθείας από τα δεδομένα του MONARC, διαφοροποιούμενοι ρητά σε επίπεδο Ασφάλειας και πλήρους λειτουργικότητας.

Παράλληλα με τα θετικά ευρήματα, η πρακτική εφαρμογή ανέδειξε περιορισμούς μεθοδολογικής και πρακτικής φύσης που οφείλουν να αναφερθούν με ακαδημαϊκή ειλικρίνεια. Ο ενσωματωμένος κατάλογος απειλών και ευπαθειών του MONARC αποδείχθηκε ότι ακολουθεί τη δομή παλαιότερης έκδοσης του προτύπου ISO/IEC 27005 (2018) και όχι της τρέχουσας (2022), γεγονός που δημιουργεί ποσοτική στρέβλωση στην αξιολόγηση εξειδικευμένων ναυτιλιακών απειλών: η ενεργητική παρεμβολή δορυφορικού σήματος, ελλείπει ακριβούς κατηγορίας, αντιστοιχίστηκε αναγκαστικά σε γενική κατηγορία υποκλοπής, με αποτέλεσμα το υπολογιζόμενο ρίσκο (10) να υπολείπεται σημαντικά του θεωρητικά ορθού μεγέθους (40). Παράλληλα, ο ακριβής τεχνικός μηχανισμός με τον οποίο οι Πληροφοριακοί κίνδυνοι των Δευτερευόντων Αγαθών συνδέονται υπολογιστικά με τους Επιχειρησιακούς κινδύνους των Πρωτευόντων παρέμεινε τεχνικά αδιερεύνητος εντός των ορίων του λογισμικού. Τέλος, η ίδια η φύση της μελέτης περίπτωσης —ένας υποθετικός, όχι πραγματικός, τερματικός σταθμός— περιορίζει αναπόφευκτα την άμεση εξωτερική εγκυρότητα των ποσοτικών ευρημάτων, τα οποία οφείλουν να ερμηνεύονται ως απόδειξη μεθοδολογικής ορθότητας και όχι ως ακριβής πρόβλεψη για συγκεκριμένη πραγματική εγκατάσταση.

Με βάση τα ανωτέρω, ο αρχικός στόχος της εργασίας, όπως ορίστηκε στο Υποκεφάλαιο 1.2 —η πρακτική εφαρμογή ενός μαθηματικού μοντέλου επικινδυνότητας και η εξαγωγή ενός ρεαλιστικού Σχεδίου Αντιμετώπισης Κινδύνων για σύγχρονη λιμενική υποδομή— επιτεύχθηκε σε πλήρη έκταση, καλύπτοντας το σύνολο του κύκλου διαχείρισης κινδύνου, από τη χαρτογράφηση αγαθών έως την οργανωτική θεσμοθέτηση πολιτικών και διαδικασιών.

Η συνεισφορά της παρούσας εργασίας εντοπίζεται σε πέντε επίπεδα. Πρώτον, στην ίδια τη μεθοδολογική σύνθεση: η ρητή, συστηματική εφαρμογή της Διπλής Προσέγγισης εντός ενός ενιαίου, αναπαραγωγίμου ψηφιακού περιβάλλοντος απαντά άμεσα στο κενό που είχε εντοπίσει ο ENISA. Δεύτερον, στην εμπειρική επιβεβαίωση της θεωρητικής διάκρισης CIA/AIC μέσα από πραγματικά, μετρήσιμα δεδομένα εργαλείου, προσδίδοντας στη θεωρητική θεμελίωση του Κεφαλαίου 2 απτή, ποσοτική ισχύ. Τρίτον, στην ανακάλυψη ότι ο εσωτερικός διαχωρισμός κινδύνων του MONARC συνδέεται με το ιεραρχικό επίπεδο του αγαθού και όχι με τη θεματική του φύση — ένα εύρημα που προέκυψε από την ίδια την πειραματική διαδικασία, όχι από τη βιβλιογραφία τεκμηρίωσης του εργαλείου. Τέταρτον, στην αντίστοιχη σύγκλιση που εντοπίστηκε σε επίπεδο διακυβέρνησης: ο Έλεγχος 5.2 του ISO/IEC 27002 και η απαίτηση ORG 1.3 του IEC 62443-2-1, προερχόμενοι από εντελώς διαφορετικές επιτροπές τυποποίησης, κατέληξαν ανεξάρτητα στην ίδια θεμελιώδη επιταγή ορισμού ρόλων ασφαλείας, επιβεβαιώνοντας ότι η Διπλή Προσέγγιση ισχύει και σε οργανωσιακό, όχι μόνο τεχνικό, επίπεδο. Πέμπτον, στη μεθοδολογία παραγωγής δεικτών RTO/RPO απευθείας και ιχνηλάσιμα από τα δεδομένα αξιολόγησης κινδύνου, αντί για γενικόλογα βιομηχανικά πρότυπα, αναδεικνύοντας έμπρακτα τη σύνδεση ανάλυσης κινδύνου και επιχειρησιακής συνέχειας.

Τρεις κατευθύνσεις μελλοντικής έρευνας προκύπτουν άμεσα από τα ίδια τα όρια της παρούσας μελέτης. Καταρχάς, η επέκταση της πρακτικής μοντελοποίησης στη Ζώνη 4 (Ναυσιπλοΐα και Επικοινωνίες), η οποία εξετάστηκε θεωρητικά στο Κεφάλαιο 2 αλλά δεν συμπεριλήφθηκε στο πρακτικό σενάριο αξιολόγησης του Κεφαλαίου 3, θα προσέφερε πληρέστερη εικόνα του λιμενικού κυβερνοκινδύνου. Δεύτερον, η ανάπτυξη μιας εξειδικευμένης βιβλιοθήκης απειλών για το ναυτιλιακό ΟΤ περιβάλλον, στη βάση του ήδη ενσωματωμένου καταλόγου, θα διόρθωνε ρητά την ποσοτική στρέβλωση που εντοπίστηκε στην απειλή παρεμβολής δορυφορικού σήματος. Τέλος, η επικύρωση της μεθοδολογίας σε πραγματική λιμενική εγκατάσταση, με πραγματικά επιχειρησιακά δεδομένα και τη συμμετοχή στελεχών ασφαλείας, θα επέτρεπε τη μετάβαση από τη μεθοδολογική απόδειξη ορθότητας στην πλήρη πρακτική εφαρμοσιμότητα του προτεινόμενου πλαισίου.

Πίνακας Ορολογίας

Πίνακας Ορολογίας

Ξενόγλωσσος Όρος	Ελληνικός Όρος
3-2-1 Backup Rule	Κανόνας Αντιγράφων 3-2-1
Acceptance Thresholds	Όρια Αποδοχής Κινδύνου
Air-gap	Φυσικός Διαχωρισμός Δικτύων / Ψηφιακή Απομόνωση
AIS Spoofing	Παραπλάνηση Στίγματος AIS
Asset Model	Μοντέλο Αγαθών
Asset-based Approach	Προσέγγιση (εκτίμησης κινδύνου) βασισμένη στα αγαθά
Asset-to-Risk Trees	Δενδρική Συσχέτιση Αγαθών-Κινδύνων

Assets Library	Βιβλιοθήκη Αγαθών
Attack Surface	Επιφάνεια Επίθεσης
Auto-steering	Αυτόματη Πλοήγηση / Κατεύθυνση
Automated Gates	Αυτοματοποιημένες Πύλες Ελέγχου
Best Practices	Βέλτιστες Πρακτικές
Bridged Networking	Γεφυρωμένη Δικτύωση
Bridging Zone / Asset	Ζώνη Σύγκλισης / Γεφυροποιό Αγαθό
Business Continuity Plan	Σχέδιο Επιχειρησιακής Συνέχειας
Business Impact Analysis (BIA)	Ανάλυση Επιχειρησιακών Επιπτώσεων
Cartography / Heatmap	Χαρτογράφηση Κινδύνων
Cascading Effects	Αλυσιδωτές Επιπτώσεις / Φαινόμενο Ντόμινο
Client / Project	Πελάτης / Έργο
Cloud Computing	Υπολογιστικό Νέφος
Cloud Scrubbing	Φιλτράρισμα Δικτυακής Κίνησης στο Νέφος
Command and Control	Ροή Εντολής και Ελέγχου
Command Injection	Έγχυση Κακόβουλων Εντολών
Commercial Implementation Tools	Εμπορικά Εργαλεία Υλοποίησης (Λογισμικού)
Compliance Checklist	Λίστα Ελέγχου Συμμόρφωσης
Composition	Σύνθεση (Διασύνδεση Αγαθών)
Consequence-based Risk Assessment	Αξιολόγηση Κινδύνου βασισμένη στις συνέπειες
Consequences	Συνέπειες

Container Terminal	Τερματικός Σταθμός Εμπορευματοκιβωτίων
Countermeasures	Αντίμετρα / Μέτρα Προστασίας
Current Risk	Τρέχων Κίνδυνος

Cyber Risk Assessment	Αξιολόγηση / Ανάλυση Κυβερνοκινδύνων
Cyber Security	Κυβερνοασφάλεια
Dashboard	Πίνακας Ελέγχου
Data Array	Συστοιχία Δεδομένων
Dead-reckoning	Αδρανειακή Πλοήγηση
Dependency Chain	Αλυσίδα Εξάρτησης
Deployment	Ανάπτυξη / Εγκατάσταση Συστήματος
Design Structure Matrix (DSM)	Μήτρα Εξαρτήσεων
Directed Acyclic Graph (DAG)	Κατευθυνόμενος Άκυκλος Γράφος
Dual Approach	Διπλή Προσέγγιση
Essential Entities	Ουσιώδεις Οντότητες
Event-based Approach	Προσέγγιση (εκτίμησης κινδύνου) βασισμένη στα συμβάντα
GNSS/GPS Jamming	Παρεμβολή Δορυφορικού Σήματος
Human Element	Ανθρώπινος Παράγοντας
Hypervisor	Λογισμικό Εικονικοποίησης
Immutable Backups	Αμετάβλητα Αντίγραφα Ασφαλείας
Impact Assessment	Αποτίμηση / Εκτίμηση Επιπτώσεων
Impact Propagation	Διάδοση Επιπτώσεων
Incremental Backup	Αυξητικό Αντίγραφο Ασφαλείας
Information Risks	Πληροφοριακοί Κίνδυνοι
Information Technology (IT)	Τεχνολογίες Πληροφορικής / Πληροφοριακά Συστήματα
Insider Threat	Εσωτερική Απειλή
IT/OT Convergence	Σύγκλιση Πληροφορικής (IT) και Επιχειρησιακής Τεχνολογίας (OT)
Joiner-Mover-Leaver (JML)	Κύκλος Διαχείρισης Ταυτοτήτων JML

Lateral Movement	Πλευρική Μετακίνηση
Least Privilege	Αρχή Ελάχιστων Προνομίων
Likelihood	Πιθανότητα Εκδήλωσης
Log Tampering	Αλλοίωση Καταγραφών
Logical Loops	Λογικοί Κύκλοι
Loss of Essential Services	Απώλεια Βασικών Υπηρεσιών

Management Reporting	Διοικητική Αναφορά
Manual Fallback	Χειροκίνητη Παράκαμψη
Max Associated Risk Level	Μέγιστο Επίπεδο Σχετιζόμενου Κινδύνου
MFA Fatigue	Κόπωση Ελέγχου Ταυτότητας
Misconfiguration	Εσφαλμένη Ρύθμιση / Παραμετροποίηση
Open Standard / Methodology	Ανοιχτό Πρότυπο / Ανοιχτή Μεθοδολογία
Open-Source Software	Λογισμικό Ανοιχτού Κώδικα
Operational Risks	Επιχειρησιακοί / Λειτουργικοί Κίνδυνοι
Operational Technology (OT)	Επιχειρησιακές Τεχνολογίες
Primary / Secondary Assets	Πρωτεύοντα / Δευτερεύοντα Αγαθά
Private 5G Network	Ιδιωτικό Δίκτυο 5G
Privilege Creep	Συσσώρευση Προνομίων
Qualitative / Quantitative / Hybrid	Ποιοτική / Ποσοτική / Υβριδική (Μεθοδολογία)
RACI Matrix	Μήτρα Κατανομής Αρμοδιοτήτων (RACI)
Ransomware	Λυτρόβουλο Λογισμικό
Recovery Point Objective (RPO)	Στόχος Σημείου Ανάκαμψης
Recovery Time Objective (RTO)	Στόχος Χρόνου Ανάκαμψης
Redundant Firewall	Εφεδρικό Τείχος Προστασίας
Reefer Containers	Εμπορευματοκιβώτια Ψυγεία
Remote Maintenance Access	Απομακρυσμένη Πρόσβαση Συντήρησης
Residual Risk	Υπολειπόμενος Κίνδυνος

Risk Assessment	Αξιολόγηση Κινδύνων / Ανάλυση Επικινδυνότητας
Risk Assessment Tools	Εργαλεία Αξιολόγησης Κινδύνων
Risk Treatment (Plan)	(Σχέδιο) Αντιμετώπισης / Θεραπείας Κινδύνου
Safety (Maritime)	Φυσική Ασφάλεια / Προστασία Ανθρώπινης Ζωής
Scenario-based Approach	Προσέγγιση (ανάλυσης) βασισμένη σε σενάρια
Scientific Reproducibility	Επιστημονική Αναπαραγωγικότητα
Security Controls	Μέτρα Ελέγχου Ασφάλειας / Δικλείδες Ασφαλείας
Security Governance	Διακυβέρνηση Ασφάλειας
Security Levels (SL)	Επίπεδα Ασφάλειας
Segregation of Duties	Διαχωρισμός Αρμοδιοτήτων
Sensitive Security Information	Διαβαθμισμένο Πληροφοριακό Υλικό Ασφάλειας
Ship-to-Shore (STS) Interface	Διεπαφή Πλοίου-Λιμένα
Smart Container Terminal	Έξυπνος Τερματικός Σταθμός Εμπορευματοκιβωτίων
Social Engineering	Κοινωνική Μηχανική
Spoofing	Πλαστογράφιση
Status Feedback / Telemetry	Ανατροφοδότηση Κατάστασης / Τηλεμετρία
Supply Chain Attack / Compromise	Κυβερνοεπίθεση / Παραβίαση Εφοδιαστικής Αλυσίδας
Supply Chain Security	Ασφάλεια Εφοδιαστικής Αλυσίδας
Targeted Phishing	Στοχευμένο "Ψάρεμα" (Ηλεκτρονική Απάτη)
Technical Failures	Τεχνικές Αστοχίες
Terminal Operations	Λειτουργίες Τερματικού Σταθμού
Threat Assessment	Αποτίμηση / Αξιολόγηση Απειλών
Threat Catalogs / Libraries	Κατάλογοι / Βιβλιοθήκες Απειλών
Threat Probability	Πιθανότητα Απειλής
Transversal Conduits Layer	Εγκάρσιο Στρώμα Αγωγών
Unauthorized Actions	Μη Εξουσιοδοτημένες Ενέργειες
Virtual Machine Appliance	Έτοιμη Εικονική Μηχανή
Vulnerability Assessment	Αποτίμηση / Αξιολόγηση Ευπαθειών
Vulnerability Qualification	Ποιότητα Ευπάθειας

Web Browser / Interface	Πρόγραμμα Περιήγησης / Διεπαφή Ιστού
Worst-Case Scenario	Χείριστο Σενάριο
Zones and Conduits	Ζώνες και Αγωγοί

Πίνακας συντμήσεων-αρτικόλεξων-ακρονύμων.

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

Σύντμηση	Πλήρης Ανάπτυξη
AIC	Availability, Integrity, Confidentiality
AIS	Automatic Identification System
ALE	Annualized Loss Expectancy
APT	Advanced Persistent Threat
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAPEX	Capital Expenditure
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
CPU	Central Processing Unit
CSET	Cyber Security Evaluation Tool
CSF	Cybersecurity Framework
DAG	Directed Acyclic Graph
DDoS	Distributed Denial of Service
DSM	Design Structure Matrix
EBIOS RM	Expression des Besoins et Identification des Objectifs de Sécurité - Risk Manager
EDR	Endpoint Detection and Response
EMSA	European Maritime Safety Agency

ERP	Enterprise Resource Planning
FAIR	Factor Analysis of Information Risk
GNSS	Global Navigation Satellite System
GNU GPL	General Public License
GPS	Global Positioning System
IACS	International Association of Classification Societies
IACS (OT)	Industrial Automation and Control Systems
IMO	International Maritime Organization
IoT	Internet of Things
IP	Internet Protocol
ISM	International Safety Management
ISPS	International Ship and Port Facility Security Code
IT	Information Technology
JML	Joiner, Mover, Leaver
LAN	Local Area Network

LIST	Luxembourg Institute of Science and Technology
LOG_APP	Business Application
MAT_FIX	Fixed Equipment
MFA	Multi-Factor Authentication
MTSA	Maritime Transportation Security Act
ORG	Organization
OT	Operational Technology
P	Probability
PA	Primary Asset
PAM	Privileged Access Management
PCS	Port Community System
PFSA	Port Facility Security Assessment

PLC	Programmable Logic Controller
PRC	People's Republic of China
RACI	Responsible, Accountable, Consulted, Informed
RAM	Random Access Memory
ROSI	Return on Security Investment
RPO	Recovery Point Objective
RTG	Rubber-Tyred Gantry
RTO	Recovery Time Objective
SA	Secondary Asset
SCADA	Supervisory Control and Data Acquisition
SL	Security Level
SMILE	Security Made in Lëtzebuerg
SMS	Safety Management System
SPOF	Single Point of Failure
SR	System Requirement
SSI	Sensitive Security Information
STS	Ship-to-Shore
T	Threat
TOS	Terminal Operating System
UI	User Interface
UNCTAD	United Nations Conference on Trade and Development
UPS	Uninterruptible Power Supply
USCG	United States Coast Guard
V	Vulnerability
VM	Virtual Machine
VPN	Virtual Private Network
VTs	Vessel Traffic Services
WAF	Web Application Firewall

WAN	Wide Area Network
-----	-------------------

Βιβλιογραφία

- ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). (2024, March). EBIOS Risk Manager: The Method (Updated March 2024 for ISO/IEC 27005:2022 alignment). Paris: ANSSI.
- BIMCO et al. (2020). The Guidelines on Cyber Security Onboard Ships (4th ed.).
- BIMCO et al. (2024, November 14). The Guidelines on Cyber Security Onboard Ships (Version 5). BIMCO Publications.
- CISA (Cybersecurity and Infrastructure Security Agency). (2024). Cyber Security Evaluation Tool (CSET) Fact Sheet & User Guide. U.S. Department of Homeland Security.
- DNV. (2024). DNV Rules for Classification: Cyber secure (Essential) (Class Notation E26/E27). DNV AS.
- EMSA (European Maritime Safety Agency). (2023, November 22). Guidance on how to address cybersecurity onboard ships during audits, controls, verifications and inspections (Doc. 9209). Lisbon: EMSA.
- ENISA (European Union Agency for Cybersecurity). (2019). Port Cybersecurity: Good practices for cybersecurity in the maritime sector. Heraklion: ENISA.
- ENISA (European Union Agency for Cybersecurity). (2020). Cyber Risk Management for Ports. Heraklion: ENISA.
- ENISA (European Union Agency for Cybersecurity). (2025). ENISA Threat Landscape 2025. Heraklion: ENISA.
- European Commission. (2024). Report from the Commission to the European Parliament and the Council on the implementation and functioning of Regulation (EC) No 725/2004 and Directive 2005/65/EC (COM(2024) 192 final). Brussels.
- European Parliament and Council. (2004). Regulation (EC) No 725/2004 of 31 March 2004 on enhancing ship and port facility security. Official Journal of the European Union, L 129/6.
- European Parliament and Council. (2005). Directive 2005/65/EC of 26 October 2005 on enhancing port security. Official Journal of the European Union, L 310/28.
- European Parliament and Council. (2022). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union, L 333/80.
- FAIR Institute. (2023). An Introduction to Factor Analysis of Information Risk (FAIR). FAIR Institute Publications.
- IACS (International Association of Classification Societies). (2023a). Unified Requirement UR E26: Cyber resilience of ships. London: IACS.
- IACS (International Association of Classification Societies). (2023b). Unified Requirement UR E27: Cyber resilience of on-board systems and equipment. London: IACS.
- IEC 62443-2-1. (2024). Security for industrial automation and control systems — Part 2-1: Security program requirements for IACS asset owners (Edition 2.0).
- IMO (International Maritime Organization). (2004). International Ship and Port Facility Security (ISPS) Code. London: IMO Publishing.
- IMO (International Maritime Organization). (2017). Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems. London: IMO.
- IMO (International Maritime Organization). (2025, April 4). MSC-FAL.1/Circ.3/Rev.3: Guidelines on maritime cyber risk management. London: IMO.

- International Electrotechnical Commission (IEC). (2020). IEC 62443-3-2: Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design. Geneva: IEC.
- ISA/IEC 62443-3-3. (2013). Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels.
- ISO 22301. (2019). Security and resilience — Business continuity management systems — Requirements (ISO 22301:2019).
- ISO/IEC 27002. (2022). Information security, cybersecurity and privacy protection — Information security controls (ISO/IEC 27002:2022).
- ISO/IEC 27005. (2018). Information technology — Security techniques — Information security risk management.
- ISO/IEC 27005. (2022). Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva: ISO.
- ISO/TS 22317. (2021). Security and resilience — Business continuity management systems — Guidelines for business impact analysis (BIA).
- NC3 (Luxembourg House of Cybersecurity). (2025, April 17). MONARC (Version 2.13.3) [Computer software]. <https://www.monarc.lu/>
- NIST (National Institute of Standards and Technology). (2023). Guide to Operational Technology (OT) Security (NIST Special Publication 800-82, Rev. 3). U.S. Department of Commerce.
- NIST (National Institute of Standards and Technology). (2024, February 26). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper CSWP 29). U.S. Department of Commerce.
- NIST (National Institute of Standards and Technology). (2025, April 3). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (NIST Special Publication 800-61, Revision 3). U.S. Department of Commerce.
- UNCTAD (United Nations Conference on Trade and Development). (2025). Review of Maritime Transport 2025: Staying the course in turbulent waters. United Nations Publications.
- U.S. Coast Guard (USCG). (2024a, February 23). Notice of Availability: MARSEC Directive 105–4; Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies. Federal Register, Vol. 89, No. 37, pp. 13726–13727.
- U.S. Coast Guard (USCG). (2024b, November 19). Notice of Availability: MARSEC Directive 105–5; Additional Cyber Risk Management Actions for OT Port Equipment. Federal Register, Vol. 89, No. 223, pp. 91338-91339.
- U.S. Coast Guard (USCG). (2025, January 17). Final Rule: Cybersecurity in the Marine Transportation System (33 CFR Parts 101, 104, 105, and 106). Department of Homeland Security.
- Εφημερίδα της Κυβερνήσεως. (2024, 27 Νοεμβρίου). Νόμος 5160/2024: Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 (NIS 2) για την επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ένωση. ΦΕΚ Α' 195/2024. Εθνικό Τυπογραφείο.