Πανεπιστήμιο Θεσσαλίας

Σχολή Θετικών Επιστημών

Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών

Πληροφορική και Υπολογιστική Βιοϊατρική

Βέλτιστη Επιλογή Στρατηγικών Κυβερνοασφάλειας σε Έξυπνα Συστήματα Μεταφορών

Optimal cybersecurity strategy selection for intelligent transportation systems

Σακαβέλης Γιώργης (00786)

Ευχαριστίες

Φτάνοντας λοιπόν στην παράδοση της μεταπτυχιακής διπλωματικής μου εργασίας θέλω να ευχαριστήσω θερμά όλους όσους συνέβαλαν, άμεσα και έμμεσα, στην επιτυχή ολοκλήρωσή της.

Θερμές ευχαριστίες οφείλω να δώσω στον επιβλέπων καθηγητή μου κύριο Γεώργιο Σπαθούλα κυρίως για την εμπιστοσύνη που μου έδειξε από την αρχή, αναθέτοντάς μου το συγκεκριμένο θέμα και για την άψογη συνεργασία που είχαμε σε ολόκληρη τη διαδρομή εκπόνησης της εργασίας αυτής. Δεν θα ξεχάσω ποτέ τον πολύτιμο χρόνο που με προθυμία διέθεσε για βοήθεια και υποστήριξη πάνω στην επιστημονική προσέγγιση του θέματος.

Ευχαριστώ θερμά τον κύριο Γεώργιο Καβαλλιεράτο που μοιράστηκε μαζί μου την επιστημονική εμπειρία του στο αντικείμενο της εργασίας και μου έδειξε το δρόμο όταν άρχισε να «χτίζεται» αυτή η εργασία.

Τέλος θα ήθελα να ευχαριστήσω τους γονείς μου, τον αδερφό μου και τους φίλους μου που είναι δίπλα μου να με στηρίζουν σε κάθε επιλογή ακαδημαϊκή ή όχι.

1. Εισαγωγή

Τα έξυπνα συστήματα μεταφορών (ITS - Intelligent Transport Systems) εφαρμόζονται τόσο σε οχήματα όσο και σε οδικά δίκτυα μεταφορών έχοντας κύριο στόχο τη βελτίωση και τη διασφάλιση της ποιότητας και της ασφάλειας σε πάσης φύσης λειτουργίες των οδικών μεταφορών. Μέσα από αυτά μπορούμε να έχουμε πληροφορίες σε πραγματικό χρόνο για τους διαχειριστές των συστημάτων και των χρηστών των οδικών μεταφορών μέσα από ένα σύνολο διασυνδεδεμένων υποσυστημάτων.

Οι έξυπνες πόλεις βασίζονται εξ' ορισμού στα data, αλλά κλειδί για την αποτελεσματικότητά τους είναι ο τρόπος με τον οποίο χρησιμοποιούνται. Η ψηφιακή κοινωνία διευκολύνει την ζωή των πολιτών και τα ITS θεωρούνται σήμερα αναπόσπαστο κομμάτι για την καθημερινότητα.

Σε όλες τις μεγαλουπόλεις παρατηρείται τεράστιος αριθμός μετακινήσεων σαν αποτέλεσμα σημαντικό μέλημα των αρχών να είναι όσο το δυνατόν αποτελεσματικότερη κυκλοφορία των διάφορων μέσων μεταφοράς. Με τα ITS δύναται να εξοικονομηθεί χρόνος και σταδιακά να γίνουν οι πόλεις εξυπνότερες. Με αυτά ελαχιστοποιούνται τα προβλήματα κυκλοφορίας, εμπλουτίζοντας τους χρήστες με σημαντικές πληροφορίες όπως την κίνηση ενός δρόμου σε πραγματικό χρόνο, τη διαθεσιμότητα των θέσεων στάθμευσης κ.ά., πράγμα που μειώνει σημαντικά το χρόνο των μετακινήσεων. Αλλά επιπλέον της μείωσης χρόνου το μετακινήσεων, η όλη διαδικασία βελτιώνει την ασφάλεια και την άνεσή των πολιτών.

Τα ITS είναι πλέον ευρέως αποδεκτά και χρησιμοποιούνται σε πολλές πόλεις, με τη χρήση τους να μην περιορίζεται στον έλεγχο της κυκλοφοριακής συμφόρησης αλλά και στην πληροφόρηση και την οδική ασφάλεια. Εν δυνάμει οι δυνατότητες των ITS είναι άπειρες και για αυτό το λόγω αντιμετωπίζεται πλέον σαν πολυεπιστημονικό πεδίο και πολλοί οργανισμοί στον κόσμο αναπτύσσουν εφαρμογές ITS. Χαρακτηριστικό παράδειγμα τα λεωφορεία, όπου παρέχονται καθημερινά πλήθος πληροφοριών στους επιβάτες (διαθεσιμότητα θέσεων, χρόνους άφιξης, τρέχουσα θέση λεωφορείου, εκτιμώμενους χρόνους άφιξης, την επόμενη στάση και τον αριθμό επιβατών. Μπορούν επίσης να περιλαμβάνουν συστήματα ειδοποίησης έκτακτης ανάγκης, διαχείρισης κυκλοφορίας για διαφορετικά όρια ταχύτητας, αποφυγή και πρόληψη συγκρούσεων, αυτόματη αναγνώριση πινακίδων με τη χρήση καμερών ασφαλείας, αυτόματη ανίχνευση συμβάντων, ανίχνευση σταματημένων οχημάτων, διαθεσιμότητα θέσεων στάθμευσης με αισθητήρες και γενικότερα πολλές τεχνικές προβλέψεων.

Όπως γίνεται κατανοητό με την ραγδαία ανάπτυξη των ITS προκύπτουν ζητήματα ασφάλειας κατά την δικτύωση των συστημάτων τεχνολογίας που ρόλος τους είναι η μεταφορά ευαίσθητων δεδομένων και πληροφοριών και η προστασία τους από κακόβουλες επιθέσεις, μη εξουσιοδοτημένη πρόσβαση και οτιδήποτε άλλο μπορεί να επηρεάσει την ασφαλή λειτουργία τους. Αυτή είναι η γνωστή σε όλους μας πλέον κυβερνοασφάλεια όπου εξ ορισμού περιλαμβάνει το σύνολο μέτρων διασφάλισης που υιοθετούνται για την προστασία συστημάτων και χρηστών από τις παραπάνω απειλές ώστε να εξασφαλίζονται η εμπιστευτικότητα (confidentiality), η ακεραιότητα (integrity)

και η διαθεσιμότητα των δεδομένων (availability of data). Μέσω της κυβερνοασφάλειας προλαμβάνονται και ανιχνεύονται cyber περιστατικά, προετοιμάζονται αντιδράσεις για αυτά και ανάκαμψη από αυτά. Μπορεί να είναι εσκεμμένα ή μη και να είναι από τυχαία κοινοποίηση δεδομένων μέχρι και επιθέσεις εναντίον επιχειρήσεων και υποδομών ζωτικής σημασίας, κλοπή δεδομένων προσωπικού χαρακτήρα έως και παρέμβαση σε δημοκρατικές διαδικασίες. Όλα αυτά τα μπορούν να έχουν ποικίλες ζημιές σε πρόσωπα, οργανισμούς και κοινότητες.

Ταυτόχρονα όμως πέρα από ψηφιακά δικτυακά συστήματα τα ITS έχουν μία υλική υπόσταση η οποία συμπεριφέρεται ανάλογα με τα αποτελέσματα των αλγορίθμων του λογισμικού. Αυτή η ταυτόχρονη συνύπαρξη και λειτουργία συστημάτων – τμημάτων υλικού και λογισμικού είναι ο ορισμός των Cyber Physical συστημάτων, εν συντομία CPS. Οι δύο αυτές «φύσεις» είναι βαθιά συνυφασμένες αλλά και ικανές να λειτουργούν σε διαφορετικές χωρικές και χρονικές κλίμακες, να επιδεικνύουν πολλαπλές και διακριτές μεθόδους συμπεριφοράς και να αλληλεπιδρούν μεταξύ τους με τρόπους που αλλάζουν ανάλογα με το πλαίσιο λειτουργίας τους. Τα Cyber Physical Συστήματα περιλαμβάνουν διεπιστημονικές προσεγγίσεις, τη συγχώνευση της θεωρίας της κυβερνητικής, της μηχανοτρονικής, του σχεδιασμού και της επιστήμης των διαδικασιών. Το Cyber Physical συστήματα είναι παρόμοια με το Internet of Things (IoT) και μοιράζονται την ίδια βασική αρχιτεκτονική. Ωστόσο τα Cyber Physical συστήματα παρουσιάζει υψηλότερο συνδυασμό και συντονισμό μεταξύ των στοιχείων υλικού και λογισμικού.

Σε αντίθεση με τα πιο παραδοσιακά ενσωματωμένα συστήματα, ένα πλήρες Cyber Physical σύστημα σχεδιάζεται συνήθως σαν ένα δίκτυο αλληλεπιδρώντων στοιχείων με φυσική είσοδο και έξοδο αντί αυτόνομες συσκευών. Η ιδέα είναι στενά συνδεδεμένη με τις έννοιες της ρομποτικής και των δικτύων αισθητήρων σε συνδυασμό με μηχανισμούς τεχνητής νοημοσύνης. Οι συνεχείς εξελίξεις στην επιστήμη και τη μηχανική βελτιώνουν τη σύνδεση μεταξύ στοιχείων υλικού και λογισμικού μέσω έξυπνων μηχανισμών, αυξάνοντας την προσαρμοστικότητα, την αυτονομία, την αποτελεσματικότητα, τη λειτουργικότητα, την αξιοπιστία, την ασφάλεια και τη χρηστικότητα των Cyber Physical συστημάτων. Έτσι διευρύνεται το δυναμικό των υλικών συστημάτων στον κυβερνοχώρο σε διάφορες κατευθύνσεις όπως: παρέμβαση (αποφυγή σύγκρουσης), ακρίβεια (ρομποτική χειρουργική, νανοκατασκευές), λειτουργία σε επικίνδυνα ή απρόσιτα περιβάλλοντα (έρευνα και διάσωση, πυρόσβεση και εξερεύνηση βαθέων υδάτων), συντονισμός (έλεγχος εναέριας κυκλοφορίας), αποδοτικότητα (κτίρια μηδενικής ενέργειας) και αύξηση των ανθρώπινων ικανοτήτων (παρακολούθηση – παροχή υγειονομικής περίθαλψης).

Αυτό που χαρακτηρίζει τα Cyber-Physical Systems είναι η διασύνδεση υλικού, απτών εργαλείων, με τον μαγικό κόσμο του διαδικτύου. Παρά τις πολλές και αυστηρές διαδικασίες ελέγχων η ολοένα και μεγαλύτερη ένταξη εξοπλισμού σε online ομάδες συστημάτων, τα περισσότερα αν όχι όλα Cyber Physical συστήματα είναι ευάλωτα σε κυβερνοεπιθέσεις διάφορων τύπων. Ταυτόχρονα έχουμε διασύνδεση εξαιρετικά κρίσιμων Cyber Physical συστημάτων από τα οποία εξαρτώνται μέχρι και ανθρώπινες

ζωές (Ιατρικά, Οδικά, Βιομηχανικά, Τραπεζικά) με αποτέλεσμα να αυξάνεται κατακόρυφα ο αντίκτυπος μιας επιτυχημένης κυβερνοεπίθεσης άρα και η προκλήσεις αντιμετώπισης των κινδύνων. Γενικά ο κόσμος σήμερα αποτελείται από ομάδες Cyber Physical συστημάτων που με κάποιο τρόπο συνδέονται με άλλα συστήματα και υπάρχουν συνεχείς ροές μετάδοσης δεδομένων μεταξύ όλων αυτών. Κατά τη μετάδοση όλων αυτών τα δεδομένα τα ίδια γίνονται στόχος των επιθέσεων είτε για υποκλοπή είτε για τροποποίησή τους και μετάδοση άλλων κακόβουλων τα οποία μεταδίδονται ευκολότερα από το ένα σύστημα στο άλλο. Έτσι αυξάνονται οι πιθανότητες, ο αντίκτυπος και η διάδοση μιας κυβερνοεπίθεσης. Εφόσον εξ ορισμού οι κίνδυνοι στον κυβερνοχώρο υπολογίζονται από τον αντίκτυπο και την πιθανότητα έχουμε και την γενική αύξηση των κινδύνων σε όλα τα γνωστά Cyber Physical συστήματα. Εν συνεχεία αν γνωρίζουμε τους κινδύνους που υπάρχουν στα μικρότερα επιμέρους συστήματα και μπορούμε να βαθμονομήσουμε το πόσο επικίνδυνος είναι ο κάθε ένας μπορούμε σε δεύτερο χρόνο να έχουμε μια μεγαλύτερη εικόνα, με νούμερα, για τους κινδύνους στα μεγαλύτερα και κεντρικά συστήματα με τα οποία συνδέονται τα μικρότερα. Μιλώντας σε πιο ελεύθερη γλώσσα η διαδικασία αυτή εξομοιώνει την τακτική του «διαίρει και βασίλευε» στο έργο της τμηματικής αξιολόγησης κινδύνων στην κυβερνοασφάλεια.

Μέσα από ελέγχους που έχουν στόχο τη μείωση ή την αποφυγή του κινδύνου αξιολογείται ο ίδιος ο κίνδυνος και αυτό είναι το βασικό τμήμα των διαδικασιών διαχείρισης ρίσκου. Με ένα εύρος ελέγχων κυβερνοασφάλειας με διαφορετικά χαρακτηριστικά απόδοσης και αποτελεσματικότητας προσπαθούμε να αντιμετωπίσουμε τον κάθε πιθανό κίνδυνο. Είναι σημαντικό πως κάθε ένας έλεγχος δύναται να αντιμετωπίζει περισσότερους από έναν κινδύνους. Έτσι οδηγούμαστε σε διαμόρφωση σχεδίων αντιμετώπισης κινδύνων με στόχο τη βέλτιστη επιλογή του συνόλου των ελέγχων κυβερνοασφάλειας πάντα με κριτήριο την αποτελεσματικότητα και την αποδοτικότητα. Μια τέτοια διαδικασία είναι τόσο πολύπλοκη που δημιουργούνται προβλήματα βελτιστοποίησης ειδικά σε περιπτώσεις με περισσότερα από ένα κριτήρια βελτιστοποίησης. Σε αυτές τις περιπτώσεις η επιλογή των ελέγχων κυβερνοασφάλειας γίνεται σε μεγάλο βαθμό εμπειρικά και σπανιότερα με αυτοματοποιημένες διαδικασίες λήψης αποφάσεων.

Σε αυτή την εργασία εφαρμόζουμε τη μέθοδο που έχει ήδη προταθεί στο paper Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems[71] μελετώντας αυτή την φορά σας κεντρικό Cyber Physical σύστημα ένα μεγάλου εύρους Intelligent Transportation System αντί για ένα Cyber Enabled Ship. Το κοινό μας χαρακτηριστικό είναι πως υποδεικνύουμε ένα σύνολο αποτελεσματικών και αποδοτικών ελέγχων κυβερνοασφάλειας για ένα μεγάλης κλίμακας, πολύπλοκο Cyber Physical σύστημα που περιλαμβάνουν άλλα μικρότερα Cyber Physical συστήματα σαν τμήματά του. Επίσης αναλύουμε και μελετάμε μια μέθοδο αξιολόγησης του συνολικού ρίσκου που προκύπτει αν λάβουμε υπόψη και αθροίσουμε το ρίσκο του κάθε επιμέρους στοιχείου του συστήματος και την αλληλεπίδραση μεταξύ δύο επιμέρους μικρότερων συστημάτων μεταξύ τους. Πιο

συγκεκριμένα κάνοντας χρήση της εξελικτικής πληροφορική οδηγούμαστε στη δημιουργία και χρήση ενός αλγόριθμου επιλογής controls κυβερνοασφάλειας που χρησιμοποιεί τον συνολικό ρίσκο στον κυβερνοχώρο ενός πολύπλοκου και πολυσύνθετου Cyber Physical Συστήματος για να συνθέσει το βέλτιστο σύνολο controls κυβερνοασφάλειας, βάση αποτελεσματικότητας και αποδοτικότητας για τη μείωση του κινδύνου. Ο αλγόριθμος επιλέγει τα controls κυβερνοασφάλειας μέσα σε μία λίστα controls βάση των κατευθυντήριων γραμμών NIST για την ασφάλεια των συστημάτων βιομηχανικού ελέγχου[76].

Συνοψίζοντας, η συμβολή αυτής της εργασίας είναι η εξής:

• Στην εφαρμογή μίας γνωστής μεθόδου αξιολόγησης του συνολικού κινδύνου κυβερνοασφάλειας άλλων συστημάτων (Cyber Enabled Ships) σε ένα μεγάλης κλίμακας και πολύπλοκων Cyber Physical συστημάτων (Intelligent Transportation Systemς) που περιλαμβάνουν επιμέρους τμήματα διασυνδεδεμένα μεταξύ τους πάνω στα οποία υπάρχει ροή δεδομένων και πληροφοριών με ταυτόχρονη χρήση controls περιορισμού των κινδύνων μεταξύ αυτών των τμημάτων.

• Στην εφαρμογή μίας γνωστής μεθόδου σε νέα Cyber Physical συστήματα για την επιλογή ενός συνόλου αποτελεσματικών και αποδοτικών controls κυβερνοασφάλειας από μια καθιερωμένη βάση γνώσεων, που μειώνουν τον κίνδυνο, ενώ ταυτόχρονα ελαχιστοποιούν το κόστος.

Η δομή της εργασίας στο σύνολό της έχει ως εξής:

Στο κεφάλαιο 2 εξετάζονται εργασίες σχετικές με το αντικείμενο των έξυπνων Συστημάτων μεταφορών, συναφών Cyber Physical Συστημάτων με ταυτόχρονη παρουσίαση των κινδύνων του κυβερνοχώρου και την επιλογή controls για τη διαχείριση τους. Στο κεφάλαιο 3 κάνουμε για γενική επισκόπηση και μια ιστορική αναδρομή επί των Έξυπνων Συστημάτων Μεταφορών και των πιο σημαντικών επιμέρους τμημάτων αυτών. Ένα σημαντικό Background των ITS θα αναφέρουμε στο κεφάλαιο 4 με ανάλυση αρχιτεκτονικών εξέλιξης και ανάπτυξης αυτών (βλ. Advanced Access Control Concepts, ICSI DPP Security & Privacy Architecture, DDP Platform Security: DDS Security). Στη συνέχεια έχουμε ένα από τα πιο σημαντικά κεφάλαια της εργασίας με περιγραφή της Ποιοτικής Εκτίμησης των Κινδύνων και ανάλυση των μεθόδων αξιολόγησης κινδύνων STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privileges) και DREAD (Damage, Reproducibility, Exploitability, Affected users/systems, Discoverability). Η διάδοση και η άθροιση του διαδικτυακού ρίσκου παρουσιάζονται στο κεφάλαιο 6 μέσα από το μαθηματικό μοντέλο του συστήματος καθώς και τη συνολική άθροιση του. Στη συνέχεια στο κεφάλαιο 7 παρουσιάζεται ο τρόπος βέλτιστης επιλογής των Cyber Security Controls, κατ' αρχήν λαμβάνοντας υπόψη τα εξεταζόμενα Controls βελτιστοποίησης των cyber κινδύνων και στη συνέχεια με τη μέθοδο βελτιστοποίησης των εξεταζόμενων συστημάτων. Σημαντικό κεφάλαιο αποτελεί και το 8ο όπου εξετάζουμε την εφαρμογή του μοντέλου μας στα σύγχρονα ITS παραθέτοντας τα components του υπό εξέταση συστήματός μας, τα εξεταζόμενα controls και τέλος την βέλτιστη επιλογή των controls στα εξεταζόμενα ITS.

2. Σχετικές Εργασίες – Related Work

Ο κίνδυνος στο διαδίκτυο προκύπτει συναρτήσει των εξής πιθανοτήτων: της πιθανότητας εμφάνισης ανεπιθύμητων συμβάντων, για παράδειγμα μια επίθεση και των αρνητικών αποτελεσμάτων που θα προκύψουν όταν συμβούν αυτές οι ανεπιθύμητες καταστάσεις. Για να οδηγηθούμε σε μια κατάσταση να βρισκόμαστε σε διαδικτυακό κίνδυνο κύριος εκφραστής αυτή της κατάστασης είναι ένας επιτιθέμενος. Αυτός λοιπόν για να διεξάγει κάποια επίθεση ή έστω κάποια απειλή πρέπει να εκμεταλλευτεί με επιτυχία ένα ή περισσότερα τρωτά σημεία του συστήματος μας. Αυτό μπορεί να το πετύχει εφαρμόζοντας διάφορες πιθανές τακτικές επιθέσεων.

Αντίστοιχα, καταλήγουμε σε ένα σημείο όπου πρέπει να αναλύσουμε πως αναπτύσσονται και επεκτείνονται οι κυβερνοαπειλές σε σύνθετα συστήματα. Αυτά τα συστήματα αποτελούνται από άλλα διασυνδεδεμένα components (τμήματα – στοιχεία), τα οποία και από μόνα τους συνήθως αποτελούν ξεχωριστά και αυτόνομα συστήματα. Σε ξεχωριστό βήμα εντός των αυτόνομων αυτών συστημάτων χρειάζεται να αναλυθεί, σε προγενέστερο ή σε επόμενο βήμα, ο τρόπος ανάπτυξης και επέκτασης των κυβερνοαπειλών και των επιδράσεων τους. Με την ολοκλήρωση των αναλύσεων μπορούν να γίνουν εκτιμήσεις για το συνολικό κίνδυνο στον κυβερνοχώρο του κεντρικού πολύπλοκου και σύνθετου συστήματος.

Στα διεθνή συγγράμματα εμφανίζονται αρκετές μέθοδοι που αξιολογούν τους κινδύνους ασφαλείας που εφαρμόζονται σε IT συστήματα[1]. Πολλές είτε έχουν ήδη εφαρμοστεί είτε μπορούν να εφαρμοστούν σε ITS αλλά δε δύναται να αξιολογήσουν με ακρίβεια τους κινδύνους στον κυβερνοχώρο που σχετίζονται με Cyber Physical Systems (βλ.[2] που παρατίθενται προσεγγίσεων για την αξιολόγηση κινδύνων). Ανασκόπηση μεθόδων αξιολόγησης κινδύνων ασφαλείας για Cyber Physical Systems συμπεριλαμβανομένων και προτάσεων για κάποια κριτήρια ταξινόμησης υπάρχουν στην αναφορά[3].

Μια έρευνα για κυβερνοεπιθέσεις σε IoT συστήματα συμπεριλαμβάνει ένα τμήμα το οποίο επικεντρώνεται σε περιβάλλοντα Cyber Physical είναι και η[4]. Τις περισσότερες φορές οι μέθοδοι αξιολόγησης κινδύνων για CPS είναι συγκεκριμένες. Αυτό διότι πρέπει να λαμβάνουν υπόψη την ασφάλεια ως έναν επιπλέον παράγοντα που έχει αντίκτυπο και πως αυτός ο παράγοντας είναι επιπλέον των παραδοσιακών (confidentiality, integrity, availability). Ένα παράδειγμα είναι το[5] όπου χρησιμοποιούνται συγκεκριμένες μέθοδοι για περιπτώσεις έξυπνων δικτύων (smart grid).

Επίσης αρκετές εργασίες στη βιβλιογραφία έχουν μελετήσει πώς μεμονωμένα στοιχεία του κινδύνου στον κυβερνοχώρο διαδίδονται σε ένα δίκτυο διασυνδεδεμένων συστημάτων. Για το σκοπό αυτό έχουν χρησιμοποιηθεί τόσο ντετερμινιστικές όσο και στοχαστικές προσεγγίσεις. Ένα μοντέλο διάδοσης πιθανότητας απειλής για πληροφοριακά συστήματα που βασίζονται στη διαδικασία Markov μελετήθηκε[6]. Μια προσέγγιση για τον προσδιορισμό της διάδοσης των σφαλμάτων σχεδιασμού ενός πληροφοριακού συστήματος, μέσω μιας πιθανολογικής μεθόδου μελετήθηκε[7]. Ένα μοντέλο ανάλυσης κινδύνου ασφαλείας (SRAM) που επιτρέπει την ανάλυση της διάδοσης τρωτών σημείων στα πληροφοριακά συστήματα, βασισμένο στα δίκτυα

Bayesian, μελετήθηκε στο[8]. Μέθοδοι για την αξιολόγηση της διάδοσης των επιπτώσεων, των επιθέσεων στον κυβερνοχώρο σε CPS έχουν προταθεί[9,10].

Τα επιδημιολογικά μοντέλα χρησιμοποιήθηκαν αρχικά για τη μελέτη της διάδοσης κακόβουλου λογισμικού σε συστήματα πληροφοριών[6]. Η διάδοση περιστατικών κυβερνοασφάλειας σε ένα CPS θεωρείται ως μία επιδημική έξαρση στην μελέτη[11] και αναλύεται χρησιμοποιώντας τη θεωρία διήθησης. Η μέθοδος αποδείχθηκε ότι είναι εφαρμόσιμη για τη μελέτη περιστατικών μόλυνσης από κακόβουλο λογισμικό, αλλά είναι αμφίβολο εάν το μοντέλο έξαρσης της επιδημίας, μπορεί να χρησιμοποιηθεί για άλλου τύπου περιστατικά. Η θεωρία της διήθησης χρησιμοποιήθηκε επίσης στην μελέτη[12] για την ανάλυση της διάδοσης αστοχιών κόμβων σε ένα δίκτυο CPS που περιλαμβάνει cyber και φυσικούς κόμβους οργανωμένους σε δύο διακριτά επίπεδα, όπως και στην περίπτωση του ηλεκτρικού δικτύου. Το επιδημιολογικό μοντέλο (SEIR) (Susceptible–Exposed–Inverted–Recovered) χρησιμοποιήθηκε[13] για τη μελέτη της διάδοσης μόλυνσης από κακόβουλο λογισμικό στο έξυπνο δίκτυο. Ένα μοντέλο ποσοτικής αξιολόγησης κινδύνου, για ένα δεδομένο CPS θεωρώντας την διάδοση του κινδύνου μεταξύ εξαρτημένων κόμβων μελετήθηκε[14].

Προτάθηκε επίσης μία μέθοδος για την αξιολόγηση του συνολικού κινδύνου ενός συνόλου αλληλεξαρτώμενων κρίσιμων υποδομών[15,16]. Η μέθοδος παρέχει μία συγκεντρωτική τιμή cyber κινδύνου, σε επίπεδο υποδομής, αντί για μία λεπτομερή αξιολόγηση του κινδύνου στον κυβερνοχώρο σε επίπεδο συστήματος. Έτσι, είναι κατάλληλο για την αξιολόγηση της κρισιμότητας των τομέων της υποδομής, αλλά όχι για το σχεδιασμό αρχιτεκτονικών κυβερνοασφάλειας ή για την επιλογή κατάλληλων ελέγχων κυβερνοασφάλειας.

Ακολουθήθηκε μία παρόμοια προσέγγιση για το Ενεργειακό Διαδίκτυο (IoE)[17] για να αναπτυχθεί ένας αλγόριθμος εκτίμησης ρίσκου, σε επίπεδο συστημάτων ασφαλείας που βασίζεται στη δυναμική διάδοση του κινδύνου[18]. Ένα πλαίσιο για τη μοντελοποίηση και την αξιολόγηση του συνολικού κινδύνου, των προτύπων δραστηριότητας, των χρηστών σε κοινωνικά δίκτυα, προτάθηκε στην μελέτη[19]. Ένα ιεραρχικό μοντέλο δύο επιπέδων χρησιμοποιήθηκε[20], για την αναπαράσταση της δομής των βασικών υπηρεσιών στον εθνικό κυβερνοχώρο, και να αξιολογήσει την συνολική εκτίμηση ρίσκου, σε εθνικό επίπεδο, λαμβάνοντας υπόψη τις απειλές του κυβερνοχώρου και τα τρωτά σημεία που εντοπίστηκαν στο χαμηλότερο επίπεδο.

Οι περισσότερες από τις προηγούμενες εργασίες για τα αυτόνομα πλοία επικεντρώνονται στα συστήματα και την αρχιτεκτονική επικοινωνίας ως μέρος της εργασίας στο πλαίσιο του έργου EU MUNIN[21]. Συγκεκριμένα, η αρχιτεκτονική των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ICT) των μη επανδρωμένων εμπορικών πλοίων παρέχεται από τον Rodseth στο[22], και η αρχιτεκτονική επικοινωνίας παρουσιάζεται σε επόμενη εργασία[23]. Περαιτέρω, το έργου MUNIN αναλύει τις αρχιτεκτονικές και τις λειτουργίες της γέφυρας[24], το Κέντρο Ελέγχου ακτής (Shore Control Center)[25] και τα μηχανοστάσια[26]. Επίσης, ο O.J. Rodseth στο[27] περιγράφει μια μέθοδο αξιολόγησης κινδύνου η οποία είναι προσανατολισμένη στην ασφάλεια και όχι στο να εξετάσει τις απειλές και τα τρωτά σημεία για την ασφάλεια στον κυβερνοχώρο. Σημαντική δουλειά στον χώρο των αυτόνομων σκαφών έχει γίνει επίσης στο έργο AAWA, στο οποίο αναγνωρίζεται και η ανάγκη για κυβερνοασφάλεια, και αναδεικνύονται γενικά ζητήματα ασφάλειας και θέματα ασφάλειας που είχαν τεθεί αρχικά από τους Jalonen [28].

Ωστόσο, η ασφάλεια του αυτόνομου πλοίου έχει εξεταστεί και αναλυθεί ελάχιστα. Συγκεκριμένα, η Lloyds[29] σχολίασε την ασφάλεια στον κυβερνοχώρο του ικανού cyber πλοίου, αλλά μόνο ως θεωρία. Επίσης, ο Tam[30] πρότεινε μια μέθοδο για την αξιολόγηση του κυβερνοκινδύνου του C-ES, αλλά η ανάλυση έγινε για τρία συγκεκριμένα μοντέλα πλοίων χωρίς να επεκτείνονται σε όλα τα συστήματα και τα υποσυστήματα, ενώ οι πιθανές επιθέσεις εξετάστηκαν μόνο από την οπτική γωνία του εισβολέα. Στο[31] μια generic αρχιτεκτονική συστήματος συζητείται από τον Κάτσικα καθώς και οι απειλές, τρωτών σημείων και κινδύνων έναντι αυτής της generic αρχιτεκτονικής. Ωστόσο, η αρχιτεκτονική του συστήματος και τα στοιχεία του δεν έχουν καθοριστεί.

Πολλές μεθοδολογίες ανάλυσης απειλών έχουν προταθεί στη βιβλιογραφία[32,33]. Από τα πιο επιφανή, τα Attack Trees, απαιτούν την κατανόηση κάθε υποσυστήματος ξεχωριστά και παρέχουν μια επισκόπηση σχετικά με το επίπεδο επίθεσης, χωρίς να λαμβάνεται υπόψη βασικά δεδομένα για το σενάριο της απειλής. Ο Chun Yu Cheung[34] καταλήγει στο συμπέρασμα ότι τα στα Δέντρα επίθεσης, θα πρέπει να γίνει αντιληπτός, ο αρχικός στόχος του επιτιθέμενου και η μέθοδος δίνει περισσότερη έμφαση στην πολυπλοκότητα της επίθεσης. Το πλαίσιο εργασίας του μοντέλου απειλής, βασιζόμενο στην ανάλυση της διαδρομής της επίθεσης (T-MAP), είναι μια άλλη μέθοδος, η οποία εξετάζει την σοβαρότητα (το βάρος) που προέρχεται από τα Attack Trees. Αυτή η μέθοδος[32], λειτουργεί με συστήματα Commercial Off the Shelf (COTS), επομένως είναι ακατάλληλο για την περίπτωση C-ES.

Η Risk Reduction Overview (RRO) είναι μια μέθοδος η οποία εξαρτάται από τον σχεδιασμό του συστήματος στόχου[35]. Αυτό απαιτεί τη γνώση των πιθανών τρωτών σημείων ήδη από τη φάση του σχεδιασμού, γεγονός που περιορίζει τη δυνατότητα εφαρμογής του σε υποθέσεις C-ES, των οποίων ο σχεδιασμός των εξαρτημάτων δεν είναι διαθέσιμος με επαρκείς λεπτομέρειες. Η μεθοδολογία Petri net είναι αρκετά περίπλοκη, ενώ η Attack Library μέθοδος, βασίζεται στην οπτική γωνία του εισβολέα[36]. Σε αντίθεση, οι μέθοδοι με την προοπτική της αμυντικής λειτουργείας, εξετάζουν διεξοδικά τα στοχευμένα συστήματα και το πεδίο εφαρμογής τους είναι η υπεράσπιση αυτών.

Ο Shafiq Hussain[32] σύγκρινε διαφορετικές μεθοδολογίες μοντέλων απειλών και κατέληξε στο συμπέρασμα ότι το μεγαλύτερο μέρος του ακαδημαϊκού χώρου και της βιομηχανίας χρησιμοποιεί τη μεθοδολογία STRIDE ή τις παραλλαγές της. Μια άλλη συγκριτική ανάλυση των μοντέλων απειλών έχει πραγματοποιηθεί[33] και οι συγγραφείς κατέληξαν στο συμπέρασμα ότι η μέθοδος STRIDE και οι παραλλαγές της εξάγουν τα πιο αυστηρά αποτελέσματα σε αντίθεση με τις άλλες έξι μεθοδολογίες και πλαίσια που εξετάστηκαν. Είναι σημαντικό να σημειωθεί ότι το μεγαλύτερο μέρος των μεθοδολογιών απαιτούν να είναι διαθέσιμη η ανάλυση της αρχιτεκτονικής του στόχου με πλήρη λεπτομέρεια. Αυτό τις καθιστά ακατάλληλες για το C-ES, γιατί αυτές οι λεπτομέρειες δεν είναι ακόμη διαθέσιμες και αναμένεται να εξαρτώνται από συγκεκριμένες υλοποιήσεις.

Με βάση τα παραπάνω ευρήματα, το STRIDE επιλέχθηκε ως το πλέον κατάλληλη μέθοδο για χρήση, για την ανάλυση απειλών κατά του C-ES. Καμία προηγούμενη δουλειά δεν έχει πρότεινε μια λεπτομερή αρχιτεκτονική συστήματος ή έχει εφαρμόσει μια ολιστική απειλή ανάλυση για τον εντοπισμό πιθανών επιθέσεων που μπορεί να

συμβούν στα συστήματα μιας τέτοιας αποστολή αξιοποιώντας συγκεκριμένα τρωτά σημεία.

Αρκετές επίσης εργασίες στη βιβλιογραφία, έχουν αναλύσει απειλές ασφαλείας και κινδύνων πάνω σε συγκεκριμένα συστήματα που χρησιμοποιούνται σε συγκεκριμένους τύπους αυτόνομων και τηλεκατευθυνόμενων σκαφών. Ο B. Svilicic [37] πρότεινε ένα πλαίσιο για την αξιολόγηση των κινδύνων στον κυβερνοχώρο στα πλοία το οποίο είχε εφαρμογή πάνω στο Ηλεκτρονικό Σύστημα Απεικόνισης και Πληροφοριών Χαρτών (ECDIS).

Ο Bolbot [38] εντόπισε και ανέλυσε κυβερνοεπιθέσεις που σχετίζονται με την ασφάλεια σε αυτόνομο πορθμείο εσωτερικής ναυσιπλοΐας. Η ανάλυσή τους καλύπτει πτυχές ασφάλειας σχετικά με το σύστημα πλοήγησης και πρόωσης του πορθμείου. Ο Silverajan[39] διερεύνησε ζητήματα ασφάλειας και επιθέσεις στον κυβερνοχώρο που στοχεύουν συστήματα smart πλοίων. Ο Awan[40] ανέλυσαν 59 τεκμηριωμένα ατυχήματα, για καλύτερη κατανόηση των τρωτών σημείων των στοιχείων του Integrated Bridge System (IBS). Ο Svilicic[41] παρουσίασε μια μελέτη σχετικά με την ανθεκτικότητα, σε θέματα ασφάλειας (στον κυβερνοχώρο) ενός Ολοκληρωμένου Συστήματος Πλοήγησης (INS), το οποίο ήταν εγκατεστημένο σε πλοίο RoPax, που ασχολείται με το διεθνές εμπόριο. Ο

Ο Wang[42] πρότεινε μία παρόμοια ασφαλή ενσωματωμένη μέθοδος πλοήγησης για την εξουδετέρωση επιθέσεων εισαγωγής εσφαλμένων μέτρων. Ο Balduzzi[43] παρουσίασε μια αξιολόγηση της ασφάλειας του Συστήματος Αυτόματης Αναγνώρισης (AIS), εισάγοντας απειλές που επηρεάζουν τόσο την εφαρμογή σε διαδικτυακούς παρόχους όσο και την διασάφηση του πρωτοκόλλου. Ο Lund[44] περιέγραψε μια επίθεση (proof of concept) σε ένα INS και το ενσωματωμένο ECDIS του και παρουσίασε την επίθεση σε ένα σκάφος. Ο Καβαλλιεράτος[45] εντόπισε ενδεχόμενα (cyber attack) σενάρια επίθεσης και αξιολόγησε ποιοτικά τους αντίστοιχους κινδύνους για έναν αριθμό CPS του C-ES οικοσυστήματος, επί του σκάφους και στο SCC.

Οι συστηματικές μέθοδοι για την επιλογή των ελέγχων ασφαλείας για ITS συστήματα είτε βλέπουν το πρόβλημα από την σκοπιά του ελέγχου της επιλογής ως επενδυτικό πρόβλημα και εφαρμόζουν εργαλεία διαχείρισης και οικονομικής ανάλυσης για την βελτιστοποίηση της επιλογής, ή στο πλαίσιο της απόκρισης σε μια εισβολή, δηλαδή όταν μια συγκεκριμένη επίθεση έχει ήδη ανιχνευθεί ότι λαμβάνει χώρα. Ένα συνδυαστικό μοντέλο βελτιστοποίησης για αποτελεσματική επιλογή ελέγχων ασφαλείας προτάθηκε[46,47]. Ωστόσο, η επιλογές των ελέγχων ασφαλείας εξακολουθούν να εκτελούνται σε μεγάλο βαθμό εμπειρικά, ιδιαίτερα για Cyber Physical Συστήματα.

Στον θαλάσσιο τομέα, cyber security controls έχουν επίσης προταθεί για συστήματα σε αυτόνομα και τηλεκατευθυνόμενα πλοία. Ο Bothur[48] συζήτησε τις ευπάθειες ασφαλείας που αντιμετωπίζουν τα έξυπνα πλοία και περιέγραψε αντίμετρα ασφαλείας, ιδιαίτερα διαδικαστικές και τεχνικές λύσεις, ακολουθώντας μια άμυνα σε βάθος προσέγγισης. Ο Silverajan[39] ανέλυσε τα κύρια συστήματα ενός μη επανδρωμένου έξυπνου πλοίου και πρότεινε στρατηγικές άμυνας έναντι επιθέσεων και απειλών στον κυβερνοχώρο που είδη έχουν συζητηθεί. Ο Bolbot[38] ανέλυσε τις επιθέσεις στον κυβερνοχώρο που σχετίζονται με την ασφάλεια των συστημάτων για την πλοήγηση και την πρόωση, αξιολογώντας τους κινδύνους και πρότειναν γενικές συστάσεις ασφάλειας. Ο Sahay[49] πρότεινε ένα πλαίσιο SDN για τον μετριασμό των επιθέσεων

στον κυβερνοχώρο και τη βελτίωση της ανθεκτικότητας στο δίκτυο επικοινωνίας του έξυπνου πλοίου.

Καμία από τις παραπάνω εργασίες δεν ακολούθησε συστηματική, βασισμένη στον κίνδυνο διαδικασία για την επιλογή των χειριστηρίων. Περαιτέρω, οι προαναφερθείσες αναλύσεις επικεντρώθηκαν σε αμυντικές στρατηγικές και στοιχεία ελέγχου που δεν είναι ειδικά για το σύστημα.

3. Background – Γενική Επισκόπηση των ITS[50]

i. Εισαγωγή

Ο όρος «Intelligent Transport Systems» (Έξυπνα Συστήματα Μεταφορών) ή «ITS» χρησιμοποιείται για να ορίσει τη χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ή ΤΠΕ) στον τομέα των μεταφορών. Ορίζει επίσης τη δημιουργία ροής πληροφοριών και δεδομένων έτσι ώστε να είναι δυνατή η όσο το δυνατό πιο «έξυπνη» χρήση των υποδομών και των οχημάτων και να βελτιώνεται η διαχείριση κυκλοφορίας της κινητικότητας. Το όραμα γύρω από τα ITS είναι: «ευφυής κινητικότητα προς πλήρως ενημερωμένα άτομα, μηδενικά ατυχήματα, μηδενικές καθυστερήσεις, με μειωμένο αντίκτυπο στο περιβάλλον, όπου οι υπηρεσίες είναι προσιτές και απρόσκοπτες, με σεβασμό της ιδιωτικής ζωής και της παρεχόμενης ασφάλειας»[51].

Τα ITS είναι τομέας υψηλών δυνατοτήτων για την αντιμετώπιση των προκλήσεων που αντιμετωπίζει ο τομέας των μεταφορών. Τόσο στους τρόπους μεταφοράς όσο και (σημαντικότερο) στη δημιουργία διεπαφών και αλληλοσυμπλήρωσης των τρόπων μεταφοράς. Εκτός από την υποδομή, το ITS θεωρείται ως ο μοναδικός σημαντικός «παράγοντας» που μπορεί να χρησιμοποιηθεί για την επίτευξη συνεργασίας μεταξύ των διαφόρων τρόπων μεταφορών και δημιουργία ενός απρόσκοπτου συστήματος μεταφορών σε όλο τον κόσμο. Υπάρχει επίσης μια σημαντική και πολυάριθμη κοινότητα ενδιαφερομένων που είτε παρέχει είτε χρησιμοποιεί εφαρμογές και υπηρεσίες ITS και εν τέλει ο τομέας παρέχει ουσιαστική συμβολή στην οικονομική και κοινωνική ανάπτυξη.

Η ανάπτυξη συστημάτων και υπηρεσιών ITS ήταν μέχρι πρότινος σε μεγάλο βαθμό μονόπλευρη σε έκταση, αφήνοντας πίσω την όποια πολυτροπική εφαρμογή των σημερινών συστημάτων και δεν ευνοούσε περαιτέρω ανάπτυξη στο μέλλον. Η ανάπτυξη μονοτροπικών εφαρμογών ITS, θεωρήθηκε ως ελλιπής και όχι αρκετά διαδεδομένη για να καλύπτει το σύνολο των πιθανών εφαρμογών και της αγοράς. Η επίτευξη «αυτάρκειας» και βιωσιμότητας των ολοκληρωμένων εφαρμογών ITS παραμένει κεντρικός στόχος που πρέπει να επιτευχθεί σε πολλές περιπτώσεις.

Οι προσπάθειες για διάδοσης των ITS σε επίπεδο ΕΕ έχουν ενταθεί από τα μέσα της δεκαετίας του 2000 μέσω νομοθετικών και τεχνικών αναπτυξιακών μέτρων. Οι πρώτες «θεσμικές» προσπάθειες για την προώθηση των ITS στην Ευρώπη έγιναν στις αρχές της δεκαετίας του '90. Έκτοτε σταδιακά τα συστήματα και οι εφαρμογές ITS αναπτύσσονται συνεχώς στην Ευρώπη αλλά και σε όλο τον ανεπτυγμένο κόσμο. Το 2008 η Commission ανακοίνωσε εξέδωσε το «Σχέδιο δράσης για την ανάπτυξη ITS στην Ευρώπη». Μέσω αυτό «χάραξε» τις προτεραιότητες της πολιτικής για επιλογή γενικών στοιχείων ITS προς κοινή χρήση ή επαναχρησιμοποίηση και όρισε το χρονοδιάγραμμα εφαρμογής στους ακόλουθους τομείς δράσης:

- Βέλτιστη χρήση δεδομένων που δρόμων, κυκλοφορίας, ταξιδιών.

- Οδική ασφάλεια.
- Ενσωμάτωση των οχημάτων στην υποδομή μεταφορών.
- Συνέχεια διαχείρισης της κυκλοφορίας και των εμπορευματικών υπηρεσιών ITS τόσο στις ευρωπαϊκές «αρτηρίες» μεταφορών όσο και στα αστικά κέντρα.
- Ασφάλεια και προστασία δεδομένων, και ορθή απόδοση ευθυνών.
- Συντονισμός και συνεργασία στα Ευρωπαϊκά ITS θέματα.

Η Οδηγία 2010/40 του Ευρωπαϊκού Κοινοβουλίου παρείχε το απαραίτητο πλαίσιο για την ανάπτυξη και τη χρήση προδιαγραφών και προτύπων. Όριζε πως όλα αυτά είναι απαραίτητα για την εξασφάλιση διαλειτουργικότητας, συμβατότητας και συνέχειας στην ανάπτυξη της επιχειρησιακής χρήση των ITS. Στην οδηγία αυτή ορίζονται οι ακόλουθοι τομείς προτεραιότητας για την ανάπτυξη και τη χρήση προδιαγραφών και προτύπων για την παροχή διαλειτουργικότητας, συμβατότητας και συνέχειας στην ανάπτυξη και τη επιχειρησιακή χρήση των ITS:

- Βέλτιστη χρήση δεδομένων δρόμου, κυκλοφορίας, ταξιδιών
- Συνέχεια των υπηρεσιών ITS διαχείρισης κυκλοφορίας και μεταφοράς εμπορευμάτων,
- Εφαρμογές οδικής ασφάλειας και ασφάλειας,
- Σύνδεση του οχήματος με τις υποδομές μεταφορών.

Στο πλαίσιο της προτεραιότητας που δόθηκε σε αυτούς τους τομείς, ορίζονται κάποιες δράσεις με προτεραιότητα για την ανάπτυξη και τη χρήση προδιαγραφών και προτύπων στα ITS ως εξής:

- Παροχή υπηρεσιών πολυτροπικών πληροφορίας ταξιδιού σε όλη την ΕΕ.
- Παροχή υπηρεσιών πληροφοριών κυκλοφορίας σε πραγματικό χρόνο σε όλη την ΕΕ.
- Δεδομένα και διαδικασίες για την παροχή, όπου είναι δυνατόν, ελάχιστων καθολικών πληροφοριών κυκλοφορίας που σχετίζονται με την οδική ασφάλεια δωρεάν στους χρήστες.
- Εναρμονισμένη διάταξη για κοινό αριθμό κλήση (ακόμα και διαδικτυακά) όλη την σε όλη την ΕΕ.
- Παροχή υπηρεσιών πληροφορίας για ασφαλείς θέσεις στάθμευσης φορτηγών και επαγγελματικών οχημάτων.

Μέσω νομοθετικών δράσεων, και ιδιαίτερα της Οδηγίας ITS, η ΕΕ πέτυχε να προσφέρει ευρεία κάλυψη σε διαλειτουργικές υπηρεσίες ITS δίνοντας προτεραιότητα στην έρευνα και την ανάπτυξη:

- Κοινές ευρωπαϊκές προδιαγραφές ITS με βάση τη διαλειτουργικότητα και τα δημόσια / ελεύθερα πρότυπα (λειτουργικές, τεχνικές, οργανωτικές, παροχής υπηρεσιών)
- Υπηρεσίες πληροφορίας για πολυτροπικά ταξιδιών σε επίπεδο ΕΕ,
- Υπηρεσίες πληροφορίας κυκλοφορίας σε πραγματικό χρόνο σε επίπεδο ΕΕ
- Υπηρεσίες σχετικές με την οδική ασφάλεια, όπως η εναρμονισμένη, διαλειτουργική ηλεκτρονική κλήση σε όλη την ΕΕ, υπηρεσίες πληροφορίας για ασφαλείς λειτουργίες εμπορευματικών μεταφορών κτλ

Τα διάφορα συστήματα ITS, που σχετίζονται τόσο με τη λειτουργία μονοτροπικών ή πολυτροπικών μεταφορών, εξετάζονται και ταξινομούνται σε έναν – ή και περισσότερους – από τους ακόλουθους 8 τομείς εφαρμογής των ITS:

- Πληροφορίες ταξιδιού και κυκλοφορίας
- Διαχείριση Κυκλοφορίας και Δημοσίων Συγκοινωνιών
- Υπηρεσίες πλοήγησης
- Έξυπνη έκδοση εισιτηρίων και είσπραξη τελών
- Ασφάλεια των μεταφορών
- Μεταφορές εμπορευμάτων και Logistics (συμπεριλαμβανομένων των αστικών)
- Έξυπνες υπηρεσίες κινητικότητας και συν-τροπικότητας
- Περιβαλλοντική και ενεργειακή απόδοση (συμπεριλαμβανομένης της ηλεκτροκίνησης).

Στη συνέχεια γίνεται απολογισμός των τρεχουσών τεχνολογικών και πολιτικών/νομοθετικών εξελίξεων σε καθέναν από τους παραπάνω 8 τομείς εφαρμογής των ITS στα πλαίσια επιστημονικών αξιολογήσεων του κλάδου.

ii. ITS για πληροφορίες κυκλοφορίας και ταξιδιού (Traffic and Travel Information – TTI)

Οι τεχνολογίες, τα συστήματα και οι νομοθετικές διατάξεις για πληροφορίες κυκλοφορίας και ταξιδιού (TTI) που αποσκοπούν στην παροχή πληροφοριών σε πραγματικό χρόνο στους ταξιδιώτες, ήταν τα πρώτα στοιχεία ITS που αναπτύχθηκαν και προωθήθηκαν εμπορικά. Απώτερο πεδίο εφαρμογής και στόχος των συστημάτων TTI είναι να παρέχουν συνεχή και αξιόπιστα δεδομένα κίνησης και ταξιδιού και πληροφορίες σχετικές διαμέσου όλων των τρόπων και των δικτύων. Αυτό πετυχαίνετε με καθολική πρόσβαση σε τέτοιες πληροφορίες και ανταλλαγή δεδομένων και διαμέσου εφικτών επιχειρηματικών μοντέλων .

Το TTI αφορά τη συλλογή, επεξεργασία, μετάδοση και βέλτιστη χρήση των δεδομένων κίνησης και ταξιδιού για πανευρωπαϊκές πληροφορίες ταξιδιού σε πραγματικό χρόνο και την παροχή τους σε χρήστες τέτοιων πληροφοριών είτε δωρεάν είτε επί πληρωμή. Κατά την αξιολόγηση του επιστημονικής και αναπτυξιακά ερευνητικής δύναμης των τεχνολογιών και υπηρεσιών TTI, υπάρχουν τέσσερα κύρια ζητήματα που πρέπει να ληφθούν υπόψη. Συγκεκριμένα:

- Νομικό πλαίσιο για την παροχή TTI,
- Τα χρησιμοποιούμενα τεχνικά πρότυπα και η διαλειτουργικότητα τους,
- Επιχειρηματικά μοντέλα που χρησιμοποιούνται για την παροχή αυτών των δεδομένων και
- Η έκταση στην οποία οι ίδιοι οι ταξιδιώτες μπορούν να επιδράσουν και συνδράμουν σε αυτές τις διατάξεις TTI .

Το νομικό πλαίσιο για τις υπηρεσίες TTI είναι η νομοθεσία που αναφέρεται στα ITS, η οποία σε ευρωπαϊκό επίπεδο θεσπίστηκε σταδιακά την τελευταία εικοσαετία περίπου. Κύριο του πλαισίου είναι η Οδηγία 2010/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου η οποία θέτει τις βάσεις για περαιτέρω νομοθετική δράση από τα κράτη-μέλη. Επίσης θεσπίζει ένα πλαίσιο για συντονισμένη στήριξη της ανάπτυξης και χρήσης των ITS εντός της ΕΕ, κυρίως στην αλλαγή συνόρων μεταξύ κρατών μελών. Ακόμη ορίζει τις γενικές προϋποθέσεις που απαιτούνται γι’ αυτό το σκοπό. Προβλέπει τη θέσπιση

προδιαγραφών των δράσεων που μπορούν να γίνουν εντός των τομέων που δίδεται βαρύτητα καθώς και την ανάπτυξη, όπου ενδείκνυται, των απαραίτητων προτύπων. Με τη σειρά τους, τα κράτη μέλη πρέπει να διασφαλίζουν ότι η επεξεργασία προσωπικών δεδομένων στο πλαίσιο λειτουργίας των εφαρμογών και υπηρεσιών ITS πραγματοποιείται σύμφωνα με τους κανόνες της ΕΕ.

Παρά την πρόοδο που σημειώθηκε στη δεκαετία του 2000, το ευρωπαϊκό νομοθετικό πλαίσιο για τις υπηρεσίες ΤΤΙ εξελίσσεται ακόμη. Ειδικά σε επίπεδο μεμονωμένων κρατών μελών προϋπήρχαν σχετικές διατάξεις από την ευρωπαϊκή οδηγία και χρειάζονταν εναρμόνιση, είτε δεν υπάρχουν καθόλου. Κρίσιμο πεδίο για τη νομοθετική εναρμόνιση είναι το πλήθος των νομικών διατάξεων στον τομέα της περαιτέρω χρήσης των πληροφοριών του δημόσιου τομέα. Οι διαφορετικές εθνικές νομοθεσίες ποικίλλουν όσον αφορά την παροχή αυτών των δεδομένων δωρεάν και τον βαθμό στον οποίο διασφαλίζουν ότι η παροχή τους είναι δίκαιη, διαφανής και χωρίς διακρίσεις. Στο Ηνωμένο Βασίλειο για παράδειγμα υπάρχει ελεύθερη πρόσβαση και χρήσης, συμπεριλαμβανομένων των πληροφοριών κυκλοφορίας των ΜΜΜ. Στη Γερμανία υπάρχουν συμβάσεις πώλησης των αντίστοιχων δεδομένων από τις ομοσπονδιακές υπηρεσίες και τις τοπικές αρχές ελέγχου της κυκλοφορίας στους παρόχους υπηρεσιών ITS και τους κατασκευαστές κοκ.

Όσον αφορά τα τεχνικά πρότυπα που χρησιμοποιούνται για τη διακίνηση πληροφοριών και δεδομένων κίνησης και ταξιδιού, την τελευταία δεκαετία αναπτύχθηκε μια σειρά προτύπων ΤΤΙ και μια σχετικά καινοτόμος προσπάθεια να δημιουργηθεί διαλειτουργικότητα μεταξύ αυτών των προτύπων. Τα πιο γνωστά παραδείγματα προτύπων ΤΤΙ στην Ευρώπη σήμερα είναι τα:

- DATEX I και DATEX II (Data Traffic Exchange).
- CORBA (Common Object Request Broker Architecture).
- OTAP (Open Travel Data Access Protocol).
- TPEG (Transport Protocol Experts Group).
- RDS-TMC (Radio Data System-Traffic Message Channel).
- Άλλα λιγότερο διαδεδομένα (ALERT C, CAM, DENM, κοκ).

Αυτά τα πρότυπα έχουν ωριμάσει σημαντικά έχοντας επίσης σημαντικές κοινότητες ανάπτυξης στο πλαίσιο των φορέων και των διαδικασιών δημιουργίας τους (π.χ. στα ISO/TC204 WG10, CEN/TC278 WG4, CEN/TC278 WG8, ETSI TC ITS WG1).

Όσον αφορά τη διαλειτουργικότητα αυτών των προτύπων εξελίχθηκε με μάλλον αργούς ρυθμούς. Ένα μνημόνιο συνεργασίας μεταξύ EasyWay και TISA γύρω από τις επικοινωνία DATEX II και TPEG ήταν από τις πρώτες προσπάθειες διαλειτουργικότητας. Μπορεί ένα έργο διαλειτουργικότητας μπορεί να απαιτεί κάποια εκ νέου επεξεργασίας των προτύπων αλλά η συντριπτική ανάγκη είναι να δημιουργηθεί τελικά ένα ενιαίο κοινό λεξικό/μητρώο δεδομένων για δεδομένα ΤΤΙ. Στο μέλλον θα συμβούν τυποποιήσεις σε τομείς όπως:

- Προειδοποίηση Τροχαίων Ατυχημάτων.
- Δεδομένα Διαχείρισης Κυκλοφορίας.
- Συνεργατική Ταξιδιωτική Βοήθεια.

Όσον αφορά τα επιχειρηματικά μοντέλα που παρέχουν υπηρεσίες ΤΤΙ, ο κύκλος της αλυσίδας παροχής υπηρεσιών ΤΤΙ απεικονίζεται διαγραμματικά παρακάτω:

Τα πιο διαδεδομένα μοντέλα επιχειρηματικών δομών για την παροχή υπηρεσιών ITS/TTI, βασίζονται σε συμφωνίες συνεργασίας δημόσιου και ιδιωτικού τομέα. Συνήθως προβλέπουν την ανάθεση της συλλογής και αποθήκευσης δεδομένων σε ιδιώτες και τη διανομή των δεδομένων σε παρόχους υπηρεσιών με υψηλή ποιότητα παροχής ταξιδιωτικών πληροφοριών. Ο ολλανδικός οργανισμός NDW (National Data Warehouse for traffic information) που ιδρύθηκε το 2007 είναι ένα καλό παράδειγμα ευρωπαϊκού επιχειρηματικού μοντέλου PPP υπηρεσιών ΤΤΙ. Πρόκειται για συνεργασία μεταξύ 15 αρχών για τη συλλογή, επεξεργασία, αποθήκευση και διανομή δεδομένων κυκλοφορίας.

Αυτή η βάση δεδομένων αποτελείται από:

- Πληροφορίες κυκλοφορίας
- Τρέχουσες πληροφορίες για την κατάσταση στους δρόμους π.χ. ένταση κυκλοφορίας, χρόνος ταξιδιού, ταχύτητες ανά σημείο
- Πληροφορίες κατάστασης
- Πληροφορίες για την λειτουργική κατάσταση των δρόμων π.χ. οδικά έργα, αναφορές συμφόρησης και περιστατικών
- Κατάσταση λωρίδων σε ώρα αιχμής, κατάσταση γεφυρών, σενάρια λειτουργίας
- Ιστορικά στοιχεία.

Η NDW αναθέτει τη συλλογή και αποθήκευση δεδομένων σε ιδιώτες. Ιδιοκτήτες των δεδομένων παραμένουν οι δημόσιες αρχές που συμμετέχουν στο NDW. Τα δεδομένα διανέμονται στους παρόχους υπηρεσιών, έναντι αντιτίμου, οι οποίοι αναπτύσσουν και παρέχουν τις υπηρεσίες στους τελικούς χρήστες πάλι επί πληρωμή.

Τα δεδομένα για υπηρεσίες ΤΤΙ αυξάνονται σε διαθεσιμότητα λόγω:

- Τεχνολογικής προόδου (μια πιο αξιοσημείωτη τάση είναι η συλλογή δεδομένων μέσω του λεγόμενου «συνεργατικού» μοντέλου όπου κάθε όχημα στο δίκτυο γίνεται και πομπός και δέκτης πληροφοριών),
- Διαφοροποίηση και εναλλαγή πηγών δεδομένων ,
- Καλύτερη οργάνωση και καλύτερη διαχείριση δεδομένων ,
- Επαναχρησιμοποίηση πληροφοριών και δεδομένων του δημόσιου τομέα και
- Δραστηριοποίηση πολλών εμπορικών και επιχειρηματικών δομών σε αυτόν τον τομέα.

Από την πλευρά της ζήτησης, δηλαδή του αριθμού των χρηστών και του τρόπου που οι χρήστες του ΤΤΙ αντιδρούν, αναμένεται διευθέτηση για τα εξής ζητήματα:

- Πώς χρησιμοποιεί ο πελάτης το ΤΤΙ,
- Πόσες πληροφορίες μπορούν να αφομοιωθούν,
- Ποια είναι η σχέση μεταξύ πληροφοριών και συμπεριφοράς (συνήθειες, αβεβαιότητα, ατελείς πληροφορίες, κόστος προσαρμογής κτλ),
- Ποια είναι η καλύτερη μορφή και ο καλύτερος χρόνος για την ενημέρωση,

- Ποια είναι τα προτιμώμενα κανάλια διάδοσης πληροφοριών,
- Ποια είναι η προθυμία για πληρωμή.

Ο τομέας του TTI/ITS στην Ευρώπη, αν και αρκετά προχωρημένος διαμορφώνεται ακόμη σε τεχνικό, οργανωτικό και νομικό επίπεδο. Σημαντική πρόοδος σημειώθηκε την τελευταία σε πολλούς τομείς, αλλά εκτιμάται ότι θα χρειαστεί τουλάχιστον άλλη μια δεκαετία για να επιλυθούν τα σχετικά ζητήματα που θα οδηγήσουν σε πανευρωπαϊκά διαλειτουργικές υπηρεσίες TTI σε όλες τις λειτουργίες που έχουν :

- Υψηλή ποιότητα δεδομένων με πολυτροπικό και κωδικοποιημένο περιεχόμενο κάνοντας χρήση κοινών ή καλά εναρμονισμένων και διαλειτουργικών προτύπων.
- Οργανωτικά συστήματα που διασφαλίζουν δίκαιη και διαφανή διαθεσιμότητα δεδομένων.
- Ομαλή συνεργασία μεταξύ ιδιωτικών ή ιδιωτικών-δημοσίου βασισμένη σε υγιή επιχειρηματικά μοντέλα.
- Πλήρης διασυνοριακή ανταλλαγή και χρήση δεδομένων πλήρως διαθέσιμα σε όλους τους χρήστες (ανεξαρτήτως γλώσσας ή άλλων φραγμών).
- Πλήρως εναρμονισμένα δεδομένα τοποθεσίας σε όλη την Ευρώπη.

Τα παραπάνω αφορούν την Ευρώπη, αλλά σε όλο τον κόσμο η ανάπτυξη των υπηρεσιών TTI/ITS προχωρά επίσης γρήγορα, αν και με άλλες ταχύτητες και σε διαφορετικά επίπεδα. Στην Ιαπωνία, για παράδειγμα, οι υπηρεσίες TTI θεωρητικά προηγούνται των υπηρεσιών στην Ευρώπη και τις ΗΠΑ. Στην Άπω Ανατολή, το μοντέλο «καθολικής συνεργασίας» για τη συλλογή δεδομένων εφαρμόστηκε πριν από αρκετά χρόνια. Αυτό έγινε μέσω της πλατφόρμας VICS αλλά υπάρχουν πολλές άλλες εφαρμογές που λειτουργούν σε άλλα επιχειρηματικά μοντέλα.

Και στις ΗΠΑ, υπάρχει πληθώρα μέσων παροχής TTI. Η ανάπτυξη συστημάτων TTI ακολούθησε την εμπορική άνθηση όλων των καινοτομιών. Το παρακάτω είναι ένα αμερικάνικο παράδειγμα σημαντικών ιστοσελίδων και οργανισμών παροχής TTI:

Ιστοσελίδες Σύνδεσμοι Εθνικών Πληροφοριών στις ΗΠΑ:

- Πληροφορίες εθνικής κυκλοφορίας και κλειστών δρόμων (FHWA)
- Καιρικές συνθήκες/σχετικές συνθήκες δρόμων:
- AccuWeather (Τίτλοι Καιρού)
- Intellicast (Συνθήκες Αυτοκινητοδρόμων)
- Εθνική Μετεωρολογική Υπηρεσία
- Διαδραστικό δίκτυο πληροφοριών εθνικής υπηρεσίας καιρού
- Safe Travel USA - Καιρικές και οδικές συνθήκες για τις Κεντρικό και Βόρειο τμήμα των ΗΠΑ
- AccuTraffic - Πληροφορίες για τις συνθήκες κυκλοφορίας
- Beat – Πληροφορίες κυκλοφορίας για διάφορες πόλεις
- Iteris - Πληροφορίες κυκλοφορίας σε πραγματικό χρόνο, χάρτες, χρόνοι
- MSN - Αναφορές κυκλοφορίας και κίνησης
- SmartTraveler - Πληροφορίες κυκλοφορίας για διάφορες μεγάλες πόλεις
- Total Traffic Network - Πληροφορίες κυκλοφορίας για διάφορες πόλεις
- Traffic.com - Πληροφορίες κυκλοφορίας για διάφορες πόλεις
- TrafficLand.com - Κάμερες κυκλοφορίας για διάφορες πόλεις

- TravelForecast.com – Προβλέψεις συνθηκών οδικής κυκλοφορίας
- Σύνδεσμοι περιφερειακών πληροφοριών :
    - I-95 Πληροφορίες ταξιδιωτών από το Συνασπισμό αυτοκινητοδρόμων
    - I-95 SafeTrip-21. Ιστοσελίδα σχεδιασμού ταξιδιών μεγάλων αποστάσεων του Συνασπισμού αυτοκινητοδρόμων
    - I-95 Ειδοποιήσεις ταξιδιωτών (από τη Starsystems)

Τα Τμήματα Μεταφορών (DOT) όλων των πολιτειών διαθέτουν ιστοσελίδες ενημέρωσης και υπηρεσίες παροχής TTI .

Ένας καινούριος «παίκτης», η Κίνα, μπαίνει στο χάρτη με την κινεζική κυβέρνηση να δεσμεύεται για επενδύσεις στην παροχή TTI και στα ITS γενικότερα. Είναι πιθανό η Κίνα να υιοθετήσει δική της μοναδική προσέγγιση για την ανάπτυξη TTI/ITS που αντλεί τα θετικά σημεία και τα διδάγματα που έχουν ήδη φανεί στις άλλες αγορές, αλλά λαμβάνοντας υπόψη τα χαρακτηριστικά των προβλημάτων κυκλοφορίας στην Κίνα.

iii. ITS για την Κυκλοφορία και τη Διαχείριση Δημοσίων ΜΜΜ

Η ανάπτυξη και η διαχείριση των ITS με στόχο τη βελτίωση της διαχείρισης της κυκλοφορίας σε αστικά και υπεραστικά δίκτυα μεταφορών είναι ένα κύριο πεδίο εφαρμογών ITS. Στον τομέα των οδικών μεταφορών, όπου αναπτύχθηκαν οι πρώτες εφαρμογές διαχείρισης ITS, οι συνήθεις εφαρμογές που αναπτύσσονται σήμερα εκτενώς είναι:

- Έξυπνος έλεγχος φωτεινών σηματοδοτών κυκλοφορίας,
- Ανίχνευση και διαχείριση διάφορων περιστατικών ,
- Προτεραιότητα σε συγκεκριμένους τύπους οχημάτων όπως έκτακτης ανάγκης και ΜΜΜ,
- Έξυπνος έλεγχος στις λωρίδες κυκλοφορίας ,
- Επιβολή ορίων ταχύτητας,
- Εκτροπή κυκλοφορίας σε μεγαλύτερες αποστάσεις και εκ νέου δρομολόγηση,
- Συλλογή δεδομένων (πχ από αυτοκίνητα και άλλες μεθόδους).

Οι φωτεινοί σηματοδότες (φανάρια ελέγχου κυκλοφορίας) θεωρούνται η ραχοκοκαλιά των ITS όταν πρέπει να υλοποιηθεί κάτι σε μεγάλη κλίμακα, με διαχείριση μεγάλων ποσοτήτων δεδομένων που αποθηκεύονται και επεξεργάζονται σε πραγματικό χρόνο από διάφορες πηγές, με τη χρήση προηγμένων μοντέλων κίνησης, αλγορίθμων πρόβλεψης και στρατηγικών διαχείρισης που μπορούν να ανταποκριθούν σε πραγματικό χρόνο στις επικρατούσες συνθήκες κυκλοφορίας. Σημαντική πρόοδο στα συστήματα διαχείρισης κυκλοφορίας στο πλαίσιο εφαρμογής μεγάλης κλίμακας ITS είναι: οι μέθοδοι πρόβλεψης κυκλοφορίας και οι έξυπνες στρατηγικές ελέγχου δικτύου που βασίζονται σε ορισμένα κυρίαρχα κριτήρια (πχ η ελαχιστοποίηση του συνολικού χρόνου ταξιδιού ή η ελαχιστοποίηση των περιβαλλοντικών επιπτώσεων κ.α.).

Η έρευνα στα ITS για τη διαχείριση της οδικής κυκλοφορίας υποστηρίζεται στην ΕΕ από τη δεκαετία του 1980. Οι έλεγχοι έγιναν πιο αυστηροί από τα μέσα της δεκαετίας του 1990 με τα ευρωπαϊκά έργα, για τη βελτίωση της διαχείρισης της κυκλοφορίας και των υπηρεσιών των χρηστών, εστιάζοντας στους διασυνοριακούς αυτοκινητοδρόμους. Ταυτόχρονα, έργα στο πλαίσιο της πρωτοβουλίας CIVITAS υλοποίησαν και διέδωσαν λύσεις κυκλοφορίας και αστικών μεταφορών, που επίσης περιλαμβάνουν τη διαχείριση φωτεινών σηματοδοτών, την προτεραιότητα των

δημόσιων συγκοινωνιών και πιο πρόσφατα την ολοκληρωμένη προσέγγιση διαχείρισης της κινητικότητας. Ωστόσο η κυρίαρχη δύναμη για ανάπτυξη ολοκληρωμένων εφαρμογών διαχείρισης κυκλοφορίας ITS, ήρθε με το πρόγραμμα TEMPO (2001-2006), όπου έλαβαν χώρα επτά μεγάλα έργα σχετικά με τα ITS που ενεργοποίησαν τη διαχείρισης κυκλοφορίας. Αυτά ήταν τα ARTS, CENTRICO, CONNECT, CORVETTE, SERTI, STREETWISE και VIKING. Στη συνέχεια δημιουργήθηκε η πρωτοβουλία EASYWAY, με τη συμμετοχή 21 κρατών μελών που είχε στόχο τη βελτίωση της χρήσης και της αποτελεσματικότητας των ITS προκειμένου μέχρι το 2020 να μειωθούν τα:

- Θύματα των τροχαίων κατά 25%
- Κυκλοφοριακή Συμφόρηση κατά 25%
- Εκπομπές CO_2 κατά 10 %

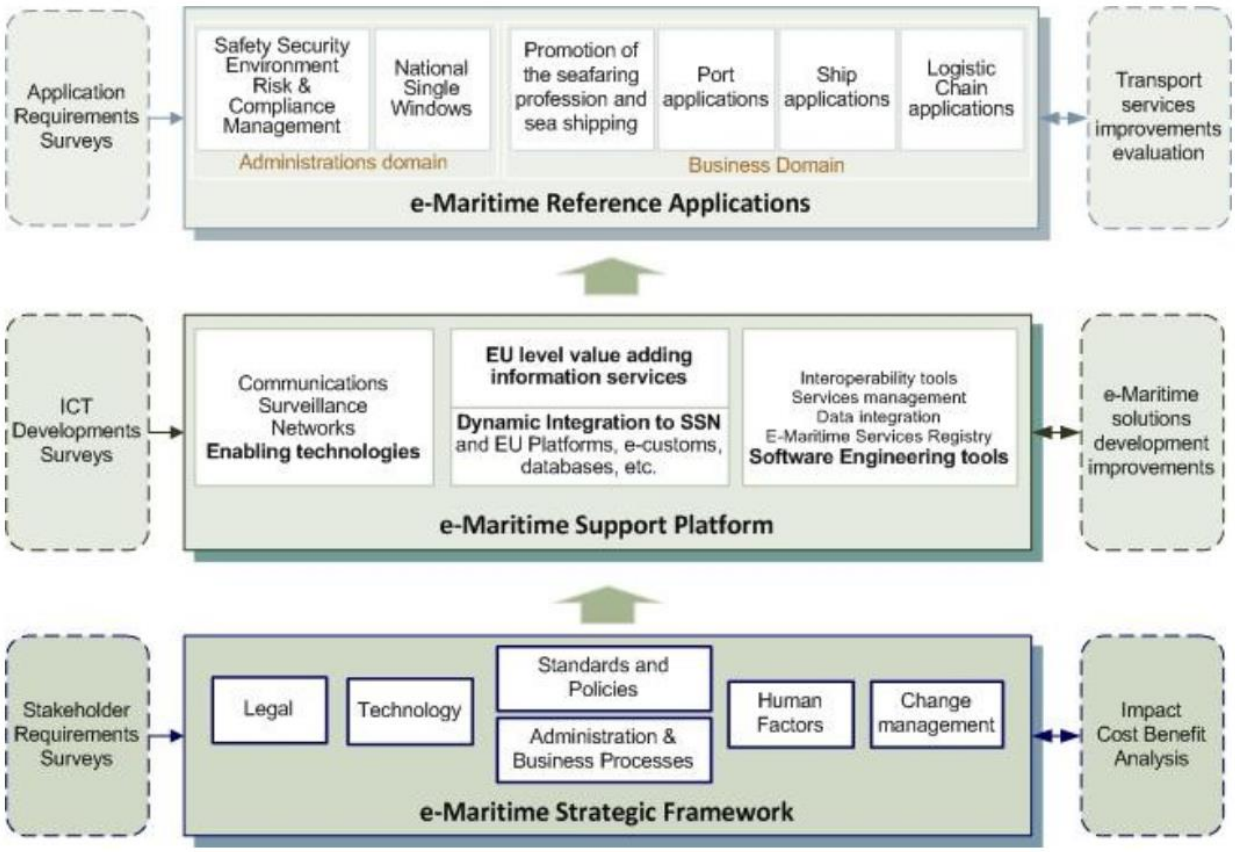
Παράλληλα με τη διαχείριση της οδικής κυκλοφορίας, υπάρχουν συστήματα ITS που έχουν αναπτυχθεί για τη διαχείριση των Δικτύων Δημόσιων Μεταφορών (κυρίως σε αστικές περιοχές). Αυτές οι εφαρμογές περιλαμβάνουν:

- Πληροφορίες δημόσιων συγκοινωνιών σε πραγματικό χρόνο,
- Αυτόματη αναγνώριση οχήματος και πληροφορίες σε πραγματικό χρόνο για στάσεις λεωφορείων ή τρένων,
- Προτεραιότητα για τα λεωφορεία και άλλα ΜΜΜ στις διασταυρώσεις,
- Ευέλικτο έλεγχο λεωφορειολωρίδας (για να επιτρέπεται η χρήση των λεωφορειολωρίδων και από άλλους τύπους οχημάτων) κτλ

Η διαχείριση στόλου των ΜΜΜ με τη χρήση «συνεταιριστικών» συστημάτων αναμένεται να αναπτυχθεί πλήρως στο εγγύς μέλλον, αν και θα χρειαστεί περισσότερος χρόνος από την εφαρμογή των ίδιων συστημάτων σε στόλους ιδιωτικών οχημάτων.

Στον τομέα των σιδηροδρομικών μεταφορών, η ανάπτυξη και η εφαρμογή του Ευρωπαϊκού Συστήματος Διαχείρισης Σιδηροδρομικής Κυκλοφορίας (ERTMS - European Rail Traffic Management System), που περιλαμβάνει το Ευρωπαϊκό Σύστημα Ελέγχου Τρένων (ETCS - European Train Control System) και το Παγκόσμιο Σύστημα για Κινητές Επικοινωνίες Σιδηροδρόμων (GSM-R - Global System for Mobile communications in Railways), επιτρέπει τη διαλειτουργικότητα σε ολόκληρο το Ευρωπαϊκό Δίκτυο Σιδηροδρόμων με ενιαία σηματοδότηση και έλεγχο ταχύτητας τρένου σε όλη την Ευρώπη.

Στις πλωτές μεταφορές, τα Συστήματα Διαχείρισης Κυκλοφορίας Σκαφών (VTMS - Vessel Traffic Management Systems) ισχύουν σε όλες σχεδόν τις μεγάλες θαλάσσιες περιοχές της ΕΕ, ιδιαίτερα κοντά σε μεγάλα λιμάνια. Η προτεινόμενη από την ΕΕ πρωτοβουλία ναυτιλίας βασισμένη στα ITS, εφεξής e- maritime, (μία από τις πολλές ηλεκτρονικές πρωτοβουλίες της ΕΕ, όπως: e-Government; e-Administration; e-Commission; e-Business κτλ) θα αναπτύξει ένα ολοκληρωμένο σύστημα διαχείρισης πληροφοριών βασισμένο σε ITS συστήματα για αναγνώριση, παρατήρηση, παρακολούθηση και αναφορά θαλάσσιων σκαφών. Το πλαίσιο του e-maritime μπορεί να θεωρηθεί ότι αποτελείται από τρία κύρια στοιχεία:



1. Το Στρατηγικό Πλαίσιο (Strategic Framework) του e-Maritime περιγράφει τις βασικές απαιτήσεις των ενδιαφερομένων. Περιγράφει επίσης πώς θα μπορούσε να επιτευχθεί μέσα από τις κατάλληλες διαδικασίες, πρότυπα και πολιτικές πάντα εντός καθορισμένων χρονικών πλαισίων. Αυτό γίνεται λαμβάνοντας υπόψη την τεχνολογία, τον ανθρώπινο παράγοντα και τις συνεχιζόμενες εξελίξεις που σχετίζονται μερικώς με τα SSN, τα ηλεκτρονικά τελωνεία (e-customs) και τις πρωτοβουλίες ασφάλειας και περιβάλλοντος.
2. Η Πλατφόρμα Υποστήριξης (Support Platform) του e-Maritime διευκολύνει την ανάπτυξη και λειτουργία των εφαρμογών e-Maritime αξιοποιώντας τις πρόσφατες εξελίξεις επικοινωνιών και πληροφοριών, και κυρίως τις τεχνολογίες που σχετίζονται με την ηλεκτρονική ναυτιλία (επικοινωνίες, επιτήρηση, δίκτυα συστημάτων) και το software engineer (σχετικά με τη διαλειτουργικότητα και την ενοποίηση δεδομένων και υπηρεσιών). Αποτελείται από τα «εργαλεία» για την υποστήριξη της δυναμικής ενοποίησης των εφαρμογών e-Maritime με άλλες πλατφόρμες της ΕΕ, όπως το e-Customs και την παροχή υπηρεσιών πληροφοριών προστιθέμενης αξίας σε επίπεδο ΕΕ από στατιστικές και άλλες υπηρεσίες αναλύσεων.
3. Τέλος, οι Εφαρμογές Αναφοράς (Reference Applications) του e-Maritime παρέχει εφαρμογές που αναδεικνύουν την επίδειξη των πλεονεκτημάτων του e-Maritime σε πραγματικές καταστάσεις που αφορούν διοικήσεις και επιχειρήσεις σε όλη την Ευρώπη.

Στον τομέα των αεροπορικών μεταφορών, υπάρχει πλάνο ενοποίησης των διάφορων συστήματα ελέγχου εναέριας κυκλοφορίας (ATC - Air Traffic Control) μέσω Ευρωπαϊκών πολιτικών και έτσι προκύπτουν τα πιο προηγμένα παραδείγματα ITS συστήματα διαχείρισης εναέριας κυκλοφορίας. Το 2007, η ΕΕ ίδρυσε μια κοινή

επιχείρηση για την ανάπτυξη του SESAR (Single European Sky ATM Research), του Master Plan για τη διαχείριση της εναέριας κυκλοφορίας (ATM - Air Traffic Management) για την Ευρώπη και την ανάπτυξη της νέας γενιάς ATM. Ταυτόχρονα εκπονήθηκε ένα σχέδιο δράσης για την χωρητικότητα, αποδοτικότητα και ασφάλεια των αεροδρομίων στην Ευρώπη προτείνοντας τρόπους ορθότερης χρησιμοποίησης των παραπάνω χαρακτηριστικών στα Ευρωπαϊκά αεροδρόμια.

Συνοψίζοντας, τα κυριότερα τεχνολογίες και συστήματα που σχετίζονται με τα ITS στον τομέα της διαχείρισης της εναέριας κυκλοφορίας είναι:

- Διαχείριση και έλεγχος οδικής κυκλοφορίας :
    - Συνεργαζόμενα συστήματα και τεχνολογίες (V2V, V2I).
    - Υπηρεσίες κυκλοφορίας και πληροφοριών ταξιδιού σε πραγματικό χρόνο, υποστήριξης της διαχείρισης κυκλοφορίας (RTTI - Real Time Traffic and Travel Information).
    - Συστήματα διαχείρισης της κυκλοφορίας, συμπεριλαμβανομένης της διαχείρισης έκτακτης ανάγκης.
    - Εφαρμογή και χρήση της τεχνολογίας μετάδοσης RDS-TMC/GSM .
    - TMC και TPEG -TISA πλοήγηση πραγματικού χρόνου και συλλογή δεδομένων οχήματος.
    - Συστήματα ενσωμάτωσης MMM.
- Διαχείριση και έλεγχος εναέριας κυκλοφορίας :
    - Ενιαίο Σύστημα Διαχείρισης Εναέριας Κυκλοφορίας στην Ευρώπη (SESAR).
    - Σύστημα Υποβοήθησης Διαχωρισμού Απογειώσεων (ASAS - Airborne Separation Assistance System).
    - Αυτόματη Εξαρτώμενη Επιτήρηση - Μετάδοση (ADS-B - Automatic Dependent Surveillance) και εφαρμογές επιτήρησης εδάφους και αέρος (GS-AS -).
- Διαχείριση και έλεγχος της θαλάσσιας κυκλοφορίας :
    - Θαλάσσια Επιχειρησιακά Συστήματα (MOS Maritime Operational Systems).
    - Πληροφοριακά Συστήματα Διαχείρισης Κυκλοφορίας Πλοίων (VTIMS - Vessel Traffic Management and Information Systems).
    - Ολοκληρωμένος έλεγχος πλοίου (ISC - Integrated Ship Control).
    - Ηλεκτρονικό Σύστημα Απεικόνισης Χαρτών και Πληροφοριών (ECDIS - Electronic Chart Display & Information System).
    - Πληροφοριακά Συστήματα Ποταμών (RIS - River Information Systems).
- Διαχείριση σιδηροδρομικού δικτύου :
    - Ευρωπαϊκό Σύστημα Διαχείρισης Σιδηροδρομικής Κυκλοφορίας (ERTMS - European Rail Traffic Management System).
    - Ευρωπαϊκό Σύστημα Ελέγχου Τρένων (ETCS - European Train Control System).
    - Παγκόσμιο Σύστημα Ασύρματων Επικοινωνιών Σιδηροδρόμων (GSM-R - Global System for Mobile communications Railway).

Κοιτώντας το μέλλον, και δεδομένου ότι τα περισσότερα από τα παραπάνω συστήματα διαχείρισης κυκλοφορίας που βασίζονται ITS, σήμερα είναι μονότροπα δηλαδή έχουν αναπτυχθεί και εφαρμοστεί μόνο εντός ενός μεταφορικού μέσου, μια

μελλοντική εξέλιξη έχει να κάνει με τη μεταμόρφωσή τους. Αυτή αναμένεται να είναι στην την ανάπτυξη πολυτροπικών συστημάτων διαχείρισης κυκλοφορίας, δηλαδή συστημάτων που βελτιστοποιούν τη διαχείριση της κυκλοφορίας μεταξύ δύο ή περισσότερων λειτουργιών με στόχο την επίτευξη συνεργατικών μεθόδων λειτουργίας.

Τέτοια πολυτροπικά συστήματα μεταφορών: α) ανταλλάσσουν πληροφορίες και δεδομένα σε πραγματικό χρόνο μεταξύ των κέντρων διαχείρισης κυκλοφορίας με δύο ή και περισσότερους τρόπους, β) αναλύουν και συγκρίνουν τις συνθήκες κυκλοφορίας στα δύο (ή περισσότερα) δίκτυα και γ) βελτιστοποιούν τη ροή της κυκλοφορίας σε όλα τα δίκτυα βάσει των συνθηκών στο αντίστοιχο σύστημα (π.χ. εναρμόνιση της διαχείρισης της κυκλοφορίας με τη διαχείριση των εμπορευματικών μεταφορών, ιδίως σε αστικές περιοχές ή ρύθμιση των φωτεινών σηματοδοτών για αντιμετώπιση της ζήτησης που προκαλεί η άφιξη ενός σκάφους RO-RO σε ένα λιμάνι).

Επίσης στο μέλλον περιμένουμε μια «μετατόπιση» για μεγαλύτερη συνεργασία μεταξύ των υπηρεσιών πληροφοριών και των εργαλείων διαχείρισης δικτύου. Αυτό θα επιτρέψει μια πιο έξυπνη επιχειρησιακή υποστήριξη των αποφάσεων διαχείρισης των δικτύων μεταφορών. Τα συστήματα πλοήγησης αναμένεται να χρησιμοποιηθούν για το σκοπό αυτό, μέσω δημόσιας και ιδιωτικής συνεργασίας μεταξύ διαχειριστών δικτύου και παρόχων υπηρεσιών.

iv. ITS για υπηρεσίες πλοήγησης

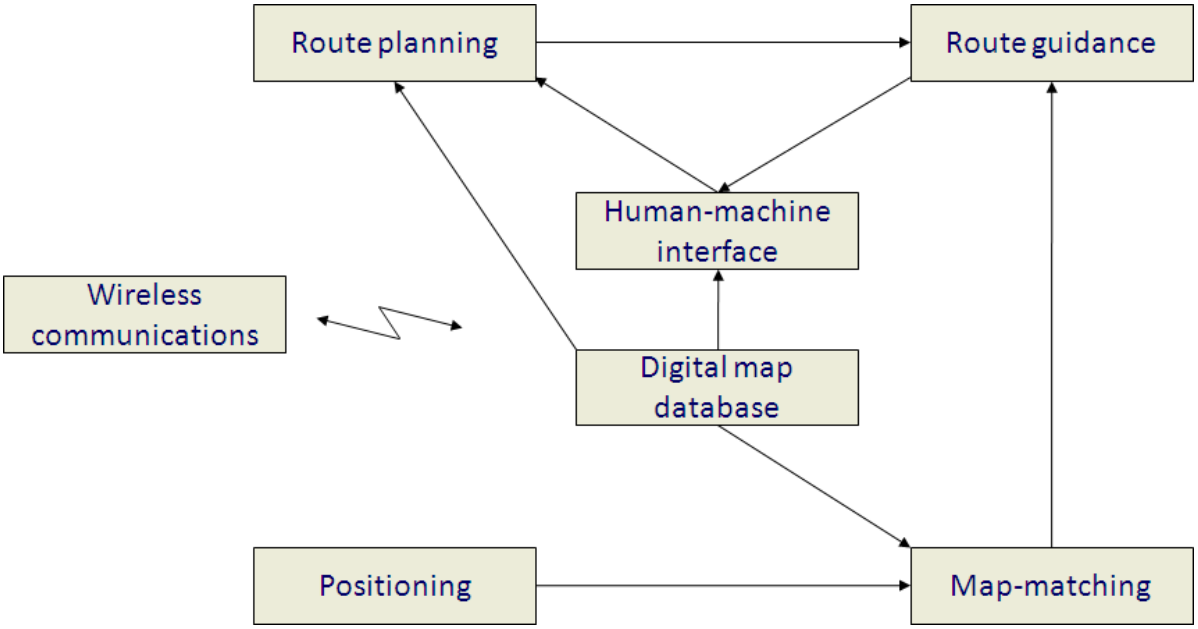
Η σύγχρονη ιστορία των ITS στις υπηρεσίες πλοήγησης ξεκινά στις αρχές της δεκαετίας του '60, όταν η Ομοσπονδιακή Ένωση Αυτοκινητοδρόμων των ΗΠΑ ανέπτυξε το Ηλεκτρονικό Σύστημα Καθοδήγησης Διαδρομών - ERGS (Electronic Route Guidance System), το οποίο είχε ως στόχο να παρέχει καθοδήγηση διαδρομής σε οδικά οχήματα, αποτελούμενο από συσκευές επί του οχήματος και εγκατεστημένους αισθητήρες στην άκρη των δρόμων. Το Ιαπωνικό Σύστημα Ολοκληρωμένου Ελέγχου Κυκλοφορίας Αυτοκινήτων – CACS (Comprehensive Automobile Traffic Control System) αναπτύχθηκε στα τέλη της δεκαετίας του 70, χρησιμοποιώντας ανίχνευση κίνησης οχημάτων, με εξοπλισμό στην άκρη των δρόμων και έναν απομακρυσμένο κεντρικό «πυρήνα» επεξεργασίας δεδομένων. Λίγα χρόνια αργότερα, αναπτύχθηκαν δύο ευρωπαϊκά συστήματα, παρόμοια με τα ERGS και CACS. Αυτά ήταν: το Autoguide στο Ηνωμένο Βασίλειο και το ALI-SCOUT στη Γερμανία, γνωστό και ως EUROSCOUT ή LISB. Στο Autoguide , η αναγνώριση θέσης του οχήματος επιτεύχθηκε μέσω αισθητήρων εγκατεστημένων στην άκρη των δρόμων, ενώ η διαδρομή υπολογιζόταν με δεδομένα της κίνησης, σε πραγματικό χρόνο, τα οποία προέρχονταν από άλλα οχήματα και από ένα κέντρο ελέγχου. ALI-SCOUT είχε αναπτυχθεί γύρω από μια παρόμοια ιδέα με αυτή του Autoguide.

Η είσοδος των τεχνολογιών πλοήγησης μέσω δορυφόρου επέτρεψε την ανάπτυξη μιας νέας γενιάς συστημάτων πλοήγησης αρχικά στις ΗΠΑ και τον Καναδά. Παραδείγματα πρώιμων πειραματικών εφαρμογών είναι τα συστήματα ADVANCE, Travtek και Travelguide. Το ADVANCE χρησιμοποίησε τεχνολογίες εντοπισμού θέσης GPS μαζί με αποκλειστικές και αμφίδρομες ραδιοεπικοινωνίες με ένα Κέντρο Πληροφοριών Κυκλοφορίας, προκειμένου να στέλνει και να λαμβάνει δεδομένα κίνησης σε πραγματικό χρόνο. Η πιλοτική εφαρμογή του ADVANCE έγινε στο Σικάγο. Η Travtek προσέφερε πληροφορίες κυκλοφορίας σε πραγματικό χρόνο, πλοηγό διαδρομής και δοκιμάστηκε πιλοτικά στο Ορλάντο των ΗΠΑ. Το Travelguide ήταν μια

φορητή συσκευή που παρείχε επιπλέον των παραπάνω και πληροφορίες σχετικές με τα ΜΜΜ σε πραγματικό χρόνο.

Ακολουθώντας την ανάπτυξη τέτοιων «κεντρικών» συστημάτων, η περαιτέρω πρόοδος των τεχνολογιών GPS τη δεκαετία του '90 είχε ως αποτέλεσμα την ανάπτυξη «αυτόνομων» συσκευών πλοήγησης. Μια περίοδο τέτοιες συσκευές καταλάμβαναν το αντίστοιχο μερίδιο αγοράς των προηγούμενων «κεντρικών» συστημάτων και σήμερα έχουν ενσωματωθεί στα smartphones.

Οι υπηρεσίες πλοήγησης, γενικά, περιλαμβάνουν τεχνολογίες σχετικές με τον προσδιορισμό της θέσης ενός οχήματος και την παροχή οδηγιών για τη βέλτιστη διαδρομή προς κάποιον προορισμό. Τα βασικά στοιχεία ένα σύγχρονου συστήματος πλοήγησης φαίνονται στο ακόλουθο σχήμα. Το εύρος και το περιεχόμενο καθενός τμήματος είναι προφανές από το όνομά του.



Ο χειρισμός του τμήματος εντοπισμού θέσης των υπηρεσιών πλοήγησης γίνεται μέσω ενός από τα υπάρχοντα συστήματα εντοπισμού θέσης GPS. Το ευρωπαϊκό σύστημα δορυφορικής πλοήγησης Galileo αναμένεται να είναι λειτουργικό έως το 2013 και θα παρέχει μια εξαιρετικά ακριβή, εγγυημένη υπηρεσία παγκόσμιου εντοπισμού θέσης υπό πολιτικό έλεγχο. Θα είναι διαλειτουργικό τόσο με το GPS όσο και με το GLONASS που είναι τα άλλα δύο υπάρχοντα παγκόσμια συστήματα δορυφορικής πλοήγησης.

Χρησιμοποιούνται διαφορετικοί τύποι συσκευών πλοήγησης και μπορούν να κατηγοριοποιηθούν ως εξής [52]:

- Αφιερωμένες μονάδες πλοήγησης ενσωματωμένες στο όχημα (από τον κατασκευαστή του οχήματος ή τον κατασκευαστή γνήσιου εξοπλισμού - ΚΑΕ).
- Συσκευές ψυχαγωγίας εντός οχήματος με εγκαταστάσεις πλοήγησης εγκατεστημένες ως αξεσουάρ ή αντικατάσταση συμβατικής λειτουργίας (π.χ. ραδιόφωνο, CD, κασέτα).
- Ειδικές συσκευές μετά την αγορά που είναι μόνιμα εγκατεστημένες στο όχημα.
- Αφιερωμένες δωρεάν συσκευές μετά την αγορά που μπορούν να εγκατασταθούν προσωρινά στο όχημα.

- Προσωπικοί ψηφιακοί βοηθοί (PDA) με κατάλληλο λογισμικό και σύνδεση με δέκτη δορυφορικής πλοήγησης .
- Κινητά τηλέφωνα με λειτουργίες πλοήγησης .
- Τερματικά δεδομένων κινητής τηλεφωνίας .

Ένα σημαντικό χαρακτηριστικό των συστημάτων πλοήγησης ITS είναι η σύζευξη των υπηρεσιών πλοήγησης με δεδομένα κίνησης σε πραγματικό χρόνο (πάντα βελτιωμένα με σύνολα δεδομένων ιστορικού και βραχυπρόθεσμη πρόβλεψη κίνησης), ώστε να παρέχουν καθοδήγηση διαδρομής με βάση τις συνθήκες κυκλοφορίας σε πραγματικό χρόνο.

Μέχρι στιγμής, οι υπηρεσίες πλοήγησης ITS έχουν βασιστεί σε μεγάλο βαθμό στις εξελίξεις που σημειώθηκαν στις τεχνολογίες επικοινωνίας και στα κινητά δίκτυα κινητής τηλεφωνίας ειδικότερα. Το πρωτόκολλο επικοινωνιών 3G και η διάδοση των τεχνολογιών ασύρματου διαδικτύου συνέβαλαν στις δυνατότητες ανταλλαγής μεγαλύτερων ποσοτήτων δεδομένων που σχετίζονται με την κυκλοφορία, σε πραγματικό ή σχεδόν πραγματικό χρόνο, σε προσιτό επίπεδο κόστους. Ωστόσο, οι υπηρεσίες πλοήγησης που εξαρτώνται από καθαρά δεδομένα σε πραγματικό χρόνο είναι μάλλον δαπανηρές, λόγω του κόστους διατήρησης των μόνιμων (ή σχεδόν μόνιμων) καναλιών επικοινωνίας ανοιχτά για τη μεταφορά δεδομένων κίνησης μέσω φορέα κινητής τηλεπικοινωνίας. Για το λόγο αυτό, οι υπηρεσίες πλοήγησης εξαρτώνται επί του παρόντος σε μεγάλο βαθμό από ιστορικά δεδομένα κίνησης και προφίλ κίνησης, με ελάχιστη ανταλλαγή δεδομένων σε πραγματικό χρόνο και επικεντρώνονται κυρίως σε περιστατικά, δηλαδή ατυχήματα ή άλλα γεγονότα που ενοχλούν την κυκλοφορία. Τέτοια μικρά σύνολα δεδομένων διακινούνται συνήθως μέσω λιγότερο δαπανηρών καναλιών, όπως το RDS-TMC.

Κάθε εταιρεία που παρέχει υπηρεσίες πλοήγησης χρησιμοποιεί σύνολα δεδομένων και χρησιμοποιώντας κοινότυπα πρωτόκολλα επικοινωνίας. Οι πηγές των δεδομένων για την κίνηση που χρησιμοποιούνται στην παροχή υπηρεσιών πραγματικού χρόνου μερικές φορές ξεφεύγουν από τους συνηθισμένους τρόπους αποθήκευσης δεδομένων (π.χ. κέντρα διαχείρισης κυκλοφορίας) λόγω του κόστους των δεδομένων σε πραγματικό χρόνο. Ενδέχεται να περιλαμβάνουν την ανίχνευση των συσκευών πλοήγησης, έτσι ώστε να εξάγουν πληροφορίες σχετικές με την κυκλοφορία σε πραγματικό χρόνο με βάση τους καθ' οδόν χρήστες.

Ένα άκρως ενδιαφέρον έργο ολοκληρώθηκε στις ΗΠΑ, με τη συνεργασία του Πανεπιστημίου της Καλιφόρνια στο Berkeley και της Nokia, με στόχο να συμβάλει στην παροχή υπηρεσιών πλοήγησης σε πραγματικό χρόνο και την ανεύρεση τρόπων διαχείρισης ανώνυμων δεδομένων με της χρήση smartphone και σαν αισθητήρες (συλλέκτες δεδομένων κυκλοφορίας) και σαν συσκευές παροχής υπηρεσιών.

Σύμφωνα με πρόσφατες έρευνες, στο πεδίο των υπηρεσιών πλοήγησης οδικών μεταφορών περιλαμβάνονται:

- Παροχή υψηλής ακρίβειας πλοήγησης, με στόχο την παρακολούθηση και την υποστήριξη των ελιγμών των οδηγών παρέχοντας πληροφορίες για τις λωρίδες κυκλοφορίας .
- Μικρο-δρομολογήσεις, πχ. Παροχή πληροφοριών καθοδήγησης διαδρομής πολύ λεπτομερών, που περιλαμβάνουν βοηθητικές πληροφορίες για το περιβάλλον.

- Στρατηγική δρομολόγηση, δηλαδή βελτιωμένες λειτουργίες δρομολόγησης που λαμβάνουν υπόψη ορισμένες προκαθορισμένες στρατηγικές.
- Λήψη ειδοποιήσεων ή/και υπενθυμίσεις που σχετίζονται με την οδική ασφάλεια απευθείας από άλλα οχήματα (όχημα σε όχημα - V2V - vehicle to vehicle).
- Λήψη πληροφοριών σχετικά με το χρονισμό του σήματος κατά την προσέγγιση σε διασταυρώσεις με σηματοδότηση, με κατάλληλες οδηγίες σχετικά με τη βέλτιστη ταχύτητα του οχήματος, ώστε να φτάσει στη διασταύρωση όταν οι φωτεινοί σηματοδότες γίνονται πράσινοι (υποδομή προς όχημα - I2V - infrastructure to vehicle).
- Στόλος δημόσιων μεταφορών και συστήματα διαχείρισης δρομολογίων, τα οποία είναι τμήματα της διαχείρισης στόλου δημόσιων μεταφορών και των κέντρων παροχής πληροφοριών .

Η πλοήγηση στο μέλλον θα ζήσει εξέλιξη προς μία εξατομικευμένη παροχή πληροφοριών όπως εκτενείς γνώσεις επί του περιβάλλοντος για να λειτουργήσουν βέλτιστα οι υπηρεσίες δρομολόγησης και πλοήγησης και να βοηθούν τους ταξιδιώτες στην κατανόηση των περιβαλλοντικών επιπτώσεων των διαφορετικών ταξιδιωτικών επιλογών ενώ ταυτόχρονα θα δίδονται συμβουλές για πιο πράσινες επιλογές. Επίσης σε αντίθεση με τους σημερινούς τρόπους, θα παρέχει βελτιστοποιημένες στρατηγικές δρομολόγησης έτσι ώστε να επιτυγχάνονται διαδρομές με όσο το δυνατό πιο έγκυρο χρόνο ταξιδιού. Η αξιοπιστία των προβλέψεων είναι μια διαρκής πρόκληση για την ανάπτυξη συστημάτων κυρίως όσο αυξάνεται το ποσοστό διείσδυσης στην αγορά διάφορων ανταγωνιστών αγορών για την παροχή τέτοιων πληροφοριών. Τα συστήματα αυτά παρέχουν ήδη δρομολόγηση σε περιπτώσεις έκτακτης συμφόρησης, π.χ. ατυχήματα ή δυσμενείς καιρικές συνθήκες καθώς επίσης «επικοινωνούν» με κεντρικά συστήματα για τη διαχείριση έκτακτων περιστατικών.

Στην υλοποίηση των παραπάνω οφείλεται στην εξέλιξη του βασικό στοιχείου των συστημάτων πλοήγησης και δρομολόγησης, δηλαδή στους αλγόριθμους που λειτουργούν στο παρασκήνιο. Η ανάπτυξη αυτών των «τρίτης γενιάς» αλγορίθμων θα είναι ιδιαίτερα χρήσιμη για τις μελλοντικές υπηρεσίες πλοήγησης όπου η εκτέλεση τους θα γίνεται με κατανάλωση χαμηλών υπολογιστικών απαιτήσεων και για τη χρήση τους χρειάζονται προχωρημένα μαθηματικά εργαλεία όπως η μέθοδος συναιρετικών ιεραρχιών (CHM – Contraction Hierarchies Method)[53], ή την αναπαράσταση στρατηγικών ταξιδιού ως υπερμονοπάτια δυναμικών δικτύων[54], που παραδοσιακά εφαρμόζονταν στα μοντέλα επιλογή διαδρομής για συστήματα αστικών συγκοινωνιών σε περιπτώσεις με υψηλή συχνότητα ή/και χαμηλή κανονικότητα.

v. ITS για Smart Ticketing και Τιμολόγηση

Οι τεχνολογίες και οι υπηρεσίες ITS για είσπραξη τελών στον τομέα των μεταφορών έχουν αναπτυχθεί τα τελευταία 20 χρόνια. Ξεκινώντας από τα συστήματα είσπραξης διοδίων και την φορολόγηση των μετακινήσεων - μεταφορών, σύμφωνα με ορισμένα κριτήρια (π.χ. εκπομπές ρύπων). Ένα τμήμα του τομέα είναι τα συστήματα «έξυπνης έκδοσης εισιτηρίων», δηλαδή οι τρόποι πληρωμής των εισιτηρίων στα ΜΜΜ ή άλλες υπηρεσίες μεταφοράς με δυνατότητα ITS.

Υπάρχει μεγάλος αριθμός αποφάσεων διαφορετικής φύσης (πολιτικής, τυποποίησης, νομοθετικής) που δημιουργούν το τοπίο σήμερα σε αυτόν τον τομέα. Οι αρχές της χρέωσης επί των υποδομών παρουσιάζονται από την ΕΕ στο Green Paper «Προς δίκαιη και αποδοτική τιμολόγηση στις μεταφορές» *(***Towards Fair and Efficient**

Pricing in Transport)[55] και στο White Paper «Δίκαιη πληρωμή για τη χρήση υποδομών: μια φάση προσέγγισης σε ένα σύνηθες πλαίσιο χρέωσης υποδομών μεταφορών στην ΕΕ» (Fair Payment for Infrastructure Use: a Phase Approach to a Common Transport Infrastructure Charging Framework in the EU)[56].

Το 1999, η Eurovignette πρότεινε τη χρέωση των βαρέων οχημάτων για χρήση σε ορισμένους δρόμους, εφαρμόζοντας την έννοια «ο χρήστης πληρώνει» επιτρέποντας έτσι την ισοστάθμιση του κόστους κατασκευής, συντήρησης και λειτουργίας των δρόμων από τα κράτη μέλη. Το 2003, μια νέα Οδηγία της ΕΕ τροποποίησε την πρόταση της Eurovignette αλλάζοντας την έννοια στην πιο ολοκληρωμένη «ο ρυπαίνων πληρώνει». Εισήγαγε τη διανυθείσα απόσταση, τα ατυχήματα, τα περιβαλλοντικά κόστη, τα επίπεδα συμφόρησης ανά χρονική περίοδο, την πυκνότητα τοπικού πληθυσμού, τις κατηγορίες εκπομπών οχημάτων και άλλες τέτοιες παραμέτρους σε ολόκληρη την ιδέα των διοδίων. Με ανακοίνωση της η Commission το 2009 για το βιώσιμο μέλλον στις μεταφορές ανέλυσε την προτεινόμενη εσωτερίκευση του «εξωτερικού» κόστους που εισήχθη με την οδηγία 2006/38. Με το σχέδιο δράσης για την αστική κινητικότητα του 2009 πρότεινε τη χρήση ITS σαν λύση-μέσο τιμολόγησης, και συμπεριλάμβανε δύο δράσεις σχετικές με τη χρήση του ITS για την έξυπνη τιμολόγηση. Η πρώτη δράση είχε στόχο την ανταλλαγή πληροφοριών σχετικών με τα συστήματα τιμολόγησης αστικών περιοχών στην ΕΕ έτσι ώστε το οικονομικά στοιχεία να συμπεριληφθούν σε διαδικασίες διαβούλευσης, σχεδιασμούς συστημάτων, παροχή πληροφοριών στους πολίτες, δημόσια αποδοχή, λειτουργικά κόστη/έσοδα και τεχνολογικές/περιβαλλοντικές επιπτώσεις. Η δεύτερη δράση στόχευε στην εφαρμογή των ITS στην αστική κινητικότητα συμπληρωματικά στο σχέδιο δράσης ITS (πχ έκδοση εισιτηρίων και πληρωμή, βελτίωση της διαλειτουργικότητας των συστημάτων έκδοσης εισιτηρίων και πληρωμών σε υπηρεσίες και τρόπους μεταφοράς, χρήση έξυπνων καρτών στις αστικές συγκοινωνίες με έμφαση στα αεροδρόμια και σιδηροδρομικούς σταθμούς).

Τα συστήματα ηλεκτρονικής είσπραξης (EFC - Electronic Fee Collection) προσφέρουν τη δυνατότητα «έξυπνης» χρέωσης για τη χρήση της υποδομής μεταφορών (κυρίως των δρόμων) σύμφωνα με τις τιμολογιακές πολιτικές που καθορίζονται στις Οδηγίες της ΕΕ. Αυτό ονομάζεται «έξυπνη τιμολόγηση» σε αντίθεση με την έξυπνη έκδοση εισιτηρίων που αναφέρεται στη συλλογή ναύλων σε ένα σύστημα δημόσιων μεταφορών. Η έξυπνη τιμολόγηση απευθύνεται σε μια αγορά όπου οι διαχειριστές υποδομής, μαζί με τη βιομηχανία οχημάτων και οι πάροχοι ITS, θα συνεργαστούν για την δημιουργία μιας οδικής ή άλλης υπηρεσίας που θα την παρέχει σε συγκεκριμένη τιμή στους «καταναλωτές» με μια δεδομένη τεχνολογία ή με εναρμονισμένες.

Στην παροχή μιας τέτοιας υπηρεσίας, η αγορά των διαχειριστών υποδομής δημιουργεί συνεργασίες ενώ η αγορά των παρόχων ITS έχουν κυρίως δημιουργούν ανταγωνισμό.

Η διαλειτουργικότητα είναι το κρίσιμο στοιχείο που πρέπει ακόμη να επιτευχθεί σε τέτοια συστήματα με τους εξής τρόπους:

- Τεχνική διαλειτουργικότητα (εξοπλισμός).
- Διαδικαστική διαλειτουργικότητα (συμβάσεις συμφωνιών).
- Ενσωμάτωση των χρηστών άνευ εξοπλισμού.
- Προστασία προσωπικών δεδομένων.

Η τεχνική και διαδικαστική διαλειτουργικότητα είναι βασικό ζήτημα για την επιτυχή εφαρμογή της έξυπνης τιμολόγησης στην Ευρώπη, ειδικά στα διόδια. Ένα παράδειγμα τέτοιας διαλειτουργικότητας είναι η ετικέτα E-ZPass που χρησιμοποιείται σε δρόμους με διόδια, γέφυρες και σήραγγες σε δεκατέσσερις πολιτείες κατά μήκος των ΗΠΑ. Στην ΕΕ, έχουν θεσπιστεί προδιαγραφές στην Οδηγία για τα διαλειτουργικά ηλεκτρονικά συστήματα διοδίων στην Ευρώπη.

Η οδηγία 2004/52/ΕΚ είχε θέσει το πλαίσιο για μια ευρωπαϊκή υπηρεσία ηλεκτρονικών διοδίων (ΕΕΤΣ). Ο λεπτομερής καθορισμός των ΕΥΤ, συμπεριλαμβανομένων τεχνικά, διαδικαστικά και νομικά ζητήματα και το χρονοδιάγραμμα υλοποίησης, έχει ήδη ρυθμιστεί σε μια ευρωπαϊκή απόφαση της Επιτροπής που εγκρίθηκε το τον Οκτώβριο του το 2009.

Με την ντιρεκτίβα EFC 2004/52/EC για τη διαλειτουργικότητα των ηλεκτρονικών συστημάτων οδικών διοδίων, τυποποιήθηκε το ευρωπαϊκό σύστημα είσπραξης διοδίων που εφαρμόστηκε μετά την 1η Ιανουαρίου 2007. Βασισμένη σε αυτή δημιουργήθηκε στα τέλη της περασμένης δεκαετίας μια αρχιτεκτονική υψηλού επιπέδου (βασισμένη στις τεχνολογίες DSRC, GNSS, CESARE III) για τη διαλειτουργικότητα οδικών χρεώσεων. Συνεργάστηκαν οι επιτροπές τυποποίησης CEN και ISO, οι φορείς διοδίων ASECAP και η ομάδα κρατών που ονομάζεται "Stockholm Group" (οι πέντε χώρες, που ενδιαφέρονται για μια κοινή προσέγγιση στην είσπραξη ηλεκτρονικών τελών: Βέλγιο, Γερμανία, Σουηδία, Ελβετία, Ηνωμένο Βασίλειο). Το σύστημα επέτρεπε σε οποιονδήποτε χρήστη να έχει πρόσβαση σε μια Ευρωπαϊκή Υπηρεσία Ηλεκτρονικών Διοδίων (EETS - European Electronic Toll Service) οπουδήποτε στην Ευρώπη, χρησιμοποιώντας τον σωστό εξοπλισμό (OBE – on board equipment). Παρά τις προσπάθειες, η απρόσκοπτη διαλειτουργικότητα των συστημάτων EFC στην Ευρώπη δεν επιτεύχθηκε γρήγορα η οποία αναμένετε να υλοποιηθεί την τρέχουσα δεκαετία.

Παρόμοια χαρακτηριστικά με την είσπραξη διοδίων αλλά διαφορετικά σε μέγεθος και πολυπλοκότητα είναι τα συστήματα είσπραξης τελών χρήσης δρόμων σε μια μεγαλύτερη περιοχή. Τέτοια συστήματα εγκαταστάθηκαν σε πολλές ευρωπαϊκές χώρες και πόλεις. Πχ Νορβηγία (Bergen, 1986, Oslo, 1990 και Trondheim 1991), Ρώμη το 2001, Λονδίνο το 2007, Βαλέτα (Μάλτα) το 2007, Στοκχόλμη το 2006-2007, Μιλάνο το 2008 . Οι τιμολογιακές πολιτικές τιμολόγησης διαφέρουν ανάλογα με τη γεωγραφική κάλυψη της τιμολόγησης των δρόμων και διακρίνονται σε:

- Περιοχή τιμολόγησης (εντός άλλης περιοχής) - Area pricing
- Οριζόντια τιμολόγηση (για είσοδο εντός περιοχής) - Cordon pricing
- Τιμολόγηση εγκατάστασης (για συγκεκριμένες εγκαταστάσεις όπως αυτοκινητόδρομοι) - Facility pricing
- Τιμολόγηση δικτύων (για συστήματα συνεργασίας αυτοκινητοδρόμων) - Network pricing

Οι πιο συνηθισμένες τεχνολογίες ITS που χρησιμοποιούνται για έξυπνη τιμολόγηση, διοδίων ή περιοχών τιμολόγησης:

- Αυτοματοποιημένες τεχνολογίες αναγνώρισης οχημάτων (με τη χρήση barcode, RFID, αναγνώριση πινακίδας κυκλοφορίας, GPS)

- Αυτοματοποιημένη ταξινόμηση οχημάτων (χρησιμοποιώντας κάμερες, αισθητήρες ή με αποθήκευση του οχήματος του πελάτη στο αρχείο).
- Επεξεργασία συναλλαγών (με συστήματα προπληρωμής ή και όχι).
- Επιβολή μέτρων τήρησης (οδικές μπάρες, αναγνώριση πινακίδας κυκλοφορίας, αστυνόμευση κτλ)

Στον τομέα των εφαρμογών ITS για έκδοση εισιτηρίων χρειάζεται να σημειωθεί πως απαιτούν ένα διαφορετικό σύνολο τεχνολογιών. Διάφοροι τύποι έξυπνων καρτών (smartcards) αποτελούν την κύρια τεχνολογία που χρησιμοποιείται. Πρότυπα έξυπνων καρτών μετακινήσεων αναπτύχθηκαν στην ΕΕ με την οδηγία 2009/110/EC η οποία έφερε σημαντικές αλλαγές εισάγοντας νέους όρους διασφάλισης διαλειτουργικότητα των έξυπνων εισιτηρίων. Έγιναν προσπάθειες διαλειτουργικότητας στις εκδόσεις έξυπνων εισιτηρίων αλλά δυστυχώς δεν υπήρχε η ανάλογη επιτυχία. Χαρακτηριστικό παράδειγμα είναι το ερευνητικό πρόγραμμα FP6 η αλλιώς IFM (Interoperable Fare Management) που στόχο είχε να διασφαλίσει τη διαλειτουργικότητα των διασυνοριακών Έξυπνων καρτών μεταφοράς (Transport Smartcards). Το πρόγραμμα αυτό ανέπτυξε χάρτες για χρήση ηλεκτρονικών εισιτηρίων στην Ευρώπη όπου οι μετακινούμενοι θα χρησιμοποιούσαν τις έξυπνες κάρτες τους μακριά από την περιοχή τους.

Κλείνοντας να αναφέρουμε πως τα ITS συστήματα με τα έξυπνα εισιτήρια και την έξυπνη τιμολόγηση στις μεταφορές έχουν ήδη μπει στη ζωή μας και αναμένεται να καθημερινά εργαλεία στα αστικά και υπεραστικά δίκτυα μεταφορών μέσα στην επόμενη δεκαετία.

Υπάρχει μια τάση ενοποίησης των συστημάτων πληρωμών για υπηρεσίες μεταφορών και των χρεώσεων τους. Πρόκληση εξακολουθεί να είναι η εφαρμογή διαλειτουργικών εφαρμογών μεταξύ διαφορετικών συστημάτων πληρωμών έτσι ώστε διάφορα μέσα (πληρωμές πιστωτικών καρτών, τηλεφωνίας, εισιτηρίων κτλ) θα μπορούν να λειτουργούν μέσα στην ίδια ενιαία πλατφόρμα (διαλειτουργικότητα).

vi. ITS και Ασφάλεια

Η ασφάλεια αποτελεί προτεραιότητα στις μεταφορές τόσο εντός των διοικητικών ορίων της ΕΕ όσο και επιμέρους στα κράτη μέλη της. Στην ΕΕ από θανατηφόρα ατυχήματα που σχετίζονται με οποιοδήποτε τρόπο το 97% συμβαίνουν στο δρόμο. Έτσι η οδική ασφάλεια αποτελεί κύρια προτεραιότητα στις εφαρμογές ITS. Μια συνηθισμένη εφαρμογή ITS φτιαγμένη να βελτιώνει την ασφάλεια δίνει στους οδηγούς πληροφορίες που τους βοηθούν να αποφύγουν ένα ατύχημα αλλά σε ορισμένες περιπτώσεις παρέχει πληροφορίες που απλώς θα το μετριάζουν. Ο προσδιορισμός των εφαρμογών ITS που θα μπορούν να βοηθήσουν πραγματικά στη μείωση των ατυχημάτων και η αξιολόγηση της σοβαρότητάς της κάθε εφαρμογής απαιτεί ένα πλαίσιο στο οποίο θα γίνεται σύνδεση των εφαρμογών ITS με τις αιτίες των ατυχημάτων.

Ένα τέτοιο πλαίσιο βασίζεται στην εξέταση των τριών βασικών συντελεστών: του οδηγού, του οχήματος και του περιβάλλοντος κυκλοφορίας. Το καλύτερο δυνατό ITS σχετικό με την ασφάλεια είναι εκείνο που συνδυάζει δεδομένα από τους τρεις αυτούς συντελεστές, καθώς από εκείνα που βασίζονται στην αλληλεπίδραση με κάθε στοιχείο του περιβάλλοντος.

Οι τεχνολογίες και τα συστήματα ITS σχετικές με την ασφάλεια των μεταφορών διακρίνονται ως εξής:

- Αυτόνομη λύσεις (Autonomous solutions) συστήματα που αφορούν μονομερώς είτε μόνο την υποδομή, το πρόγραμμα οδήγησης, το όχημα κτλ.
- Συνεργατικές λύσεις (Co-operative solutions) συστήματα που βασίζονται στη συνεργασία μεταξύ δύο ή περισσοτέρων συντελεστών (π.χ. από όχημα προς όχημα - V2V (Vehicle to Vehicle) ή από υποδομή προς το όχημα - I2V (Infrastructure to Vehicle) κτλ.

Επιπλέον ανάλογα με τον τρόπο που το κάθε ITS συμβάλλει στην ασφάλεια τα συνεργαζόμενα συστήματα κατηγοριοποιούνται σε Συστήματα ***Παθητικής*** και ***Ενεργητικής*** Ασφάλειας ανάλογα με το αν προλαμβάνουν και προστατεύουν παθητικά και εκ των υστέρων σε ένα ατύχημα ή αν ενεργούν πριν από ένα πιθανό ατύχημα τον οδηγό να παραμείνει σε ένα επιθυμητό επίπεδο εγρήγορσης.

Τα επονομαζόμενα ADAS (Advanced Driver Assistance Systems) και ARAS (Advanced Rider Assistance Systems) είναι δύο συστήματα και ενεργητικής και συνεργατικής ασφάλειας βασισμένα σε ITS .

Υπάρχουν πολλά παραδείγματα συνεργατικών - ενεργητικών ή παθητικών - συστημάτων ITS. Ενδεικτικά αναφέρουμε έναν αριθμό από αυτά παρακάτω χωρίς αυτό να αποτελεί αναλυτική απαριθμητική λίστα αλλά ως ένδειξη του μεγάλου αριθμού τέτοιων συστημάτων που έχουν αναπτυχθεί και των δυνατοτήτων των ITS στον τομέα αυτό:

- Υποβοήθηση οδηγού:
    - Σταθεροποιητής ταχύτητας (μέσω V2I και I2V επικοινωνίας).
    - Λωρίδες κυκλοφορίας με αναστρέψιμη ροή (V2I και I2V).
    - Τοπικός κίνδυνοι και προειδοποιήσεις (V2V).
    - Προειδοποίηση μετά από ατύχημα (V2V).
    - Παρακολούθηση με κάμερα της πλευρικής και οπίσθιας πλευράς οχήματος (LRM – Lateral Rear Monitoring).
    - Προειδοποίηση αλλαγής και διατήρησης λωρίδας (LDWS - Lane Departure Warning/Lane keeping).
    - Συστήματα αποφυγής σύγκρουσης (CAS - Collision Avoidance Systems), συμπεριλαμβανομένης της υποστήριξης αλλαγής λωρίδας.
    - Συστήματα ελέγχου: Cruise Control και Advanced Cruise Control (ACC).
    - Προειδοποίηση και αποφυγή σύγκρουσης (CWS/CAS).
    - Έξυπνος Προσαρμογέας Ταχύτητας (ISA - Intelligent Speed Adaptation).
    - Ενίσχυση νυχτερινής όρασης.
    - Ανίχνευση αντικειμένων στο δρόμο.
    - Προστασία Πεζών και άλλων Ευπαθών ομάδων στο δρόμο (VRU - Vulnerable Road Users) προστασία: Οι εφαρμογές στοχεύουν κυρίως στην παροχή καθοδήγησης και άλλων πληροφοριών (πχ ύπαρξη ειδικών εγκαταστάσεων πρόσβασης) για VRU και έχουν αναπτυχθεί από τα μέσα της δεκαετίας του '90.
- Υποβοήθηση οδηγού δίκυκλου
    - Προειδοποίηση μετωπικής σύγκρουσης.

    - Ειδοποίηση ταχύτητας.
    - Ειδοποίηση υποστήριξης διασταυρώσεων.
    - Υποστήριξη αλλαγής λωρίδας.
    - Advanced Rider Assistance Systems – HMI.
    - Δονούμενα γάντια.
    - Έξυπνο κράνος.
    - Δόνηση καθίσματος.
    - Καθρέφτης προειδοποίησης τυφλού σημείου.
- Υποβοήθηση Δρόμων και Οδικών Διασταυρώσεων
    - Συνεργατική προειδοποίηση σύγκρουσης σε διασταυρώσεις.
    - Ολοκληρωμένο έξυπνο σύστημα ασφαλείας διασταυρώσεων.
    - Άλλα χαρακτηριστικά ασφάλειας διασταυρώσεων.

Πολλά συνεργατικά συστήματα (πχ CVIS, Copper, FREILOT, SMARTFREIGHT κτλ) έχουν επιδοτηθεί χρηματικά και έχουν δοκιμασθεί σε πραγματικό περιβάλλον από την ΕΕ. Σε αυτά περιλαμβάνονται η διαχείριση και ο έλεγχος των διασταυρώσεων, η διαχείριση του στόλου με κρατήσεις χώρων φόρτωσης και παράδοσης σε πραγματικό χρόνο μέχρι και εφαρμογές δρομολόγησης (για μεταφορές και άλλα), πληροφορίες στάθμευσης κτλ.

vii. ITS για μεταφορές εμπορευμάτων και Logistics

Για τις εμπορευματικές μεταφορές τα ITS υλοποιούνται μέσα από μια σειρά «έξυπνων» υπηρεσιών, προγραμμάτων εφαρμογών και τεχνολογιών για τη συλλογή, αποθήκευση, ανάλυση και παροχή πρόσβασης σε δεδομένα φορτίων τα οποία βοηθούν τους χρήστες να λάβουν καλύτερες αποφάσεις. Τα ITS κάνουν αποτελεσματικότερες τις μεταφορές εμπορευμάτων, αναπτύσσοντας διαλειτουργικές υπηρεσίες πληροφοριών σε παγκόσμιο επίπεδο μέσω έξυπνων εφαρμογών υπηρεσιών σε τυποποιημένες δομές δεδομένων.

Κύριοι τομείς εφαρμογής των ITS στις εμπορευματικές μεταφορές και τα Logistics είναι οι εξής:

- Ανάπτυξη και εφαρμογή του ηλεκτρονικού περιβάλλοντος νέας γενιάς γνωστού και ως «ηλεκτρονικό φορτίο» (σύνδεση των πληροφοριών μεμονωμένων ειδών φορτίου και αλληλεπίδραση με το ίδιο το αντικείμενο σε όλη την αλυσίδα μεταφορών).
- Εφαρμογές διαχείρισης εμπορευματικών μεταφορών (ασχολούνται με τη διαχείριση της μεταφοράς από την παραλαβή της παραγγελίας μέχρι την πληρωμή και τον έλεγχο τιμολογίων).
- Εφαρμογές διαχείρισης του στόλου των οχημάτων με στόχο τη βέλτιστη χρήση του και προγραμματισμού ενός στόλου εμπορευματικών οχημάτων (ή βαγονιών ή πλοίων).
- Διαχείριση ειδικών κατηγοριών εμπορευμάτων όπως Επικίνδυνα υλικά (Dangerous Goods).
- Διαχείριση τερματικών, συμπεριλαμβανομένου του ελέγχου πρόσβασης, του χώρου φόρτωσης και της διαχείρισης της ζώνης στάθμευσης κτλ.

Το αρχικό σχέδιο ITS της ΕΕ καθιέρωσε το γενικό πλαίσιο για την ανάπτυξη των ITS σε ολόκληρο τον τομέα των εμπορευματικών μεταφορών και των Logistics. Αυτό πλαίσιο έδινε μια καθοδήγηση προς: την καινοτομία (στις εμπορευματικές μεταφορές),

την απλούστευση των διαδικασιών, την ποιότητα και την αποτελεσματικότητα των επιχειρήσεων, του ποιοτικού περιβάλλοντος («πράσινες» εμπορευματικές μεταφορές), και την αναδιοργάνωση του νομικού πλαισίου για τις εμπορευματικές μεταφορές στην Ευρώπη. Το σχέδιο δράσης για τα ITS του 2008 αναφέρεται σε συγκεκριμένες υπηρεσίες ITS που θα αναπτυχθούν για να υποστηρίξουν τις εμπορευματικές μεταφορών. Μεταξύ των υπηρεσιών που καθορίζονται σε αυτό το Σχέδιο Δράσης είναι:

- Παρακολούθηση φορτίου (όλες οι λειτουργίες).
- Ηλεκτρονική είσπραξη τελών (ισχύει για τις οδικές μεταφορές και αντιμετωπίζεται χωριστά).
- Συστήματα για τη μείωση των καθυστερήσεων μεταφοράς εμπορευμάτων στα σιδηροδρομικά δίκτυα.
- Αποτελεσματικές και καθαρές παραδόσεις αστικών εμπορευματικών μεταφορών (τα ITS μπορούν να παρέχουν συντονισμό και ενοποίηση φορτώσεων και μεταφορών για μια φιλική προς το περιβάλλον λειτουργία εντός πόλεων).

Όσον αφορά τις τεχνολογίες ITS που χρησιμοποιούνται στις εμπορευματικές μεταφορές, μπορεί να ειπωθεί ότι όλες οι προαναφερθείσες τεχνολογίες χρησιμοποιούνται και στον τομέα των εμπορευματικών μεταφορών και των Logistics με τα ακόλουθα να παρουσιάζουν ιδιαίτερο ενδιαφέρον:

- Τεχνολογίες δρομολόγησης βαρέων φορτηγών οχημάτων (HGV - Heavy Goods Vehicles) οχήματα) προκειμένου να οδηγούνται μακριά από ευαίσθητες περιοχές (είναι συχνά διαφορετικό από τη μια τυπική δρομολόγηση μέσω δορυφόρου που μπορεί να έχει σχεδιαστεί χωρίς εξέταση των βαρέων φορτηγών οχημάτων). Αυτό είναι από ιδιαίτερα ενδιαφέρον για τις αστικές περιοχές και τις τοπικές αρχές όπως και το επόμενο στοιχείο.
- Επιβολή περιορισμών στάθμευσης, φόρτωσης, εκφόρτωσης, είσοδος σε απαγορευμένες ζώνες, δρόμους κτλ.
- Διαδικτυακός προγραμματισμός πριν από το ταξίδι, καθώς και δρομολόγηση εντός του οχήματος βάσει του σχεδιασμού και διαχείρισης που έχει γίνει από το κέντρο ελέγχου των μεταφορών, καθώς και στρατηγικών δρομολόγησης σχεδιασμένων από τις τοπικές αρχές (αντί για διαδρομές που μπορεί να βασίζονται στη συντομότερη απόσταση ή τον συντομότερο χρόνο για τα HGV).
- Διαδικτυακή παρακολούθηση μεμονωμένων φορτίου σε ολόκληρη την αλυσίδα μεταφοράς καθώς και παροχή λεπτομερών πληροφοριών στους σχετικούς φορείς σε όλο αυτό το μήκος των αλυσίδων.
- Έξυπνες εφαρμογές φορτίου (e-freight).

viii. ITS για Έξυπνη Κινητικότητα και συν-τροπικών (Co-modality) υπηρεσιών

Ο όρος «έξυπνη κινητικότητα» αναφέρεται στην παροχή αναλυμένων πληροφοριών που βασίζονται σε δεδομένα πραγματικού χρόνου για αποτελεσματικό και βιώσιμο σχεδιασμό κατά την εκτέλεση ταξιδιών καθώς και τη διαχείριση της ζήτησης πληροφοριών σε τέτοια ταξίδια. Η έξυπνη κινητικότητα των μεταφορών δεν αφορά μόνο μετακινήσεις σε αστικά κέντρα αλλά και τα ταξίδια μεγάλων αποστάσεων και τη ζήτηση για μεταφορές. Οι τρόποι με τους οποίους μπορεί να αντιμετωπιστεί

αποτελεσματικά η ζήτηση για μεταφορές ονομάζονται διαχείριση κινητικότητας και συστήματα κινητικότητας.

Οι παραπάνω τομείς ανάπτυξης ITS θεωρείται πως προωθούν την έξυπνη τη διαχείριση της κινητικότητας και την κινητικότητα αυτή καθαυτή ταυτόχρονα με μια «συντροπικότητα» (γενική επεξήγηση – η συνεργασία μεταξύ των τρόπων). Αυτό οφείλεται στο γεγονός πως προάγουν συνεχώς:

- Ελεύθερη ροή κυκλοφορίας στα δίκτυα όλων των τρόπων (αστικές και υπεραστικές περιοχές).
- Πιο πράσινες μεταφορές μέσα από έξυπνη διαχείριση του στόλου και των αποστάσεων που διανύονται.
- Εξυπνότερη και παροχή πληροφοριών πραγματικό χρόνο για την κινητικότητα.
- Συστήματα και δίκτυα δημόσιων μεταφορών που διαχειρίζονται καλύτερα.
- Ασφαλέστερες μεταφορές μέσα από ασφαλέστερη συμπεριφορά, ασφαλέστερες υποδομές και ασφαλέστερης χρήσης των οχημάτων.

Το Σχέδιο Δράσης του 2009 για την Αστική Κινητικότητα καθορίζει τις κύριες συνεισφορές των ITS στην κινητικότητα και τη συντροπικότητα, θέτοντας ένα πλαίσιο στις πρωτοβουλίες της ΕΕ πάνω σε αυτόν τον τομέα. Στο σχέδιο αυτό προτείνονται είκοσι δράσεις, που βασίζονται μεταξύ άλλων παραγόντων στην ύπαρξη και τη λειτουργία των ITS σαν παράγοντα διευκόλυνσης. Παράλληλα, ορισμένες μορφές συνεργατικής κινητικότητας που βασίζονται σε smartphones, αναπτύσσονται προοδευτικά, σε μεγάλο βαθμό ανεξάρτητα από τα οχήματα και τις υποδομές μεταφορών.

Οι είκοσι δράσεις του σχεδίου κατανέμονται σε 6 θέματα

1. **Προώθηση ολοκληρωμένων πολιτικών**
    1. Επιτάχυνση της υιοθέτησης σχεδίων βιώσιμων σχεδίων αστικής κινητικότητας
    2. Βιώσιμη αστική κινητικότητα και περιφερειακή πολιτική
    3. Μεταφορές για υγιή αστικά περιβάλλοντα
2. **Εστίαση στους πολίτες**
    4. Πλατφόρμα για τα δικαιώματα των επιβατών στις δημόσιες αστικές συγκοινωνίες
    5. Βελτίωση της προσβασιμότητας των ατόμων με μειωμένη κινητικότητα
    6. Βελτίωση ταξιδιωτικών πληροφοριών
    7. Πρόσβαση σε «πράσινες» ζώνες
    8. Καμπάνιες για συμπεριφορές βιώσιμης κινητικότητας
    9. Οδήγηση ενεργειακά αποδοτική στο πλαίσια της εκπαίδευσης οδήγησης
3. **«Πράσινες» αστικές συγκοινωνίες**
    10. Έρευνα και ανάπτυξη οχημάτων χαμηλών και η δυνατόν μηδενικών εκπομπών
    11. Οδηγός στο διαδίκτυο για «καθαρά» και ενεργειακά αποδοτικά οχήματα
    12. Μελέτες αστικών πτυχών της εσωτερίκευσης του εξωτερικού κόστους
    13. Ανταλλαγή πληροφοριών σχετικά με τα συστήματα αστικής τιμολόγησης
4. **Ενίσχυση των χρηματοδοτήσεων**
    14. Βελτιστοποίηση των υφιστάμενων πηγών χρηματοδότησης
    15. Ανάλυση των αναγκών για μελλοντικές χρηματοδοτήσεις

5. **Ανταλλαγή εμπειριών και γνώσεων**
    16. Αναβάθμιση δεδομένων και στατιστικών
    17. Δημιουργία κέντρου παρατηρήσεων της αστικής κινητικότητας
    18. Συμβολή στον διεθνή διάλογο και ανταλλαγή πληροφοριών
6. **Βελτιστοποίηση της αστικής κινητικότητας**
    19. Αστικές εμπορευματικές μεταφορές
    20. ITS για την αστική κινητικότητα

Σχετικά με την έννοια της έξυπνης κινητικότητας γίνεται επίσης συζήτηση για χρήση των ITS για «καθαρές» μορφές κινητικότητας. Είναι απίθανο οποιοδήποτε μεμονωμένο μέτρο για τα ITS να καταφέρει τη σημαντική μείωση στις εκπομπές CO2. Στο σύνολό τους όμως τα ITS μπορούν να βοηθήσουν τη μείωση των εκπομπών ρύπων. Ως εκ τούτου, τα μέτρα σχετικά με τα ITS με στόχο την «καθαρή κινητικότητα» πρέπει να εισαχθούν μέσα από στιβαρά πολιτικά σχέδια που περιλαμβάνει άλλα μέτρα όπως η προώθηση των ΜΜΜ, η χρήση μη μηχανοκίνητων μέσων, η πολιτική στάθμευσης κτλ.

Για να επιτευχθεί έξυπνη κινητικότητα σε τοπικό αστικό επίπεδο, μερικά από τα βασικά στοιχεία είναι:

- Ενσωμάτωση πληροφοριών για το τοπικό οδικό δίκτυο (κυκλοφορία, υποδομές, κτλ) στα σημεία πληροφόρησης που χρησιμοποιούν οι διοργανωτές ταξιδιών .
- Ενσωμάτωση στη διαχείρισης οδικών δικτύων πληθώρας υπηρεσιών πληροφόρησης και κινητικότητας.
- Ενοποίηση των συστημάτων πληρωμών.
- Ανεμπόδιστες εναλλαγές μεταξύ δικτύων μεγάλων και μικρών αποστάσεων, για μεταφορά εμπορευμάτων και επιβατών .

ix. ITS για περιβαλλοντική και ενεργειακή απόδοση

Κύριοι στόχοι των ITS για την ενεργειακή απόδοση είναι η συμβολή στην παροχή καθαρότερων, ασφαλέστερων και αποδοτικότερων ενεργειακά μεταφορών. Στο σχέδιο δράσης του 2008 για την ανάπτυξη των ITS στην Ευρώπη, αναφέρεται πως οι εφαρμογές ITS έχουν ουσιαστικό ρόλο στην βελτίωση της ενεργειακής αποδοτικότητας του τομέα των μεταφορών.

Οι βασικές ενέργειες που έχουν σχέση με τις ενέργειες ανάπτυξης ITS είναι :

- Βελτιστοποίηση χρήσης των υποδομών.
- Αποτελεσματικότερη διαχείριση της κυκλοφορίας και καλύτερη αλληλεπίδραση μεταξύ διαφορετικών τρόπων λειτουργίας της.
- Μείωση της κυκλοφοριακής συμφόρησης στους εμπορευματικούς διαδρόμους.
- Ανάπτυξη ευρωπαϊκών λύσεων για πιο ευέλικτη διαχείριση των απαιτήσεων.
- Βελτίωση των φιλικών προς το περιβάλλον και των αποδοτικότερων ενεργειακά λύσεων στις μεταφορές.
- Βελτίωση της αποτελεσματικότητας των logistics.

Οι περισσότεροι από τους τομείς εφαρμογής των ITS που αναφέρονται στις προηγούμενες παραγράφους μπορούν να επηρεάσουν θετικά την περιβαλλοντική και ενεργειακή απόδοση των μεταφορών.

Άλλες εφαρμογές ITS, πιο άμεσα σχετικές στην ενεργειακή απόδοση είναι αυτές που σχετίζονται με:

- Συστήματα παρακολούθησης της συντήρησης και της λειτουργίας των οχημάτων ως προς την απόδοση καυσίμου,
- Περιβαλλοντική χάραξη διαδρομής σε πραγματικό χρόνο με στόχο αποφυγή προβλεπόμενης συμφόρησης,
- Περιβαλλοντικά ευαίσθητος σχεδιασμός ταξιδιού,
- Οικολογική οδήγηση ή περιβαλλοντικά ευαίσθητη οδήγηση,
- Καλύτερη διαχείριση και χρήση των υποδομών μεταφορών, συμπεριλαμβανομένης της μείωσης των κενών δρομολογίων οχημάτων κ.ά.,

Το ITS έχει να διαδραματίσει κρίσιμο ρόλο στην εξέλιξη και τη λειτουργία ηλεκτρικών αυτοκινήτων και λεωφορείων (είτε πλήρως ηλεκτρικών, είτε plug-in υβριδικών), της λεγόμενης δηλαδή ηλεκτροκίνησης παρέχοντας:

- Πληροφορίες για τα διαθέσιμα σημεία φόρτισης στο οδικό δίκτυο.
- Διαχείριση της παροχής ενέργειας σε αυτά τα σημεία και συμβολή στην εξισορρόπηση της παροχής ηλεκτρικής ενέργειας εκεί.
- Ενσωμάτωση των ηλεκτρικών αυτοκινήτων στην κυκλοφορία, ειδικά σε αστικές περιοχές, κυρίως από την άποψη ασφάλειας.
- Παρακολούθηση οχημάτων, κυρίως σε δημόσιους στόλους,
- Διαχείριση των σημείων στάθμευσης και φόρτισης ,
- Πρόβλεψη των τρόπων πληρωμών που σχετίζονται με τις υπηρεσίες ηλεκτρικής κινητικότητας.

Είναι πιθανό στην ταυτόχρονη ανάπτυξη ITS και ηλεκτρικής κινητικότητας, θα κατευθύνουν η μία την άλλη με τρόπο συμπληρωματικό.

Σχετικά με τη χρήση των ITS προς όφελος της ενεργειακής απόδοσης, αξίζει να αναφέρουμε δύο ερευνητικά έργα συγχρηματοδοτούμενα από την ΕΕ μέσα από το 7ου Κοινοτικού Πλαισίου Προγράμματος.

Το πρώτο είναι το project Eco-Move που στοχεύει να εφαρμόσει τις πιο πρόσφατες τεχνολογίες επικοινωνίας V2I και V2V ώστε να δημιουργηθεί μια ολοκληρωμένη λύση που περιλαμβάνει υποστήριξη οικολογικής οδήγησης και διαχείριση οικολογικής κυκλοφορίας.

Το δεύτερο είναι το project FREILOT, που στοχεύει στην αύξηση της ενεργειακής απόδοσης των οδικών μεταφορών εμπορευμάτων σε αστικές περιοχές. Εξετάζει συστήματα διαχείρισης στόλου, τον τύπο των οχημάτων παράδοσης, τα συστήματα υποστήριξης του οδηγού κτλ και καταδεικνύει ότι μια μείωση έως και 25% της κατανάλωσης καυσίμου στις αστικές μεταφορές εμπορευμάτων είναι εφικτή διαμέσου μέτρων που βασίζονται στα ITS.

Έχουν επίσης αναπτυχθεί δύο project για την ανάπτυξη των εργαλείων που απαιτούνται για την αξιολόγηση του αντίκτυπου των μέτρων από ICT (Information Communication Technologies – Τεχνολογίες Πληροφορίας και Επικοινωνιών) και ITS στις εκπομπές καυσαερίων που εντείνουν το φαινόμενο του θερμοκηπίου. Αυτά είναι:

- AMITRAN που αναπτύσσει ένα πλαίσιο για την αξιολόγησης των επιπτώσεων των μέτρων του ICT στην κυκλοφορία και τις μεταφορές ως προς την

ενεργειακή απόδοση και τις εκπομπές CO2, με στόχο να μπουν οι βάσεις μια τυποποιημένης αξιολόγησης των μελλοντικών ευρωπαϊκών εξελίξεων στα ICT.
- ICT-EMISSIONS που αναπτύσσει μιας νέα μεθοδολογία αξιολόγησης του αντίκτυπου των μέτρων που σχετίζονται με τις ICT στην κινητικότητα, την κατανάλωση ενέργειας των οχημάτων και τις εκπομπές διοξειδίου του άνθρακα ενός στόλου οχημάτων σε τοπική κλίμακα.

x. Ενοποίηση και ιεράρχηση τεχνολογιών και συστημάτων ITS

Στα προηγούμενα κεφάλαια έγινε απολογισμός του πεδίου των ITS, σε όλους τους τρόπους μεταφορών, όσον αφορά τις κύριες τεχνολογικές του εξελίξεις όσο και τις διάφορες πολιτικές και οράματα της ΕΕ στο πεδίο για το μέλλον. Αυτό έγινε για να οριοθετήσουμε το πεδίο και να χαρτογραφήσουμε τις πολλές διαφορετικές εφαρμογές και δυνατότητες που εξαρτώνται όχι μόνο από την τεχνολογική πρόοδο αλλά και από ρυθμιστικές πολιτικές.

Ο κύριος στόχος των εφαρμογών ITS σε όλες τις λειτουργίες, που σήμερα βρίσκονται σε μεταβατικό στάδιο, είναι να μεταφράσουν τις επί του παρόντος λύσεις που αναπτύσσονται σε περιορισμένη γεωγραφική κλίμακα - με πολύ περιορισμένη ανταλλαγή δεδομένων μεταξύ δικτύων και έλλειψη διαλειτουργικότητας – σε μια ολοκληρωμένη συντροπική ανταλλαγή δεδομένων μέσω δικτύου και υπηρεσίες αδιάλειπτης κινητικότητας, όπου άνθρωποι, αγαθά και οχήματα είναι συνεχώς και παντού συνδεδεμένα και λαμβάνουν ή στέλνουν χρήσιμα δεδομένα/πληροφορίες. Ως εκ τούτου, το πιο δύσκολο έργο για τα ευρωπαϊκά θεσμικά όργανα στο άμεσο μέλλον θα είναι η ίδρυση ενός κοινού οράματος με κοινούς στόχους, κοινούς χάρτες πορείας και μια μακροπρόθεσμη συνεκτική στρατηγική για να υποστηριχθεί η ανάπτυξη των σχετικών υπηρεσιών προς τον παραπάνω στόχο. Έτσι προκύπτουν ορισμένα ζητήματα προτεραιότητας τα οποία μπορούν να συνοψιστούν ως εξής:

- Διαλειτουργικά – ολοκληρωμένα συστήματα πληροφοριών κυκλοφορίας ταξιδιωτών σε όλους τους τρόπους λειτουργίας.
- Συνεργατικά συστήματα και υπηρεσίες κινητικότητας για αστικές περιοχές.
- Εφαρμογές ασφάλειας (π.χ. η πανευρωπαϊκή εφαρμογή του e-Call).
- Διαλειτουργικότητα οδικής χρέωσης και διοδίων.
- ITS και ηλεκτροκίνηση.
- Μεταφορές εμπορευμάτων και logistics για ασφαλείς και φιλικές προς το περιβάλλον μεταφορές ειδικά σε αστικές περιοχές (π.χ. στάθμευση φορτηγών).
- Δημόσιες συγκοινωνίες/πολυτροπικές υπηρεσίες ταξιδιωτών .

Τα ακόλουθα ζητήματα θα χρειαστούν ιδιαίτερη προσοχή στην ενεργοποίηση και την απρόσκοπτη λειτουργία ένα συστήματος ITS σύστημα σε ολόκληρο το φάσμα των λειτουργιών του:

- Φορείς επικοινωνίας για υπηρεσίες των ITS ,
- Τόπος αποθήκευσης δεδομένων/τόπος πώλησης δεδομένων,
- Μέθοδοι αναφοράς τοποθεσίας,
- Εφαρμογές ηλεκτρονικών μεταφορών (e-freight) για όλες τις λειτουργίες.

Ο ρόλος της Ευρώπης θεωρείτε κυρίως η παροχή όσο το δυνατό περισσότερων διευκολύνσεων για τη διαλειτουργικότητα των ITS σε όλο το φάσμα των λειτουργιών

τους και η προώθηση αξιόπιστων και αποτελεσματικών υπηρεσιών ITS εντός και μεταξύ αυτών των τρόπων πάντα προς όφελος του Ευρωπαίου πολίτη μέσω:

- Διασφάλιση διαθεσιμότητας καλής ποιότητας δεδομένων σε όλα τα επίπεδα,
- Διασφάλιση ποιότητας ανάπτυξης και λειτουργίας των συστημάτων,
- Τυποποίηση σε διαλειτουργικές υπηρεσίες,
- Προώθηση της έρευνας και της ανάπτυξης, λαμβάνοντας υπόψη τη σωστή αντιμετώπιση των δικαιωμάτων πνευματικής ιδιοκτησίας και της ιδιωτικής ζωής.

Δεδομένου ότι ο σκοπός του project του Στρατηγικού Πλάνου Τεχνολογικών μεταφορών ή STTP (Strategic Transport Technologies Plan) είναι να καταρχήν να εδραιώσει και σε δεύτερο χρόνο να παρουσιάσει τον τομέα των μεταφορών με βάση κάποιες βασικές τεχνολογίες (μεταξύ των οποίων και τα ITS). Οι τεχνολογίες αυτές θεωρούνται κρίσιμες για τη μελλοντική εφαρμογή και επιτυχία των πολιτικών για τις μεταφορές στην ΕΕ, απαριθμούνται παρακάτω οι βασικές τεχνολογίες ITS και συστήματα που πιθανώς επηρεάζουν ή να επηρεάζονται από τις πολιτικές μεταφορών που πρέπει να ακολουθηθούν.

Αυτό γίνεται με ταξινόμηση σε ένα από τους ακόλουθους 9 τεχνολογικούς τομείς που σχετίζονται με τα ITS και καλύπτουν (έχουν δηλαδή εφαρμογή) όλους ή σχεδόν όλους τους οκτώ τομείς της εφαρμογής ITS που αναφέρονται παραπάνω:

- Ανταλλαγή δεδομένων κίνησης και ταξιδιωτικών πληροφοριών (πρότυπα παγκοσμίως διαλειτουργικά με βιώσιμα επιχειρηματικά μοντέλα):
    - μίας διακριτής λειτουργίας
    - σε ξεχωριστές/διακριτές λειτουργίες εντός και εκτός συνόρων.
- Καθοδήγηση διαδρομών / συστήματα πλοήγησης :
    - προκαθορισμένες στρατηγικές
    - μικρο- στρατηγικές
    - εξατομικευμένη στρατηγική
    - ευαίσθητες περιβαλλοντικά και ενεργειακά στρατηγικές.
- Έξυπνη διαχείριση κίνησης σε πραγματικό χρόνο σε:
    - Χερσαίες μεταφορές
    - Σιδηροδρομικές μεταφορές
    - Θαλάσσιες μεταφορές
    - Αεροπορικές μεταφορές
    - σε όλες τις λειτουργίες.
- Διαχείριση δικτύων αστικών δημόσιων συγκοινωνιών
- Έξυπνη είσπραξη τελών
- Συνεργαζόμενα συστήματα (V2I, V2V) για :
    - Αυξημένη Υποβοήθηση Οδηγού - ADAS (Advanced Driver Assistance)
    - Αυξημένη Υποβοήθηση Οδηγού Δίκυκλου - ARAS (Advanced Rider Assistance)
- Έξυπνες μεταφορές εμπορευμάτων (αστικές και υπεραστικές)
    - Παγκοσμίως διαλειτουργικό περιβάλλον ενσωματωμένο σε όλες τις λειτουργίες για ηλεκτρονικά φορτία (e-freight)
    - Έξυπνα συστήματα διαχείρισης στόλου και μεταφορών

    - Ενοποιημένες διαλειτουργικές και παγκοσμίως διαθέσιμες πλατφόρμες για ενιαία παροχή πληροφοριών στις εμπορευματικές μεταφορές.
- Έξυπνη ενέργεια (οικολογική οδήγηση, περιβαλλοντικής διαχείριση κυκλοφορίας, ενεργειακή διαχείριση κυκλοφορίας, παρακολούθηση συντήρησης οχημάτων κτλ)
- Υπηρεσίες βιώσιμης κινητικότητας (διαχείριση ζήτησης, ηλεκτρονική πληροφόρηση κινητικότητας, επιλογή μεταφορών φιλική προς το περιβάλλον, κτλ).

Συνοψίζοντας μπορούμε να πούμε πως οι εθνικές κυβερνήσεις οφείλουν να αναπτύξουν τις στρατηγικές τους θέσεις σε θέματα ITS. Λίγες από αυτές διαθέτουν κάποια στρατηγική σήμερα. Αυτό αποτελεί πιθανό εμπόδιο για την ανάπτυξη και την καλύτερη χρήση των ITS, καθώς αυξάνει τον κίνδυνο, τόσο τον αντιληπτό όσο και τον πραγματικό, από την οπτική γωνία των ιδιωτών .

4. Background – Διαχείριση Ασφάλειας στα ITS

i.Εισαγωγή

Τα Ευφυή Συστήματα Μεταφορών (ITS) είναι η μελλοντική κατεύθυνση. Τα μέσα μεταφοράς θα ενσωματώνονται όλο και περισσότερο και θα επικοινωνούν μέσω ενός συστήματος ασύρματων επικοινωνιών. Οι ταξιδιώτες και οι μεταφορείς εμπορευμάτων θα έχουν πλήρη γνώση της απόδοσης του συστήματος και θα μπορούν να προγραμματίζουν ανάλογα τα ταξίδια τους. Η αρχιτεκτονική υποδομή, ICT για την υποστήριξη ITS είναι καθαρά ιεραρχική (Δενδρική δομή), με δεδομένα ανίχνευσης που ρέουν από τα φύλλα (δηλαδή, αισθητήρες στην άκρη του δρόμου ή εγκατεστημένοι στο όχημα) προς τη ρίζα (δηλαδή, το κέντρο διαχείρισης κυκλοφορίας). Η τρέχουσα προσέγγιση δεν ανταποκρίνεται επαρκώς, με τη συμπερίληψη σημαντικού αριθμού νέων στοιχείων, δεν είναι ευέλικτη στην υποστήριξη μιας σταδιακής ανάπτυξης ή αλλαγών του ITS και παρουσιάζει ζητήματα καθυστέρησης και ασφάλειας.

Για να ξεπεραστούν οι περιορισμοί των σημερινών συστημάτων, το έργο ICSI αναπτύσσει μια νέα αρχιτεκτονική, όπου η νοημοσύνη για την ανίχνευση και την ενεργοποίηση, κατανέμεται σε ορισμένα από τα στοιχεία, που ονομάζονται πύλες (gateways), τα οποία φιλοξενούν μια πλατφόρμα λογισμικού, για την εκτέλεση των εφαρμογών ITS, χρησιμοποιώντας τον τοπικό χώρο αποθήκευσης και τους υπολογιστικούς πόρους (δυνατοτήτων) που είναι διαθέσιμοι. Το προτεινόμενο σύστημα ICSI στοχεύει στην επίτευξη σημαντικής ενεργειακής απόδοσης στα συστήματα μεταφορών μέσω ταχύτερων, αξιόπιστων και ακριβέστερων κύκλων και αντιδράσεων ανίχνευσης, αφού η πλήρως κατανεμημένη αρχιτεκτονική τα καθιστά ικανά.

Το όραμα επικεντρώνεται στο ότι οι πιο αισθητές μειώσεις στις εκπομπές CO2 θα σημειωθούν στα συστήματα αστικών μεταφορών. Ο στόχος του έργου είναι ο καθορισμός μιας νέας αρχιτεκτονικής που θα επιτρέψει τη συνεργατική ανίχνευση σε ευφυή συστήματα μεταφορών και την ανάπτυξη μιας εφαρμογής αναφοράς end-to-end. Τα αποτελέσματα του έργου θα επιτρέψουν προηγμένες στρατηγικές διαχείρισης κυκλοφορίας και ταξιδιών, βασισμένες σε αξιόπιστα και σε πραγματικό χρόνο δεδομένα. Η αποτελεσματικότητα τέτοιων νέων στρατηγικών, μαζί με το προτεινόμενο σύστημα, αξιολογήθηκε με δύο επιτόπιες δοκιμές.

Η ασφάλεια τον ITS, είναι ένα θέμα το οποίο έχει αναλυθεί και τεκμηριωθεί αρκετά, παρά το γεγονός ότι υπάρχουν ακόμη πολλά λεπτομερή προβλήματα προς επίλυση. Η κύρια διαφορά μεταξύ της αρχιτεκτονικής ασφαλείας, ETSI TR 102 893 ITS[57,58] και της αρχιτεκτονικής ασφαλείας ICSI[59] δεν έγκειται στην επικοινωνία κατά την φάση λειτουργείας (αρχική επεξεργασία δεδομένων), αλλά στις υπόλοιπες λειτουργίες στο παρασκήνιο (backend). Το ETSI TR 102 893, είναι ένα κεντρικό "Κέντρο εξυπηρέτησης ITS" και επομένως επιτρέπει τη συγκέντρωση του μεγαλύτερου μέρους επιβολής της ασφάλειας σε αυτές τις λειτουργείες που γίνονται στο παρασκήνιο (backend). Δεν υπάρχει επίσης ανάγκη προστασίας της επικοινωνίας μεταξύ διαφορετικών στοιχείων του backend, επειδή όλα εκτελούνται στο ίδιο αξιόπιστο τομέα.

Στο ICSI, από την άλλη πλευρά, το backend είναι μια γεωγραφικά εξαιρετικά κατανεμημένη υπολογιστική υποδομή με εσωτερική επικοινωνία σε περισσότερο ή λιγότερο ανοιχτά δίκτυα. Αυτό έχει σημαντικό αντίκτυπο στην αρχιτεκτονική ασφάλειας. Τα επιμέρους στοιχεία των συστημάτων ICSI δεν βρίσκονται πλέον σε έναν ενιαίο αξιόπιστο τομέα εμπιστοσύνης και δεν είναι δυνατή η προστασία ενός μόνο σημείου εισόδου στο backend, καθώς αυτό δεν υπάρχει πλέον. Επομένως, η πλέον ενδιαφέρουσα πτυχή ασφαλείας του ICSI είναι κυρίως η ασφάλεια του ICSI DDP, του backend, το οποίο είναι ένα αρκετά γενικό και σε μεγάλο βαθμό άλυτο πρόβλημα ασφάλειας για τα κατανεμημένα συστήματα γενικά.

Από τα παραπάνω πηγάζουν κάποιες κύριες απαιτήσεις ασφαλείας στο ICSI. Πρώτα από όλα, η προστασία του συστήματος ICSI ως συστήματος πληροφορικής. Οι επιτιθέμενοι δεν πρέπει να αποκτήσουν πρόσβαση σε οποιοδήποτε μέρος του συστήματος ICSI, προκειμένου να κάνουν κακή χρήση της υποδομής ή να την κλείσουν. Δεύτερον, οι εισβολείς δεν πρέπει να μπορούν να κάνουν κατάχρηση του ICSI ως ITS και εμπορικό σύστημα, (π.χ. παραβίαση των πινακίδων μεταβλητών μηνυμάτων (VMS) ή πρόσβαση σε πληροφορίες χρέωσης.

Το απόρρητο των χρηστών πρέπει να προστατεύεται και η προστασία δεδομένων αποτελεί κανονιστική απαίτηση. Το απόρρητο είναι μια ιδιαίτερα περίπλοκη πρόκληση. Είναι μια απλή έννοια αλλά αρκετά πολύπλοκη κατά την προσπάθεια προστασίας της. Δυστυχώς, η ελλείψει κοινών απαιτήσεων (προδιαγραφών) απορρήτου, οδηγούν σε διάφορα θέματα, αφού υπάρχουν λίγες προδιαγραφές απορρήτου για τους προγραμματιστές για τη δημιουργία τεχνολογιών ενίσχυσης της ιδιωτικής ζωής (PET). Το ICSI περιλαμβάνει ένα "Open Privacy Framework" (OPF) επειδή η προστασία του απορρήτου για τους τελικούς χρήστες του ICSI είναι μια κρίσιμη απαίτηση. Βασίζεται στο Privacy by Design (PbD), τα νέα 24 στοιχεία ελέγχου απορρήτου στο NIST 800-3a Παράρτημα J και ευθυγραμμίζεται με το Πλαίσιο Διαχείρισης Κινδύνων (RMF) και το Πλαίσιο Κυβερνοασφάλειας (CSF) του NIST. Για το ICSI, ακολουθείται μια προσέγγιση από κάτω προς τα πάνω για την εφαρμογή της ασφάλειας.

ii. Advanced Access Control Concepts

Μια καινοτόμος, νέα αρχιτεκτονική ελέγχου πρόσβασης είναι απαραίτητη για το ICSI, ειδικά για την επιβολή του απορρήτου των χρηστών. Αυτό συμβαίνει επειδή το ICSI είναι ουσιαστικά ένα εξαιρετικά αρθρωτό, δυναμικό/ευκίνητο τοπίο πληροφορικής όπου πολλές δυναμικά μεταβαλλόμενες ροές πληροφοριών πρέπει να ελέγχονται με βάση λεπτομερείς, δυνητικά εξαιρετικά δυναμικές και συμφραζόμενες πολιτικές

ελέγχου πρόσβασης. Με άλλα λόγια, το σύστημα ελέγχου πρόσβασης πρέπει να μπορεί να υποστηρίζει την επιβολή (και τη διαχείριση) σύνθετων, δυναμικά μεταβαλλόμενων πολιτικών για δυναμικά μεταβαλλόμενες ροές πληροφοριών, σε ένα δυναμικά μεταβαλλόμενο τοπίο πληροφορικής. Αυτή είναι μια εξαιρετικά περίπλοκη ερευνητική πρόκληση, η οποία αντιμετωπίζεται ως μέρος του ICSI και πολλών άλλων έργων FP[60,61,62,63].

Στην ασφάλεια της πληροφορικής, υπάρχουν πολλά καθιερωμένα μοντέλα ασφαλείας για τον έλεγχο της πρόσβασης ενός θέματος (π.χ. ένας χρήστης, σε ένα αντικείμενο, π.χ. ένας διακομιστής). Υπάρχει, για παράδειγμα, ο Διακριτικός Έλεγχος Πρόσβασης (DAC) με λίστες ελέγχου πρόσβασης βάσει ταυτότητας (ACL), ο Έλεγχος πρόσβασης βάσει ρόλου (RBAC) που ομαδοποιεί ταυτότητες σε ρόλους και ο Υποχρεωτικός Έλεγχος Πρόσβασης (MAC) με βάση την έννοια των αδειών ασφαλείας και της ετικέτας. Επιπλέον, υπάρχουν και μοντέλα ασφαλείας που βασίζονται σε δυνατότητες ή δικαιώματα. Δυστυχώς αυτά τα μοντέλα είναι μη εφαρμόσιμα και μη διαχειρίσιμα για το πολύπλοκο περιβάλλον μηχανής-2-μηχανής ICSI (επεκτασιμότητα και διαχειρισιμότητα ταυτοτήτων, μέγεθος και αλλαγή τεράστιων ACL, σύνθετες αντιστοιχίσεις ρόλων, υποστήριξη σύνθετων απαιτήσεων απορρήτου και απαιτήσεις εγγύτητας).

Επομένως, τα καθιερωμένα κλασικά μοντέλα ασφαλείας για τον έλεγχο πρόσβασης δεν είναι κατάλληλα. Απαιτείται μια πιο εξελιγμένη προσέγγιση για την εφαρμογή πολύπλοκων πολιτικών με βάση την τοποθεσία, την εγγύτητα, μεγάλης κλίμακας, μηχανή σε μηχανή, δυναμικά μεταβαλλόμενες, σύνθετες πολιτικές. Νέα μοντέλα ασφαλείας ελέγχου πρόσβασης, όπως ο έλεγχος πρόσβασης βάσει χαρακτηριστικών (ABAC) και ο έλεγχος πρόσβασης βάσει εγγύτητας (PBAC), μαζί με την ασφάλεια βάσει μοντέλου (MDS) μπορούν να εκφράσουν και να επιβάλουν τέτοιες απαιτήσεις ασφαλείας.

Για να προσπαθήσουμε να ενοποιήσουμε την ορολογία και τις έννοιες του ABAC, το προσχέδιο NIST 800-162 (2013) ορίζει το ABAC ως εξής. Ο έλεγχος πρόσβασης βάσει χαρακτηριστικών (ABAC) είναι "μια λογική μεθοδολογία ελέγχου πρόσβασης όπου η εξουσιοδότηση για εκτέλεση ενός συνόλου των λειτουργιών προσδιορίζεται με την αξιολόγηση των χαρακτηριστικών που σχετίζονται με το θέμα, το αντικείμενο, τις ζητούμενες λειτουργίες και, σε ορισμένες περιπτώσεις, τις συνθήκες περιβάλλοντος έναντι πολιτικής, κανόνων ή σχέσεων που περιγράφουν τις επιτρεπόμενες λειτουργίες για ένα δεδομένο σύνολο χαρακτηριστικών." Χαρακτηριστικά που σχετίζονται με ένα θέμα μπορεί, για παράδειγμα, να είναι η κατάσταση των πληρωμών διοδίων για ένα όχημα (ενσωματωμένη μονάδα, OBU), αλλά και τα κλασικά χαρακτηριστικά ασφαλείας, όπως μεμονωμένα αναγνωριστικά, ρόλοι ή άδειες. Οι πληροφορίες περιβάλλοντος μπορεί να περιλαμβάνουν, για παράδειγμα, ώρα ή καιρικές συνθήκες.

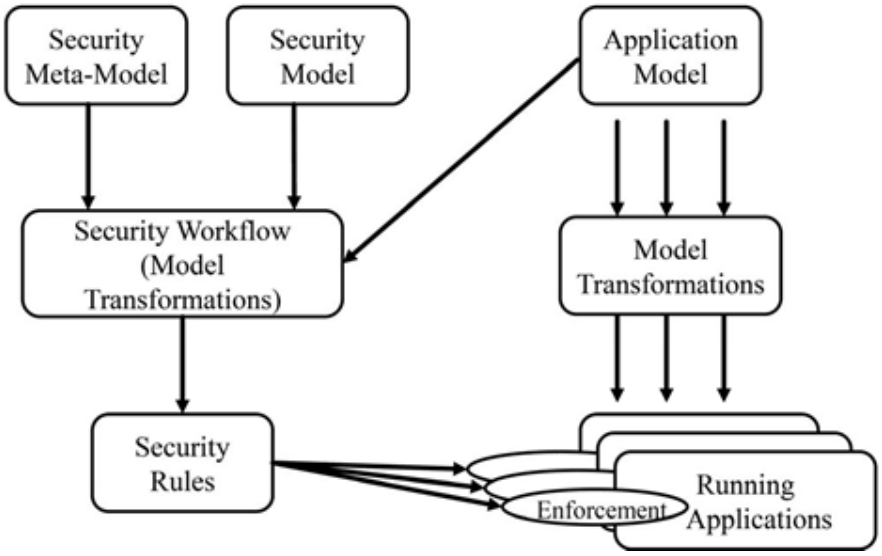
Τα κύρια πλεονεκτήματα του ABAC είναι ότι μπορεί να βοηθήσει στην επίτευξη καλύτερης πολιτικής και ευελιξία των χαρακτηριστικών της. Μπορεί να μειώσει το χάσμα μεταξύ της πολιτικής ασφάλειας της επιχείρησης και του τεχνικού ελέγχου πρόσβασης. Μπορεί να βοηθήσει στην εξωτερίκευση του ελέγχου πρόσβασης από εφαρμογές και στη φορητότητα/δια λειτουργικότητα κανόνων πολιτικής. Οι κύριες προκλήσεις του ABAC περιστρέφονται γύρω από την πολυπλοκότητα, την ευαισθησία, την ευελιξία, τη δυνατότητα εφαρμογής, τη δυνατότητα ελέγχου, αλλά πάντα σε ένα διαχειρίσιμο επίπεδο.

Ο έλεγχος πρόσβασης βάσει εγγύτητας (PBAC) προχωρά ακόμη περισσότερο από το συμβατικό ABAC. Βασίζει τις αποφάσεις του για τον έλεγχο πρόσβασης στην εγγύτητα μεταξύ δύο οντοτήτων, στις περισσότερες περιπτώσεις μεταξύ υποκειμένου και αντικειμένου. Το PBAC μπορεί για παράδειγμα να χρησιμοποιηθεί για τον καθορισμό πολιτικών ασφαλείας που επιτρέπουν συγκεκριμένες ενέργειες μόνο σε συγκεκριμένες περιοχές. Αυτό συχνά επιτρέπει τη δηλωτική έκφραση των πολιτικών ασφαλείας που καθοδηγούνται από λειτουργικές απαιτήσεις με πολύ φυσικό τρόπο, αντί να τις κωδικοποιούν σκληρά στον πηγαίο κώδικα της εφαρμογής.

Στο ICSI, το PBAC είναι ο έλεγχος πρόσβασης που χρησιμοποιεί πολιτικές που βασίζονται στη σχετική εγγύτητα/απόσταση μεταξύ ενός ή περισσότερων χαρακτηριστικών εγγύτητας που σχετίζονται με ένα εργαλείο πρόσβασης και ενός ή περισσότερων χαρακτηριστικών εγγύτητας που σχετίζονται με έναν πόρο ο οποίος είναι προσβάσιμος. Η εγγύτητα μπορεί να βασίζεται για παράδειγμα σε γεωγραφική θέση, χωρική εγγύτητα (δηλαδή φυσική τοποθεσία), οργανωτική εγγύτητα (π.χ. σχέσεις στην αλυσίδα διοίκησης), επιχειρησιακή εγγύτητα (π.χ. υποστηριζόμενες/ μονάδες υποστήριξης, κοινές αποστολές), κοινωνική εγγύτητα, εγγύτητα επιχειρηματικής διαδικασίας. Για παράδειγμα, ένας αρχηγός ομάδας για μια ομάδα πρώτης απάντησης που ανταποκρίνεται σε ένα ατύχημα μπορεί να θέλει να αποκτήσει πληροφορίες για δεδομένα από άλλες ομάδες σε μια κοινή γεωγραφική περιοχή (χωρική εγγύτητα) προκειμένου να αυξήσει την υλικοτεχνική απόδοση, να κατανοήσει καλύτερα τι σχεδιάζουν οι άλλες ομάδες ή τι κάνουν (οργανωτική εγγύτητα) προκειμένου να συντονιστούν καλύτερα ή να λάβουν αξιολογήσεις και άλλες πληροφορίες που αναπτύχθηκαν από μια ήδη αναπτυγμένη ομάδα υποστήριξης (επιχειρησιακή εγγύτητα) προκειμένου ο προγραμματισμός να είναι πιο αποτελεσματικός.

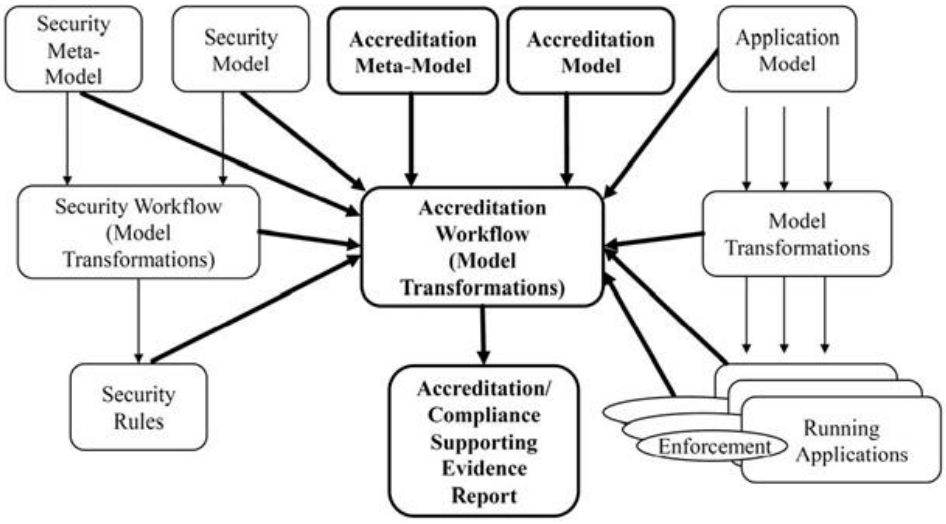
Προκειμένου να καταστεί το ABAC και το PBAC διαχειρίσιμο, στην πληροφορική, χρησιμοποιείτε η "ασφάλεια βάσει μοντέλου" (MDS), η οποία - στη συγκεκριμένη εφαρμογή του Πλαισίου Διαχείρισης Πολιτικής ICSI OpenPMF αποτελείται από διάφορα μέρη.

Ο αυτοματισμός του μοντέλου πολιτικής ασφαλείας, είναι το εργαλείο που υποστηρίζει την διαδικασία μοντελοποίησης των απαιτήσεων ασφαλείας, σε υψηλό επίπεδο αφαίρεσης και χρήσης άλλων πηγών πληροφοριών που είναι διαθέσιμες για το σύστημα (που παράγονται από άλλα ενδιαφερόμενα μέρη). Αυτές οι είσοδοι, οι οποίες στο ISCI εκφράζονται σε Domain Specific Languages (DSL), στη συνέχεια μετατρέπονται σε επιβαλλόμενους κανόνες ασφαλείας με όσο το δυνατόν λιγότερη ανθρώπινη παρέμβαση.



Η αυτοματοποίηση της διαπίστευσης ασφαλείας (βάσει μοντέλων), αυτοματοποιεί την ανάλυση της ανιχνεύσιμης αντιστοιχίας μεταξύ της εφαρμογής της τεχνικής πολιτικής ασφάλειας (π.χ. ABAC) και των απαιτήσεων διασφάλισης πληροφοριών, που αποτυπώνονται σε "μη παραμορφωμένα" μοντέλα απαιτήσεων (π.χ. Κοινά κριτήρια, στόχοι ελέγχου). Τεκμηριώνει επίσης "αποδεικτικά στοιχεία" για διαπίστευση με βάση διάφορες πληροφορίες (π.χ. σχεδίαση – χρόνος συστήματος / μοντέλα ασφαλείας, σύστημα/τεχνουργήματα ασφάλειας, μετασχηματισμοί συστήματος/μοντέλων ασφαλείας και αρχεία καταγραφής χρόνου εκτέλεσης συμβάντων συστήματος/ασφάλειας). Επιπλέον, επιτρέπει την αυτοματοποιημένη ανίχνευση και ανάλυση αλλαγών για να προσδιορίσει εάν η διαπίστευση εξακολουθεί να ισχύει. Λειτουργεί επίσης ως εργαλείο υποστήριξης αποφάσεων.

Το ABAC και το PBAC είναι πολύ νέες και καινοτόμες προσεγγίσεις για τον έλεγχο πρόσβασης, οι οποίες είναι οι πιο χρήσιμες για την προστασία του ITS, των Υπηρεσιών που βασίζονται στη Θέση και άλλων πολύπλοκων εφαρμογών που απαιτούν κάτι περισσότερο από απλό έλεγχο πρόσβασης βάσει ταυτότητας ή ρόλου. Έχει αναλυθεί η χρησιμότητα των ABAC και PBAC για τον έλεγχο πρόσβασης και το φιλτράρισμα πληροφοριών στο ICSI, τόσο από πλευράς λειτουργικότητας όσο και από πλευράς υλοποίησης.



Το ABAC/PBAC επιτρέπει πλέον τον καθορισμό και την επιβολή πολιτικών με τους όρους του τομέα εφαρμογής, όπως για παράδειγμα οι χειριστές (π.χ. διαχειριστές κυκλοφορίας, πρώτοι ανταποκριτές, αστυνομικοί) που είναι υπεύθυνοι για μια συγκεκριμένη γεωγραφική περιοχή ή σε ένα συγκεκριμένο πλαίσιο (έκτακτη ανάγκη ή έκτακτες καταστάσεις όπως το κακό καιρός). Μειώνει επίσης την «ευθραυστότητα» των πολιτικών ασφαλείας, επειδή είναι λιγότερο περίπλοκες και πιο κοντά στην επιχειρηματική λειτουργικότητα του συστήματος, σε αντίθεση με έναν τεράστιο αριθμό πολύπλοκων κανόνων που κανείς δεν καταλαβαίνει. Το μεγαλύτερο πλεονέκτημα είναι η δυνατότητα καθορισμού και εφαρμογής καλύτερου απορρήτου των χρηστών, επειδή η ροή πληροφοριών μπορεί πλέον να ελεγχθεί με πολύ πιο λεπτομερή τρόπο.

Η έρευνά που έγινε τόσο στο έργο ICSI όσο και σε άλλα έργα, έδειξε ότι η υλοποίηση ως μέρος του OpenPMF είναι εφικτή τόσο για επικοινωνίες αιτήματος/απάντησης όσο και για δημοσίευση/συνδρομές (π.χ. DDS) . Στην περίπτωση του DDS είναι πολύ πιο περίπλοκη και πιο απαιτητική. Το Object Security έχει αναπτύξει μια βιώσιμη υλοποίηση ως Access Control SPI του DDS Security 1.0 Beta1, με βάση την τρέχουσα υλοποίηση, η οποία υποστηρίζει DAC/RBAC, λαμβάνοντας υπόψη πρόσθετες πληροφορίες και κάνοντας πρόσθετη επεξεργασία όπως αναλύεται παρακάτω.

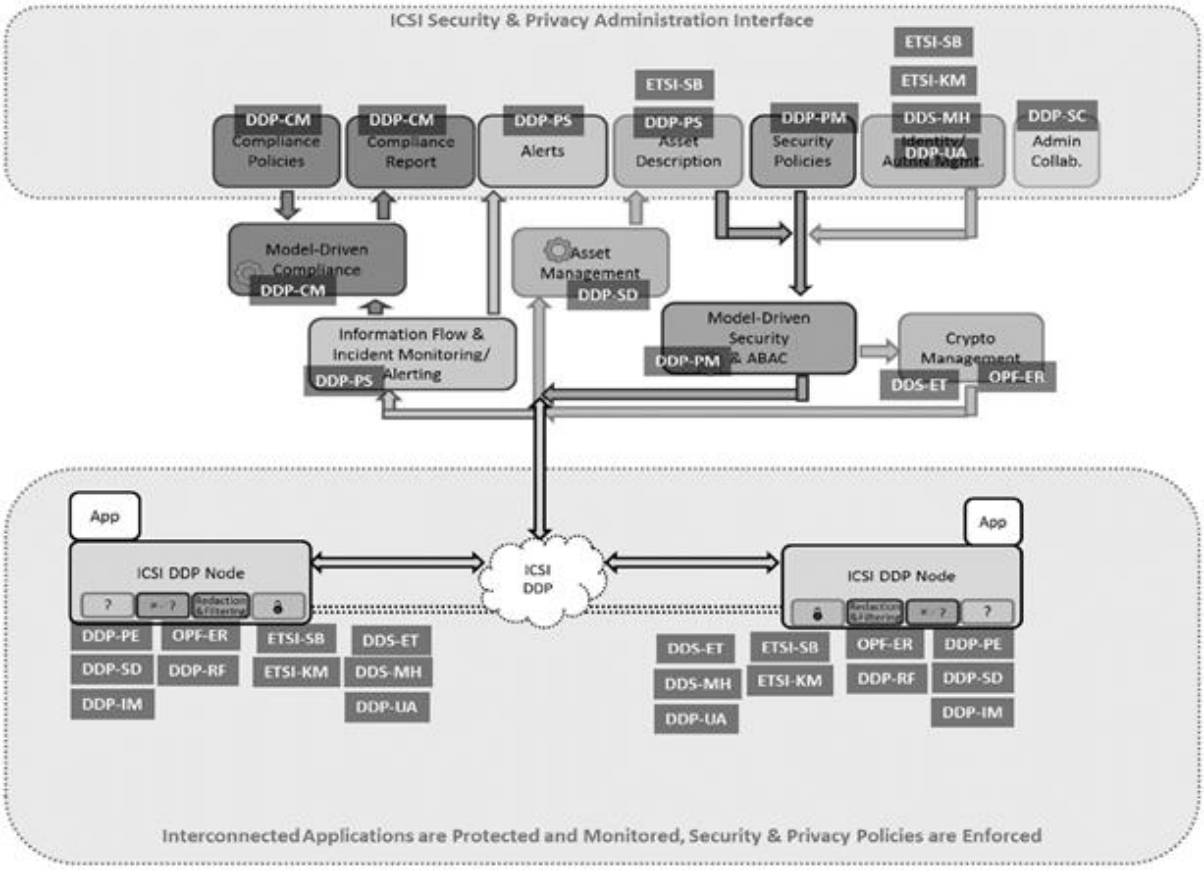
iii. ICSI DPP Security & Privacy Architecture

Η αρχιτεκτονική ασφάλειας και απορρήτου ICSI[5] που φαίνεται στην παρακάτω εικόνα (Εικόνα 3) περιλαμβάνει ασφάλεια ETSI M2M, ασφάλεια DDS, καθώς και MDS με ABAC και PBAC, απόρρητο και αξιοπιστία. Αυτά τα χαρακτηριστικά ασφαλείας συνδυάζονται στη μεγαλύτερη εικόνα μιας ολοκληρωμένης αρχιτεκτονικής ασφάλειας και απορρήτου ICSI, η οποία περιλαμβάνει τον ορισμό πολιτικής, τη διαχείριση πολιτικής και, τέλος, την επιβολή πολιτικής και την παρακολούθηση. Η αρχιτεκτονική PBAC της ICSI βασίζεται στην ενσωμάτωση του MDS με το ABAC, τη σύνταξη/φιλτράρισμα και τις δυνατότητες απορρήτου, στο πλαίσιο ενός περιβάλλοντος εφαρμογής ενδιάμεσου λογισμικού που βασίζεται σε DDS. Η αρχιτεκτονική ασφάλειας και απορρήτου ICSI πρέπει να εφαρμόζει τις απαιτήσεις ασφάλειας και απορρήτου των διαφορετικών ενδιαφερομένων μερών, αλλά σε σύγκριση με τις τυπικές εφαρμογές Ιστού, υπάρχουν ορισμένες τεχνικές προκλήσεις.

- Το σύστημα ICSI είναι ετερογενές και υλοποιείται χρησιμοποιώντας διαφορετικές πλατφόρμες ενδιάμεσου λογισμικού.
- Το σύστημα ICSI είναι πολύ κατανεμημένο, τόσο λογικά όσο και γεωγραφικά. Αποτελείται από έναν αριθμό ανεξάρτητων κόμβων.
- Η περίπλοκη κατανεμημένη αρχιτεκτονική και οι αλληλεπιδράσεις του ICSI εγείρουν ένα επιπλέον σημαντικό ζήτημα. Πώς να ορίσουμε, να διαχειριστούμε και να επιβάλλουμε πολιτικές ασφαλείας στο ICSI.

Η λύση βασίζεται σε μια ανάπτυξη του OpenPMF Policy Management Framework[64] που αναπτύχθηκε για την προστασία πολύπλοκων κατανεμημένων συστημάτων.

Η συνολική αρχιτεκτονική ασφάλειας και απορρήτου ICSI αποτελείται από τα ακόλουθα στοιχεία τεχνολογίας, τα οποία απλώνονται γύρω από τα κύρια αρχιτεκτονικά χαρακτηριστικά, όπως παρουσιάζεται παρακάτω.



DDP-PM, (Policy Management) : Διαχείριση πολιτικών (συμπεριλαμβανομένου OPF-PM). Βασίζεται στον αυτοματισμό πολιτικών OpenPMF MDS, υποστηρίζει διαχειρίσιμη, διαισθητική, με επίκεντρο τον χρήστη, με δυνατότητα σύνταξης πολιτικής ασφάλειας και απορρήτου (S&P), ώστε οι χρήστες να ορίζουν πολιτικές που διέπουν τους χρήστες, τα συστήματα, τις εφαρμογές και τις αλληλεπιδράσεις (ροές πληροφοριών).

DDP-PE, (Policy Enforcement) : Αυτοματοποιημένη επιβολή πολιτικής και ειδοποίησης (περιλαμβάνει OPF-PE). Βασίζεται σε OpenPMF ABAC, PBAC, επιβολή επεξεργασίας και φιλτραρίσματος τεχνικών κανόνων S&P και διαμορφώσεων που δημιουργούνται από το DDP-PM τεχνικά (έλεγχος πρόσβασης, εμπιστευτικότητα κ.λπ.) σε όλο το IT τοπίο (πολλαπλά επίπεδα του συστήματος /εφαρμογή /δίκτυο /εικονική μηχανή κ.λπ.), σε όλο τον κύκλο ζωής των πληροφοριών και στον κύκλο ζωής του λογισμικού.

DDP-RF, (Redaction & Filtering) : Μια υπηρεσία επεξεργασίας και φιλτραρίσματος που βασίζεται σε ABAC στο OpenPMF, η οποία ρωτά την πηγή δεδομένων (κυρίως το περιεχόμενο του μηνύματος, αλλά ενδεχομένως και μια βάση δεδομένων) και καθοδηγεί τη λήψη αποφάσεων/επιβολής του ABAC. Αυτή η αρχιτεκτονική έχει σχεδιαστεί για ευελιξία.

DDP-CM, (Compliance Management) : Διαχείριση και αυτοματοποίηση συμμόρφωσης (περιλαμβάνει OPF-CM). Με βάση την αυτοματοποίηση της διαπίστευσης OpenPMF MDS, συσχετίζει αυτόματα, αναλύει και τεκμηριώνει την ανιχνεύσιμη αντιστοιχία μεταξύ της εφαρμογής της τεχνικής πολιτικής ασφάλειας (π.χ. ABAC, ροές πληροφοριών, συμβάντα, περιουσιακά στοιχεία, πολιτικές ασφαλείας και

άλλες πληροφορίες) και των απαιτήσεων διασφάλισης πληροφοριών που αποτυπώνονται σε μοντέλα απαιτήσεων που δεν έχουν παραμορφωθεί.

DDP-SD, (System of Systems Discovery) : Βασίζεται στην υπηρεσία εντοπισμού RTI DDS[65] (περιλαμβάνει OPF-SD) που επιτρέπει τον αυτόματο εντοπισμό περιουσιακών στοιχείων, καθώς και εκδοτών/συνδρομητών. Το σύστημα προαιρετικά δημιουργεί αυτόματα ένα μοντέλο ("περιγραφή συστήματος") των εταιρικών δικτύων, συστημάτων, εφαρμογών, ροών πληροφοριών και χρηστών. Αυτό χρησιμοποιείται για σκοπούς παρακολούθησης και επίσης τροφοδοτεί το MDS.

DDP-IM, (Incident Monitoring) : Η Παρακολούθηση περιστατικών (περιλαμβάνει OPF-IM). Με βάση ένα σύστημα ανίχνευσης εισβολής τρίτου μέρους (IDS) και σύστημα πρόληψης εισβολής (IPS) (Promia Raven), τα περιστατικά παρακολουθούνται και μετριάζονται.

DDP-PS, (Presentation of current Status) : Παρουσίαση Τρέχουσας Κατάστασης (περιλαμβάνει OPF-PS) . Βασισμένο σε προϊόν διαχείρισης περιουσιακών στοιχείων τρίτου μέρους (Promia) εμφανίζει την τρέχουσα στάση του S&P, σε συνεχή βάση με ενοποιημένο τρόπο, χρησιμοποιώντας τη δυνατότητα παρακολούθησης του OpenPMF.

DDP-ER, (Encryption for data at Rest) : Κρυπτογράφηση για δεδομένα σε κατάσταση ηρεμίας (περιλαμβάνει OPF-ER). Βασίζεται σε τυπικούς αλγόριθμους για την κρυπτογράφηση και τον έλεγχο της ακεραιότητας των δεδομένων. Η διαχείριση του υλικού του κρυπτογραφικού κλειδιού γίνεται με χρήση ETSI-KM. Η κρυπτογραφία διαμορφώνεται και διαχειρίζεται με ενιαίο τρόπο μαζί με τις άλλες πολιτικές στο DDP-PM.

DDS-ET, (Encryption for Data in Transit) : Κρυπτογράφηση για δεδομένα κατά τη μεταφορά (περιλαμβάνει OPF-ET). Βασίζεται στην προστασία μηνυμάτων (κρυπτογραφούνται) που παρέρχονται από το DDS Security. Η διαχείριση του υλικού κρυπτογραφικού κλειδιού γίνεται με χρήση ETSI-KM.

DDP-UA, (User Continuous Authentication) : Συνεχής έλεγχος ταυτότητας χρήστη (περιλαμβάνει OPF- AH). Βασισμένο σε εργαλεία τρίτων, έλεγχος ταυτότητας με βάση έως και πέντε (5) παράγοντες. Δηλαδή ο κωδικός πρόσβασης ή το PIN που έχει απομνημονεύσει ο χρήστης, (ένας κρυπτογραφικά ασφαλής κωδικός πρόσβασης ή διακριτικό) βασίζεται στον χρόνο, τα μοτίβα του προσώπου που ταιριάζουν με επιτυχία, την τοποθεσία του χρήστη καθώς και ο χρόνος αιτήματος από τον χρήστη. Εάν οι χρήστες συσχετίζονται απευθείας με συμμετέχοντες στο DDS, τότε θα χρησιμοποιηθούν επίσης οι δυνατότητες ελέγχου ταυτότητας DDS Security. Η διαχείριση του υλικού κρυπτογραφικού κλειδιού γίνεται με χρήση ETSI-KM, εάν είναι εφικτό. Η διαχείριση των ταυτοτήτων των χρηστών γίνεται στο DDP'S, στη διεπαφή διοίκησης της διαχείρισης των ταυτοτήτων.

DDP-MA, (Machine Continuous Authentication) (περιλαμβάνει OPF-AH). Έλεγχος ταυτότητας από μηχανή σε μηχανή που βασίζεται σε χαρακτηριστικά ελέγχου ταυτότητας DDS Security στο επίπεδο DDS (προαιρετικά με έλεγχο ταυτότητας ETSI M2M Security Architecture για το επίπεδο δικτύου). Η διαχείριση του υλικού του κρυπτογραφικού κλειδιού γίνεται με χρήση ETSI-KM.

ETSI-KM, (Cryptographic Key Management) : Η Διαχείριση των κρυπτογραφικών κλειδιών. Για να λειτουργήσει το ICSI DDP S&P, πρέπει να γίνει διαχείριση ενός αριθμού κρυπτογραφικών κλειδιών. Το ETSI M2M Security Architecture παρέχει ένα χρήσιμο πλαίσιο βασισμένο σε πρότυπα για αυτόν τον σκοπό, το οποίο επαναχρησιμοποιείται για το ICSI DDP.

ETSI-SB, (Secure Machine Bootstrap) : Μόνο οι συσκευές των οποίων η ακεραιότητα (κρυπτογραφική, δακτυλικό αποτύπωμα ή άλλη) έχει επαληθευτεί επιτρέπεται να επικοινωνούν στον κορμό του ICSI DDP. Το ETSI M2M Security Architecture παρέχει ένα χρήσιμο πλαίσιο βασισμένο σε πρότυπα για αυτόν τον σκοπό, το οποίο χρησιμοποιείτε και για το ICSI DDP.

DDP-SC, (Security Administrator Collaboration:) : Συνεργασία διαχειριστών ασφαλείας (περιλαμβάνει το OPF-SC). Η λύση περιλαμβάνει επίσης έναν τρόπο συνεργασίας των διαχειριστών για την επίλυση προβλημάτων, όπως για παράδειγμα. ένα ασφαλές κοινωνικό δίκτυο για τη διευκόλυνση της συνεργασίας μεταξύ των διαχειριστών.

iv. DDP Platform Security: DDS Security

Μία από τις καινοτομίες της αρχιτεκτονικής ασφάλειας ICSI είναι η ανάπτυξη μιας διαχειρίσιμης λύσης ασφάλειας για το μεγάλης κλίμακας, διασυνδεδεμένο τοπίο πληροφορικής της ICSI's που περιλαμβάνει εκδότες και συνδρομητές.

Η Υπηρεσία Διανομής Δεδομένων[7] για Συστήματα Πραγματικού Χρόνου (DDS) είναι μία ομάδα διαχείρισης αντικειμένων (OMG- Object Management Group) από μηχανή σε μηχανή που στοχεύει να επιτρέψει την κλιμάκωση, σε πραγματικό χρόνο, αξιόπιστα, υψηλής απόδοσης δια λειτουργικών ανταλλαγών δεδομένων μεταξύ εκδοτών και συνδρομητών. Το DDS εφαρμόζει ένα μοντέλο δημοσίευσης/συνδρομής για την αποστολή και λήψη δεδομένων, συμβάντων και εντολών μεταξύ των κόμβων. Οι κόμβοι που παράγουν πληροφορίες (εκδότες) δημιουργούν "θέματα" (π.χ. θερμοκρασία, τοποθεσία, πίεση) και δημοσιεύουν "δείγματα". Το DDS παραδίδει τα δείγματα σε συνδρομητές που δηλώνουν ενδιαφέρον για αυτό το θέμα. Δηλαδή το DDS χειρίζεται αυτόματα τις δουλειές της μεταφοράς. Οποιοσδήποτε κόμβος μπορεί να είναι εκδότης, συνδρομητής ή και τα δύο ταυτόχρονα. Οι επικοινωνίες DDS αποσυνδέονται και το μοντέλο δημοσίευσης-συνδρομής DDS εξαλείφει ουσιαστικά τον πολύπλοκο προγραμματισμό δικτύου για κατανεμημένες εφαρμογές. Έτσι και για το ICSI, το DDS επιτρέπει στο χρήστη να προσδιορίσει τις παραμέτρους Quality of Service (QoS) για να διαμορφώσει εκ των προτέρων τους μηχανισμούς εντοπισμού και συμπεριφοράς.

1. Ασφάλεια DDS

Η προδιαγραφή DDS Security προωθείται από μια ομάδα εταιρειών στον τομέα DDS. Η εργασία γίνεται πάνω στην προδιαγραφή, προκειμένου να λυθούν ζητήματα που σχετίζονται με την ασφάλεια, (με την τρέχουσα προδιαγραφή DDS) παρέχοντας τα απαραίτητα χαρακτηριστικά ασφαλείας (έλεγχο ταυτότητας, εξουσιοδότηση και έλεγχο πρόσβασης, εμπιστευτικότητα, ακεραιότητα και μη απόρριψη όλων των δεδομένων που αποστέλλονται μέσω του DDS). Εκτός αυτού, καθορίζει επίσης χαρακτηριστικά ελέγχου ασφαλείας. Η προδιαγραφή χωρίζεται σε δύο κύρια μέρη. Το πρώτο αφορά τον ορισμό του μοντέλου ασφαλείας και το δεύτερο καθορίζει μια αρχιτεκτονική διασύνδεσης προσθηκών υπηρεσίας (SPI) για συμβατή υλοποίηση DDS. Το Μοντέλο

Ασφαλείας επιβάλλεται από την εκτέλεση του DDS, με την επίκληση της SPI's διεπαφής υλοποιήσεων.

Η ασφάλεια των συστημάτων Publish / Subscribe γενικά είναι ένα δύσκολο και όχι πολύ καλά καθιερωμένο θέμα, σε σύγκριση με τις αρχιτεκτονικές Request / Reply, Πρώτα από όλα, το κύριο εννοιολογικό ζήτημα είναι το γεγονός ότι (τουλάχιστον σε συστήματα Publish / Subscribe όπως ως DDS) δεν υπάρχει πλέον πλαίσιο μεταξύ πελάτη και διακομιστή. υπάρχουν απλώς αποσυνδεδεμένοι εκδότες και συνδρομητές. Οι εκδότες στέλνουν μηνύματα σε έναν κοινόχρηστο "χώρο δεδομένων" και δεν γνωρίζουν ποιος λαμβάνει τα μηνύματά τους. Οι συνδρομητές λαμβάνουν μηνύματα από αυτό το σύννεφο και δεν γνωρίζουν ποιος έστειλε τα μηνύματα που έλαβαν. Αυτό καθιστά, για παράδειγμα, την άμεση επιβολή της ιδιότητας, του Υποχρεωτικού Ελέγχου Πρόσβασης, πολύ δύσκολη, επειδή ο εκδότης δεν γνωρίζει ποια άδεια έχει ένας συνδρομητής και εάν επομένως, επιτρέπεται να λάβει το μήνυμα. Η επικοινωνία πραγματοποιείται μέσω "θεμάτων", τα οποία δεν αποτελούν οντότητα ασφαλείας από μόνα τους, απλώς χρησιμοποιούνται για τη δομή του χώρου δεδομένων DDS. Ωστόσο, είναι ο μόνος σύνδεσμος μεταξύ εκδοτών και συνδρομητών, και ως εκ τούτου πρέπει να χρησιμοποιούνται για λόγους ασφαλείας.

Προκειμένου να επιτευχθεί υψηλή απόδοση και επεκτασιμότητα με μεγάλο αριθμό συμμετεχόντων και για την κάλυψη ιδιοτήτων σε πραγματικό χρόνο, οι υλοποιήσεις DDS πολύ συχνά βασίζονται σε επικοινωνία πολλαπλής διανομής και UDP, αντί για TCP. Σε πολλές περιπτώσεις, δεν χρησιμοποιούν επίσης έναν κεντρικό διαμεσολαβητή όπου μπορεί να επιβληθεί ασφάλεια. Αυτό καθιστά αδύνατη τη χρήση τυπικών μηχανισμών ασφαλείας όπως το TLS ή την έκδοση του datagram DTLS, καθώς και την τυπική εξουσιοδότηση σε ένα μόνο σημείο.

Οι συγγραφείς έχουν εμπειρία με την εφαρμογή μιας αποκλειστικής υπηρεσίας ασφαλείας DDS στο παρελθόν και τώρα έχουν εφαρμόσει και αξιολογήσει τον έλεγχο πρόσβασης που βασίζεται στο OpenPMF πάνω από το πρωτότυπο DDS Security της RTI, το οποίο περιγράφεται παρακάτω.

2. DDS Security & OpenPMF Integration Prototype for ICSI

Για την αρχική εργασία ICSI DDP Security & Privacy Architecture, χρησιμοποιήθηκε το πρωτότυπο DDS Security, από τον κορυφαίο προμηθευτή DDS Real Time Innovations (RTI). Το DDS Security παρέχεται από την RTI με τη μορφή πηγαίου κώδικα, με την ελπίδα να προωθηθεί η ενοποίηση και η χρήση της ασφάλειας στον τομέα της εφαρμογής DDS. Η πρόσβαση στον πηγαίο κώδικα είναι επίσης πολύ επωφελής για τρίτους που ασχολούνται με την αναβάθμιση των πλαισίων ασφαλείας, καθώς δεν χρειάζεται να εφαρμόσουν πλήρη λειτουργικότητα των SPI, αλλά μπορούν απλώς να επαναχρησιμοποιήσουν ό,τι παρέχεται ήδη στον κώδικα του RTI και να ενσωματωθούν απευθείας με τα είδη υλοποιημένα πρόσθετα που έχουν αναλυθεί καλά και δοκιμαστεί. Η ομάδα του Object Security έχει ακολουθήσει αυτήν ακριβώς την προσέγγιση για την ενσωμάτωση του Object Security OpenPMF Policy Management Framework στην υλοποίηση του DDS Security. Δεδομένου ότι το ίδιο το OpenPMF είναι κυρίως ένα πλαίσιο ελέγχου πρόσβασης, έχει ενσωματώσει απευθείας στο παρεχόμενο πρόσθετο Access Control Service.

Η RTI αποφάσισε να εφαρμόσει το μεγαλύτερο μέρος της υλοποίησης DDS στη γλώσσα προγραμματισμού C. Αυτή η σχεδιαστική απόφαση ανοίγει ένα ευρύ φάσμα

δυνατοτήτων για τις θύρες αρχιτεκτονικής DDS και επιτρέπει επίσης στο RTI να υποστηρίζει ένα ευρύ φάσμα γλωσσών προγραμματισμού. Από την άλλη πλευρά, αυτή η προσέγγιση περιπλέκει κάπως την τεχνική ενοποίησης με πρόσθετα τρίτων.

Η υλοποίηση του DDS Security του RTI μεταγλωττίζεται στο αρχείο κοινόχρηστης βιβλιοθήκης librtisecurity.so. Το αρχείο περιέχει υλοποιήσεις όλων των απαραίτητων SPIs ασφαλείας του DDS. Αυτό το αρχείο ενδέχεται να μην συνδεθεί απευθείας στην εφαρμογή DDS, καθώς το RTI DDS υποστηρίζει δυναμική φόρτωση κοινόχρηστων βιβλιοθηκών όταν απαιτείται από τις ιδιότητες QoS της εφαρμογής. Με αυτόν τον τρόπο ένα μεμονωμένο δυαδικό αρχείο εφαρμογής DDS μπορεί να υποστηρίξει ασφάλεια όταν χρειάζεται και να εκτελείται χωρίς καμία ασφάλεια όταν δεν απαιτείται. Όπως ήδη αναφέρθηκε παραπάνω, η μόνη διεπαφή υπηρεσίας που είναι σημαντική για το OpenPMF είναι το πρόσθετο Access Control Service. Χρειάστηκε να επεκταθεί αυτή η υπηρεσία διεπαφής, για να γίνει σωστή επιβολή της πολιτικής ασφαλείας που βασίζεται στο OpenPMF.

Η επέκταση είναι ενσωματωμένη σε δύο λειτουργίες του πρόσθετου, οι οποίες καλούν το OpenPMF Policy Enforcement Point (PEP) για να αξιολογήσει την πολιτική ασφαλείας και εάν η πολιτική που διαχειρίζεται το OpenPMF αρνηθεί την επίκληση, τότε αναγκάζει τη συνάρτηση AccessControl να επιστρέψει την τιμή DDS_BOOLEAN_FALSE ως τιμή επιστροφής. Με αυτόν τον τρόπο, η επίκληση απορρίπτεται επίσης από το ίδιο το πρόσθετο της DDS (DDS security Access Control Service plugin). Προκειμένου η εφαρμογή DDS να χρησιμοποιεί την επιβολή ασφαλείας OpenPMF, ο πηγαίος κώδικας της τροποποιήθηκε ελαφρώς.

Όπως αναφέρθηκε παραπάνω, το RTI DDS έχει υλοποιηθεί σε καθαρό κώδικα C, επειδή γίνεται χρήση σε πραγματικό χρόνο, αλλά και για φορητότητα με τους wrappers και τους προσαρμογείς που παρέχονται για την υλοποίηση . Στην συγκεκριμένη περίπτωση ως dropped γλώσσα, για την ανάπτυξη εφαρμογής ενσωμάτωσης, στο OpenPMF DDS χρησιμοποιήθηκε η Java γλώσσα προγραμματισμού.

v. Συμπεράσματα

Με βάση τα παραπάνω παρουσιάζεται μια σύντομη ανάλυση της ασφάλειας ITS και μια επισκόπηση της αρχιτεκτονικής ασφάλειας ITS για το έργο ICSI ITS. Πρώτα από όλα παρουσιάζονται οι απαιτήσεις ασφαλείας που πρέπει να επιβληθούν στο ICSI. Την προστασία του ίδιου του συστήματος ICSI, την προστασία των δεδομένων της εφαρμογής και το απόρρητο των χρηστών. Εξετάστηκε επίσης εν συντομία η ασφάλεια ETSI M2M και τα σημαντικά κενά που εντοπίστηκαν γύρω από τον σημερινό έλεγχο πρόσβασης και την επιβολή απορρήτου για το ICSI DDP.

Στη συνέχεια παρουσιάστηκαν δύο βασικές πτυχές στο έργο ISCI:

Πρώτον, η εργασία στον προηγμένο έλεγχο πρόσβασης (βασισμένο σε εγγύτητα και επεξεργασία και φιλτράρισμα) είναι η βάση για την προστασία του απορρήτου των χρηστών στο ICSI, επειδή στο ISCI τα τυπικά μοντέλα ελέγχου πρόσβασης όπως τα DAC, RBAC και MAC δεν επαρκούν. Το μεγαλύτερο μέρος της ερευνητικής εργασίας στο έργο ISCI ήταν εννοιολογικό, αλλά δύο πρώτα πρωτότυπα υλοποιούνται. Παρουσιάστηκαν προηγμένες προσεγγίσεις ελέγχου πρόσβασης που βασίζονται στην εγγύτητα και στη διόρθωση και το φιλτράρισμα, μια αρχιτεκτονική απορρήτου που βασίζεται στις έννοιες του Privacy By Design. και την εφαρμογή του Πλαισίου Διαχείρισης Πολιτικής OpenPMF.

Δεύτερον, παρουσιάστηκε μια αρχιτεκτονική και υλοποίηση ασφάλειας για την Υπηρεσία Διανομής Δεδομένων OMG. Η αρχιτεκτονική και η υλοποίηση ασφαλείας DDS, η οποία είναι διαθέσιμη ως πρωτότυπο που επιβάλλει πολιτικές ασφαλείας βάσει θεμάτων, εκδοτών και συνδρομητών, είναι η βάση για την προστασία της υποδομής του ICSI DDP. Η πρωτότυπη εφαρμογή βασίζεται στα επερχόμενα πρότυπα ασφαλείας OMG και αξιοποιεί τη λειτουργικότητα OpenPMF για καθορισμό και διαχείριση πολιτικής με βάση την "ασφάλεια βάσει μοντέλου", καθώς και για την καταγραφή, προκειμένου να εφαρμοστεί η υπευθυνότητα, όπως απαιτείται από τους κανονισμούς προστασίας δεδομένων.

5. Μεθοδολογίες STRIDE & DREAD

i. Ποιοτική Εκτίμηση Κινδύνου - Qualitative Risk Assessment

Με τον όρο ποιοτική ανάλυση κινδύνου εννοούμε κάποια τεχνική που θα χρησιμοποιήσουμε για να «μετρήσουμε» τα αποτελέσματα ενός συγκεκριμένου κίνδυνου. Η αξιολόγηση αυτή του κινδύνου χρησιμοποιείται για πιθανά και αβέβαια γεγονότα που θα μπορούσαν να έχουν πολλά και διάφορα αποτελέσματα και τα οποία στη συνέχεια θα μπορούσαν να δημιουργήσουν άλλες σημαντικές συνέπειες. Ο κίνδυνος προκύπτει από τη συνάρτηση των πιθανοτήτων των γεγονότων (ένας συγκεκριμένος κίνδυνος που μπορεί να συμβεί) και των συνεπειών που θα ακολουθήσουν αυτό το συμβάν. Η πιθανότητα αναφέρεται στο κατά πόσο είναι δυνατόν προκύψει ένας κίνδυνος. Κάνοντας μια ποιοτική αξιολόγηση, οι πιθανότητες και οι συνέπειες δεν εκτιμώνται αριθμητικά, αλλά αξιολογούνται προσδιορίζοντας τις με κλίμακες όπως υψηλή, χαμηλή πιθανότητα κτλ ώστε να μπορούμε να φτάσουμε στο σημείο να γίνουν αριθμητικές εκτιμήσεις πιθανοτήτων ή συνεπειών. Από τη στιγμή που θα εισαχθούν αριθμοί στην ανάλυση μας, ποσοτικοποιώντας είτε την πιθανότητα ενός κινδύνου είτε τις συνέπειες, η ανάλυση μεταβαίνει σε μια ποσοτική, ή έστω ημιποσοτική εκτίμηση κινδύνου.

ii. STRIDE

Η μέθοδος STRIDE[66] είναι αναπτύχθηκε από τη Microsoft το 1999 και διαπραγματεύεται τη δημιουργία ενός μοντέλου αξιολόγησης και διαχείρισης των απειλών στον κυβερνοχώρο. Μέσω της STRIDE εδραιώνεται μια διαδικασία εντοπισμού και ανάλυσης έξι χαρακτηριστικών απειλών του κυβερνοχώρου. Αυτές επεξηγούνται στον ακόλουθο πίνακα:

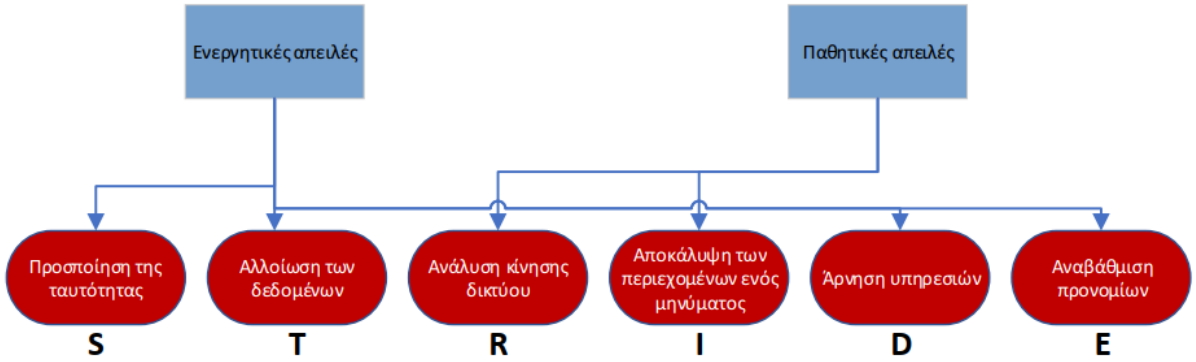
Spoofing	Παραβίαση της Αυθεντικοποίησης (Authentication)	Αφορά την προστασία της πληροφορίας από μη εξουσιοδοτημένη μεταβολή, τροποποίηση ή διαγραφή
Tampering	Παραβίαση της Ακεραιότητας (Integrity)	Αφορά την προστασία της πληροφορίας από μη εξουσιοδοτημένη μεταβολή, τροποποίηση ή διαγραφή
Repudiation	Παραβίαση της Αδυναμίας Αποποίησης (Non-Repudiation)	Αφορά την διαδικασία αδιαμφισβήτητου καταλογισμού ευθύνης για την επιτέλεση μιας ενέργειας στο σύστημα
Information Disclosure	Παραβίαση της Εμπιστευτικότητας (Confidentiality)	Αφορά την προστασία της πληροφορίας από μη εξουσιοδοτημένη αποκάλυψή ή ανάγνωση

Denial of Service	Παραβίαση της Διαθεσιμότητας (Availability)	Αφορά τη διαφύλαξη της εξουσιοδοτημένης πρόσβασης, είτε από αποκάλυψη είτε από μεταβολή της πληροφορίας χωρίς εμπόδια ή/και καθυστέρηση.
Elevation of Privileges	Παραβίαση της Εξουσιοδότησης (Authorization)	Αφορά τη διαδικασία λήψης απόφασης σχετικά με την αποδοχή ή απόρριψη αιτήματος πρόσβασης αυθεντικοποιημένης οντότητας στο σύστημα βάση δικαιωμάτων πρόσβασης που της έχουν ήδη εκχωρηθεί και της πολιτικής ελέγχου πρόσβασης του συστήματος

Από το αρχικό γράμμα της κάθε χαρακτηριστικής απειλής σχηματίζεται το ακρωνύμιο STRIDE. Όπως βλέπουμε και στον πίνακα κάθε μία από αυτές τις απειλές αντιστοιχεί στην παραβίαση μιας άκρως επιθυμητής ιδιότητας, που είναι και στόχος ασφαλείας στη ύπαρξη και τη μελέτη ενός συστήματος.

Το STRIDE μπορεί να χρησιμοποιηθεί για την ανάλυση απειλών σε συστήματα που βρίσκονται σε διάφορες φάσεις ανάπτυξης, ακόμη και στο στάδιο του σχεδιασμού και έτσι τηρούνται οι αρχές ασφάλειας-σχεδιασμού[67].

Παρόλο που σχεδιάστηκε αρχικά για συστήματα λογισμικού, το STRIDE χρησιμοποιείται σε οικοσυστήματα τα οποία είτε έχουν ένα σημαντικό τμήμα είτε είναι εξ ολοκλήρου Cyber-Physical[68,70]. Συγκεκριμένα, μια τροποποιημένη έκδοση του STRIDE προτάθηκε και χρησιμοποιήθηκε στην Παραπομπή 45 για να μοντελοποιήσει απειλές, να αναπτύξει σενάρια κυβερνοεπιθέσεων και να αξιολογήσει ποιοτικά τους αντίστοιχους κινδύνους για έναν αριθμό Cyber Physical Systems (εφεξής CPS) στο οικοσύστημα C-ES (Cyber Enabled Ship). Με τις αντίστοιχες προσαρμογές και παραμετροποιήσεις η μέθοδος STRIDE είναι ένα από τα βασικά εργαλεία μας για την επιλογή βέλτιστης επιλογής στρατηγικών κυβερνοασφάλειας σε ITS (intelligent Transport Systems).



Όπως προείπαμε η STRIDE είναι μια μέθοδος μοντελοποίησης πιθανών απειλών. Αντίστοιχα όπως γίνεται πρόταση και στη συναφή εργασία «Cyber-attacks against the autonomous ship»[45] έτσι και εδώ προτείνουμε τη χρήση μιας τροποποιημένης έκδοσης του STRIDE. Με τη χρησιμοποίηση της θα γίνουν προσπάθειες μοντελοποίησης των απειλών, ανάπτυξης σεναρίων κυβερνοεπιθέσεων και ποιοτικής

αξιολόγησης των αντίστοιχων κινδύνων για τα components των ITS που επιλέξαμε να μελετήσουμε. Τα components αυτά είναι τα παρακάτω:

- Personal Information Device (**PID**) – Ατομικές Συσκευές Πληροφόρησης
- ITS Rodway Equipment (**ITSRE**) – ITS Εξοπλισμός Αυτοκινητόδρομων
- Safety and Security Monitoring Equipment (**SSME**) – Εξοπλισμός Παρακολούθησης Ασφάλειας
- Parking Management System (**PMS**) – Σύστημα Διαχείρισης Στάθμευσης
- Payment Administration Center (**PAC**) – Κέντρο Διαχείρισης και Επιχειρήσεων Πληρωμών
- Transportation Information Center (Including Information Disseminator System) (**TIC**) – Κέντρο Πληροφοριών Μεταφορών (Συμπεριλαμβανομένου του Συστήματος Μετάδοσης Πληροφοριών)
- Maintenance Management Center (**MMC**) – Κέντρο Διαχείρισης Συντήρησης
- Emergency Management Center (**EMC**) – Κέντρο Διαχείρισης Επειγόντων Περιστατικών
- Transit and Traffic Management Center (**TTMC**) – Κέντρο Διαχείρισης Μεταφορών και Συγκοινωνιών
- Data Distribution System (**DDS**) – Σύστημα Διανομής Δεδομένων
- Map Management System (**MMS**) – Σύστημα Διαχείρισης Χαρτών
- Public Transportation Vehicle (**PTV**) – Οχήματα Δημοσίων Μεταφορών
- Private Vehicle (**PV**) – Οχήματα Ιδιωτικής Χρήσης
- Emergency Vehicle OBE (**EVOBE**) – Εξοπλισμός Οχήματος Επειγόντων Περιστατικών

iii. DREAD

Η μέθοδος DREAD είναι ένα μοντέλο εκτίμησης των κινδύνων κινδύνου ασφαλείας που αναπτύχθηκε από τη Microsoft, όπως και το STRIDE, σαν τμήμα μιας διαδικασίας κατασκευής ενός εξελιγμένου συστηματικού τρόπου ανάλυσης κινδύνων. Και εδώ η ονομασία πρόκειται για αρκτικόλεξο. Προκύπτει από τα αρχικά των τμημάτων που κατηγοριοποιήθηκαν οι κίνδυνοι ασφαλείας και σχετίζονται με κάθε σενάριο επίθεσης που θα αναλυθεί. Η ονομασία λοιπόν προκύπτει από τις απειλές όπως αυτές φαίνονται και επεξηγούνται στον παρακάτω πίνακα.[69]

Damage	Ποια είναι η έκταση της ***ζημιάς*** που αναμένεται να προκαλέσει η επίθεση στο σύστημα
Reproducibility	Πόσο εύκολα μπορεί να ***αναπαραχθεί*** / να ξαναγίνει η ίδια επίθεση
Exploitability	Το μέγεθος των πόρων που πρέπει να ***εκμεταλλευτεί*** και χρειάζεται ο αντίπαλος για να ξεκινήσει την επίθεση
Affected users/systems	Πόσα άτομα ή/και συστήματα ***επηρεάζονται***
Discoverability	Πόσο εύκολα μπορεί ο επιτιθέμενος να ***εντοπίσει*** τρωτά σημεία που θα εκμεταλλευτεί για κάνει την επίθεση

STRIDE και DREAD είναι αλληλένδετα. Το μοντέλο STRIDE από την πλευρά του επιτρέπει να γίνεται μία ποιοτική ανάλυση ασφαλείας των συστημάτων. Το μοντέλο DREAD από την δική του μεριά μας «ποσοτικοποιεί» τους κινδύνους που προσδιορίστηκαν. Σύμφωνα με την προσέγγιση στην αναφορά 10 γίνεται κατηγοριοποίηση τιμών ως εξής: Υψηλή, Μέση, Χαμηλή στις μεταβλητές από το μοντέλο DREAD. Αυτές στη συνέχεια σχετίζονται με κάθε απειλή του μοντέλου STRIDE και προσδιορίζονται εφαρμόζοντας συγκεκριμένα σύνολα κριτηρίων όπως αυτά αποτυπώνονται στον ακόλουθο πίνακα. Έχουν γίνει οι απαραίτητες προσαρμογές στο[69] έτσι ώστε να συμπεριληφθούν στοιχεία για περεταίρω ανάλυση από το «Attack Path Analysis for Cyber Physical Systems. In Computer Security: ESORICS» που αναφέρεται σε Cyber Physical Systems (CPS).

Κριτήρια για τον καθορισμό των τιμών των μεταβλητών DREAD (Damage, Reproducibility, Exploitability, Affected, and Discoverability)			
	Υψηλή (3)	**Μέση (2)**	**Χαμηλή (1)**
D	Ο επιτιθέμενος είναι σε θέση να παρακάμψει τους μηχανισμούς ασφαλείας, να αποκτήσει πρόσβαση διαχειριστή, να μεταφορτώσει ή/και να τροποποιήσει τα περιεχόμενα των CPS.	Διαρροή εμπιστευτικών πληροφοριών CPS (λειτουργίες/πηγαίος κώδικας). Μερική δυσλειτουργία/διακοπή του συστήματος.	Διαρροή μη ευαίσθητων πληροφοριών. Η επίθεση δεν είναι δυνατό να επεκταθεί σε άλλα γειτονικά CPS.
R	Η επίθεση μπορεί να αναπαραχθεί ανά πάσα στιγμή.	Ο αντίπαλος είναι σε θέση να αναπαράγει την επίθεση, αλλά υπό συγκεκριμένες συνθήκες κινδύνου.	Αν και ο εισβολέας γνωρίζει τα τρωτά σημεία/σφάλματα του CPS, δεν είναι σε θέση να ξεκινήσει την επίθεση.
E	Η επίθεση μπορεί να πραγματοποιηθεί ακόμα και από έναν αρχάριο αντίπαλο, σε σύντομο χρονικό διάστημα.	Ένας έμπειρος αντίπαλος μπορεί να ξεκινήσει την επίθεση άμεσα.	Η επίθεση απαιτεί ένα εξαιρετικά εξειδικευμένο άτομο και σε βάθος γνώση του στοχοποιημένου CPS.
A	Όλα τα CPS επηρεάζονται.	Επηρεάζονται ορισμένοι χρήστες / συστήματα, με μη-προεπιλεγμένη διαμόρφωση.	Η επίθεση επηρεάζει μόνο το στοχευμένο CPS.
D	Τα τρωτά σημεία του CPS είναι γνωστά και ο εισβολέας μπορεί να έχει πρόσβαση στις σχετικές πληροφορίες για να τα εκμεταλλευτεί.	Τα τρωτά σημεία/σφάλματα του CPS δεν είναι πολύ γνωστά και ο αντίπαλος πρέπει να έχει πρόσβαση στο CPS.	Η απειλή έχει αναγνωριστεί και τα τρωτά σημεία έχουν διορθωθεί.

Στη συνέχεια η τιμή του Ρίσκου (Risk) υπολογίζεται σε σχέση με κάθε κατηγορία απειλής του STRIDE με τη χρήση των ακόλουθων σχέσεων.[67,69,70]

$$Επίπτωση_t^s = \frac{Ζημία + Επηρεαζόμενα\ Συστήματα}{2}$$

$$Πιθανότητα_t^s = \frac{Αναπαραγωγιμότητα + Εκμεταλλευσιμότητα + Ανακαλυπτικότητα}{3}$$

$$Ρίσκο_t^s = \frac{Επίπτωση_t^s + Πιθανότητα_t^s}{2}$$

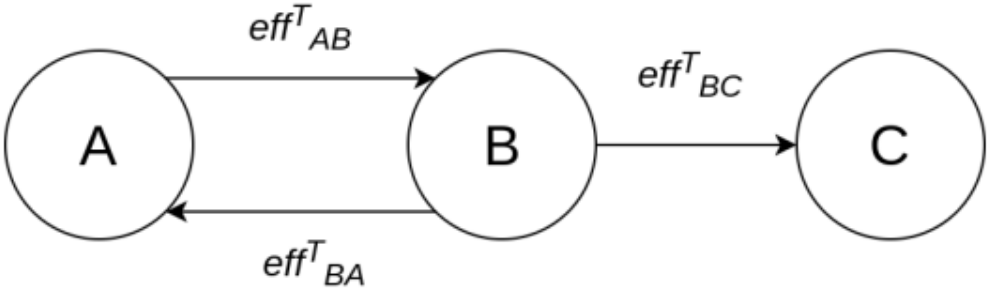
Η μεταβλητή της Επίπτωσης (Impact) αντιπροσωπεύει ένα κάποιο μέτρο των διάφορων επιδράσεων μια επιτυχημένης επίθεσης που κάνει πραγματικότητα και υλοποιεί την απειλή t στο component s. Η Πιθανότητα (Likelihood) αντιπροσωπεύει ένα μέτρο του πόσο πιθανό είναι να υλοποιηθεί η απειλή t στο component s. Αμφότερα STRIDE και DREAD έχουν χρησιμοποιηθεί στο[70] για να εκτιμηθεί το ρίσκο των CPS σε C-ES (Cyber Enabled πλοία).

6. Cyber Ρίσκο: Διάδοση και Άθροιση

i. Μαθηματικό Μοντέλο Συστήματος

Το μαθηματικό μοντέλο διάδοσης και η άθροισης του Cyber ρίσκου που χρησιμοποιείται στην παρούσα εργασία παρουσιάζεται αναλυτικά στην παράγραφο Cyber Risk Propagation and Aggregation του Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems[71] των Γεώργιου Καβαλλιεράτου, Γεώργιου Σπαθούλα και Σωκράτη Κάτσικα.

Ας ξεκινήσουμε υποθέτοντας πως ένα Cyber Physical Σύστημα αποτελείται από N αλληλοεπιδρώντα στοιχεία – περιεχόμενα συστήματα, εφεξής components. Το κάθε ένα από αυτά τα components θα συμβολίζεται με c_i, με i = 1,…..N. Αυτό το σύστημα μπορεί να αναπαρασταθεί με ένα γράφημα N + 1 κόμβων. Το ίδιο το σύστημα αποτελεί και αυτό έναν κόμβο, ο οποίος δηλώνεται σαν ο κόμβος c_0. Στα γραφήματα αυτά υπάρχουν κάποια ακραία σημεία τα οποία αντιπροσωπεύουν πληροφορίες και ροές ελέγχου μεταξύ των κόμβων. Ένα ακραίο σημείο από τον κόμβο A προς τον κόμβο B μας υποδηλώνει πως υπάρχει είτε μια ροή πληροφοριών είτε μια ροή ελέγχου από τον κόμβο A προς τον κόμβο B. Εφόσον λοιπόν υπάρχει μια τέτοια ακραία θέση αυτό που επακολουθεί είναι πως εάν συμβεί ένα περιστατικό κυβερνοασφάλειας στον κόμβο A θεωρείται απολύτως φυσιολογικό να επηρεαστεί και ο κόμβος B.



Για παράδειγμα στο παραπάνω απλό γράφημα, όπου ένα περιστατικό κυβερνοασφάλειας στον κόμβο A θα επηρεάσει και τον κόμβο B επίσης. Από την άλλη ένα περιστατικό κυβερνοασφάλειας στον κόμβο B θα επηρεάσει και τους δύο άλλους κόμβους, τους A και C. Το μέγεθος της αλληλεπίδρασης μεταξύ των κόμβων μπορεί να ποσοτικοποιηθεί ορίζοντας έναν συντελεστή επίδρασης σε κάθε ροή.

Εφεξής αυτά θα συμβολίζονται με eff_{AB}^{α}. Για τη ροή της πληροφορίας θα έχουμε $a=I$ και αντίστοιχα για τη ροή του ελέγχου $a=C$. Ένας τρόπος με τον οποίο μπορούμε να κάνουμε εκχώρηση τιμών σε αυτούς τους συντελεστές είναι χρησιμοποιώντας το

αντίστροφο της κεντρικότητας του βαθμού του κόμβου. Αυτό σημαίνει δηλαδή τον αριθμό των ροών οι οποίες φτάνουν σε αυτόν τον κόμβο και συμβολίζονται με IDC. Ακολουθώντας αυτή την προσέγγιση, υπάρχει τουλάχιστον μία περίπτωση κατά την οποία οι πληροφορίες καταλήγουν στον κόμβο Β μονάχα διαμέσου του κόμβου Α. Σαν αποτέλεσμα αυτής της συνθήκης θα είναι μια πολύ υψηλότερη τιμή για το eff^{I}_{AB} συγκριτικά πάντα με τις περιπτώσεις όπου οι πληροφορίες φτάνουν στον κόμβο διαμέσου περισσότερων κόμβων (αριθμός μεγαλύτερος από 1) συμπεριλαμβανομένου και του Α. Εξ ορισμού οι τιμές οι οποίες επιδρούν στους συντελεστές βρίσκονται στην περιοχή από 0 έως 1 [0,1] και μας δίνουν με τη μορφή ποσοστού τη ζημία που διαδίδεται από τον ένα κόμβο προς τον άλλο. Ο συνολικός συντελεστής επίδρασης eff^{T}_{AB} υπολογίζεται συναρτήσει των eff^{I}_{AB} και eff^{C}_{AB} από την ακόλουθη εξίσωση.

$$\boldsymbol{eff^{T}_{AB} = f(eff^{I}_{AB}, eff^{C}_{AB})}$$

όπου $\boldsymbol{eff^{I}_{AB} = \frac{1}{IDC^{I}_{B}}}$, $\boldsymbol{eff^{C}_{AB} = \frac{1}{IDC^{C}_{B}}}$

Η παραπάνω συνάρτηση f εντός της εξίσωσης πρέπει να δημιουργηθεί σύμφωνα με τις απαιτήσεις που έχει ο τομέας πάνω στον οποίο εφαρμόζεται η μεθοδολογία. Επίσης να διαθέτει τα συγκεκριμένα χαρακτηριστικά των στοιχείων Α και Β όσον αφορά την κρισιμότητα των πληροφοριών και τις ροές ελέγχου μεταξύ τους. Για παράδειγμα, μια επιλογή είναι να επιλεγεί ο μέσος όρος της επιρροής που έχουν οι συντελεστές. Αυτή η επιλογή μας δείχνει πόσο σημαντικές είναι οι ροές των πληροφοριών και οι ροές του ελέγχου για να διαδοθεί και να αθροιστεί εν τέλει το ρίσκο και κατ' επέκταση ο κίνδυνος. Φυσικά και έχει χρησιμοποιηθεί παρακάτω στην παρούσα εργασία. Ένα άλλο χαρακτηριστικό παράδειγμα είναι εκείνο ενός Cyber Physical που στοχεύει κυρίως να ανιχνεύσει και να επεξεργαστεί δεδομένα τα οποία έχουν προέλθει από κάποια διαδικασία, π.χ., έναν έξυπνο μετρητή ηλεκτρικής ενέργειας.

ii. Συνολική Άθροιση του Ρίσκου

Για οποιαδήποτε απειλή t, το συνολικό ρίσκο $R_t^{agg_{cj}}$ του στοιχείου c_j, κι αυτό αφού εκ των προτέρων έχουμε λάβει υπόψη πως λαμβάνει χώρα η χειρότερη περίπτωση είναι στο σενάριο μας, είναι η ακόλουθη:

$$R_t^{agg_{c_j}} = max\,(R_t^{dir_{c_j}}, R_t^{prop_{c_j}})$$

Όπου $R_t^{dir_{cj}}$ είναι το άμεσο ρίσκο, το οποίο ρίσκο είναι εκείνο που όταν το στοιχείο c_j δεν είναι συνδεδεμένο με κανένα άλλο στοιχείο (component) c_k , $k \neq j$. υπολογίζεται από τις εξισώσεις που αναφέραμε στην προηγούμενη παράγραφο για τον υπολογισμό της Επίπτωσης, της Πιθανότητας και του Ρίσκου. Το μεταδιδόμενο ρίσκο $R_t^{prop_{cj}}$ είναι το ρίσκο εκείνο που «συναντά» το c_j εξαιτίας των συνδέσεών του με άλλα στοιχεία components. Οι συνδέσεις αυτές είναι πολύ πιθανόν να μεταπηδούν – μεταφέρονται, πιθανόν και προς τα πολλές και διαφορετικές κατευθύνσεις, ακολουθώντας μία διαδρομή, η αλλιώς ένα «μονοπάτι», p_l από οποιοδήποτε κόμβο k προς έναν άλλο

κόμβο *j*. Αν εφαρμόσουμε ξανά το χειρότερο πιθανό σενάριο για τη μετάδοση του ρίσκου μας το μεταδιδόμενο ρίσκο $R_t^{prop_{cj}}$ υπολογίζεται ως εξής:

$$R_t^{prop_{c_j}} = \max_{p_l} R_t^{prop_{c_j}^{p_l}}$$

όπου το $R_t^{prop_{c_j}^{p_l}}$ είναι το ρίσκο του στοιχείου component c_j το οποίο με τη σειρά του σχετίζεται με την απειλή t και μεταδίδεται δια μέσου της διαδρομής p_l.

Όταν μια απειλή υλοποιείται εναντίον ενός στοιχείου component c_i, επίσης σαν συνέχεια της απειλής θα δημιουργήσει κάποια αποτελέσματα πάνω στο άλλο στοιχείο component c_j, κι αυτό πάντα εφόσον τα στοιχεία components που προαναφέραμε, c_i και c_j είναι συνδεδεμένα. Εφόσον απουσιάζουν στοιχεία ελέγχου, η πιθανότητα να συμβεί κάτι τέτοιο είναι ίση με την πιθανότητα η απειλή να πραγματοποιηθεί εξαρχής εναντίον του c_i. Εν αντιθέσει ο αντίκτυπος που θα έχει αυτό το συμβάν στο c_j εκφράζεται μονάχα με τη μορφή κλάσματος επί του αντίκτυπου που έχει το συμβάν αυτό σε οποιοδήποτε c_k πάνω σε οποιοδήποτε διαδρομή p_l μέσω του οποίου μεταφέρεται η απειλή από το c_i προς το c_j. Αυτό το κλάσμα αντιπροσωπεύεται από $\boldsymbol{eff}_{p_l}^{\boldsymbol{T}}$ το οποίο υπολογίζεται με τον παρακάτω τύπο:

$$\prod_{i=1}^{j-1} \boldsymbol{eff}_{c_i c_i+1}^{\boldsymbol{T}}$$

Αντίστοιχα το ρίσκο, και κατ' επέκταση ο κίνδυνος, που διαδίδεται στη διαδρομή p_l, ο οποίος ξεκινά από τον κόμβο του component c_i και καταλήγει στον κόμβο component c_j υπολογίζεται από τον παρακάτω τύπο:

$$\mathrm{R_t^{prop_{c_j}^{p_l}}} = \frac{\boldsymbol{eff}_{c_i c_j}^{Tp_l} \times Επιπτωση_t^{c_i} + L_t^{C_i}}{2}$$

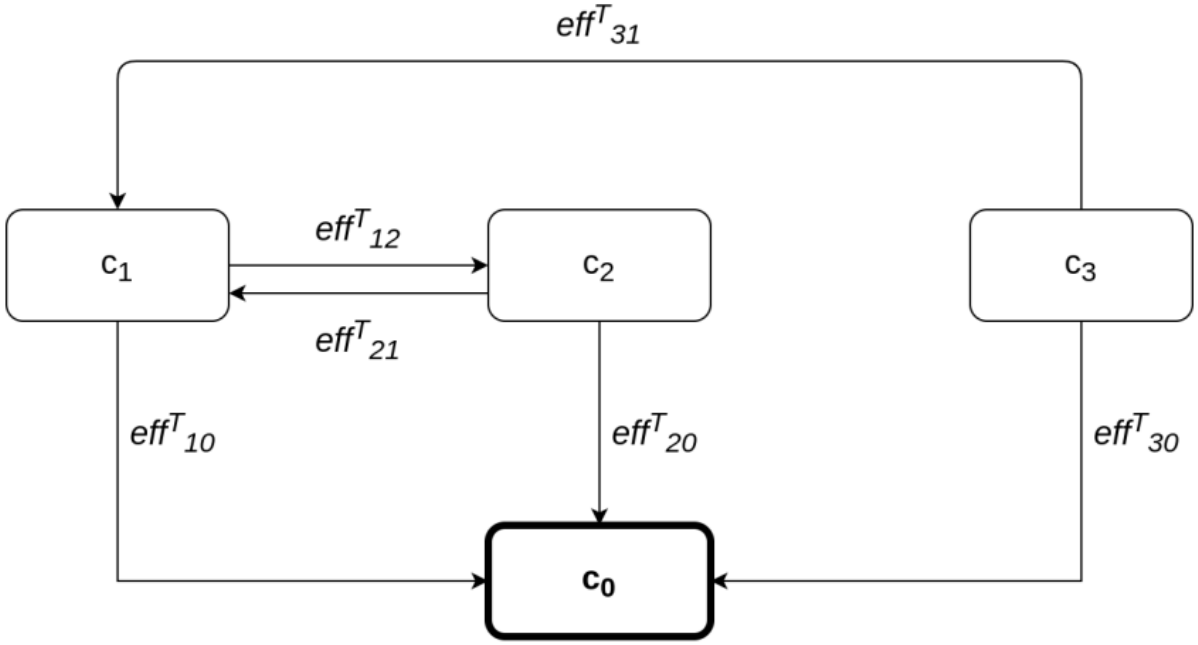
Το σύστημα σαν ένα ενιαίο σύνολο αλλά ταυτόχρονα και σαν ένας κόμβος αντιπροσωπεύεται με c_0. Από εκεί και πέρα ένα παγκόσμιο ρίσκο μιας απειλής t για το σύστημα δίδεται από τον τύπο:

$$R_t^s = R_t^{agg_{c_0}} = max\,(R_t^{dir_{c_0}}, R_t^{prop_{c_0}})$$

Εκεί όπου κάποιος άμεσος κίνδυνος για το σύστημά μας δεν μπορεί να έχει ισχύ $(R_t^{dir_{c_0}} = 0)$ και το μεταδιδόμενο προς το σύστημά μας ρίσκο, και κατ' επέκταση ο μεταδιδόμενος κίνδυνος, υπολογίζεται όπως για οποιονδήποτε άλλο κόμβο $(R_t^{prop_{c_0}} = max_{p_l} R_t^{prop_{c_0}^{p_l}})$ παρόλο που: $R_t^s = \max_{p_l} R_t^{prop_{c_0}^{p_l}}$.

Για να δείξουμε πώς λειτουργεί ο υπολογισμός του παγκόσμιου ρίσκου (κινδύνου) πρέπει ταυτόχρονα πρέπει να εστιάσουμε και να εξετάσουμε και σε μια ιδιαίτερη κατάσταση μέσω του παραδείγματος όπως αυτό παρουσιάζεται στο Cyber Risk Propagation and Aggregation του Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems[71] που αναφέραμε στην αρχή του κεφαλαίου και παρατίθεται αυτούσιο.

Για να υπολογίσουμε τον συνολικό κίνδυνο κάθε c_i, i = 1, 2, 3, πρέπει να υπολογίσουμε τα ρίσκα μαζί με τους κινδύνους που διαδίδονται. Αυτό απαιτεί τον εντοπισμό όλων των πιθανών διαδρομών οι οποίες μπορούν να ξεκινούν από οποιονδήποτε κόμβο και να τελειώνουν αντίστοιχα σε οποιοδήποτε σε c_i, i = 1, 2, 3. Ο κίνδυνος που διαδίδεται c_3 είναι ίσος με το μηδέν, καθώς δεν υπάρχει τέτοιο εναλλακτική διαδρομή. Οι κόμβοι c_1 και c_2 προφανώς διασυνδέονται μεταξύ τους καθόσον υπάρχει μεταξύ τους ένας βρόχος σύνδεσης. Κατά συνέπεια, εάν επιτρέψουμε να ληφθούν υπόψη κυκλικές διαδρομές, θα υπάρχουν άπειρες διαδρομές μεταξύ αυτών των δύο κόμβων και ο υπολογισμός στην $\prod_{i=1}^{j-1} \boldsymbol{eff}^{\boldsymbol{T}}_{c_i c_i+1}$ θα ήταν ατελείωτες. Ωστόσο, παρατηρώντας ότι η τιμή του συνολικού συντελεστή επίδρασης εξ ορισμού γίνεται αμελητέα μετά από την εκτέλεση μερικών επαναλήψεις των διαδρομών κυκλικής πορείας μεταξύ των κόμβων, εμείς σαν μελετητές μπορούμε να αγνοήσουμε τις κυκλικές διαδρομές στους υπολογισμούς.



Επομένως, το συνολικό ρίσκο και ο συνολικός κίνδυνος ενός συστήματος μπορεί να υπολογιστεί από τον αλγόριθμο που ακολουθεί. Όπως φαίνεται στον αλγόριθμο λοιπόν, οι κόμβοι κατά μήκος μιας διαδρομής επεξεργάζονται αναδρομικά, ξεκινώντας από το τέλος της εκάστοτε διαδρομής. Εάν ένας κόμβος βρίσκεται ήδη στη διαδρομή, δεν συμπεριλαμβάνεται ξανά, ώστε να αποφευχθούν κυκλικές διαδρομές.

Algorithm 1: Global system risk calculation algorithm.

Result: Global system risk is calculated as R_t^s

Function `process_node`$(c_j,\ eff,\ p_l)$**:**

- $L = L_t^{c_j}$;
- $I = I_t^{c_j}$;
- $R = \frac{L+I}{2}$;
- **foreach** *edge from* c_i *to* c_j **do**
  - **if** $c_i \notin p_l$ **then**
    - $p_l = p_l \cup \{c_i\}$;
    - $L', I' = process\_node(c_i, eff_{c_i c_j}, p_l)$;
    - $R' = \frac{L'+I'}{2}$;
    - **if** $R' > R$ **then**
      - $L = L'$;
      - $I = I'$;
      - $R = R'$;
    - **end**
  - **end**
- **end**
- **return** $eff \times L, I$;

L, I=`process_node`$(c_0, 1, \{c_0\})$;

$R_t^s = \frac{L+I}{2}$;

7. Βέλτιστη Επιλογή Controls Στοιχείων Ελέγχου Κυβερνοασφάλειας

i. Controls - Στοιχεία Ελέγχου Κυβερνοασφάλειας

Ας ξεκινήσουμε υποθέτοντας πως υπάρχει μια κατάσταση με διαθέσιμα στοιχεία ελέγχου, εφεξής controls, τα οποία μπορούμε να τα εφαρμόσουμε στα components του συστήματος μας. Κάθε στοιχείο ελέγχου, control m, όταν εφαρμόζεται στο στοιχείο c_i δυνητικά έχει μια σημαντική επίδραση επί των τιμών των $Επίπτωση_t^{c_i}$ και $Πιθανότητα_t^{c_i}$, οι οποίες τιμές χρησιμοποιούνται για τον υπολογισμό του ρίσκου και των κινδύνων στον κυβερνοχώρο. Μια τέτοια επίδραση βέβαια εξαρτάται σημαντικά τόσο από την αποτελεσματικότητα όσο και από την ίδια τη φύση του ελέγχου. Στη συνέχεια θα δηλώσουμε τις νέες τιμές των $Επίπτωση$ και $Πιθανότητα$ μιας απειλής t που προκύπτουν μετά από την εφαρμογή του control m στο c_i. Αυτές είναι $Επίπτωση_{t^m}^{c_i}$ και $Πιθανότητα_{t^m}^{c_i}$ αντίστοιχα. Αυτές οι τιμές μπορούν να υπολογιστούν αφού θα εφαρμόσουμε ξανά το DREAD στο σύστημα μας, το οποίο πλέον έχει «θωρακιστεί και προστατεύεται από το control m.

Επιπλέον, για κάθε control m, ορίζεται ταυτόχρονα και ένα μέτρο του κόστους $Cost_m$ που εκφράζεται με μία κλίμακα από το 1 έως το 5. Το μέτρο αυτό αντιστοιχεί στις ποιοτικές ταξινομήσεις πολύ χαμηλό κόστος, χαμηλό κόστος, μεσαίο κόστος, υψηλό κόστος και πολύ υψηλό κόστος. Να σημειώσουμε εδώ ότι η χρήση αυτής της κλίμακας

στην ουσία έχει προταθεί από το γεγονός ότι είναι δύσκολο να μετρηθεί αριθμητικά ακριβώς το κέρδος επί του κόστους έπειτα από την εφαρμογή ενός control. Ωστόσο, εάν κάποια τέτοια μέτρα είναι διαθέσιμη, μια αντικατάσταση της τιμής επί της κλίμακας 1 έως 5 επί του πραγματικού κόστους είανι προφανώς πολύ απλούστερη.

Για ένα σύστημα με N components και ένα κατάλογο με M controls και το διάνυσμα μέτρησης του κόστους $C = [\text{κόστος}_1, \text{κόστος}_2, ..., \text{κόστος}_M]$, ο ακόλουθος δυσδιάστατος πίνακας AC απεικονίζει συμπαγή τα controls που εφαρμόστηκαν σε όλο το σύστημα:

$$AC = \begin{bmatrix} ac_{1,1} & ac_{1,2} & \dots & ac_{1,N} \\ ac_{2,1} & ac_{2,2} & \dots & ac_{2,N} \\ \dots & \dots & \dots & \dots \\ ac_{M,1} & ac_{M,2} & \dots & ac_{M,N} \end{bmatrix}$$

όπου $$ac_{i,j} = \begin{cases} 0, \textit{if control } i \textit{ is not applied to component } j \\ 1, \textit{if control } i \textit{ is applied to component } j \end{cases}$$

Εν συνεχεία το συνολικό κόστος TC_{AC} από τη λύση AC που προκύπτει έπειτα από την εφαρμογή των controls δίδεται από τον τύπο $TC_{AC}=AC \times C$.

ii. Μέθοδος Βελτιστοποίησης

Το πρόβλημα της βελτιστοποίησης που στην ουσία έχει προκύψει στην παρούσα εργασία μας, και το οποίο πρέπει να επιλυθεί είναι: Η επιλογή των βέλτιστων στοιχείων ελέγχου ή, όπως πρότερα τα αποκαλέσαμε νωρίτερα, controls. Λέγοντας βέλτιστα εννοούμε εκείνα με τη μέγιστη απόδοση από πλευράς αποτελεσματικότητας και αποδοτικότητας μέσα από το σύνολο μιας λίστας – κατάστασης που περιέχει όλα τα πιθανά controls. Αυτό ισοδυναμεί με την επιλογή του συνόλου των controls AC τα οποία ελαχιστοποιούν το υπολειπόμενο ρίσκο του συστήματος $R^s_{t_{AC}}$, με το χαμηλότερο δυνατό κόστος TC. Ένας κλειστός μαθηματικός τύπος που θα επέτρεπε την εφαρμογή μιας μεθόδου βελτιστοποίησης με ακριβή αποτελέσματα, και κατ' επέκταση και τον ακριβή υπολογισμό της βέλτιστης συνολικά λύσης επί του προβλήματος δεν είναι δυνατό να δημιουργεί, εκτός και εάν γίνουν πάρα πολλές, στην πραγματικότητα όχι ρεαλιστικές, υποθέσεις. Από την άλλη πλευρά, το μεγάλο μέγεθος του χώρου αναζήτησης των υποψήφιων λύσεων, στην ουσία απαγορεύει να προσεγγίσουμε εξαντλητικά μια αναζήτηση λύσης. Ως εκ τούτου, πρέπει να χρησιμοποιηθεί μια μέθοδος ανεύρεσης βέλτιστης λύσης (heuristics)[72]. Παρόλο που οποιαδήποτε άλλη μέθοδος ανεύρεσης βέλτιστης λύσης (heuristics) θα μπορούσε σε πρώτη φάση να εφαρμοστεί στην περίπτωσή μας, εμείς επιλέξαμε να χρησιμοποιήσουμε έναν γενετικό αλγόριθμο.

Οι παράμετροι γύρω από το σχεδιασμού του γενετικού αλγόριθμου που επιλέξαμε είναι οι ακόλουθοι:

- Το πεδίο αναζήτησης της πιθανής βέλτιστης λύσης συμπεριλαμβάνει όλους τους πιθανούς συνδυασμούς controls που εφαρμόζονται στα components.

- Κάθε μοναδικής λύση αποτυπώνεται πάνω στον πίνακα AC, ο οποίος στη συνέχεια μετασχηματίζεται σε ένα δυσδιάστατο διάνυσμα μεγέθους $M \times N$. Η τιμή για κάθε στοιχείου του διανύσματος αντιπροσωπεύει την απόφαση να εφαρμοστεί ένα συγκεκριμένο control επί ενός συγκεκριμένου component ή και όχι. Για παράδειγμα, για ένα σύστημα με τρία components και δύο controls, η λύση θα συμβολίζεται με το διάνυσμα $[ac_{11}, ac_{21}, ac_{12}, ac_{22}, ac_{13}, ac_{23}]$, υποθέτοντας ότι όλα τα controls έχουν ισχύ σε όλα τα components.
- Κάνουμε χρήση μιας συνάρτησης καταλληλότητας, γνωστή και ως fitness, η οποία ορίζεται ως εξής: $fit(AC) = R^S_{t_{AC}} + C_{\text{norm}}(AC)$, όπου $C_{norm}(AC) = \frac{TC_{AC}}{TCmax}$, με το TC_{max} να είναι το μέγιστο δυνατό κόστος, που προκύπτει όταν γίνεται εφαρμογή όλων των controls στα components του συστήματός μας.
- Το αρχικό μέγεθος δείγματος πληθυσμού είναι 100.
- Η πιθανότητα μετάλλαξης είναι 0,1.
- Η επόμενη γενιά καθορίζεται από ομοιόμορφη διασταύρωση, με την πιθανότητα διασταύρωσης να είναι ίση με 0,5. Η elite αναλογία είναι από 0,01 έως και 0,3 επί του πληθυσμού ο οποίος αποτελείται από τα πιο κατάλληλα μέλη της προηγούμενης γενιάς (γνωστοί και ως γονείς).
- Ο αλγόριθμος τερματίζεται όταν χρησιμοποιηθεί ο μέγιστος αριθμός των επιτρεπόμενων επαναλήψεων. Ο μέγιστος αυτός αριθμός υπολογίζεται από τον τύπο: $\text{iter}_{\max} = 50 \times \Sigma_{\text{i=1, j=1}}^{\text{i=M, j=N}} \text{ac}_{\text{ij}}$.

Ο αλγόριθμος για την επιλογή του βέλτιστου συνόλου των controls απεικονίζεται στον Αλγόριθμο 2 (Algorithm 2) που ακολουθεί. Να σημειώσουμε εδώ ότι η συνάρτηση καταλληλότητας (fitness) αποτελείται από δύο στοιχεία. Αυτά είναι το παραμένον ή υπολειπόμενο ρίσκο, το οποίο λαμβάνει τιμές από 0 έως 3 [0, 3]) και το κανονικοποιημένο κόστος, το οποίο λαμβάνει τιμές από 0 έως 1 [0, 1]). Έχει γίνει επιλογή αυτής της μη συμμετρικής προσέγγισης προκειμένου να δοθεί έμφαση στο πόσο σημαντική είναι η μείωση του παραμένοντος ή υπολειπόμενου ρίσκου, ακόμη και αν επιβαρυνόμαστε με μεγαλύτερο κόστος. Αυτή η προσέγγιση έχει σαν αποτέλεσμα ο οδηγηθούμε σε κάποιες αρχικές επαναλήψεις του αλγορίθμου οι οποίες τείνουν να δημιουργήσουν λύσεις οι οποίες με τη σειρά τους ελαχιστοποιούν τον παραμένον ή υπολειπόμενο ρίσκο. Σε επαναλήψεις του αλγορίθμου που λαμβάνουν χώρα σε δεύτερο χρόνο, επικρατούν οι λιγότερο κοστοβόροι συνδυασμοί μεταξύ των controls, μεταξύ αυτών που οδηγούν στη μέγιστη δυνατή μείωση του ρίσκου.

Algorithm 2: Algorithm for selecting the optimal set of security controls

Result: Optimal set of security controls is identified

Function `calc_fitness`(*control_sets*)**:**
    control_sets_fit_scores = [];
    foreach *c in control_sets* **do**
        control_sets_fit_scores[c] = fit_score(*c*);
    end
    return control_sets_fit_scores;

Function `select_parents`(*control_sets,control_sets_fit_scores*)**:**
    parents_control_sets = [] ;
    foreach *c in control_sets* **do**
        if *control_sets_fit_scores[c]* $\in$ *upper 30% of control_sets_fit_scores* **then**
            parents_control_sets $\leftarrow$ *c*;
        end
    end
    return parents_control_sets;

Function `select_elite`(*control_sets,control_sets_fit_scores*)**:**
    elite_control_sets = [] ;
    foreach *c in control_sets* **do**
        if *control_sets_fit_scores[c]* $\in$ *upper 1% of control_sets_fit_scores* **then**
            elite_control_sets $\leftarrow$ *c*;
        end
    end
    return elite_control_sets;

Function `crossover`(*parent_control_sets*)**:**
    control_sets = parent_control_sets;
    pop = |control_sets| ;
    while *pop<100* **do**
        $parent_a = random(parent\_control\_sets)$;
        $parent_b = random(parent\_control\_sets)$;
        $control\_set_{new} = crossover(parent_a, parent_b)$;
        $control\_sets \leftarrow control\_set_{new}$;
        $pop = pop + 1$;
    end
    return control_sets;

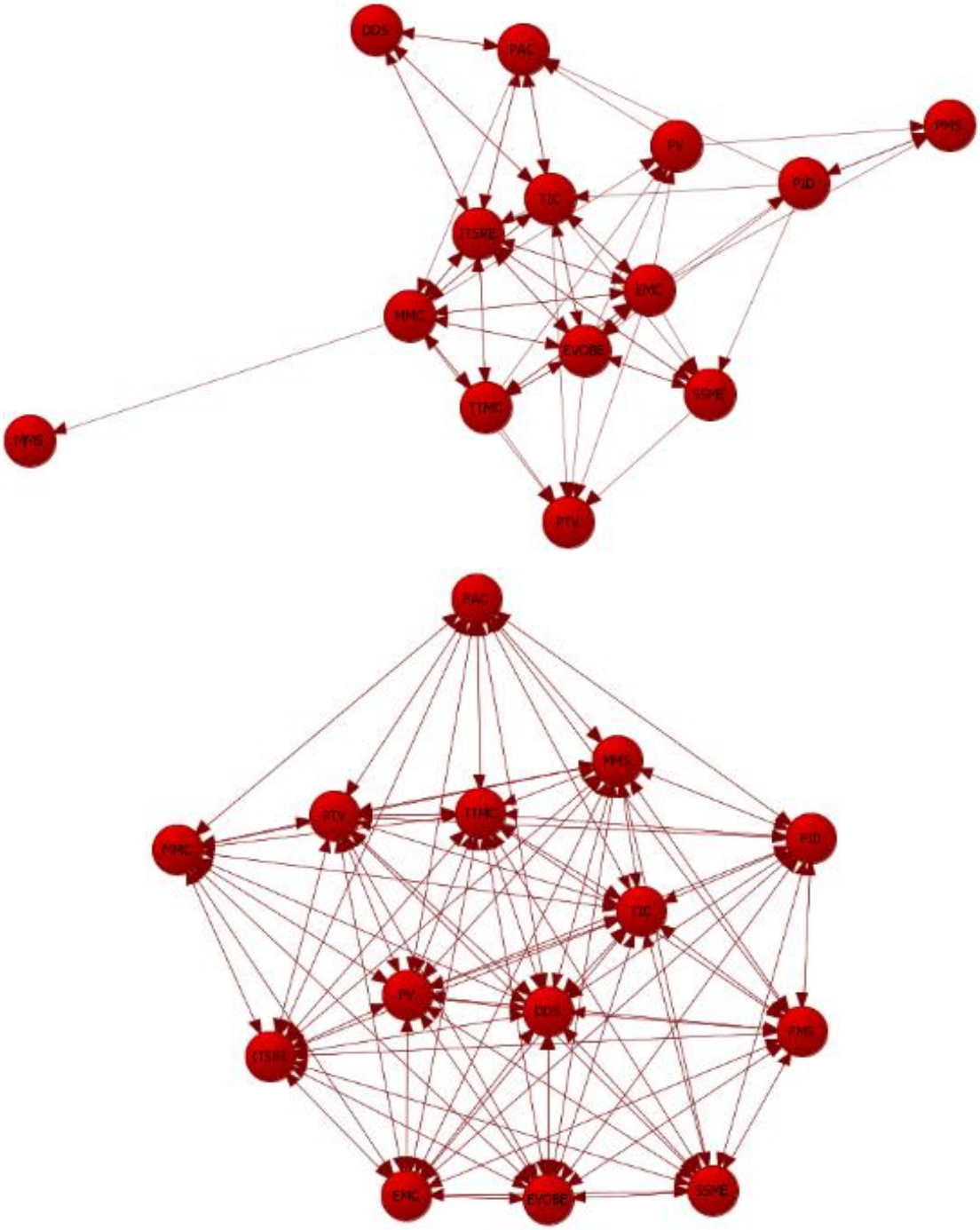
Function `mutation`(*control_sets,elite_control_sets*)**:**
    mutated_control_sets = [];
    foreach *c in control_sets* **do**
        if $c \in elite\_control\_sets$ **then**
            $mutated\_control\_sets \leftarrow c$;
        else
            $mut\_c = mutate(c)$;
            $mutated\_control\_sets \leftarrow mut\_c$;
        end
    end
    return *mutated_control_sets*;

Algorithm 2: *Cont.*

```
Function find_solution():
    iter_max = 50 × Σ_{i=1,j=1}^{i=M,j=N} ac_ij;
    iter = 0;
    control_sets ← 100 random sets;
    while iter < iter_max do
        control_sets_fit_scores = calc_fitness(control_sets);
        parents_control_sets = select_parents(control_sets,control_sets_fit_scores);
        elite_control_sets = select_elite(control_sets,control_sets_fit_scores);
        control_sets = crossover(parents_control_sets);
        control_sets = mutation(control_sets);
        iter = iter + 1
    fittest_control_set = fittest c ∈ control_sets return fittest_control_set;
find_solution()
```

8. Εφαρμογή στα Έξυπνα Συστήματα Μεταφορών - ITS

Δεν τίθεται θέμα ότι τα Έξυπνα Συστήματα Μεταφορών (ITS - Intelligent Transport Systems) και η κυβερνοασφάλεια τους είναι ένας ταχύτατα και κατακόρυφα αναπτυσσόμενος τομέας τεχνολογίας. Ολοένα και περισσότεροι οργανισμοί και ιδιωτικές εταιρείες προσφέρουν υπηρεσίες και εξοπλισμό ITS με αποτέλεσμα όλοι μας να έχουμε κάποια τριβή – εμπλοκή με τέτοια συστήματα τακτικά στην καθημερινή μας ζωή. Δύο τομείς οι οποίοι επηρεάζονται από αυτό είναι ο οικονομικός καθώς επενδύονται πολλά χρήματα πάνω στις τεχνολογίες ITS και ο τομέας της ιδιωτικότητας διότι για τη συμμετοχή του ανθρώπου σε στις τεχνολογίες αυτές γίνεται «ψηφιακή καταγραφή» πολλών προσωπικών δεδομένων. Συνεπώς δεν αποτελεί έκπληξη, το γεγονός ότι η κυβερνοασφάλεια συστημάτων σχετικών με τα ITS έχει χαρακτηριστεί ως πολύ υψηλή προτεραιότητα τόσο από διεθνείς οργανισμούς όσο και από τις εθνικές κυβερνήσεις. Τα τμήματα των ITS σαν Cyber Physical Systems για τον καθορισμό της αρχιτεκτονικής τους, στην παρούσα εργασία εξετάζονται, με όμοιο τρόπο με αυτόν που γίνεται στο *«Cyber-attacks against the autonomous ship»*[45] το οποίο χρησιμοποιεί δενδρική δομή αρχιτεκτονικής. Μέσω εκείνου προτείνεται ένα εκτεταμένο Αρχιτεκτονικό πλαίσιο όπου παρουσιάζονται οι διασυνδέσεις, οι εξαρτήσεις και οι αλληλεπιδράσεις μεταξύ των με τα components των ITS που εξετάζουμε στους τομείς τόσο των πληροφοριών όσο και των Controls. Τα αποτελέσματα αυτά απεικονίζονται στα ακόλουθα σχεδιαγράμματα και θα αναλυθούν σε μεταγενέστερη παράγραφο.

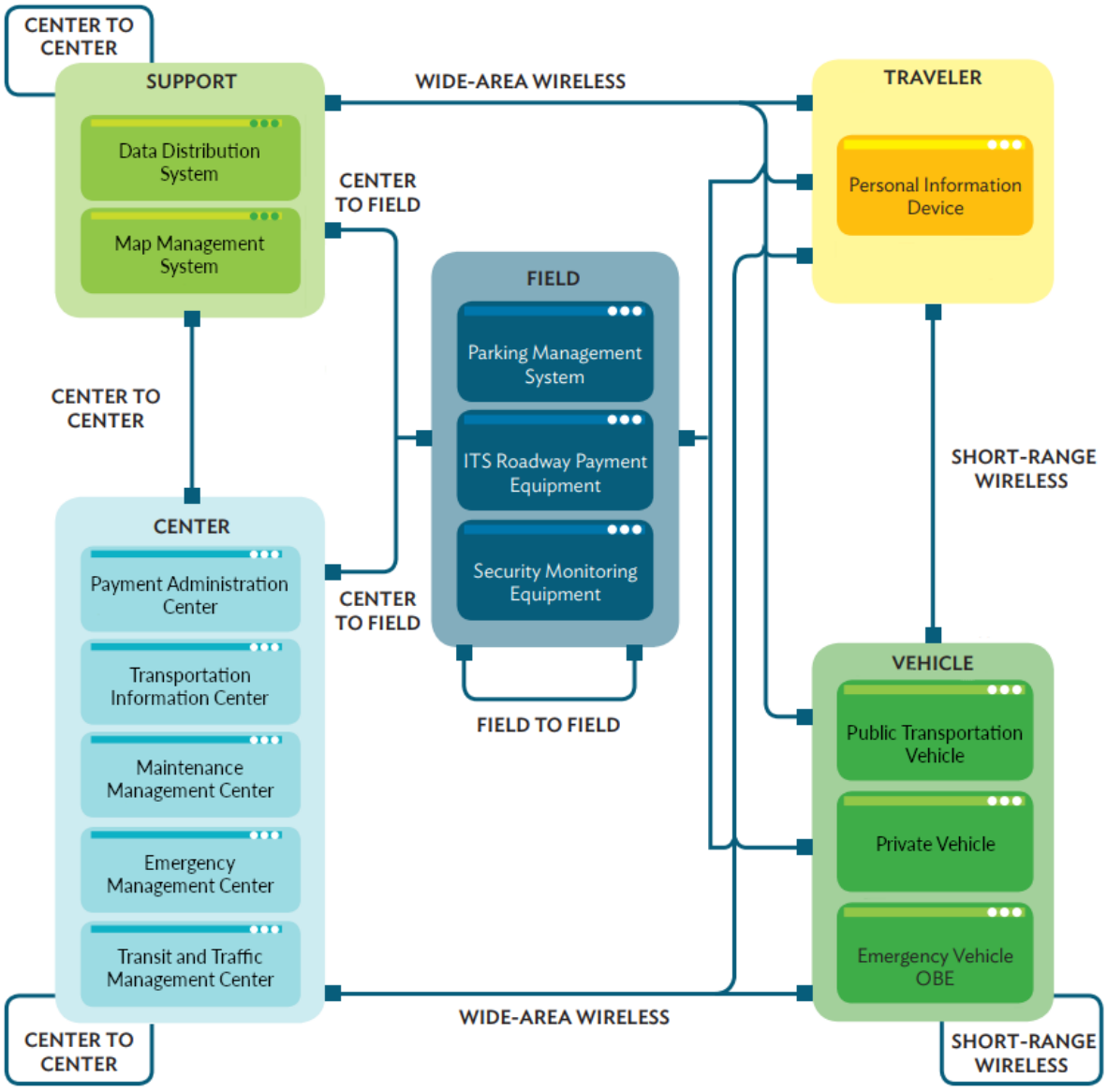


Προφανώς και έχουμε βασιστεί σε υπάρχουσες εργασίες τα ευρήματα των οποίων προσπαθούμε να εξελίξουμε καθορίζοντας τις κατάλληλες αρχιτεκτονικές κυβερνοασφάλειας ITS συστημάτων. Αυτά τα συστήματα που επιλέγουμε για να δείξουμε τις δυνατότητες εφαρμογής των μεθόδων που προτείνονται σε αυτή την εργασία παρουσιάζονται στη συνέχεια.

i.Components των Εξεταζόμενων ITS

Για τον καθορισμό των components που αρχικά αναγνωρίσθηκαν και στη συνέχεια περιγράφονται σε αυτή εδώ την εργασία χρησιμοποιήθηκε σαν πηγή το *Conceptual Design of the Intelligent Transport Systems Project – Case in Gui'an New District*[73]. Στη συνέχεια πραγματοποιείται ανάλυση των απειλών και ποιοτική ανάλυση του

ρίσκου και έτσι εντοπίζονται τα πιο ευάλωτα συστήματα επί των ITS. Ακολουθεί μια περιγραφή των Components που εξετάσθηκαν[74].



- **Ατομικές Συσκευές Πληροφόρησης - Personal Information Device (PID)**

Πρόκειται για συσκευές που με κάποιο τρόπο παρέχουν εξατομικευμένες πληροφορίες στους ταξιδιώτες για τις συγκοινωνίες, για πολυτροπικές μετακινήσεις. Αυτές μπορεί να είναι υπολογιστές (φορητοί και μη), tablet, smartphones ή κάποιο άλλο σύστημα.

Πρόκειται για σύστημα ζωτικής σημασίας τόσο για τους ταξιδιώτες όσο και για εκείνους που συντονίζουν μεταφορές και ταξίδια. Μπορεί να παρέχουν από απλές ταξιδιωτικές πληροφορίες μέχρι πολύ εξειδικευμένες πληροφορίες σχετικές με κάποιο ταξίδι ή μετακίνηση. Επιτρέπουν στους επαγγελματίες του κλάδου να αξιοποιούν και ταυτόχρονα να στηρίζονται σε λιγότερο προσωπικό που ασχολείται με την παροχή πληροφοριών. Για να λειτουργήσει μία PID έχουν λειτουργία ενός ευρέος φάσματος τεχνολογιών, από υπολογιστές και απλές τηλεφωνικές γραμμές εξυπηρέτησης πελατών μέχρι και προσωπικές συσκευές πληροφοριών συγκοινωνίας που υπάρχουν σε διάφορα μέσα για εξατομικευμένη πληροφόρηση.

Τα δεδομένα που παρέχονται από τα PID μπορούν να κυμαίνονται από έναν χάρτη συστημάτων συγκοινωνίας, απλές πληροφορίες χρονοδιαγραμμάτων και ναύλων μέχρι πιο δυναμικές πληροφορίες όπως εκτιμώμενοι χρόνοι άφιξης ή αναμονής, καθυστερήσεις, κυκλοφορία, καιρό και πληροφορίες έκτακτης ανάγκης. Μπορούν επίσης να παρέχονται τοπικές πληροφορίες βοήθειας ταξιδιωτών για προγραμματισμό ταξιδιού. (πχ αξιοθέατα, ονομασία δρόμων, διευθύνσεις, διαθέσιμες επιλογές μετακίνησης, οδικοί χάρτες, μονοπάτια κτλ).

Τα PID και οι τεχνολογίες τους μπορούν να χρησιμοποιηθούν σε διάφορες φάσεις ενός ταξιδιού όπως πριν το ταξίδι, στον τερματικό σταθμό και εντός οχήματος - καθ' οδόν.

Μια συνηθισμένη διαδικασία συλλογής και διάδοσης πληροφορίας περιλαμβάνει τη χρήση ενός AVL-GPS (αυτόματου συστήματος εντοπισμού θέσης οχήματος) για την επικοινωνία με τους αντίστοιχους επιχειρησιακούς servers. Ο server μεταβιβάζει επιλεκτικές πληροφορίες στον αντίστοιχο ιστότοπο, ο οποίος με χρήση συστημάτων γεωγραφικών πληροφοριών (GIS) και του κατάλληλο λογισμικού εμφανίζει τις πληροφορίες σε μια φιλική για το χρήστη μορφή. Εν τέλει πληροφορίες τοποθεσίας και προγραμμάτων καταλήγουν να μεταδίδονται σε ασύρματες συσκευές, περίπτερα, πινακίδες, αυτόματες φωνητικές ανακοινώσεις, σταθερά & κινητά τηλέφωνα, ιστοσελίδων και εφαρμογών smartphone.

- **Έξυπνος Εξοπλισμός Αυτοκινητοδρόμων - ITS Roadway Equipment (ITSRE)**

Ο «Έξυπνος Εξοπλισμός Αυτοκινητοδρόμων» (ITS Roadway Equipment) αντιπροσωπεύει τον εξοπλισμό ITS που χρησιμοποιείται σε όλα τα μήκη όχι μόνο των αυτοκινητοδρόμων αλλά και γενικά σε οποιοδήποτε σημείο δρόμου. Παρακολουθεί και ελέγχει την κυκλοφορία και μέσω καταγραφής και διαχείρισης της κυκλοφορίας. Σαν component και τμήμα ενός ευρύτερου ITS συστήματος περιλαμβάνει ανιχνευτές κυκλοφορίας, αισθητήρες σχετικούς με το περιβάλλον, φωτεινούς σηματοδότες κυκλοφορίας, ραδιόφωνα αυτοκινητοδρόμων παροχής συμβολών και υποδείξεων, δυναμικές πινακίδες μηνυμάτων προς τους οδηγούς, κάμερες κλειστών κυκλωμάτων καταγραφής εικόνας, τα επονομαζόμενα CCTV, συστήματα επεξεργασίας ήχου - εικόνας - βίντεο, προειδοποιητικά συστήματα διαβάσεων και συστήματα μετρήσεων επί κόμβων και διασταυρώσεων. Περιλαμβάνονται επίσης συστήματα διαχείρισης λωρίδων κυκλοφορίας και συστήματα διακοπής της κυκλοφορίας που ελέγχουν την πρόσβαση σε διάφορες οδικές υποδομές, όπως δρόμοι, γέφυρες και σήραγγες. Σαν τμήμα παρέχει επίσης παρακολούθηση περιβάλλοντος από την επιρροή των συστημάτων μεταφορών. Συμπεριλαμβάνει επίσης αισθητήρες που μετρούν τις συνθήκες στους δρόμους, τον καιρό επιφάνειας και τις εκπομπές ρύπων από τα οχήματα. Σε αυτό το αντικείμενο ανήκουν επίσης και διάφορα συστήματα παρακολούθησης εργασίας όπως κάποια επιτηρούν ζώνες εργασίας ανθρώπων, ζώνες ελέγχου, συστήματα προειδοποίησης των οδηγών καθώς και συστήματα ασφάλειας για τα διάφορα πληρώματα εργασίας.

- **Εξοπλισμός Ασφαλείας & Παρακολούθησης Ασφαλείας - Safety & Security Monitoring Equipment (SSME)**

Ο «Εξοπλισμός Ασφαλείας & Παρακολούθησης Ασφαλείας» περιλαμβάνει εξοπλισμό επιτήρησης και αισθητήρες που χρησιμοποιούνται για την παροχή βελτιωμένης ασφάλειας και παρακολούθησης της ασφάλειας σε μεταφορικές εγκαταστάσεις ή υποδομές. Ο εξοπλισμός βρίσκεται σε δημόσιους και μη χώρους μεταφορικών

εγκαταστάσεων (π.χ. συνεργεία συντήρησης, σημεία μεταφόρτωσης), κοντά ή μακριά από σημεία εκτός αυτοκινητοδρόμων τα οποία αποτελούν τμήματα των υποδομών μεταφορών (π.χ. σιδηροδρομικοί σταθμοί διέλευσης και βαγόνια μεταφοράς) και σε δημόσιους χώρους (π.χ. σταθμοί μεταφορών και μεταφόρτωσης, σταθμοί απλής διέλευσης, τερματικοί σταθμοί πολυτροπικών μεταφορών). Σε αυτό τον εξοπλισμό συμπεριλαμβάνεται επίσης και ο γενικός εξοπλισμός επιτήρησης και οι αισθητήρες που βρίσκονται πάνω ή κοντά σε σημαντικά στοιχεία των δρόμων και των αυτοκινητοδρόμων, όπως γέφυρες, σήραγγες και κόμβους, εφόσον η κύρια λειτουργία του εξοπλισμού είναι η ασφάλεια και η παρακολούθηση της ασφάλειας. Εάν η κύρια λειτουργία του εξοπλισμού είναι η επιτήρηση της κυκλοφορίας ή η ανίχνευση συμβάντων, τότε τα συστήματα επιτήρησης και οι αισθητήρες θα συμπεριλαμβάνονται στον «Έξυπνο Εξοπλισμό Αυτοκινητοδρόμων». Ο εξοπλισμός επιτήρησης περιλαμβάνει από συστήματα βίντεο (π.χ. κάμερες CCTV) μέχρι και ηχητικά συστήματα. Ο εξοπλισμός αισθητήρων περιλαμβάνει αισθητήρες κάποιας απειλής (π.χ. χημικών παραγόντων, τοξικών βιομηχανικών χημικών ουσιών, βιολογικούς ή εκρηκτικούς ή ραδιολογικούς αισθητήρες), ανιχνευτές αντικειμένων (π.χ. ανιχνευτές μετάλλων), ανιχνευτές κίνησης ή εισβολής ή ακεραιότητας των υποδομών (π.χ. παρακολούθηση και έλεγχος για προβλήματα συνέχειας σε μια σιδηροδρομική γραμμή ή σε δομικά στοιχεία μιας γέφυρας). Η όποια περιορισμένη επεξεργασία των δεδομένων συλλογής από τους αισθητήρες και από τα συστήματα επιτήρησης περιλαμβάνεται επίσης σε αυτό το component όσον αφορά την υποστήριξη του εντοπισμού και της ταξινόμησης απειλών.

- **Σύστημα Διαχείρισης Στάθμευσης - Parking Management System (PMS)**

Κεντρικό στοιχείο για το σύστημα αυτό είναι ένα «Κέντρο Διαχείρισης Στάθμευσης» το οποίο διαχειρίζεται έναν ή και περισσότερους χώρους στάθμευσης παρέχοντας διαμόρφωση και έλεγχο των εγκαταστάσεων και των υποδομών του, οικονομική διαχείριση από το χρήστη έως τον ίδιο το χώρο στάθμευσης περιλαμβάνοντας τις απαραίτητες διασυνδέσεις με χρηματοοικονομικά συστήματα για τη διαχείριση πληρωμών. Επίσης το κέντρο αυτό έχει και το ρόλο της διάδοσης των πληροφοριών στάθμευσης σε άλλα επιχειρησιακά κέντρα στην περιοχή.

Ταυτόχρονα υπάρχουν και κάποιες άλλες λειτουργίες back office κάποιας άλλης εγκατάστασης στάθμευσης και ονομάζονται «Άλλα Κέντρα Διαχείρισης Στάθμευσης». Διαθέτουν πηγές και προορισμούς πληροφοριών τα οποία έχουν τη δυνατότητα και πρέπει να ανταλλάσσονται μεταξύ ομότιμων συστημάτων στάθμευσης. Μέσω αυτών επιτυγχάνεται ο συντονισμός δραστηριοτήτων διαχείρισης στάθμευσης μεταξύ διαφορετικών χειριστών ή συστημάτων στάθμευσης σε μια περιοχή. Συνήθως τα «Άλλα Κέντρα Διαχείρισης Στάθμευσης» λειτουργούν μακριά από τις εγκαταστάσεις του χώρου στάθμευσης.

Σε αυτό το component ανήκουν και οι έξυπνες λειτουργίες που χειρίζεται ο ανθρώπινος παράγοντας γνωστός και ως "Parking Manager" ο οποίος υποστηρίζει λειτουργίες back office για έναν ή περισσότερους χώρους στάθμευσης.

Επίσης σημαντικό ρόλο σε αυτό το τμήμα έχει και ο εξοπλισμός του χώρου στάθμευσης. Παρέχει ηλεκτρονική παρακολούθηση και διαχείριση των εγκαταστάσεων στάθμευσης. Υποστηρίζει σύνδεση επιμέρους εξοπλισμού με τα οχήματα που επιτρέπει την ηλεκτρονική είσπραξη τελών στάθμευσης, παρακολουθεί και ελέγχει τα επονομαζόμενα και παρκόμετρα τα οποία υποστηρίζουν τη συμβατική

είσπραξη τελών στάθμευσης. Περιλαμβάνει επίσης όργανα, πινακίδες και άλλες υποδομές που παρακολουθούν όλες τις χρήσεις ενός χώρου στάθμευσης. Ταυτόχρονα παρέχει και τοπικές πληροφορίες σχετικά με τη διαθεσιμότητα στάθμευσης και άλλες γενικές πληροφορίες στάθμευσης. Οι δύο κύριες προσεγγίσεις για την παρακολούθηση της χρήσης του χώρου στάθμευσης είναι η ανίχνευση της όποιας κίνησης οχημάτων εντός των σημείων στάθμευσης και η καταμέτρηση των οχημάτων καθώς εισέρχονται και καθώς φεύγουν από την περιοχή. Αυτή η λειτουργία συνήθως βρίσκεται στο χώρο στάθμευσης από όπου και δύναται να γίνεται παρακολούθηση, ταξινόμηση και διαμοιρασμός της πληροφορίας με τους πελάτες και τα οχήματά τους.

Σε αυτό το σύστημα υπάρχει και ένας χειριστής στάθμευσης ο οποίος είναι ο ανθρώπινος συνοδός που μπορεί να είναι φυσικά παρών στην εγκατάσταση του χώρου στάθμευσης για να παρακολουθεί την κατάσταση λειτουργίας της εγκατάστασης. Ο έξυπνος εξοπλισμός που τυχόν έχει στην κατοχή του και χειρίζεται ο συγκεκριμένος χειριστής ανήκει σε αυτό το component.

- **Κέντρο Διαχείρισης Πληρωμών - Payment Administration Center (PAC)**

Ένα «Κέντρο Διαχείρισης Πληρωμών» παρέχει γενικές δυνατότητες διαχείρισης πληρωμών υποστηρίζοντας ηλεκτρονικές μεταφορές χρημάτων από τον πελάτη προς τον όποιο διαχειριστή οικονομικών συστημάτων μεταφορών ή άλλου πάροχου υπηρεσιών μετακινήσεων. Οι όποιες χρεώσεις γίνονται μπορεί να είναι για διόδια, χρέωση μιλίων ανά όχημα, χρέωση ανάλογα με τη συμφόρηση και άλλα αγαθά και υπηρεσίες. Επίσης υπάρχει δυνατότητα εγγραφής ταξιδιωτών και είσπραξη των τελών μεταφοράς τόσο με προπληρωμή όσο και μετά την όποια παροχή υπηρεσιών μεταφορών, πάντα σε συντονισμό με τις οικονομικές υποδομές που υποστηρίζουν τις συναλλαγές ηλεκτρονικών πληρωμών. Αυτό το σύστημα μπορεί να έχει δημιουργήσει και να διαχειρίζεται λογαριασμούς ανάλογα με τον τύπο και τον τρόπο εκκαθάρισης των σχετικών πληρωμών. Μπορεί να δεσμεύει χρήματα από λογαριασμό ενός πελάτη έπειτα από δική του συναλλαγή, να δημιουργεί λογαριασμούς για πληρωμές που έπονται της παροχής υπηρεσιών, να χρεώνει κάποιον άλλο λογαριασμό ή να συνδέσει κάποια οικονομική υποδομή σαν λογαριασμό χρέωσης κάποιου πελάτη. Υποστηρίζει την επικοινωνία με τον ITS Εξοπλισμό Πληρωμών Αυτοκινητοδρόμων για την είσπραξη των αντίστοιχων τελών. Εναλλακτικά, φυσικά και μπορούν να χρησιμοποιηθούν ασύρματες διεπαφές δικτύων ευρείας περιοχής για απευθείας επικοινωνία με τον όποιο εξοπλισμό των οχημάτων. Επίσης το component αυτό καθορίζει και διαχειρίζεται τις δομές τιμολόγησης και μπορεί να εφαρμόζει πολιτικές τιμολόγησης χρήσης οδικού δικτύου και γενικά παροχής υπηρεσιών μεταφορών πάντα σε συντονισμό με ένα Κέντρο Διαχείρισης Κυκλοφορίας.

Υπάρχει και ένα εναλλακτικό Κέντρο Διαχείρισης Πληρωμών που σκοπό έχει να παρέχει μια πηγή και έναν προορισμό για τις διαφορετικές ροές πληροφοριών που προκύπτουν από τα διάφορα ITS και χρειάζεται να «ενώσουν» διαφορετικές λειτουργίες διαχείρισης πληρωμών.

Αυτή η διεπαφή επιτρέπει σε πραγματικό χρόνο τη ενημέρωση και συμφωνία των διάφορων χρεώσεων (πχ διοδίων κτλ) μεταξύ διαφορετικών παρόχων υπηρεσιών. Επιτρέπεται έτσι η ανταλλαγή πληροφοριών σχετικές με τους πελάτες οι οποίοι έχουν χρεωθεί για υπηρεσίες σε κάποιο άλλο Κέντρο Διαχείρισης πληρωμών διαφορετικό από το δικό τους. Αυτή η διεπαφή επιτρέπει αφενός τον επιμερισμό των χρεώσεων

ανάμεσα σε διαφορετικούς παρόχους υπηρεσιών μεταφορών και αφετέρου την «αμοιβαιότητα» ανάμεσα στα διαφορετικά τους κέντρα Διαχείρισης των πληρωμών. Επίσης σε αυτό το component συμπεριλαμβάνεται και ο ITS εξοπλισμός πληρωμών που αναφέρεται στα έξυπνα συστήματα είσπραξης διοδίων. Παρέχεται η δυνατότητα στους οδηγούς να πληρώνουν στα διόδια δίχως ακινητοποίηση των οχημάτων τους. Υποστηρίζει τη χρήση δομών τιμολόγησης που καθορίζονται τοπικά και περιλαμβάνει τη δυνατότητα εφαρμογής διαφόρων πολιτικών που μεταβάλουν την τιμολόγηση. Συνήθως, οι συναλλαγές συνοδεύονται με σχολιασμό τόσο προς όσο και από τους πελάτες. Φυσικά και υποστηρίζεται και σύστημα αρχειοθέτησης ιστορικού όλων των συναλλαγών.

Εντός του component αυτού συμπεριλαμβάνεται και ο ITS εξοπλισμός που χρησιμοποιεί ένας διαχειριστής πληρωμών. Αυτός είναι το άτομο ή τα άτομα που διαχειρίζονται τα συστήματα διαχείρισης πληρωμών χωρίς να έχουν επαφή με τους πελάτες και συμπεριλαμβάνουν ηλεκτρονικά διόδια, πληρωμή χρήσης ανάλογα με την χιλιομετρική απόσταση καθώς και άλλες υπηρεσίες που πληρώνονται ανά όχημα. Παρακολουθεί τα συστήματα που υποστηρίζουν ηλεκτρονική μεταφορά χρημάτων από τον πελάτη προς τον πάροχο των υπηρεσιών μεταφορών. Παρακολουθεί επίσης την εγγραφή πελατών και υποστηρίζει τη δημιουργία λογαριασμών που δεσμεύουν τα αντίστοιχα χρήματα ανάλογα με τον τύπο και τον τρόπο εκκαθάρισης των σχετικών πληρωμών. Μεταξύ άλλων καθορίζει και διαχειρίζεται τις δομές και τις πολιτικές τιμολόγησης.

- **Κέντρο Πληροφορίας Μεταφορών – Μετακινήσεων (Συμπεριλαμβανομένου του συστήματος διάδοσης πληροφορίας) - Transportation Information Center (Including Information Disseminator System) (TIC)**

Ένα Κέντρο Πληροφοριών Μεταφορών – Μετακινήσεων συλλέγει, επεξεργάζεται, αποθηκεύει και μεταδίδει τις πληροφορίες μεταφοράς τόσο στους διαχειριστές συστημάτων όσο και στο επιβατικό κοινό. Σαν component μπορεί να παίξει πολλούς διαφορετικούς ρόλους σε ένα ολοκληρωμένο ITS. Το TIC παρέχει μια λειτουργία συλλογής δεδομένων, ομαδοποίησης, κατηγοριοποίησης και επαναπροσδιορισμού των πληροφοριών συλλέγοντας πληροφορίες από διαχειριστές συστημάτων μεταφορών και προωθώντας τις πληροφορίες σε διαχειριστές άλλων συστημάτων στην μα και σε άλλα TIC. Όταν έχει αυτόν τον ρόλο της αναδιανομής πληροφοριών, το TIC είναι η γέφυρα μεταξύ των διαφορετικών συστημάτων μεταφορών που παράγουν τις πληροφορίες και των άλλων TIC με τους συνδρομητές τους που χρησιμοποιούν αυτές τις πληροφορίες. Ο δεύτερος ρόλος που θα μπορούσε να έχει ένα TIC εστιάζει στην παράδοση πληροφοριών από τους ταξιδιώτες προς τους άλλους συνδρομητές και γενικά στο ευρύτερο κοινό. Οι παρεχόμενες πληροφορίες περιλαμβάνουν βασικές συμβουλές, κυκλοφοριακές και οδικές συνθήκες, πληροφορίες χρονοδιαγραμμάτων συγκοινωνιών, πληροφορίες συνδυασμού διαφορετικών ΜΜΜ και πληροφορίες στάθμευσης. Το TIC έχει συνήθως μορφή ιστότοπου ή υπηρεσία web εφαρμογής στο web, αλλά αντιπροσωπεύει οποιαδήποτε υπηρεσία παροχής πληροφορίας στους ταξιδιώτες.

Ένα διαφορετικό Κέντρο Πληροφορίας Μεταφορών – Μετακινήσεων μπορεί να έχει μια πηγή και έναν προορισμό για κάθε διαφορετική ροή πληροφορίας μέσα στα ITS μεταξύ ομότιμων πληροφοριών και λειτουργιών του πάροχου των υπηρεσιών. Έτσι

δημιουργεί μια ισχυρή συνεργασία ανταλλαγής πληροφοριών μεταξύ παρόχων, πάντα κάτω από προϋποθέσεις.

Κλείνοντας να αναφέρουμε ότι ένα σύστημα διάδοσης πληροφοριών ευρείας περιοχής αντιπροσωπεύει τα συστήματα και τον εξοπλισμό των επικοινωνιών που βασίζονται σε μια κεντρική οντότητα - component. Χρησιμοποιούνται για αποστολή μηνυμάτων σε εξοπλισμένα οχήματα χρησιμοποιώντας ασύρματες επικοινωνίες ευρείας περιοχής, όπως δορυφορικό ραδιόφωνο, επίγειες κεραίες FM ή δίκτυα δεδομένων κινητής τηλεφωνίας.

- **Κέντρο Διαχείρισης Συντήρησης - Maintenance Management Center (MMC)**

Το Κέντρο Διαχείρισης Συντήρησης παρακολουθεί και διαχειρίζεται τις δραστηριότητες συντήρησης οδοποιίας και συνολικά των υποδομών. Αναφερόμαστε σε τόσο δημόσιους και ιδιωτικούς φορείς (πχ εργολάβους) που παρέχουν τέτοιες υπηρεσίες. Στο component αυτό εντάσσεται η διαχείριση συντήρησης ενός στόλου οχημάτων καθώς και διάφορες ειδικές συντηρήσεις (π.χ. εκείνη του εξοπλισμός ελέγχου χιονιού και πάγου). Έχουμε λήψη ενός ευρέος φάσματος πληροφοριών κατάστασης όλων αυτών των οχημάτων τα οποία πρέπει να είναι έτοιμα να εκτελέσουν την αποστολής τους. Επίσης διαχειρίζεται γενικότερα και δρομολογεί τους πόρους των στόλων των οχημάτων και του σχετικού εξοπλισμού. Συμμετέχει επίσης στην άμεση απόκριση σε ένα συμβάν με την ανάπτυξη των πόρων της συντήρησης σε μια σκηνή συμβάντος, πάντα σε συντονισμό με τα άλλα τμήματα που διαχειρίζεται σαν κέντρο. Παράδειγμα εξοπλισμού που διαχειρίζεται το κέντρο είναι ο εξοπλισμός στην άκρη των δρόμων, συμπεριλαμβανομένων περιβαλλοντικών αισθητήρων και αυτοματοποιημένων συστημάτων που παρακολουθούν και τις τυχόν κακές καιρικές συνθήκες στο δρόμο. Γίνεται διαχείριση των επισκευών και των συντηρήσεων του εξοπλισμού ITS και μη, συμπεριλαμβανομένων των φωτεινών σηματοδοτών, όλων των αισθητήρων, των πινακίδων δυναμικών μηνυμάτων, των πινακίδων κυκλοφορίας και λοιπού εξοπλισμού που σχετίζεται με τις οδικές υποδομές. Οι πληροφορίες για τον καιρό συλλέγονται, ενσωματώνονται και αλληλεπιδρούν με άλλες πηγές δεδομένων και εν τέλει χρησιμοποιούνται για την υποστήριξη προηγμένων συστημάτων υποστήριξης λήψης αποφάσεων.

Σε αυτό το component ανήκει και η παρακολούθηση και η εξ αποστάσεως διαχείρισης διάφορων δυνατοτήτων των ITS χωρισμένα σε ζώνες εργασίας, συλλογής, αποθήκευσης, διανομής πληροφοριών για την αποδοτικότερη διανομή των πληροφοριών τους σε άλλα συστήματα. Ακόμη διαχειρίζεται την κυκλοφορία σε αυτές τις ζώνες εργασίας και συμβουλεύει τους οδηγούς για την κυκλοφοριακή κατάσταση της περιοχής (είτε σε ζωντανό χρόνο με κάποια πινακίδα στην άκρη του δρόμου είτε μέσω διασύνδεσης με components του Κέντρου Πληροφορίας Μεταφορών ή του Κέντρου Διαχείρισης Συγκοινωνίας και Κυκλοφορίας.

Όλες οι δραστηριότητες συντήρησης πρέπει να παρακολουθούνται και συντονίζονται με λειτουργίες άλλων συστημάτων, βελτιώνοντας έτσι την ποιότητα και την ακρίβεια των διαθέσιμων πληροφοριών σχετικές με αλλαγές στις μετακινήσεις λόγω συντηρήσεων.

Μια εναλλακτική μορφή Κέντρου Διαχείρισης Συντήρησης προορίζεται για την παροχή μιας πηγής και ενός προορισμού για τις ροές πληροφοριών ITS των λειτουργιών

συντήρησης. Έτσι επιτρέπεται ο συντονισμός των εργασιών συντήρησης διαφορετικών δικαιοδοσιών ή μεταξύ δημόσιων και ιδιωτικών φορέων.

- **Κέντρο Διαχείρισης Εκτάκτων Αναγκών - Emergency Management Center (EMC)**

Το «Κέντρο Διαχείρισης Έκτακτης Ανάγκης» αντιπροσωπεύει συστήματα που υποστηρίζουν τη διαχείριση συμβάντων, την αντιμετώπιση καταστροφών, εκκενώσεις περιοχών, την παρακολούθηση της ασφάλειας και άλλες εφαρμογές ITS με γνώμονα την δημόσια ασφάλεια. Περιλαμβάνει τις λειτουργίες που σχετίζονται με σταθερά και κινητά κέντρα επικοινωνίας δημόσιας ασφάλειας, συμπεριλαμβανομένων κέντρων λήψης και αποστολής κλήσεων δημόσιας ασφάλειας που λειτουργούν από την αστυνομία (συμπεριλαμβανομένης της τροχαίας), την πυροσβεστική και τις ιατρικές υπηρεσίες έκτακτης ανάγκης. Περιλαμβάνει λειτουργίες που σχετίζονται με τα Κέντρα Επιχειρήσεων Έκτακτης Ανάγκης που ενεργοποιούνται σε τοπικό και κρατικό επίπεδο για καταστάσεις έκτακτης ανάγκης και τα φορητά και μεταφερόμενα συστήματα που υποστηρίζουν τυχόν επιχειρήσεις κεντρικών συντονιστικών συστημάτων σε ένα περιστατικό. Αντιπροσωπεύει επίσης συστήματα που σχετίζονται με τη ρυμούλκηση, την περισυλλογή, τις περιπολίες και συνολικά την αντίδραση εκτάκτου ανάγκης σε αυτοκινητόδρομους.

Διαχειρίζεται αισθητήρες και κάμερες επιτήρησης που χρησιμοποιούνται για ενίσχυση της ασφάλειας των μεταφορών της οδικής υποδομής (γέφυρες, σήραγγες, κόμβοι κτλ) και γενικά των δημόσιων μεταφορών (ΜΜΜ, δημόσιους χώρους όπως στάσεις και σταθμούς μεταφόρτωσης, ναυπηγείων, σιδηρόδρομων, γέφυρες, σήραγγες, λεωφορειολωρίδες). Παρέχει επίσης υπηρεσίες επιτήρησης για τη βελτίωση της ασφάλειας των ταξιδιωτών σε δημόσιους χώρους που δεν αποτελούν μέρος του συστήματος δημόσιων μεταφορών.

Παρακολουθεί ειδοποιήσεις, συμβουλές και άλλες πληροφορίες απειλών ώστε να προετοιμάζεται και να ανταποκρίνεται σε καταστάσεις έκτακτης ανάγκης. Συντονίζει τις ανταποκρίσεις έκτακτης ανάγκης όπου συμμετέχουν πολλοί φορείς με τα δικά τους συντονιστικά κέντρα. Χρησιμοποιεί σχέδια αντιμετώπισης έκτακτης ανάγκης και εκκενώσεων για να διευκολύνει όλους τους απαραίτητους συντονισμούς. Κοινοποιεί πληροφορίες για καταστάσεις έκτακτης ανάγκης, όπως εκτιμήσεις ζημιών, καταστάσεις ανάγκης επείγουσας επικοινωνίας και πληροφορίες εκκενώσεων. Το Κέντρο Διαχείρισης Εκτάκτων Αναγκών αποτελεί ένα κεντρικό και συντονιστικό σημείο από όπου παρέχονται πληροφορίες έκτακτης ανάγκης που παρέχονται στο επιβατικό κοινό με ειδοποιήσεις ευρείας περιοχής όταν απαιτείται άμεση δημόσια ειδοποίηση.

Παρακολουθεί και διαχειρίζεται στόλους οχημάτων έκτακτης ανάγκης χρησιμοποιώντας πληροφορίες για την κατάσταση του οδικού δικτύου σε πραγματικό χρόνο και πληροφορίες δρομολόγησης από άλλα κέντρα για να βοηθήσει στην επιλογή του οχήματος και των διαδρομών έκτακτης ανάγκης. Συνεργάζεται με άλλα αντίστοιχα κέντρα για να συντονίσει ανάλογα τον έλεγχο της κυκλοφορίας και για να υποστηρίξει τη διαχείριση των οχημάτων έκτακτης ανάγκης, την εφαρμογή ειδικών περιορισμών, η διακοπή κυκλοφορίας, σχέδια ελέγχου κυκλοφορίας εκκενώσεων και άλλες ειδικές στρατηγικές που προσαρμόζουν τα διάφορα συστήματα μεταφορών ώστε να ανταποκρίνονται με τον καλύτερο τρόπο στις απαιτήσεις μιας έκτακτης ανάγκης.

Υπάρχουν και Κέντρα Διαχείρισης Εκτάκτων Αναγκών που παρέχουν τις ροές των πληροφοριών μεταξύ των κέντρων επικοινωνίας που λειτουργούν από υπηρεσίες δημόσιας ασφάλειας, υπηρεσίες διαχείρισης εκτάκτων αναγκών και άλλες υπηρεσίες που συνεργάζονται ιδιωτικές εταιρείες που συμμετέχουν στη συντονισμένη διαχείριση συμβάντων σχετικές με τις μεταφορές, συμπεριλαμβανομένων των καταστροφών. Αυτά τα κέντρα με το διαφορετικό ρόλο έχουν στόχο το συντονισμό των δραστηριοτήτων διαχείρισης εκτάκτων αναγκών όπου δεν υπάρχουν ξεκάθαρα όρια δικαιοδοσίας υποστηρίζοντας απαιτήσεις που μπορεί να χρειαστεί να υποστηριχτούν από διάφορες συμμαχικές υπηρεσίες. Υποστηρίζει επίσης τη διασύνδεση με άλλες συμμαχικές υπηρεσίες, όπως εταιρείες δημοσίου συμφέροντος που συμμετέχουν σε συντονισμένες επιχειρήσεις ειδικών συνθηκών και συμβάντων στους αυτοκινητόδρομους.

- **Κέντρο Διαχείρισης Συγκοινωνίας & Κυκλοφορίας - Transit & Traffic Management Center (TTMC)**

Το Κέντρο Διαχείρισης αυτό από την πλευρά των συγκοινωνιών διαχειρίζεται στόλους οχημάτων μαζικών συγκοινωνιών και συντονίζεται με άλλα μέσα και υπηρεσίες μεταφορών. Παρέχει λειτουργίες συντήρησης, πληροφόρησης πελατών, προγραμματισμού και διαχείρισης για την περιουσία των οργανισμών μεταφορών. Καλύπτει διάφορα διαφορετικά συστήματα κεντρικής διαχείρισης για στάθμευση, υποστήριξης ευέλικτων διαδρομών, υπηρεσιών σιδηροδρομικών μεταφορών και των υπηρεσιών ταχέων διελεύσεων λεωφορείων. Το component αυτό επίσης υποστηρίζει επικοινωνίες μεταξύ υπηρεσιών συγκοινωνιών με άλλες λειτουργικές οντότητες, όπως υπηρεσίες απόκρισης έκτακτης ανάγκης και συστήματα διαχείρισης κυκλοφορίας.

Από την πλευρά της κυκλοφορίας γίνεται παρακολούθηση και έλεγχος της κυκλοφορίας και το οδικού δικτύου. Σε αυτή την παράγραφο αναφερόμαστε στο ρόλο του σαν κέντρο που διαχειρίζεται ένα ευρύ φάσμα μεταφορικών εγκαταστάσεων (αυτοκινητοδρόμων, αγροτικών και περιφερειακών δρόμων, συστημάτων ελέγχου αστικής και μη κυκλοφορίας). Επικοινωνεί με τον έξυπνο εξοπλισμό των αυτοκινητοδρόμων και με τα online συνδεδεμένα οχήματα για να παρακολουθεί τη διαχείριση της ροής της κυκλοφορίας, την κατάσταση του οδοστρώματος και των περιβαλλοντικών συνθηκών. Διαχειρίζεται τους πόρους της κυκλοφορίας και των μεταφορών για να υποστηρίξει τις υπηρεσίες συντονισμού στην αντιμετώπιση και την ανάκαμψη από περιστατικά που κυμαίνονται από μικρά τροχαία συμβάντα μέχρι μεγάλες καταστροφές.

Και σε αυτό το component υπάρχουν μορφές Κέντρων Διαχείρισης Συγκοινωνίας & Κυκλοφορίας με διαφορετικό ρόλο. Έχουν στόχο να παρέχουν μια πηγή και έναν προορισμό για τις ροές πληροφοριών μεταξύ κέντρων διαχείρισης ομότιμων συγκοινωνιών και μεταξύ λειτουργιών διαχείρισης κυκλοφορίας. Επιτρέπουν τον συντονισμό των δραστηριοτήτων διαχείρισης της κυκλοφορίας σε διαφορετικές περιοχές δικαιοδοσίας.

- **Κέντρο Διαχείρισης και Διανομής Δεδομένων - Data Distribution System (DDS)**

Το Σύστημα Διαχείρισης και Διανομής Δεδομένων συλλέγει, επεξεργάζεται και διανέμει δεδομένα από τα ITS, συνδέοντας τα στοιχεία που παράγουν δεδομένα με στοιχεία που χρειάζονται δεδομένα για να λειτουργήσουν και αυτό γίνεται διευκολύνοντας την ανταλλαγή αυτών των δεδομένων.

Σε αυτό το component αντιπροσωπεύονται και εναλλακτικά Κέντρα Διαχείρισης και Διανομής Δεδομένων. Προορισμός τους είναι να παρέχουν μια πηγή και έναν προορισμό για την ανταλλαγή πληροφοριών μεταξύ ομότιμων συστημάτων διανομής δεδομένων. Υποστηρίζουν μοντελοποίηση λειτουργιών, εργασιών και περιοχών που περιλαμβάνουν πολλαπλά συστήματα, διασυνδεδεμένα μεταξύ τους, τα οποία διανέμουν τα δεδομένα που διαχειρίζονται από κοινού κάποια επιπλέον διανομή δεδομένων στο περιβάλλον του συνδεδεμένου οχήματος.

- **Σύστημα Διαχείρισης Χαρτών - Map Management System (MMS)**

Ένα Σύστημα Διαχείρισης Χαρτών παρέχει τη λειτουργικότητα GIS (Geographic Information System - Σύστημα Γεωγραφικών Πληροφοριών) η οποία είναι απαραίτητη για την υποστήριξη, τη δημιουργία και τη διαχείριση των δεδομένων των χαρτών. Παρέχει ένα περιβάλλον στο χρήστη έτσι ώστε να μπορεί να διαχειριστεί τα δεδομένα ενός χάρτη και ταυτόχρονα να μπορεί να αποδίδει σε αυτόν τον έλεγχο και την ορθή απεικόνιση των χαρτών αυτών. Ταυτόχρονα δίνει τη δυνατότητα διασύνδεσης με εξωτερικές πηγές δεδομένων, συμπεριλαμβανομένων των στοιχείων στο περιβάλλον του οχήματος που είναι συνδεδεμένα με το διαδίκτυο.

Στο component αυτό συμπεριλαμβάνεται το σύστημα ενημέρωσης των χαρτών που αναφέρεται στο σύστημα διεπαφής με τις βάσεις δεδομένων των χαρτών που χρησιμοποιούνται για την υποστήριξη των υπηρεσιών ITS. Υποστηρίζει την παροχή των δεδομένων στους χάρτες που χρησιμοποιούνται σε πραγματικό χρόνο στα οχήματα (πχ σύνολα δεδομένων γεωμετρίας δρόμων και διασταυρώσεων), ταξιδιώτες (πχ δεδομένα χάρτη που χρησιμοποιούνται από φορείς κυκλοφορίας για την παρακολούθηση και διαχείριση του οδικού δικτύου και δεδομένα χαρτών που χρησιμοποιούνται όσους διαχειρίζονται στόλους οχημάτων για τη διαχείριση τους). Μπορεί να αντιπροσωπεύει έναν τρίτο πάροχο ή έναν εσωτερικό οργανισμό που παράγει δεδομένα για τους χάρτες για χρήση από την ίδια την εταιρεία. Στην τελευταία περίπτωση, το σύστημα που ενημερώνει τους χάρτες περιλαμβάνεται συνήθως ως μέρος ενός κέντρου (πχ Κέντρο Διαχείρισης Συγκοινωνίας & Κυκλοφορίας) του ιδιοκτήτη ή του διαχειριστή της υποδομής που διαχειρίζεται τα δεδομένα χάρτη. Τα προϊόντα μπορεί να περιλαμβάνουν μια απλή εμφάνιση του χάρτη, σύνολα δεδομένων χαρτών που ορίζουν με λεπτομέρεια τοπολογίες και γεωμετρίες του οδικού δικτύου ή πλήρεις βάσεις δεδομένων συστημάτων γεωγραφικών πληροφοριών που χρησιμοποιούνται για να υποστηρίξουν σχεδιασμό και λειτουργίες.

Τέλος υπάρχουν και άλλα συστήματα χαρτών που έχουν το ρόλο να παρέχουν μια πηγή και έναν προορισμό για τις ροές πληροφοριών ITS μεταξύ των ομότιμων παρόχων ενημέρωσης χαρτών. Επιτρέπει συνεργατικές ανταλλαγές πληροφοριών μεταξύ βασικών χαρτών και εξειδικευμένων χαρτών και οποιαδήποτε άλλη ανταλλαγή γεωγραφικών πληροφοριών μεταξύ παρόχων δεδομένων χαρτών.

- **Οχήματα Δημόσιων Συγκοινωνιών ή MMM - Public Transportation Vehicle (PTV)**

Τα οχήματα σαν γενική κατηγορία είναι πολύ σημαντική στο οικοδόμημα των ITS και αντιπροσωπεύουν γενικά το οποιοδήποτε μεμονωμένο όχημα. Στα δύο ακόλουθα component συμπεριλαμβάνονται και τα φυσικά χαρακτηριστικά των οχημάτων όπως ύψος, πλάτος, μήκος, βάρος και άλλες ιδιότητες (πχ αριθμός αξόνων) τα οποία χαρακτηριστικά των οχημάτων που μπορούν να ανιχνευθούν και να μετρηθούν και στη συνέχεια να ταξινομηθούν. Επίσης στις δύο αυτές ακόλουθες κατηγορίες

αποτυπώνονται και οι φυσικές ιδιότητες των οχημάτων που μπορούν να ανιχνευτούν από αισθητήρες που υπάρχουν πάνω στα οχήματα ή στις υποδομές για την υποστηρίζουν τα συστήματα του αυτοματισμού οχημάτων και των αισθητήρων κυκλοφορίας.

Όλα αυτά τα αναλογικά χαρακτηριστικά αντιπροσωπεύουν τις τιμές που συλλέγονται από τους αντίστοιχους αισθητήρες που χρησιμοποιούνται για την ανίχνευση και την αξιολόγηση οχημάτων εντός της εμβέλειας του αισθητήρα για την υποστήριξη της ασφαλούς λειτουργίας των οχημάτων και της ασφαλούς διαχείρισης της κυκλοφορίας.

Εν συνεχεία τα οχήματα των δημόσιων συγκοινωνιών και τα ΜΜΜ ταξινομούνται στις παρακάτω μεγάλες κατηγορίες για λόγους οικονομίας της παρούσας εργασίας.

Τα επαγγελματικά οχήματα είναι εκείνα που φιλοξενούν τον εποχούμενο εξοπλισμό με δυνατότητες ITS. Συμπεριλαμβάνει τους δίαυλους μεταφοράς δεδομένων βαρέων οχημάτων καθώς και όλα τα άλλα σημεία διασύνδεσης μεταξύ των εποχούμενων συστημάτων και των υπόλοιπων επαγγελματικών οχημάτων. Αυτά τα οχήματα χρησιμοποιούνται για μεταφορές εμπορευμάτων, οδηγούνται από επαγγελματίες οδηγούς που συνήθως είναι τμήμα ενός μεγαλύτερου στόλου οχημάτων και διαχειρίζονται κεντρικά. Στα επαγγελματικά οχήματα ανήκουν όλα τα οχήματα μεταφοράς εμπορευμάτων, από μικρά φορτηγά που χρησιμοποιούνται σε τοπικές υπηρεσίες παραλαβής και παράδοσης μέχρι μεγάλες ρυμουλκούμενες πλατφόρμες που εκτελούν πολύ μεγάλες αποστάσεις.

Σε αυτή την κατηγορία συμπεριλαμβάνονται κει τα οχήματα ή μέσα μαζικής μεταφοράς τα οποία διαθέτουν συστήματα για να παρέχουν λειτουργίες ITS. Και αυτά περιλαμβάνουν ειδικούς διαύλους μεταφοράς δεδομένων σε αρκετά μεγάλη έκταση γεωγραφική αλλά και με μεγάλη γκάμα ευρεία γκάμα εξαρτημάτων που συνήθως είναι μοναδικά για το κάθε ένα ΜΜΜ. Μέσα σε αυτά συμπεριλαμβάνεται ο εξοπλισμός ηλεκτρονικών εισιτηρίων, οι μετρητές επιβατών και διάφορα συστήματα ασφαλείας συγκοινωνιών. Τα οχήματα αυτά μπορεί να είναι από λεωφορεία μέχρι και τρένα ή άλλα οχήματα που μεταφέρουν μαζικά επιβάτες.

Υπάρχουν επίσης και οχήματα σχετικά με τις συντηρήσεις και με τις κατασκευές. Και όπως υποδηλώνει και το όνομα τους πρόκειται για εξειδικευμένα οχήματα που μεταφέρουν ή διαθέτουν εποχούμενο εξοπλισμό κατασκευών και συντηρήσεων και αντίστοιχα διαθέτουν κάποιο σύστημα ITS. Περιλαμβάνεται και εδώ ο απαραίτητος δίαυλος μεταφοράς δεδομένων, τους αισθητήρες και τμήματα «έξυπνου» εξοπλισμού (ενσωματωμένου ή όχι) που χρησιμοποιούνται για την παρακολούθηση και τον έλεγχο των συστημάτων του κεντρικού οχήματος. Για παράδειγμα ένα τέτοιο σύστημα είναι η συνεργασία αισθητήρων, λογισμικού και εξαρτημάτων φόρτωσης και εκφόρτωσης σε ένα εκχιονιστικό που διαθέτει έξυπνο σύστημα διανομής αλατιού πάνω σε όχημα

- **IX Οχήματα - Private Vehicle (PV)**

Σε συνέχεια της προηγούμενης κατηγορίας υπάρχουν και τα οχήματα ιδιωτικής χρήσης που διαθέτουν ITS συστήματα. Ονομάζονται αλλιώς και Βασικά Οχήματα (Basic Vehicles) και αντιπροσωπεύουν ένα όχημα που λειτουργεί και δεν ανήκει στην παραπάνω κατηγορία αλλά χρησιμοποιείται από μεμονωμένους οδηγούς και λίγους και συγκεκριμένους επιβάτες.

Περιλαμβάνονται τα του οχήματα που μπορούν να διασυνδεθούν με το διαδίκτυο και να διαθέτουν ηλεκτρονικά ITS καθώς και όλα τα συστήματα άνεσης και ψυχαγωγίας του οδηγού όπως και άλλα ηλεκτρονικά πέρα από τα ITS. Υπάρχουν διεπαφές τόσο με άλλες εποχούμενες ITS οντότητες και με άλλα συστήματα τα οποία έχουν είτε παθητική είτε ενεργητική αλληλεπίδραση με το όχημα μας καθώς υποστηρίζουν λειτουργίες όπως την παρακολούθηση και τη διαχείριση των οχήματος και της κυκλοφορίας γενικότερα.

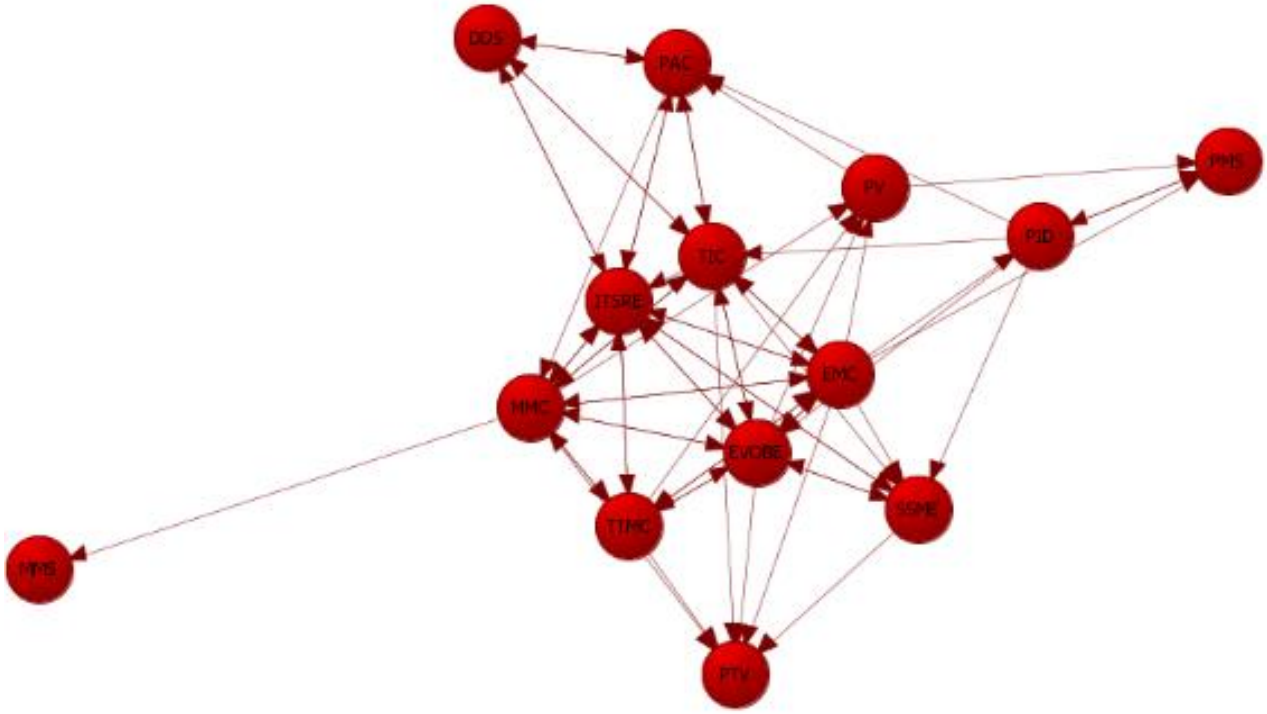
Οι εξωτερικές διεπαφές μπορεί επίσης να έχουν να κάνουν με εξοπλισμό επί του οχήματος (πχ ένα smartphone μέσα στο όχημα). Οι εσωτερικές διεπαφές συχνά υλοποιούνται μέσω ενός δίαυλο επικοινωνίας δεδομένων που και αυτός ανήκει σε αυτήν εδώ την κατηγορία. Να σημειώσουμε εδώ πως όταν αναφερόμαστε σε κάποιο «όχημα» αντιπροσωπεύει τις γενικές λειτουργίες και τις διεπαφές που σχετίζονται με IX αυτοκίνητα καθώς και με τα επαγγελματικά οχήματα, τα MMM, τα οχήματα έκτακτης ανάγκης, οχήματα μεταφοράς και άλλα εξειδικευμένα οχήματα.

- **Εξοπλισμός επί Οχήματος Έκτακτης Ανάγκης - Emergency Vehicle OBE (EVOBE)**

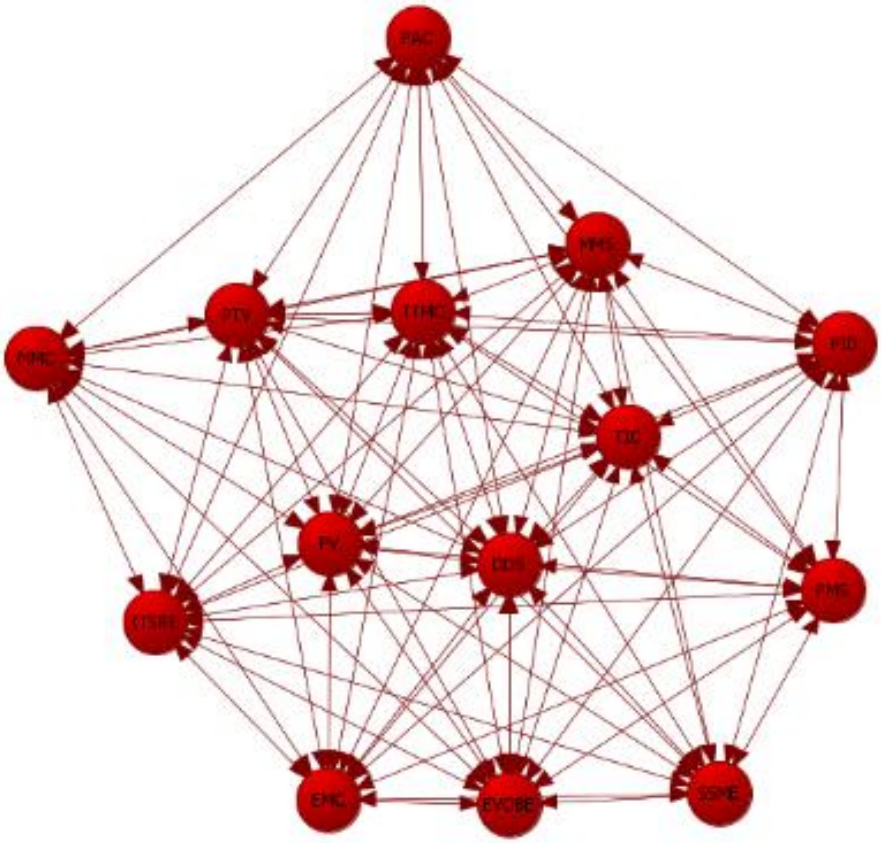
Ο Εξοπλισμός Εποχούμενου Οχήματος Έκτακτης Ανάγκης (OBE) βρίσκεται σε ένα όχημα έκτακτης ανάγκης και παρέχει τις λειτουργίες επεξεργασίας, αποθήκευσης και επικοινωνίας που υποστηρίζουν εφαρμογές συνδεδεμένων οχημάτων που σχετίζονται με τη δημόσια ασφάλεια. Αντιπροσωπεύει μια ομάδα οχημάτων τα οποία έχουν στην κατοχή τους και τα λειτουργούν η αστυνομία, η πυροσβεστική και οι ιατρικές υπηρεσίες έκτακτης ανάγκης. Επίσης αντιπροσωπεύει και άλλα οχήματα αντιμετώπισης έκτακτων περιστατικών, όπως η ρυμούλκηση, η περισυλλογή οι περιπολίες στους αυτοκινητόδρομους. Περιλαμβάνει αμφίδρομες επικοινωνίες για την υποστήριξη συντονισμένων ανταποκρίσεων σε καταστάσεις έκτακτης ανάγκης. Ένας διαφορετικός εξοπλισμός στα οχήματα έκτακτης ανάγκης υποστηρίζει τη γενική ασφάλεια του οχήματος και τις δυνατότητες άμεσης και έγκαιρης πληροφόρησης του οδηγού. Αυτός ο εξοπλισμός μπορεί να υπάρχει και σε όλα τα οχήματα. Ο Εξοπλισμός επί Οχημάτων Έκτακτης Ανάγκης συμπληρώνει αυτές τις γενικές δυνατότητες πιο στοχευμένα ανάλογα και το ρόλο του κάθε ειδικού οχήματος έκτακτης ανάγκης.

Οι μέθοδοι που προτείνονται στις πηγές ([75]) και ([76]) χρησιμοποιούνται σαν προϋπάρχοντες τρόποι επεξεργασίας και εξαγωγής αποτελεσμάτων. Αναφερόμαστε δηλαδή πρώτον στα components του συστήματος και τις διασυνδέσεις μεταξύ τους τα οποία που συνθέτουν την γραφική αναπαράσταση του συστήματος, δεύτερον στις τιμές του αντίκτυπου (impact) και της πιθανότητας (likelihood) που σχετίζονται με τις απειλές στο STRIDE και υπολογίζονται μέσω του DREAD για κάθε ξεχωριστό στοιχείο και τρίτον στη λίστα των διαθέσιμων controls κυβερνοασφάλειας τα οποία συνοδεύονται με πληροφορίες για το κόστος τους και την αποτελεσματικότητά τους. Τα σχήματα που ακολουθούν και απλά παραθέτονται σε προηγούμενη παράγραφο απεικονίζουν τις γραφικές αναπαραστάσεις των Cyber Physical Systems των ITS με τις διασυνδέσεις και τις αλληλεξαρτήσεις τους.[10,45,70]

ITS: Διασυνδέσεις – Αλληλεξαρτήσεις Ροών Ελέγχου μεταξύ των Components



ITS: Διασυνδέσεις – Αλληλεξαρτήσεις Ροών Πληροφοριών μεταξύ των Components



Οι τιμές αντίκτυπου (impact) και πιθανότητας (likelihood) που σχετίζονται με τις απειλές STRIDE και υπολογίζονται μέσω του DREAD απεικονίζονται στους πίνακες που ακολουθούν[70].

Πίνακας Πιθανότητας (Likelihood)

Likelihood														
	PID	**ITSRE**	**SSME**	**PMS**	**PAC**	**TIC**	**MMC**	**EMC**	**TTMC**	**DDS**	**MMS**	**PTV**	**PV**	**EVOBE**
S	2,67	2	2,33	2	2	2,33	2	2,33	2	2,33	2	2,33	2,33	2,33
T	1,33	1,33	1	1,33	1	1,33	1	1	1,33	1,33	1,33	1,33	1,33	1,67
R	2,33	1,33	2	2,33	3	2,67	1,33	2,67	2	2	1,33	1,67	1,33	1,67
I	2,67	2	2,67	2,33	2,67	2,67	2	2,33	2,33	2,67	2,33	2	2,67	2,33
D	2	2	3	2	2	2,33	1	2,67	2,33	3	2	2	2	2,33
E	2,67	2,33	2,67	2,33	2,33	2,67	2	2,33	2	2,33	2,33	2	2	2

Πίνακας Αντίκτυπου (Impact)

Impact														
	PID	**ITSRE**	**SSME**	**PMS**	**PAC**	**TIC**	**MMC**	**EMC**	**TTMC**	**DDS**	**MMS**	**PTV**	**PV**	**EVOBE**
S	2,5	2	2,5	2	2	2,5	2	3	2	2,5	2	2	2	2,5
T	1	1,5	1	1	1	1	1	1,5	1,5	1,5	1	1,5	1,5	2
R	2,5	1,5	1,5	2,5	3	2	1,5	2,5	1,5	2	1,5	1,5	1,5	2
I	3	3	3	3	2,5	3	2	2,5	2,5	3	3	2	3	2,5
D	2,5	1,5	3	2	2	2,5	1,5	3	3	3	2	2	2	2,5
E	2,5	2	2,5	2,5	2,5	2,5	2	3	2	2,5	2,5	2	2	2,5

Στους πίνακες αυτούς κάθε γραμμή αντιπροσωπεύει μία από τις απειλές STRIDE, που υποδεικνύεται με το αντίστοιχο αρχικό γράμμα (S-T-R-I-D-E). Κάθε στήλη αντιπροσωπεύει τα Cyber Physical συστήματα των Components μεμονωμένους CPS, που υποδεικνύονται με τα αντίστοιχα αρχικά τους, όπως αναλύονται στην Ενότητα 8.1. Οι τιμές εντός των κελιών οι αντίστοιχες τιμές του αντίκτυπου και της πιθανότητας ανά απειλή STRIDE (βλ. τίτλους) και ανά μεμονωμένο component. Αυτά έχουν υπολογιστεί αντίστοιχα μέσω των εξισώσεων της παραγράφου 5.iii που ξαναδίνονται παρακάτω. Αυτές οι τιμές στη συνέχεια χρησιμοποιούνται σαν είσοδοι στον Αλγόριθμο 1 της παραγράφου 6.ii, για τον υπολογισμό του συνολικού ρίσκου σε κάθε component.

$$Επίπτωση_t^s = \frac{Ζημία + Επηρεαζόμενα\ Συστήματα}{2}$$

$$Πιθανότητα_t^s = \frac{Αναπαραγωγιμότητα + Εκμεταλλευσιμότητα + Ανακαλυπτικότητα}{3}$$

ii. Controls προς εξέταση[77]

Σε αυτή την παράγραφο γίνεται μια συνοπτική επεξήγηση του κάθε controls ασφαλείας επί των οποίων όπως προείπαμε θα κάνουμε προσπάθειες βελτίωσης επί της ασφάλειας ξεχωριστά σε κάθε component με στόχο την cyber ασφάλεια του κάθε ενός από τα component αυτά ξεχωριστά αλλά και του κεντρικού συστήματος συνολικά.

Το NIST (National Institute of Standards and Technology) των ΗΠΑ είναι υπεύθυνο για την ανάπτυξη του NIST CSF, που θεωρείται το τελειότερο πλαίσιο πρότυπο για την ασφάλεια στον κυβερνοχώρο. Η ειδική έκδοση του NIST 800-53 (Special Publication 800-53) λειτουργεί σαν μια από τις πιο βασικές κατευθυντήριες γραμμές για την ασφάλεια στον κυβερνοχώρο καταρχήν γενικά για τις υπηρεσίες στις ΗΠΑ με στόχο πάντα τη διατήρηση της ασφάλειας στα συστήματα πληροφοριών τους. Η

οδηγία αυτή λειτουργεί για να προστατεύει από πλευράς ασφάλειας τους πολίτες τόσο στην ιδιωτική τους ζωή όσο και στις υπηρεσίες που εκείνοι εξυπηρετούνται. Η NIST Special Publication 800-53 κατά την πέμπτη αναθεώρησή του περιείχε περισσότερα από 1000 στοιχεία ελέγχου. Αυτός ο κατάλογος controls (ελέγχων) ασφαλείας επιτρέπει στον οποιοδήποτε να χρησιμοποιεί ένα ισχυρό πρότυπο με συνιστώμενους ελέγχους ασφάλειας και απορρήτου για πληροφοριακά συστήματα για προστασία από πιθανά ζητήματα ασφάλειας και κυβερνοεπιθέσεις. Στη συνέχεια θα αναφέρουμε τις 18 επονομαζόμενες «οικογένειες» controls που προτείνει η NIST Special Publication 800-53 και θα δώσουμε μια γενική επισκόπηση των απαιτήσεων καθεμιάς.

- **Access Control (AC):** Είναι η οικογένεια controls πρόσβασης σε υπολογιστικά συστήματα. Αποτελείται από απαιτήσεις ασφαλείας οι οποίες περιγράφουν λεπτομερώς τα διάφορα logs του συστήματος μας. Αυτό περιλαμβάνει λειτουργείες όπως το ποιος έχει πρόσβαση σε ποια στοιχεία και δυνατότητες ανάγνωσης αναφορών του συστήματος, όπως διαχείριση λογαριασμών, δικαιώματα επί των συστημάτων και συνδέσεις απομακρυσμένης πρόσβασης για να είναι ξεκάθαρο ποιοι χρήστες και πότε έχουν πρόσβαση στο σύστημα καθώς και ποιο είναι το επίπεδο στο οποίο «φτάνει» η πρόσβασή τους.
- **Awareness and Training (AT):** Αυτή η οικογένεια αποτελείται από controls ασφαλείας που σχετίζονται με τις δυνατότητες ελέγχου που δύναται να εκτελεί ένας οργανισμός. Περιλαμβάνει τις πολιτικές και τις διαδικασίες αυτών των ελέγχων, καταγραφή logs από αυτούς τους ελέγχους, δημιουργία εκθέσεων των logs των ελέγχων και προστασία των πληροφοριών που προέκυψαν από τους ελέγχους.
- **Audit and Accountability (AU):** Τα σύνολα των controls σε αυτή την οικογένεια της ευαισθητοποίησης και της εκπαίδευσης είναι συγκεκριμένα και, όπως φανερώνει και το όνομά τους, έχουν να κάνουν με την εκπαίδευση και τις διαδικασίες ασφαλείας, συμπεριλαμβανομένων των αρχείων που καταγράφουν τις όποιες εκπαιδεύσεις ασφαλείας.
- **Security Assessment and Authorization (CA):** Η οικογένεια του control των αξιολογήσεων και των εξουσιοδοτήσεων ασφαλείας συμπεριλαμβάνει ελέγχους που συμπληρώνουν την εκτέλεση των αξιολογήσεων ασφαλείας, των εξουσιοδοτήσεων, της συνεχούς παρακολούθησης, του μνημονίου ενεργειών και των σημαντικών σημείων (milestones) καθώς και των διασυνδέσεων με άλλα συστήματα.
- **Configuration Management (CM):** Τα στοιχεία του control μιας διαχείρισης της διαμόρφωσης είναι συγκεκριμένα όσον αφορά τις αντίστοιχες πολιτικές τους. Περιλαμβάνουν μια βασική διαμόρφωση η οποία λειτουργεί σαν βάση για μελλοντικές κατασκευές ή αλλαγές που θα γίνουν σε κάποια πληροφοριακά συστήματα. Εδώ συμπεριλαμβάνονται επιπλέον και τα ιστορικά στοιχεία ενός συστήματος πληροφοριών τα οποία στη συνέχεια αναλύονται για τις επιπτώσεις τους στην ασφάλεια των συστημάτων.
- **Contingency Planning (CP):** Η οικογένεια των controls σχεδιασμού σε καταστάσεις έκτακτης ανάγκης περιλαμβάνει ελέγχους ειδικά για σχέδια έκτακτης ανάγκης σε περίπτωση που συμβεί ένα συμβάν κυβερνοασφάλειας. Αυτό περιλαμβάνει ελέγχους όπως δοκιμές σχεδίων έκτακτης ανάγκης, ενημερώσεις, εκπαιδεύσεις, δημιουργία αντιγράφων ασφαλείας και ανασύσταση συστημάτων.
- **Identification and Authentication (IA):** Τα controls ταυτοποίησης και ελέγχου ταυτότητας αφορούν συγκεκριμένες πολιτικές αναγνώρισης στοιχείων εντός οργανισμού. Αυτό περιλαμβάνει λειτουργίες όπως τον προσδιορισμό και τον έλεγχο

ταυτότητας των χρηστών καθώς και τον τρόπο διαχείρισης αυτών των συστημάτων λειτουργιών ταυτοποίησης.

- **Incident Response (IR)**: Τα controls αντιμετώπισης περιστατικών είναι συγκεκριμένα στο κομμάτι της πολιτικής που θα επιλεγεί και της διαδικασίας αντιμετώπισης που θα ακολουθηθεί εντός ενός οργανισμού. Εντός αυτών συμπεριλαμβάνονται εκπαίδευση για την αντιμετώπιση περιστατικών, δοκιμές, συνεχής παρακολούθηση, υποβολή αναφορών καθώς και σχέδια απόκρισης
- **Maintenance (MA):** Τα controls της συντήρησης στην 5η αναθεώρηση της NIST 800-53 αποτυπώνουν με λεπτομέρεια τις απαιτήσεις που απαιτούνται έτσι ώστε να παραμείνουν συντηρημένα τα συστήματα και τα εργαλεία που χρησιμοποιούνται.
- **Media Protection (MP):** Η οικογένεια των controls προστασίας των πολυμέσων περιλαμβάνει στοιχεία ελέγχου ειδικά για την πρόσβαση, τη σήμανση, την αποθήκευση, τις πολιτικές μεταφοράς, την εκκαθάριση και την προκαθορισμένη χρήση των ίδιων των πολυμέσων.
- **Physical and Environmental Protection (PE):** Η οικογένεια των controls της φυσικής ασφάλειας και της ασφάλειας του περιβάλλοντος εργασίας βρίσκει εφαρμογή στην προστασία από διάφορες φυσικές απειλές των συστημάτων, των κτιρίων και των συναφών υποδομών υποστήριξης. Εδώ συμπεριλαμβάνονται έλεγχοι για τη όποια φυσική πρόσβαση, την παρακολούθηση φυσικών διαδικασιών, τις καταγραφές διάφορων επισκέψεων χώρων, τις τυχόν έκτακτες διακοπές λειτουργίας, την συνεχή παροχή ρεύματος, τον φωτισμό, την πυρασφάλεια και την προστασία τυχόν ζημιών από νερό.
- **Planning (PL):** Τα controls σχεδιασμού στο NIST 800-53 ειδικεύονται στις πολιτικές σχεδιασμού ασφάλειας ενός οργανισμού οι οποίες είναι σχετικές με το σκοπό του, το πεδίο εφαρμογής του, το ρόλο του, τις ευθύνες του, τις όποιες δεσμεύσεις διαχείρισης του, το συντονισμό μεταξύ των οντοτήτων του και την οργανωτική του συμμόρφωση.
- **Personnel Security (PS):** Τα controls για την ασφάλεια του προσωπικού σχετίζονται με τον τρόπο που ένας οργανισμός προστατεύει το προσωπικό του μέσω του πιθανού ρίσκου κάθε θέσης, παρακολούθησης των ενεργειών του προσωπικού, της λήξης της εργασίας, των μεταφορών, την επιβολή κυρώσεων και των συμφωνιών για παραχώρηση πρόσβασης.
- **Risk Assessment (RA):** Η οικογένεια των controls της εκτίμησης κινδύνου σχετίζεται με τις πολιτικές που επιλέγονται για να αξιολογήσουν το ρίσκο και την δυνατότητα ανεύρεσης των ευπαθειών ενός οργανισμού. Αν χρησιμοποιείται μια ολοκληρωμένης πρόταση διαχείρισης ρίσκου όπως το λογισμικό CyberStrong οι εμπλεκόμενοι φορείς μπορούν να βοηθηθούν σε μεγάλο βαθμό στις προσπάθειες που κάνουν για εξορθολογισμό και αυτοματοποίηση των όποιων προσπαθειών συμμόρφωσης του με το NIST 800-53.
- **System and Services Acquisition (SA):** Η οικογένεια των controls κτήσης συστημάτων και υπηρεσιών συσχετίζεται με ελέγχους οι οποίοι προστατεύουν τους πόρους που έχουν κατανεμηθεί σε αντίστοιχες εργασίες και τον κύκλο ζωής ανάπτυξης του συστήματος ενός οργανισμού. Αυτό περιλαμβάνει controls που τεκμηριώνουν διάφορα συστήματα πληροφοριών, controls που διαχειρίζονται και διαμορφώνουν παραμέτρους ανάπτυξης και controls δοκιμών και αξιολόγησης ασφάλειας που χρησιμοποιούν οι developers.

- **System and Communications Protection (SC):** Η οικογένεια των controls αυτή είναι υπεύθυνη για την προστασία των συστημάτων και των διαδικασιών επικοινωνίας. Συμπεριλαμβάνονται προστασία ορίων, προστασία εν αποθέσει πληροφοριών, συλλογικές υπολογιστικές συσκευές, προστασία κρυπτογραφίας, προστασία DoS (denial of services) και πολλά άλλα.
- **System and Information Integrity (SI):** Η οικογένεια των controls αυτή προφανώς συσχετίζεται με στοιχεία ελέγχου που προστατεύουν την ακεραιότητα συστημάτων και πληροφοριών. Περιλαμβάνονται αποκατάσταση ελαττωμάτων, προστασία από κακόβουλο κώδικα, παρακολούθηση πληροφοριακών συστημάτων, ειδοποιήσεις ασφαλείας, ακεραιότητα software και firmware και προστασία από ανεπιθύμητα μηνύματα.
- **Program Management (PM):** Η οικογένεια των controls της αφορά τα πρόσωπα που διαχειρίζονται το πρόγραμμα κυβερνοασφάλειας και τον τρόπο λειτουργίας του. Αυτό περιλαμβάνει, χωρίς να περιορίζεται όμως αποκλειστικά σε αυτό, ένα σχέδιο υποδομών με ζωτική σημασίας, ένα σχέδιο προγράμματος ασφάλειας πληροφοριών, ένα σχέδιο σημαντικών σημείων (milestones) και διαδικασιών, μιας στρατηγικής διαχείρισης ρίσκων και τέλος μιας εταιρικής αρχιτεκτονικής.
- **Privacy Controls (PC):** Η οικογένεια τους controls αυτών αναφέρεται στους ελέγχους διασφάλισης ιδιωτικότητας που γίνονται επί διοικητικών, τεχνικών και φυσικών στοιχείων ενός οργανισμού. Ελέγχουν και διασφαλίζουν τη συμμόρφωσή του με τις απαιτήσεις απορρήτου και τη διαχείριση του αντίστοιχου ρίσκου βάση του NIST 800-53. Από την αξιολόγηση αυτών προκύπτει αν ο οργανισμός λειτουργούν όπως προβλέπεται και αν επαρκούν για να διασφαλίζεται η συμμόρφωση με τις ισχύουσες απαιτήσεις. Η αξιολόγηση των controls αποτελεί ταυτόχρονα και ένα επίσημο έγγραφο λεπτομερούς περιγραφής της διαδικασίας και του αποτελέσματος της αξιολόγησης.

Η χρήση μιας ολοκληρωμένης λύσης διαχείρισης ρίσκου όπως το CyberStrong μπορεί να βοηθήσει στον εξορθολογισμό και την εναρμόνιση των προσπαθειών κυβερνοασφάλειας ενός οργανισμού σε πολλά διαφορετικά πλαίσια, εξοικονομώντας πολύτιμο χρόνο, ενέργεια και πόρους στις ομάδες εργασίας στην προσπάθεια τους να συμμορφώνονται συνεχώς με το NIST 800-53.

iii. Βέλτιστη επιλογή των Controls στα εξεταζόμενα ITS

Τα ITS τα οποία εξετάζονται στην παρούσα εργασία είναι εξοπλισμένα με προηγμένα διασυνδεδεμένα Cyber Physical Συστήματα τα οποία πολλές φορές έχουν κατασκευαστεί με τέτοιο τρόπο έτσι ώστε να μπορούν να διαχειρίζονται λειτουργίες των μεταφορών χωρίς ανθρώπινη παρέμβαση. Οι διασυνδέσεις και οι αλληλεξαρτήσεις των ροών των πληροφοριών και των ροών ελέγχου μεταξύ των components των ITS συστημάτων που εξετάζουμε απεικονίζονται αναλυτικά στα αντίστοιχα σχεδιαγράμματα της προηγούμενης παραγράφου. Ο πίνακας που ακολουθεί περιέχει τους συντελεστές επίδρασης μεταξύ όλων των εξεταζόμενων components. Κάθε γραμμή και κάθε στήλη του πίνακα αντιπροσωπεύει ένα Component από τα ITS που εξετάζουμε, τα οποία υποδεικνύονται με τα αντίστοιχα αρχικά τους, όπως και αυτά ορίστηκαν την προηγούμενη παράγραφο (8.i).

Πίνακας Συντελεστών Επίδρασης μεταξύ των Components των ITS

	ITS	PID	ITSRE	SSME	PMS	PAC	TIC	MMC	EMC	TTMC	DDS	MMS	PTV	PV	EVOB
ITS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
PID	0.5575	0	0	0.5575	0.5575	0.5575	0.5575	0	0.423	0.423	0.423	0.423	0.423	0.423	0.5575
ITSRE	0.75	0	0	0.75	0.4615	0.75	0.4615	0.75	0.75	0.75	0.75	0.4615	0.4615	0.4615	0.75
SSME	0.423	0.423	0.577	0	0.423	0	0.423	0	0.423	0.423	0.423	0.423	0.577	0.423	0.577
PMS	0.5	0.5	0.423	0.423	0	0.423	0.423	0	0.423	0.423	0.423	0.423	0	0.423	0.423
PAC	0.5575	0.3845	0.5575	0	0.3845	0	0.5575	0.5575	0	0.3845	0.5575	0.3845	0.3845	0.3845	0
TIC	0.769	0.5	0.769	0.769	0.5	0.769	0	0.769	0.769	0.5	0.769	0.5	0.769	0.5	0.769
MMC	0.3845	0	0.6535	0	0	0.3845	0.6535	0	0.6535	0.6535	0.3845	0.6535	0.6535	0.6535	0.6535
EMC	0.75	0.75	0.75	0.75	0.75	0	0.75	0.75	0	0.75	0.4615	0.4615	0.75	0.75	0.75
TTMC	0.5	0.5	0.6925	0.5	0.5	0.5	0.5	0.6925	0.6925	0	0.5	0.5	0.6925	0.6925	0.6925
DDS	0.5	0.5	0.6155	0.5	0.5	0.6155	0.6155	0.5	0.5	0.5	0	0.5	0.5	0.5	0.5
MMS	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0	0.5	0.5	0.5
PTV	0.4615	0.4615	0.4615	0.4615	0	0.4615	0.4615	0.4615	0.4615	0.4615	0.4615	0.4615	0	0.4615	0.4615
PV	0.5	0.5	0.5	0.5	0.6155	0.6155	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0	0.5
EVOBE	0.4615	0.4615	0.75	0.75	0.4615	0	0.75	0.75	0.75	0.75	0.4615	0.4615	0.75	0.75	0

Οι τιμές μέσα στα κελιά είναι οι συντελεστές επίδρασης μεταξύ κάθε ζεύγους αυτών των components. Πιο συγκεκριμένα όλες αυτές οι τιμές προκύπτουν από την εξίσωση:

$$\boldsymbol{eff}_{\boldsymbol{AB}}^{\boldsymbol{T}} = \frac{\boldsymbol{eff}_{\boldsymbol{AB}}^{\boldsymbol{I}} + \boldsymbol{eff}_{\boldsymbol{AB}}^{\boldsymbol{C}}}{\mathbf{2}}$$

Αυτή η εξίσωση προκύπτει από την $\boldsymbol{eff}_{\boldsymbol{AB}}^{\boldsymbol{T}} = f(\boldsymbol{eff}_{\boldsymbol{AB}}^{\boldsymbol{I}}, \boldsymbol{eff}_{\boldsymbol{AB}}^{\boldsymbol{C}})$ (βλ. παράγραφο 6.i) όταν η συνάρτηση $\boldsymbol{f}$ είναι ο μέσος όρος των συντελεστών των πληροφοριών και των ελέγχων. Στη συνέχεια αυτές οι τιμές χρησιμοποιούνται επίσης σαν είσοδοι στον Αλγόριθμο 1 της παραγράφου 6.ii για τον υπολογισμό του συνολικού ρίσκου πάνω σε κάθε εξεταζόμενο component. Εδώ πρέπει να σημειωθεί πως τα components τα οποία έχουν υψηλές ροές πληροφοριών και ελέγχου, όπως για παράδειγμα οι PID, PAC, TIC και EMC, χαρακτηρίζονται από υψηλές τιμές στο συντελεστή επίδρασης.

Τα controls ασφαλείας για τη βέλτιστη συνθήκη επιλέγονται από την αρχική λίστα των διαθέσιμων controls αφού εφαρμόσουμε τη μέθοδο που περιγράφεται στο Κεφάλαιο 7. Ο πίνακας που ακολουθεί απεικονίζει το σύνολο των controls που προκύπτει ως βέλτιστη συνθήκη για κάθε απειλή του STRIDE και ανά Component. Απεικονίζει επίσης το σχετικό ρίσκο δίχως να έχουν τεθεί σε ισχύ κάποια controls καθώς και το υπολειπόμενο ρίσκο αφότου έχουν τεθεί σε ισχύ τα βέλτιστα δυνατά controls. Όλες αυτές οι τιμές έχουν υπολογιστεί χρησιμοποιώντας τον Αλγόριθμο 1 της παραγράφου 6.ii.

Κάθε γραμμή του πίνακα αντιπροσωπεύει μία από τις απειλές STRIDE. Η πρώτη στήλη αντιπροσωπεύει τον συνολικό αρχικό ρίσκο, δηλαδή χωρίς κανέναν έλεγχο ασφαλείας επί του συστήματος όπως αυτό αξιολογείται μέσω του Αλγόριθμου 1 (παράγραφος 6.ii). Η δεύτερη στήλη αντιπροσωπεύει κάθε Component – Σύστημα και η τρίτη στήλη το βέλτιστο σύνολο ελέγχων ασφαλείας που προσδιορίζεται μέσω του Αλγόριθμου 2 της παραγράφου 7.ii. Η τέταρτη στήλη αντιπροσωπεύει το υπολειπόμενο ρίσκο, έπειτα από την εφαρμογή των βέλτιστων δυνατών controls επί του κάθε συνδυασμού component και απειλής, όπως αξιολογείται εφαρμόζοντας ξανά τον Αλγόριθμο 1 αφού έχει ενημερωθεί το ρίσκο του κάθε μεμονωμένου Component –

Συστήματος σύμφωνα πάντα με την αποτελεσματικότητα των controls που εφαρμόζονται.

Πίνακας Βελτιστοποίησης Ρίσκου στα ITS με τη Χρήση Controls Ασφαλείας επί των Components

Απειλή Threat	Αρχικό Ρίσκο Initial Risk	Component	Controls	Υπολειπόμενο Ρίσκο Residual Risk
Spoofing	2,2309	ITSRE	Access Control	2,0609
		SSME		
		MMC		
		MMC	Audit and Accountability	
		EVOVE		
		PAC	Security Assessment and Authorization	
		TIC		
		SSME	Contingency Planning	
		MMC	Identification and Authentication	
		TTMC	Maintenance	
		MMC	Media Protection	
		PV		
		ITSRE	Planning	
		TTMC	Personnel Security	
		TTMC	Risk Assessment	
		PID	System and Services Acquisition	
		TTMC	System and Information Integrity	
		PV	Program Management	
		PTV	Privacy Controls	
Tampering	1,4771	PV	Access Control	1,4771
		PAC	Identification and Authentication	
		MMS	Incident Response	
		PV		
		PAC	System and Services Acquisition	
		TTMC	System and Communications Protection	
		TTMC	System and Information Integrity	

Απειλή Threat	Αρχικό Ρίσκο Initial Risk	Component	Controls	Υπολειπόμενο Ρίσκο Residual Risk
Repudiation	2,6250	PV	Audit and Accountability	2,3616
		PID	Contingency Planning	
		SSME	Incident Response	
		PAC	Planning	
		PID	System and Information Integrity	
Information Disclosure	2,3616	TTMC	Awareness and Training	2,3616
		PID	Security Assessment and Authorization	
		PMS	Configuration Management	
		ITSRE	Planning	
		MMC	Risk Assessment	
		PID	System and Services Acquisition	
		PAC	System and Communications Protection	
		TTMC		
Denial of Service	2,6535	PAC	Security Assessment and Authorization	2,0609
		TTMC		
		SSME	Configuration Management	
		MMC	Identification and Authentication	
		MMC	Physical and Environmental Protection	
		DDS	Planning	
		SSME	System and Communications Protection	
		EMC		
		PID	System and Information Integrity	
		PTV		
		PTV	Program Management	
		PV		

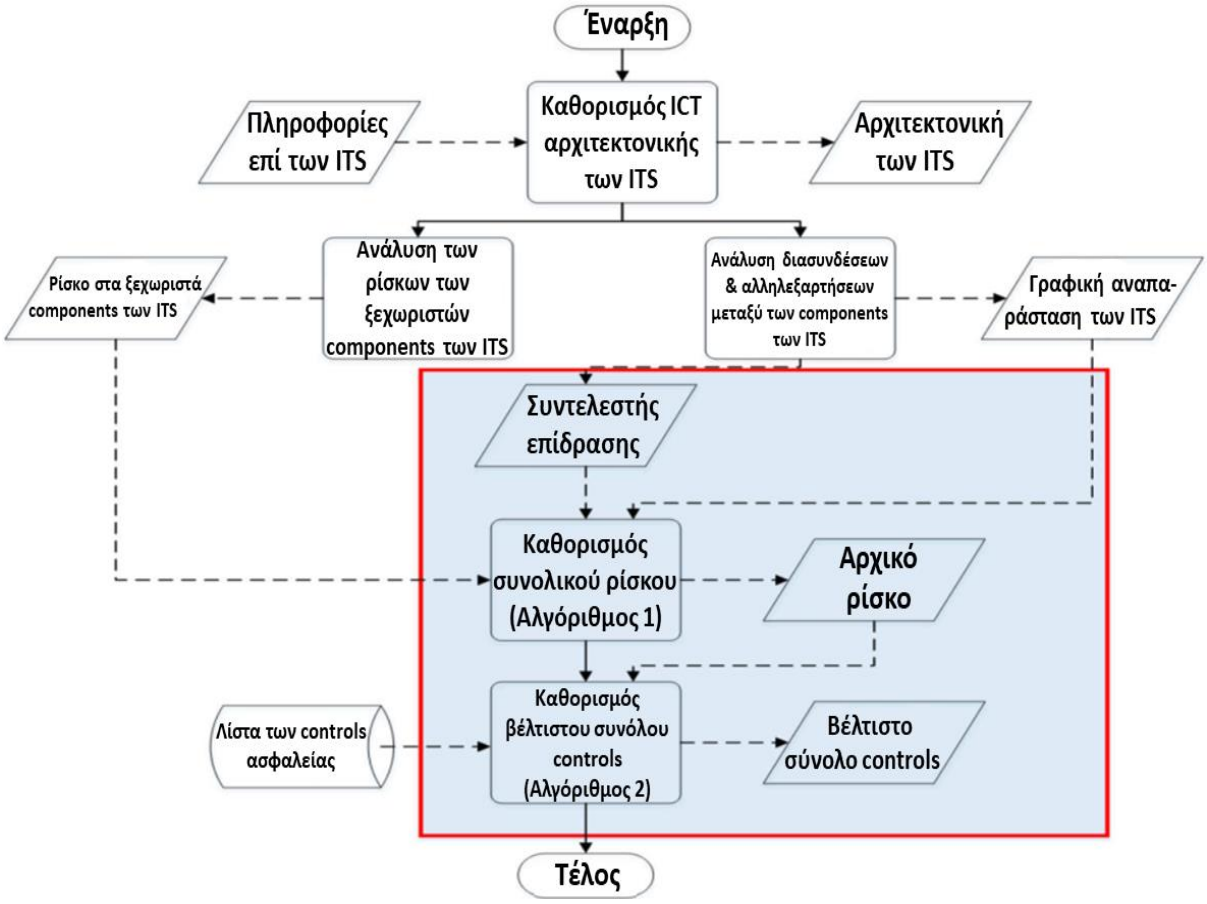
Απειλή Threat	Αρχικό Ρίσκο Initial Risk	Component	Controls	Υπολειπόμενο Ρίσκο Residual Risk
Elevation of Priviledges	2,3616	ITSRE	Access Control	1,7690
		TTMC	Awareness and Training	
		PID	Audit and Accountability	
		PAC	Security Assessment and Authorization	
		TIC		
		EMC		
		MMS		
		PTV		
		EVOVE		
		PV	Incident Response	
		EMC	Physical and Environmental Protection	
		TIC	Planning	
		PTV		
		PID	System and Services Acquisition	
		SSME	System and Communications Protection	
		EMC		
		MMS		
		PMS	Program Management	
		MMC		
		DDS		
		MMS		

iv. Συζήτηση

Όλη η διαδικασία που ακολουθήθηκε για τη διεξαγωγή της μελέτης των περιπτώσεων απεικονίζεται γραφικά στο σχήμα που ακολουθεί.

Στο σχήμα αυτό αποτυπώνονται ορθογώνια, παραλληλόγραμμα, τα οποία συνδέονται μεταξύ του με συνεχείς ή διακεκομμένες γραμμές.

Τα ορθογώνια αντιπροσωπεύουν τα βήματα επεξεργασίας και τα παραλληλόγραμμα αντιπροσωπεύουν εισόδους ή εξόδους. Οι συνεχείς γραμμές συνδέουν διαδικασίες επεξεργασίας, ενώ οι διακεκομμένες γραμμές συνδέουν εισόδους ή εξόδους με τα βήματα επεξεργασίας. Η αχνά μπλε σκιασμένη περιοχή οριοθετεί το περιεχόμενο αυτής της εργασίας.



Όπως φαίνεται στον «Πίνακα Βελτιστοποίησης Ρίσκου στα ITS με τη Χρήση Controls Ασφαλείας επί των Components», στην περίπτωση των ITS, συνιστώνται εβδομήντα δύο διαφορετικοί έλεγχοι των controls ασφαλείας για εφαρμογή (κατά περίπτωση) σε όλα τα Cyber Physical Συστήματα, τα οποία είναι δεκατέσσερα συνολικά.

Οι έλεγχοι ασφαλείας που προτείνονται από οποιαδήποτε αυτοματοποιημένη μέθοδο υποστήριξης στη λήψη αποφάσεων, συμπεριλαμβανομένων προφανώς και των μεθόδων που προτείνονται στην παρούσα εργασία, πρέπει να επανεξεταστούν, να ενοποιηθούν και να ελεγχθούν ως προς τη δυνατότητα εφαρμογής τους από ειδικούς του αντικειμένου αλλά και τους ενδιαφερόμενους μαζί. Οι μέθοδοι που προτείνονται επιτρέπουν την εκτέλεση υποθετικών σεναρίων (what-if), συμπεριλαμβανομένης της τροποποίησης της αρχικής λίστας των διαθέσιμων ελέγχων των control ασφαλείας ή/και της τροποποίησης παραμέτρων του γενετικού αλγορίθμου.

9. Επίλογος

Η συνεχώς αυξανόμενη χρήση Cyber Physical Συστημάτων τα οποία είναι σε πολύ υψηλό βαθμό διασυνδεδεμένα μεταξύ τους και κυρίως σε κρίσιμους τομείς αυξάνει το «πεδίο δράσης» ενός κακόβουλου χρήστη ο οποίος θέλει να διεξάγει επίθεση σε κάποιο σύστημα. Έτσι οι υποδομές, είτε υλικές είτε λογισμικές, καθίστανται πολύ πιο ευάλωτες σε επιθέσεις από τον κυβερνοχώρο. Σε αυτό την εργασία έχουμε παρουσιάσει και αναπτύξει ένα μοντέλο ενός πολύπλοκου κεντρικού Cyber Physical Συστήματος (ITS), το οποίο αποτελεί συνέχεια πολλών επίσης πολύπλοκα διασυνδεδεμένων άλλων Cyber Physical συστημάτων τα οποία είναι και τα components του κεντρικού συστήματος και ταυτόχρονα αποτελούν τους κόμβους που μπορούν να χαρακτηρισθούν και σαν «υπο-CPS» όπου οι ακμές αντιπροσωπεύουν πληροφορίες και ροές ελέγχου μεταξύ αυτών των υποσυστημάτων – components.

Κατά τη λειτουργία αυτού του μοντέλου προτάθηκε μια μέθοδος η οποία δύναται να αξιολογήσει τον συνολικό κίνδυνο κυβερνοασφάλειας μεγάλης κλίμακας, πολύπλοκων Cyber Physical Συστημάτων που περιλαμβάνουν διασυνδεδεμένα και αλληλοεξαρτώμενα components (όπως το δικό μας), χρησιμοποιώντας μέτρα για το ρίσκο του κάθε επιμέρους στοιχείου του καθώς και των ροών πληροφοριών και ελέγχου μεταξύ αυτών των στοιχείων.

Ξεκινώντας με μια τέτοια μέθοδο σαν κορμό σκέψης, προχωρήσαμε ένα βήμα παραπάνω σε μια διαφορετική και εξελιγμένη νέα μέθοδο η οποία βασίζεται στον εξελικτικό προγραμματισμό, για να επιλέξουμε το βέλτιστο, από άποψη απόδοσης και αποτελεσματικότητας, σύνολο controls κυβερνοασφάλειας μεταξύ αυτών που βρίσκονται σε μια καθιερωμένη βάση γνώσεων, που μειώνει το συνολικό υπολειπόμενο ρίσκο, ενώ ταυτόχρονα ελαχιστοποιεί το κόστος. Αυτά τα σύνολα οδηγούν στον ορισμό της αρχιτεκτονικής κυβερνοασφάλειας τέτοιων έξυπνων συστημάτων μεταφορών. Έχει βρεθεί ότι είναι σύμφωνες με αντίστοιχες υπάρχουσες μελέτες αντίστοιχων συστημάτων που εντόπιζαν τα πιο ευάλωτα Cyber Physical Συστήματα που ελαχιστοποιούσαν το παγκόσμιο υπολειπόμενο ρίσκο. Ο μελλοντικός στόχος είναι να αναπτυχθεί ένα λογισμικό – εργαλείο που θα υλοποιεί τις προτεινόμενες μεθόδους και που θα χρησιμοποιείται για να εξετάζεται βιωματικά η χρηστικότητα των προτεινόμενων προσεγγίσεων από ειδικούς και ενδιαφερόμενους του τομέα, τόσο στα έξυπνα συστήματα μεταφορών όσο και σε άλλους κρίσιμους τομείς εφαρμογών.

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΝΑΦΟΡΕΣ

1 Kouns, J.; Minoli, D. Information Technology Risk Management in Enterprise Environments; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2010.

2 Ali, S.; Balushi, T.; Nadir, Z.; Hussain, O. Risk Management for CPS Security. In Cyber Security for Cyber Physical Systems; Springer International Publishing AG: Cham, Switzerland, 2018; pp. 11–34.

3 Lyu, X.; Ding, Y.; Yang, S.H. Safety and security risk assessment in Cyber-Physical Systems. IET Cyber-Phys. Syst. Theory Appl. 2019, 4, 221–232.

4 Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services. IEEE Commun. Surv. Tutor. 2018, 20, 3453–3495.

5 Lamba, V.; Šimková, N.; Rossi, B. Recommendations for smart grid security risk management. Cyber-Phys. Syst. 2019, 5, 92–118.

6 Kim, Y.G.; Jeong, D.; Park, S.H.; Lim, J.; Baik, D.K. Modeling and simulation for 9security risk propagation in critical information systems. In Proceedings of the International Conference on Computational and Information Science, Guangzhou, China, 3–6 November 2006; Springer: Berlin/Heidelberg, Germany, 2006; pp. 858–868.

7 Kondakci, S. A new assessment and improvement model of risk propagation in information security. Int. J. Inf. Comput. Secur.2007, 1, 341–366.

8 Feng, N.; Wang, H.J.; Li, M. A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Inf. Sci. 2014, 256, 57–73.

9 Orojloo, H.; Azgomi, M.A. A method for evaluating the consequence propagation of security attacks in cyber–physical systems. Future Gener. Comput. Syst. 2017, 67, 57–71.

10 Kavallieratos, G.; Katsikas, S. Attack Path Analysis for Cyber Physical Systems. In Computer Security: ESORICS 2020 International Workshops, CyberICPS, SECPRE, and ADIoT, Guildford, UK, 14–18 September 2020, Revised Selected Papers; Lecture Notes in Computer Science Book Series (LNCS); Springer International Publishing: Cham, Switzerland, 2020; Volume 12501, pp. 19–33.

11 König, S.; Rass, S.; Schauer, S.; Beck, A. Risk propagation analysis and visualization using percolation theory. Int. J. Adv. Comput. Sci. Appl. (IJACSA) 2016, 7, 1–8.

12 Qu, Z.; Zhang, Y.; Qu, N.; Wang, L.; Li, Y.; Dong, Y. Method for quantitative estimation of the risk propagation threshold in electric power CPS based on seepage probability. IEEE Access 2018, 6, 68813–68823.

13 Zhu, B.; Deng, S.; Xu, Y.; Yuan, X.; Zhang, Z. Information security risk propagation model based on the SEIR infectious disease model for smart grid. Information 2019, 10, 323.

14 Malik, A.A.; Tosh, D.K. Quantitative Risk Modeling and Analysis for Large-Scale Cyber-Physical Systems. In Proceedings of the 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 3–6 August 2020;pp. 1–6.

15 Theoharidou, M.; Kotzanikolaou, P.; Gritzalis, D. A multi-layer criticality assessment methodology based on interdependencies. Comput. Secur. 2010, 29, 643–658.

16 Theoharidou, M.; Kotzanikolaou, P.; Gritzalis, D. Risk assessment methodology for interdependent critical infrastructures. Int. J. Risk Assess. Manag. 2011, 15, 128–148.

17 Zhou, X.; Wang, F.; Ma, Y. An overview on energy internet. In Proceedings of the 2015 IEEE International Conference on Mechatronics and Automation (ICMA), Beijing, China, 2–5 August 2015; pp. 126–131.

18 Hong, Q.; Jianwei, T.; Zheng, T.; Wenhui, Q.; Chun, L.; Xi, L.; Hongyu, Z. An information security risk assessment algorithm based on risk propagation in energy internet. In Proceedings of the IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 26–28 November 2017; pp. 1–6.

19 Li, S.; Zhao, S.; Yuan, Y.; Sun, Q.; Zhang, K. Dynamic security risk evaluation via hybrid Bayesian risk graph in cyber-physical social systems. IEEE Trans. Comput. Soc. Syst. 2018, 5, 1133–1141.

20 Karbowski, A.; Malinowski, K. Two-Level System of on-Line Risk Assessment in the National Cyberspace. IEEE Access 2020, 8, 181404–181410.

21 MUNIN. Maritime unmanned navigation through intelligence in networks, 2016.

22 Ø. J. Rødseth and A . Tjora. A system architecture for an unmanned ship. 05/2014.

23 Ø. J. Rødseth, B. Kvamstad, T. Porathe, and H. C. Burmeister. Communication architecture for an un manned merchant ship. In 2013 MTS/IEEE OCEANS-Bergen, pages 1{9, June 2013.

24 H.-C. Burmeister, W. Bruhn, L. Walther, J. A. Morus, and B. Sage-Fuller. Munin d8.6: Final report: Autonomous bridge. Technical report, 2015.

25 S. N. MacKinnon, Y. Man, and M. Baldauf. Munin d8.8 final report shore control centre. Technical report, 2015.

26 M. Schmidt, E. Fentzahn, G. F. Atlason, and H. Rødseth. Munin 8.7 final report autonomous engine room. Technical report, 2015.

27 Ø. J. Rodseth and H.C. Burmeister. Risk assessment for an unmanned merchant ship. TransNav, 9(3):357{364, 2015.

28 Rolls-Royce. Remote and autonomous ship-the next steps. page 88, 2016.

29 Lloyds Register. Cyber-enabled ships. page 20, 2016.

30 Tam, K.; Jones, K. Cyber-risk assessment for autonomous ships. In Proceedings of the International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 3–4 June 2018; pp. 1–8.

31 Sokratis K. Katsikas. Cyber security of the autonomous ship. In Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, CPSS '17, pages 55{56, New York, NY, USA, 2017. ACM.

32 S. Hussain, A. Kamal, S. Ahmad, G. Rasool, and S. Iqbal. Threat modelling methodologies: A survey. 26:1607{1609, 01 2014.

33 F. Sidi, A. J. Marzanah, L. S. Affendey, M. Zolkepli T. M. Ming M. F. A. Mokthi M. Daud N. B. Zainuddin I. Ishak, N. M. Sharef, and R. A. Hamid. A comparative analysis study on information security threat models: A propose for threat factor profiling. Journal of Engineering and Applied Sciences, 12:548{554, 2017.

34 Chun Yu (CY) Cheung. Threat modeling techniques, 2016.

35 H. Havinga and O. Sessink. Risk Reduction Overview Manual, version 1.0 edition, 2014.

36 S. Krishnan. A hybrid approach to threat modelling. page 24, 2017.

37 Svilicic, B.; Kamahara, J.; Celic, J.; Bolmsten, J. Assessing ship cyber risks: A framework and case study of ECDIS security. WMU J. Marit. Aff. 2019, 18, 509–520.

38 Bolbot, V.; Theotokatos, G.; Boulougouris, E.; Vassalos, D. Safety related cyber-attacks identification and assessment for autonomous inland ships. In Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV), Aalto University, Espoo, Finland, 17–20 September 2019.

39 Silverajan, B.; Ocak, M.; Nagel, B. Cyber Security Attacks and Defences for Unmanned Smart Ships. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 15–20.

40 Awan, M.; Al Ghamdi, M. Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS). J. Mar. Sci. Eng. 2019, 7, 350.

41 Svilicic, B.; Rudan, I.; Jugovi´c, A.; Zec, D. A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. J. Mar. Sci. Eng. 2019, 7, 364.

42 Wang, Y.; Wang, Y.; Feng, X. Ship Security Relative Integrated Navigation with Injected Fault Measurement Attack and Unknown Statistical Property Noises. J. Mar. Sci. Eng. 2020, 8, 305.

43 Balduzzi, M.; Pasta, A.; Wilhoit, K. A Security Evaluation of AIS Automated Identification System. In Proceedings of the 30th Annual Computer Security Applications Conference, ACSAC'14, Association for Computing Machinery, New York, NY, USA, 8–12 December 2014; pp. 436–445.

44 Lund, M.; Hareide, O.; Jøsok, Ø. An Attack on an Integrated Navigation System. J. Ocean Technol. 2017, 12, 23–27.

45 Kavallieratos, G.; Katsikas, S.; Gkioulos, V. Cyber-attacks against the autonomous ship. In Proceedings of the SECPRE 2018, CyberICPS 2018. Lecture Notes in Computer Science, Vol 11387; Springer Nature: Basel, Switzerland, 2018; pp. 20–36.

46 Nespoli, P.; Papamartzivanos, D.; Gómez Mármol, F.; Kambourakis, G. Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks. IEEE Commun. Surv. Tutor. 2018, 20, 1361–1396.

47 Schilling, A.; Werners, B. Optimal selection of IT security safeguards from an existing knowledge base. Eur. J.Oper. Res. 2016, 248, 318–327.

48 Bothur, D.; Zheng, G.; Valli, C. A critical analysis of security vulnerabilities and countermeasures in a smart ship system. In Proceedings of the Australian Information Security Management Conference, Perth, Australia ,5–6 December 2017.

49 Sahay, R.; Sepulveda, D.; Meng, W.; Jensen, C.D.; Barfod, M.B. CyberShip: An SDN-based Autonomic Attack Mitigation Framework for Ship Systems. In Proceedings of the International Conference on Science of Cyber Security, Beijing, China, 14–16 August 2018; pp. 191–198.

50 Giannopoulos, G., Mitsakis, E., & Salanova Grau, J. (2012), “Overview of Intelligent Transport Systems (ITS) developments in and across transport modes”, JRC Scientific and Policy Reports, 2012.

51 https://ertico.com/vision-mission/

52 Wood, K., Maxwell, A., Stevens, A. and Thompson, S. (2006), "Routing assessment of dynamic route guidance systems", TRL Report No PPR093.

53 H. Bast, S. Funke, P. Sanders, D. Schultes. Fast Routing in Road Networks with Transit Nodes. - Science, Vol. 316. no. 5824, p. 566, 27. April 2007.

54 Trozzi V., Bell M.G.H. Gentile G., Hosseinloo S.H. (2010) Dynamic hyperpaths in transit networks: the stop model with online information, in Proceedings of the 5th IMA Conference on Mathematics in Transportation, London, UK.

55 Commission of European Communities, Towards fair and efficient pricing in transport - Green Paper, Brussels (1995).

56 Commission of European Communities (1998), Fair payment for infrastructure use: a phased approach to a common transport infrastructure charging framework in the EU - White Paper, Brussels (1998).

57 ETSI TS 102 690, "Machine-to-Machine communications (M2M); Functional Architecture".

58 ETSI M2M Security Architecture Presentation, Alper Yegin, Samsung.

59 ICSI D1.3.1, "System Architecture".

60 Lang, U., Schreiner, R. openPMF Security Policy Framework for Distributed Systems. Proceedings of the information Security Solutions Europe (ISSE 2004) conference. Berlin, Germany, September 2004.

61 DDS Security, 1.0-FTF-Beta1, OMG document: ptc/2014-06-01.

62 Integrated IT Security: Air- Traffic Management Case Study. Proceedings of the Information Security Solutions Europe (ISSE 2005) Conference. Budapest, Hungary, 2005.

63 Air-traffic Management Case Study. Ulrich Lang, Rudolf Schreiner. Proceedings of the information Security Solutions Europe (ISSE 2007) Conference. Warsaw, Poland, 2007.

64 ObjectSecurity, OpenPMF website, http://www.objectsecurity.com/en-products-openpmf.html (2014)

65 Real- Time Innovations.DDS Discovery. http://community.rti.com/howto/detect-presence-domainparticipants-datawriters-and-datareaders-dds-domain (retrieved2014)

66 Shostack, A. Threat Modeling: Designing for Security; John Wiley & Sons: Hoboken, NJ, USA, 2014.

67 Zinsmaier, S.; Langweg, H.; Waldvogel, M. A Practical Approach to Stakeholder-driven Determination of Security Requirements based on the GDPR and Common Criteria. In Proceedings of the 6th International Conference on Information Systems Security and Privacy—Volume 1: ICISSP, Valletta, Malta, 25–27 February 2020; pp. 473–480.

68 Kavallieratos, G.; Gkioulos, V.; Katsikas, S.K. Threat analysis in dynamic environments: The case of the smart home. In Proceedings of the 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019; pp. 234–240.

69 Microsoft. Chapter 3—Threat Modeling. 2010. Available online: https://docs.microsoft.com/en-us/previous-versions/msp-np/ff648644(v=pandp.10)?redirectedfrom=MSDN (accessed on 28 February 2021).

70 Kavallieratos, G.; Katsikas, S. Managing Cyber Security Risks of the Cyber-Enabled Ship. J. Mar. Sci. Eng. 2020, 8, 768.

71 Kavallieratos, G.; Spathoulas, G.; Katsikas, S. Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems. Sensors 2021, 21, 1691. https://doi.org/10.3390/s21051691

72 Rothlauf, F. Optimization Methods. In Design of Modern Heuristics: Principles and Application; Springer: Berlin/Heidelberg, Germany, 2011; pp. 45–102.

73 Asian Development Bank, Conceptual Design of the Intelligent Transport Systems Project – Case in Gui'an New District; Manila, Philippines, 2019; pp. 23.

74 https://www.arc-it.net/html/physobjects/physobjects.html

75 International Organization for Standardization, ISO. ISO/IEC 27005:2018 Information Technology—Security Techniques—Information Security Risk Management; ISO: Geneva, Switzerland, 2018.

76 Stouffer, K.; Pillitteri, V.; Marshall, A.; Hahn, A. Guide to industrial control systems (ICS) security. NIST Spec. PUBLIC. 2015, 800, 247.

77 NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, 2020