Κανονισμός του ΟΗΕ αριθ. 155 — Ενιαίες διατάξεις σχετικά με την έγκριση οχημάτων όσον αφορά την κυβερνοασφάλεια και το σύστημα διαχείρισης της κυβερνοασφάλειας [2021/387]

Ημερομηνία έναρξης ισχύος: 22 Ιανουαρίου 2021

Το παρόν έγγραφο πρέπει να χρησιμοποιείται αποκλειστικά και μόνο ως εργαλείο τεκμηρίωσης. Τα αυθεντικά και νομικώς δεσμευτικά κείμενα είναι τα ακόλουθα:

— ECE/TRANS/WP.29/2020/79

— ECE/TRANS/WP.29/2020/94 και

— ECE/TRANS/WP.29/2020/97

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

1.1. Ο παρών κανονισμός ισχύει για οχήματα των κατηγοριών M και N και αφορά την κυβερνοασφάλεια.

Ο παρών κανονισμός ισχύει επίσης για οχήματα της κατηγορίας O, αν τα εν λόγω οχήματα διαθέτουν τουλάχιστον μία μονάδα ηλεκτρονικού ελέγχου.

1.2. Ο παρών κανονισμός ισχύει επίσης για οχήματα των κατηγοριών L_6 και L_7, αν τα εν λόγω οχήματα διαθέτουν λειτουργικές δυνατότητες αυτοματοποιημένης οδήγησης τουλάχιστον επιπέδου 3, όπως ορίζεται στο «έγγραφο αναφοράς με τους ορισμούς της αυτοματοποιημένης οδήγησης σύμφωνα με την ομάδα εργασίας του άρθρου 29 και τις γενικές αρχές για την εκπόνηση κανονισμού του ΟΗΕ σχετικά με τα αυτοματοποιημένα οχήματα» (ECE/TRANS/WP.29/1140).

1.3. Ο παρών κανονισμός ισχύει με την επιφύλαξη άλλων κανονισμών του ΟΗΕ, περιφερειακών ή εθνικών νομοθετικών πράξεων που διέπουν την πρόσβαση εξουσιοδοτημένων μερών στο όχημα, στα δεδομένα, στις λειτουργίες και στους πόρους του, καθώς και τους όρους της εν λόγω πρόσβασης. Ισχύει επίσης με την επιφύλαξη της εφαρμογής της εθνικής και περιφερειακής νομοθεσίας για την ιδιωτική ζωή και την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

1.4. Ο παρών κανονισμός ισχύει με την επιφύλαξη άλλων κανονισμών του ΟΗΕ, εθνικών ή περιφερειακών νομοθετικών πράξεων που διέπουν την παραγωγή και την εγκατάσταση/ενσωμάτωση σε συστήματα, ανταλλακτικών και κατασκευαστικών στοιχείων –υλικών και ψηφιακών– που αφορούν την κυβερνοασφάλεια.

2. ΟΡΙΣΜΟΙ

Για τους σκοπούς του παρόντος κανονισμού, ισχύουν οι ακόλουθοι ορισμοί:

2.1. «Τύπος οχήματος»: οχήματα που δεν διαφέρουν τουλάχιστον ως προς τα ακόλουθα βασικά στοιχεία:

α) τον τύπο οχήματος που προσδιορίζεται από τον κατασκευαστή·

β) βασικά στοιχεία της ηλεκτρικής/ηλεκτρονικής αρχιτεκτονικής και εξωτερικές διεπαφές σχετικά με την κυβερνοασφάλεια.

2.2. «Κυβερνοασφάλεια»: η κατάσταση στην οποία τα οδικά οχήματα και οι λειτουργίες τους προστατεύονται από απειλές του κυβερνοχώρου που θέτουν σε κίνδυνο ηλεκτρικά ή ηλεκτρονικά κατασκευαστικά στοιχεία.

2.3. «Σύστημα διαχείρισης της κυβερνοασφάλειας»: συστηματική προσέγγιση που βασίζεται στους κινδύνους και προβλέπει οργανωτικές διαδικασίες, αρμοδιότητες και μέσα διακυβέρνησης με σκοπό την αντιμετώπιση των κινδύνων που εγκυμονούν οι απειλές στον κυβερνοχώρο για τα οχήματα και την προστασία των οχημάτων από κυβερνοεπιθέσεις.

2.4. «Σύστημα»: το σύνολο των κατασκευαστικών στοιχείων και/ή υποσυστημάτων που επιτελούν λειτουργία ή λειτουργίες.

2.5. «Στάδιο ανάπτυξης»: η περίοδος που προηγείται της έγκρισης του τύπου του οχήματος.

2.6. «Στάδιο παραγωγής»: η περίοδος κατά την οποία παράγεται ο τύπος του οχήματος.

2.7. «Στάδιο μετά την παραγωγή»: η περίοδος κατά την οποία έχει σταματήσει η παραγωγή του τύπου του οχήματος και η οποία διαρκεί μέχρι το τέλος του κύκλου ζωής όλων των οχημάτων που υπάγονται στον τύπο του οχήματος. Κατά τη διάρκεια αυτού του σταδίου τα οχήματα που ανταποκρίνονται σε συγκεκριμένο τύπο οχήματος χρησιμοποιούνται αλλά η παραγωγή τους έχει σταματήσει. Το στάδιο λήγει όταν δεν χρησιμοποιείται πλέον κανένα όχημα του συγκεκριμένου τύπου οχήματος.

2.8. «Μέτρο προστασίας»: μέτρο που περιορίζει τον κίνδυνο.

2.9. «Κίνδυνος»: το ενδεχόμενο συγκεκριμένη απειλή να εκμεταλλευτεί ευπάθειες του οχήματος και να προκαλέσει έτσι βλάβη στον οργανισμό ή σε άτομο.

2.10. «Εκτίμηση κινδύνου»: η συνολική διαδικασία κατά την οποία εντοπίζονται, αναγνωρίζονται και περιγράφονται κίνδυνοι (προσδιορισμός κινδύνου), κατανοείται η φύση των κινδύνων και προσδιορίζεται η σοβαρότητα των κινδύνων (ανάλυση κινδύνου), καθώς και συγκρίνονται τα αποτελέσματα της ανάλυσης κινδύνου με τα κριτήρια κινδύνου προκειμένου να εξακριβωθεί αν ο κίνδυνος και/ή το μέγεθός του παραμένουν σε αποδεκτά ή ανεκτά επίπεδα (αξιολόγηση κινδύνου).

2.11. «Διαχείριση κινδύνου»: συντονισμένες δραστηριότητες με τις οποίες καθοδηγούνται και ελέγχονται οργανισμοί όσον αφορά τους κινδύνους.

2.12. «Απειλή»: η πιθανή αιτία ανεπιθύμητου συμβάντος που μπορεί να προκαλέσει βλάβη σε συστήματα, οργανισμούς ή άτομα.

2.13. «Ευπάθεια»: αδυναμία περιουσιακού στοιχείου ή μέτρου προστασίας την οποία μπορούν να εκμεταλλευθούν μία ή περισσότερες απειλές.

3. ΑΙΤΗΣΗ ΕΓΚΡΙΣΗΣ

3.1. Η αίτηση για τη χορήγηση έγκρισης τύπου του οχήματος όσον αφορά την κυβερνοασφάλεια υποβάλλεται από τον κατασκευαστή του οχήματος ή από τον δεόντως εξουσιοδοτημένο αντιπρόσωπό του.

3.2. Η αίτηση συνοδεύεται από τα κατωτέρω έγγραφα εις τριπλούν και από τα ακόλουθα στοιχεία:

3.2.1. Περιγραφή του τύπου οχήματος όσον αφορά τα στοιχεία που προσδιορίζονται στο παράρτημα 1 του παρόντος κανονισμού.

3.2.2. Στις περιπτώσεις στις οποίες οι πληροφορίες καλύπτονται αποδεδειγμένα από δικαιώματα διανοητικής ιδιοκτησίας ή αποτελούν ειδική τεχνογνωσία του κατασκευαστή ή των προμηθευτών του, ο κατασκευαστής ή οι προμηθευτές του παρέχουν επαρκείς πληροφορίες για να καταστήσουν δυνατή την ορθή διενέργεια των ελέγχων που αναφέρονται στον παρόντα κανονισμό. Οι πληροφορίες αυτές έχουν εμπιστευτικό χαρακτήρα.

3.2.3. Το πιστοποιητικό συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας σύμφωνα με την παράγραφο 6 του παρόντος κανονισμού.

3.3. Η τεκμηρίωση διατίθεται σε δύο μέρη:

α) ο επίσημος φάκελος τεκμηρίωσης για την έγκριση, ο οποίος περιλαμβάνει το υλικό που αναφέρεται στο παράρτημα 1 και υποβάλλεται στην αρχή έγκρισης ή στην τεχνική της υπηρεσία κατά τη χρονική στιγμή υποβολής της αίτησης για την έγκριση τύπου. Ο εν λόγω φάκελος τεκμηρίωσης χρησιμοποιείται από την αρχή έγκρισης ή από τις τεχνικές της υπηρεσίες ως το βασικό υλικό αναφοράς κατά τη διαδικασία έγκρισης. Η αρχή έγκρισης ή η τεχνική της υπηρεσία μεριμνά ώστε ο εν λόγω φάκελος τεκμηρίωσης να παραμένει διαθέσιμος για τουλάχιστον 10 έτη από τη στιγμή κατά την οποία σταματά οριστικά η παραγωγή του τύπου του οχήματος·

β) πρόσθετο υλικό σχετικό με τις απαιτήσεις του παρόντος κανονισμού μπορεί να φυλάσσεται από τον κατασκευαστή αλλά να καθίσταται διαθέσιμο προς έλεγχο κατά τη χρονική στιγμή της έγκρισης τύπου. Ο κατασκευαστής μεριμνά ώστε το υλικό που καθίσταται διαθέσιμο προς έλεγχο κατά τη στιγμή της έγκρισης τύπου να παραμένει διαθέσιμο για χρονικό διάστημα τουλάχιστον 10 ετών από τη στιγμή κατά την οποία σταματά οριστικά η παραγωγή του τύπου οχήματος.

4. ΣΗΜΑΝΣΗ

4.1. Σε κάθε όχημα που ανταποκρίνεται σε τύπο οχήματος που έχει εγκριθεί σύμφωνα με τον παρόντα κανονισμό τοποθετείται σε εμφανές και ευπρόσιτο σημείο που καθορίζεται στο έντυπο έγκρισης διεθνές σήμα έγκρισης το οποίο αποτελείται από:

4.1.1. έναν κύκλο που περιβάλλει το γράμμα «E», ακολουθούμενο από τον χαρακτηριστικό αριθμό της χώρας που έχει χορηγήσει την έγκριση.

4.1.2. τον αριθμό του παρόντος κανονισμού, ακολουθούμενο από το γράμμα «R», παύλα και τον αριθμό έγκρισης στα δεξιά του κύκλου που περιγράφεται στην παράγραφο 4.1.1 ανωτέρω.

4.2. Αν το όχημα συμμορφώνεται με τύπο οχήματος ο οποίος έχει εγκριθεί βάσει άλλου ή άλλων κανονισμών που προσαρτώνται στη συμφωνία, στη χώρα που έχει χορηγήσει έγκριση βάσει του παρόντος κανονισμού, δεν χρειάζεται να επαναλαμβάνεται το σύμβολο που ορίζεται στην παράγραφο 4.1.1· στην περίπτωση αυτή, ο κανονισμός, οι αριθμοί έγκρισης και τα πρόσθετα σύμβολα όλων των κανονισμών βάσει των οποίων έχει χορηγηθεί έγκριση στη χώρα που έχει χορηγήσει έγκριση δυνάμει του παρόντος κανονισμού τοποθετούνται σε κάθετες στήλες στα δεξιά του συμβόλου που ορίζεται στην παράγραφο 4.1.1. ανωτέρω.

4.3. Το σήμα έγκρισης είναι ευανάγνωστο και ανεξίτηλο.

4.4. Το σήμα έγκρισης τοποθετείται κοντά ή πάνω στην πινακίδα με τα στοιχεία του οχήματος που έχει τοποθετήσει ο κατασκευαστής.

4.5. Στο παράρτημα 3 του παρόντος κανονισμού παρατίθενται παραδείγματα για τον τρόπο διάταξης του σήματος έγκρισης.

5. ΕΓΚΡΙΣΗ

5.1. Οι αρχές έγκρισης χορηγούν, κατά περίπτωση, έγκριση τύπου όσον αφορά την κυβερνοασφάλεια μόνο για τους τύπους των οχημάτων που εκπληρώνουν τις απαιτήσεις του παρόντος κανονισμού.

5.1.1. Η αρχή έγκρισης ή η τεχνική υπηρεσία εξακριβώνει, μέσω της εξέτασης των εγγράφων, ότι ο κατασκευαστής του οχήματος έχει λάβει τα αναγκαία μέτρα ανάλογα με τον τύπο οχήματος προκειμένου:

α) να συλλέγει και να επαληθεύει τις πληροφορίες που απαιτούνται στον παρόντα κανονισμό μέσω της αλυσίδας εφοδιασμού, αποδεικνύοντας με τον τρόπο αυτό ότι εντοπίζει και διαχειρίζεται τους κινδύνους που προέρχονται από τους προμηθευτές·

β) να τεκμηριώνει την εκτίμηση κινδύνου (η οποία διενεργείται στο στάδιο της ανάπτυξης ή αναδρομικά), τα αποτελέσματα των δοκιμών και τα μέτρα προστασίας που εφαρμόζονται στον τύπου του οχήματος, μεταξύ άλλων με πληροφορίες για τον σχεδιασμό του οχήματος οι οποίες συμβάλλουν στην εκτίμηση κινδύνου·

γ) να εφαρμόζει κατάλληλα μέτρα για την κυβερνοασφάλεια κατά τον σχεδιασμό του τύπου του οχήματος·

δ) να εντοπίζει και να αντιμετωπίζει πιθανές επιθέσεις που πλήττουν την κυβερνοασφάλεια·

ε) να καταγράφει δεδομένα που συμβάλλουν στον εντοπισμό κυβερνοεπιθέσεων και να προσφέρει μέσα για την εγκληματολογική ανάλυση των δεδομένων, τα οποία επιτρέπουν στις αρχές να αναλύουν απόπειρες κυβερνοεπιθέσεων ή επιτυχημένες κυβερνοεπιθέσεις.

5.1.2. Η αρχή έγκρισης ή η τεχνική υπηρεσία εξακριβώνει, διενεργώντας δοκιμές σε οχήματα του τύπου οχήματος, ότι ο κατασκευαστής του οχήματος έχει εφαρμόσει τα μέτρα κυβερνοασφάλειας που αναφέρονται στα έγγραφα τεκμηρίωσης. Οι έλεγχοι διενεργούνται από την αρχή έγκρισης ή την τεχνική υπηρεσία καθαυτή ή σε συνεργασία με τον κατασκευαστή του οχήματος με τη μέθοδο της δειγματοληψίας. Η δειγματοληψία εστιάζει, μεταξύ άλλων, στους κινδύνους που χαρακτηρίζονται σοβαροί κατά τη διάρκεια της εκτίμησης κινδύνου.

5.1.3. Η αρχή έγκρισης ή η τεχνική υπηρεσία δεν χορηγεί έγκριση τύπου όσον αφορά την κυβερνοασφάλεια όταν ο κατασκευαστής του οχήματος δεν έχει εκπληρώσει μία ή περισσότερες από τις απαιτήσεις που αναφέρονται στην παράγραφο 7.3, και πιο συγκεκριμένα τις εξής απαιτήσεις:

α) ο κατασκευαστής του οχήματος δεν διενήργησε ενδελεχή εκτίμηση κινδύνου, όπως αναφέρεται στην παράγραφο 7.3.3· μεταξύ άλλων, ο κατασκευαστής δεν εξέτασε όλους τους κινδύνους που συνδέονται με τις απειλές που αναφέρονται στο παράρτημα 5, μέρος Α·

β) ο κατασκευαστής του οχήματος δεν προστάτευσε τον τύπο οχήματος από κινδύνους που εντοπίστηκαν κατά την εκτίμηση κινδύνου του κατασκευαστή του οχήματος ή δεν εφαρμόστηκαν αναλογικά μέτρα προστασίας, όπως προβλέπεται στην παράγραφο 7·

γ) ο κατασκευαστής του οχήματος δεν έθεσε σε εφαρμογή κατάλληλα και αναλογικά μέτρα για να θωρακίσει ειδικά περιβάλλοντα στον τύπο οχήματος, τα οποία χρησιμοποιούνται (αν υπάρχουν) για την αποθήκευση και την εκτέλεση λογισμικού, υπηρεσιών, εφαρμογών ή δεδομένων της δευτερογενούς αγοράς·

δ) ο κατασκευαστής του οχήματος δεν διενήργησε, πριν από την έγκριση, κατάλληλες και επαρκείς δοκιμές για να εξακριβώσει την αποτελεσματικότητα των μέτρων ασφάλειας που εφαρμόζονται.

5.1.4. Η αξιολογούσα αρχή έγκρισης δεν χορηγεί επίσης την έγκριση τύπου όσον αφορά την κυβερνοασφάλεια όταν η αρχή έγκρισης ή η τεχνική υπηρεσία δεν έχει λάβει επαρκείς πληροφορίες από τον κατασκευαστή του οχήματος για να αξιολογήσει την κυβερνοασφάλεια του τύπου του οχήματος.

5.2. Η έγκριση ή η επέκταση ή η μη χορήγηση έγκρισης του τύπου οχήματος που προβλέπεται στον παρόντα κανονισμό κοινοποιείται στα συμβαλλόμενα μέρη της συμφωνίας του 1958 που εφαρμόζουν τον παρόντα κανονισμό μέσω εντύπου που συμφωνεί με το υπόδειγμα του παραρτήματος 2 του παρόντος κανονισμού.

5.3. Οι αρχές έγκρισης δεν χορηγούν έγκριση τύπου αν δεν βεβαιωθούν ότι ο κατασκευαστής εφαρμόζει ικανοποιητικές ρυθμίσεις και διαδικασίες για την ορθή διαχείριση των πτυχών της κυβερνοασφάλειας που καλύπτονται από τον παρόντα κανονισμό.

5.3.1. Η αρχή έγκρισης και οι τεχνικές της υπηρεσίες μεριμνούν ώστε και οι ίδιες, πέραν των κριτηρίων που προβλέπονται στον πίνακα 2 της συμφωνίας του 1958:

α) να διαθέτουν ικανό προσωπικό με άρτιες δεξιότητες στον τομέα της κυβερνοασφάλειας και ειδικές γνώσεις στον τομέα των εκτιμήσεων κινδύνου για τα αυτοκίνητα ([1])·

β) να εφαρμόζουν διαδικασίες για την ενιαία αξιολόγηση σύμφωνα με τον παρόντα κανονισμό.

([1]) Π.χ. ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.

5.3.2. Κάθε συμβαλλόμενο μέρος που εφαρμόζει τον παρόντα κανονισμό ενημερώνει, μέσω της αρχής έγκρισής του, άλλες αρχές έγκρισης των συμβαλλομένων μερών που εφαρμόζουν τον παρόντα κανονισμό του ΟΗΕ σχετικά με τη μέθοδο και τα κριτήρια στα οποία βασίζεται η κοινοποιούσα αρχή για να αξιολογεί την καταλληλότητα των μέτρων που λαμβάνονται σύμφωνα με τον παρόντα κανονισμό, και ιδίως σύμφωνα με τις παραγράφους 5.1, 7.2 και 7.3.

Οι πληροφορίες αυτές κοινοποιούνται α) μόνον πριν χορηγηθεί έγκριση σύμφωνα με τον παρόντα κανονισμό για πρώτη φορά και β) όποτε επικαιροποιούνται η μέθοδος ή τα κριτήρια της αξιολόγησης.

Οι πληροφορίες αυτές κοινοποιούνται καταρχήν με σκοπό τη συλλογή και την ανάλυση των βέλτιστων πρακτικών και προκειμένου να διασφαλιστεί η ενιαία εφαρμογή του παρόντος κανονισμού από όλες τις αρχές έγκρισης που εφαρμόζουν τον παρόντα κανονισμό.

5.3.3. Οι πληροφορίες που αναφέρονται στην παράγραφο 5.3.2 αναφορτώνονται, στην αγγλική γλώσσα, στην ασφαλή διαδικτυακή βάση δεδομένων «DETA» ([2]) που δημιουργήθηκε από την Οικονομική Επιτροπή των Ηνωμένων Εθνών για την Ευρώπη, εγκαίρως και το αργότερο 14 ημέρες πριν χορηγηθεί έγκριση για πρώτη φορά βάσει των εκάστοτε μεθόδων και κριτηρίων αξιολόγησης. Με τις πληροφορίες γνωστοποιούνται επαρκώς τόσο τα ελάχιστα επίπεδα επιδόσεων που έχει καθορίσει η αρχή έγκρισης για την εκάστοτε απαίτηση που αναφέρεται στην παράγραφο 5.3.2 όσο και οι διαδικασίες και τα μέτρα που εφαρμόζει η αρχή έγκρισης για να εξακριβώσει την εκπλήρωση των εν λόγω ελάχιστων επιπέδων επιδόσεων ([3]).

5.3.4. Οι αρχές έγκρισης που λαμβάνουν τις πληροφορίες της παραγράφου 5.3.2 μπορούν να υποβάλουν παρατηρήσεις στην κοινοποιούσα αρχή έγκρισης, αναφορτώνοντάς τες στην πλατφόρμα DETA εντός 14 ημερών από την ημέρα της κοινοποίησης.

5.3.5. Αν η αρχή έγκρισης αδυνατεί να λάβει υπόψη της τις παρατηρήσεις που έλαβε σύμφωνα με την παράγραφο 5.3.4., οι αρχές έγκρισης που απέστειλαν τις παρατηρήσεις και η αρχή έγκρισης ζητούν περαιτέρω διευκρινίσεις σύμφωνα με τον πίνακα 6 της συμφωνίας του 1958. Η οικεία επικουρική ομάδα εργασίας ([4]) του παγκόσμιου φόρουμ για την εναρμόνιση των κανονισμών των οχημάτων (WP.29) που μελετά τον παρόντα κανονισμό καθορίζει κοινή ερμηνεία για τις μεθόδους και τα κριτήρια αξιολόγησης. ([5]) Εφαρμόζεται η κοινή ερμηνεία και όλες οι αρχές έγκρισης εκδίδουν αντίστοιχα εγκρίσεις τύπου βάσει του παρόντος κανονισμού.

5.3.6. Κάθε αρχή έγκρισης που χορηγεί έγκριση τύπου δυνάμει του παρόντος κανονισμού κοινοποιεί στις άλλες αρχές έγκρισης την έγκριση που χορηγεί. Η έγκριση τύπου μαζί με τα συνοδευτικά έγγραφα τεκμηρίωσης αναφορτώνονται στην αγγλική γλώσσα από την αρχή έγκρισης εντός 14 ημερών από την ημερομηνία της χορήγησης της έγκρισης στην πλατφόρμα DETA ([6]).

5.3.7. Τα συμβαλλόμενα μέρη μπορούν να μελετούν τις εγκρίσεις που χορηγούνται βάσει των πληροφοριών που αναφορτώνονται σύμφωνα με την παράγραφο 5.3.6. Αν υπάρξει διάσταση απόψεων μεταξύ των συμβαλλομένων μερών, η εν λόγω διάσταση απόψεων διευθετείται σύμφωνα με το άρθρο 10 και τον πίνακα 6 της συμφωνίας του 1958. Τα συμβαλλόμενα μέρη ενημερώνουν επίσης την οικεία επικουρική ομάδα εργασίας του παγκόσμιου φόρουμ για την εναρμόνιση των κανονισμών των οχημάτων (WP.29) σχετικά με τις διαφορετικές ερμηνείες κατά την έννοια του πίνακα 6 της συμφωνίας του 1958. Οι οικεία ομάδα εργασίας υποστηρίζει τη διευθέτηση της διάστασης απόψεων και δύναται εν προκειμένω να συμβουλεύεται την ομάδα εργασίας (WP.29), αν κρίνεται αναγκαίο.

5.4. Για τον σκοπό της παραγράφου 7.2 του παρόντος κανονισμού, ο κατασκευαστής μεριμνά για την εφαρμογή των πτυχών της κυβερνοασφάλειας που καλύπτονται από τον παρόντα κανονισμό.

([2]) https://www.unece.org/trans/main/wp29/datasharing.html

([3]) Οδηγίες για τις αναλυτικές πληροφορίες (π.χ. μέθοδος, κριτήρια, επίπεδο αποδόσεων) που πρέπει να αναφορτώνονται και για τον μορφότυπο περιλαμβάνονται στο ερμηνευτικό έγγραφο που εκπονείται επί του παρόντος από την ειδική ομάδα για ζητήματα κυβερνοασφάλειας και ασύρματων δικτύων ενόψει της έβδομης συνόδου της ομάδας εργασίας GRVA.

([4]) Η ομάδα εργασίας για τα αυτοματοποιημένα/αυτόνομα και συνδεδεμένα οχήματα (GRVA).

([5]) Η ερμηνεία αυτή περιλαμβάνεται στο ερμηνευτικό έγγραφο που αναφέρεται στην υποσημείωση της παραγράφου 5.3.3.

([6]) Περαιτέρω πληροφορίες σχετικά με τις ελάχιστες απαιτήσεις για τον φάκελο τεκμηρίωσης θα παρασχεθούν από την ομάδα GRVA κατά τη διάρκεια της έβδομης συνόδου της.

6. ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΣΥΜΜΟΡΦΩΣΗΣ ΓΙΑ ΤΟ ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

6.1. Τα συμβαλλόμενη μέρη ορίζουν αρχή έγκρισης η οποία διενεργεί την αξιολόγηση του κατασκευαστή και εκδίδει πιστοποιητικό συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας.

6.2. Η αίτηση για το πιστοποιητικό συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας υποβάλλεται από τον κατασκευαστή του οχήματος ή από τον δεόντως εξουσιοδοτημένο αντιπρόσωπό του.

6.3. Η αίτηση συνοδεύεται από τα κατωτέρω έγγραφα εις τριπλούν, στα οποία συγκαταλέγονται μεταξύ άλλων τα εξής:

6.3.1. Έγγραφα στα οποία περιγράφεται το σύστημα διαχείρισης της κυβερνοασφάλειας.

6.3.2. Υπογεγραμμένη δήλωση με βάση το υπόδειγμα που ορίζεται στο προσάρτημα 1 του παραρτήματος 1.

6.4. Στο πλαίσιο της αξιολόγησης, ο κατασκευαστής δηλώνει, χρησιμοποιώντας το υπόδειγμα που ορίζεται στο προσάρτημα 1 του παραρτήματος 1, και αποδεικνύει επαρκώς στην αρχή έγκρισης ή στην τεχνική της υπηρεσία ότι εφαρμόζει τις αναγκαίες διαδικασίες για την εκπλήρωση όλων των απαιτήσεων κυβερνοασφάλειας που προβλέπονται στον παρόντα κανονισμό.

6.5. Μετά την επιτυχή ολοκλήρωση της εν λόγω αξιολόγησης και την παραλαβή της υπογεγραμμένης δήλωσης από τον κατασκευαστή με βάση το υπόδειγμα που ορίζεται στο προσάρτημα 1 του παραρτήματος 1, χορηγείται στον κατασκευαστή πιστοποιητικό με την ονομασία πιστοποιητικό συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας, όπως περιγράφεται στο παράρτημα 4 του παρόντος κανονισμού (στο εξής: πιστοποιητικό συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας).

6.6. Η αρχή έγκρισης ή η τεχνική της υπηρεσία χρησιμοποιεί το υπόδειγμα που παρουσιάζεται στο παράρτημα 4 του παρόντος κανονισμού για το πιστοποιητικό συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας.

6.7. Το πιστοποιητικό συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας παραμένει σε ισχύ τουλάχιστον τρία έτη από την ημερομηνία έκδοσης του πιστοποιητικού, εκτός αν ανακληθεί.

6.8. Η αρχή έγκρισης που έχει χορηγήσει το πιστοποιητικό συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας μπορεί ανά πάσα στιγμή να εξακριβώνει ότι οι απαιτήσεις του πιστοποιητικού εξακολουθούν να εκπληρώνονται. Η αρχή έγκρισης ανακαλεί το πιστοποιητικό συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας αν οι απαιτήσεις που προβλέπονται στον παρόντα κανονισμό έχουν σταματήσει να εκπληρώνονται.

6.9. Ο κατασκευαστής ενημερώνει την αρχή έγκρισης ή την τεχνική της υπηρεσία για οποιαδήποτε αλλαγή επηρεάζει την εγκυρότητα του πιστοποιητικού συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας. Σε συνεννόηση με τον κατασκευαστή, η αρχή έγκρισης ή η τεχνική της υπηρεσία αποφασίζει αν χρειάζεται να διενεργηθούν νέοι έλεγχοι.

6.10. Εγκαίρως, και εφόσον η αρχή έγκρισης ολοκληρώσει την αξιολόγησή της πριν από τη λήξη της περιόδου ισχύος του πιστοποιητικού συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας, ο κατασκευαστής υποβάλλει αίτηση για νέο πιστοποιητικό συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας ή για την παράταση του εν λόγω πιστοποιητικού. Η αρχή έγκρισης, εφόσον η αξιολόγηση είναι θετική, εκδίδει νέο πιστοποιητικό συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας ή παρατείνει την ισχύ του για τρία ακόμα έτη. Η αρχή έγκρισης βεβαιώνεται ότι το σύστημα διαχείρισης της κυβερνοασφάλειας εξακολουθεί να συμμορφώνεται με τις απαιτήσεις του παρόντος κανονισμού. Αν υποπέσουν στην αντίληψη της αρχής έγκρισης ή της τεχνικής της υπηρεσίας αλλαγές και οι αλλαγές αυτές αξιολογηθούν θετικά, η αρχή έγκρισης εκδίδει νέο πιστοποιητικό.

6.11. Η λήξη ή η ανάκληση του πιστοποιητικού συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας του κατασκευαστή λογίζεται, όσον αφορά τους τύπους οχημάτων που καλύπτονταν από το οικείο σύστημα διαχείρισης της κυβερνοασφάλειας, ως τροποποίηση της έγκρισης, όπως αναφέρεται στην παράγραφο 8, η οποία ενδέχεται να περιλαμβάνει και την απόσυρση της έγκρισης, αν οι όροι χορήγησης της έγκρισης έχουν σταματήσει να εκπληρώνονται.

7. ΠΡΟΔΙΑΓΡΑΦΕΣ

7.1. Γενικές προδιαγραφές

7.1.1. Οι απαιτήσεις του παρόντος κανονισμού δεν περιορίζουν διατάξεις ή απαιτήσεις άλλων κανονισμών του ΟΗΕ.

7.2. Απαιτήσεις για το σύστημα διαχείρισης της κυβερνοασφάλειας

7.2.1. Για την αξιολόγηση, η αρχή έγκρισης ή η τεχνική της υπηρεσία βεβαιώνεται ότι ο κατασκευαστής του οχήματος εφαρμόζει σύστημα διαχείρισης της κυβερνοασφάλειας και εξακριβώνει τη συμμόρφωση του συστήματος με τον παρόντα κανονισμό.

7.2.2. Το σύστημα διαχείρισης της κυβερνοασφάλειας καλύπτει τις ακόλουθες πτυχές:

7.2.2.1. Ο κατασκευαστής του οχήματος αποδεικνύει στην αρχή έγκρισης ή στην τεχνική υπηρεσία ότι το σύστημα διαχείρισης της κυβερνοασφάλειας ισχύει για τα ακόλουθα στάδια:

α) στάδιο ανάπτυξης·

β) στάδιο παραγωγής·

γ) στάδιο μετά την παραγωγή.

7.2.2.2. Ο κατασκευαστής του οχήματος αποδεικνύει ότι οι διαδικασίες που χρησιμοποιούνται στο πλαίσιο του συστήματος διαχείρισης της κυβερνοασφάλειας διασφαλίζουν ότι η ασφάλεια, περιλαμβανομένων των κινδύνων και των μέτρων προστασίας που παρατίθενται στο παράρτημα 5, λαμβάνεται δεόντως υπόψη. Το σύστημα διαχείρισης περιλαμβάνει:

α) τις διαδικασίες που χρησιμοποιούνται στον οργανισμό του κατασκευαστή για τη διαχείριση της κυβερνοασφάλειας·

β) τις διαδικασίες που χρησιμοποιούνται για τον εντοπισμό των κινδύνων που απειλούν τους τύπους οχημάτων. Στο πλαίσιο αυτών των διαδικασιών εξετάζονται οι απειλές του παραρτήματος 5 μέρος Α και άλλες σχετικές απειλές·

γ) τις διαδικασίες που χρησιμοποιούνται για την αξιολόγηση, την κατηγοριοποίηση και την αντιμετώπιση των εντοπισθέντων κινδύνων·

δ) τις διαδικασίες που χρησιμοποιούνται για να εξακριβωθεί η επαρκής διαχείριση των εντοπισθέντων κινδύνων·

ε) τις διαδικασίες που χρησιμοποιούνται για τον έλεγχο της κυβερνοασφάλειας του τύπου οχήματος·

στ) τις διαδικασίες που χρησιμοποιούνται για να διασφαλίζεται ότι η εκτίμηση κινδύνου παραμένει επίκαιρη·

ζ) τις διαδικασίες που χρησιμοποιούνται για να παρακολουθούνται, να εντοπίζονται και να αντιμετωπίζονται οι κυβερνοεπιθέσεις, οι απειλές στον κυβερνοχώρο και οι ευπάθειες των τύπων των οχημάτων, καθώς και τις διαδικασίες που χρησιμοποιούνται για να αξιολογείται αν τα μέτρα που εφαρμόζονται για την κυβερνοασφάλεια εξακολουθούν να είναι αποτελεσματικά με βάση τις νέες απειλές και ευπάθειες που έχουν εντοπιστεί στον κυβερνοχώρο.

η) τις διαδικασίες που χρησιμοποιούνται για να διαβιβάζονται σχετικά δεδομένα στις αρχές που αναλύουν απόπειρες κυβερνοεπιθέσεων ή επιτυχημένες κυβερνοεπιθέσεις.

7.2.2.3. Ο κατασκευαστής του οχήματος αποδεικνύει ότι οι διαδικασίες που χρησιμοποιούνται στο πλαίσιο του συστήματος διαχείρισης της κυβερνοασφάλειας διασφαλίζουν, βάσει της κατηγοριοποίησης που αναφέρεται στην παράγραφο 7.2.2.2 στοιχεία γ) και ζ), ότι οι απειλές στον κυβερνοχώρο και οι ευπάθειες που πρέπει να αντιμετωπίζονται από τον κατασκευαστή του οχήματος περιορίζονται εντός εύλογου χρονικού διαστήματος.

7.2.2.4. Ο κατασκευαστής του οχήματος αποδεικνύει ότι οι διαδικασίες που χρησιμοποιούνται στο πλαίσιο του συστήματος διαχείρισης της κυβερνοασφάλειας διασφαλίζουν ότι η παρακολούθηση που αναφέρεται στην παράγραφο 7.2.2.2 στοιχείο ζ) είναι συνεχής. Οι διαδικασίες αυτές εστιάζουν:

α) στα οχήματα μετά την πρώτη τους ταξινόμηση, τα οποία παρακολουθούνται·

β) στην ικανότητα ανάλυσης και εντοπισμού των απειλών στον κυβερνοχώρο, των ευπαθειών και των κυβερνοεπιθέσεων με βάση τα δεδομένα των οχημάτων και τα αρχεία καταγραφής που διαθέτουν τα οχήματα. Η ικανότητα αυτή ασκείται με την επιφύλαξη της παραγράφου 1.3 και των δικαιωμάτων προστασίας της ιδιωτικής ζωής των ιδιοκτητών ή των οδηγών των αυτοκινήτων, κυρίως σε ό,τι αφορά τη συναίνεση.

7.2.2.5. Ο κατασκευαστής του οχήματος πρέπει να καταδεικνύει τον τρόπο με τον οποίο το σύστημα διαχείρισης της κυβερνοασφάλειας διαχειρίζεται τις αλληλεξαρτήσεις που ενδέχεται να υπάρχουν με συμβεβλημένους προμηθευτές, παρόχους υπηρεσιών ή επιμέρους οργανισμούς του κατασκευαστή όσον αφορά τις απαιτήσεις της παραγράφου 7.2.2.2.

7.3. Απαιτήσεις για τους τύπους οχημάτων

7.3.1. Ο κατασκευαστής διαθέτει έγκυρο πιστοποιητικό συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας, το οποίο ανταποκρίνεται στον τύπο οχήματος που εγκρίνεται.

Ωστόσο, όσον αφορά τις εγκρίσεις τύπου που χορηγούνται πριν από την 1η Ιουλίου 2024, αν ο κατασκευαστής του οχήματος μπορεί να αποδείξει ότι ο τύπος οχήματος ήταν αδύνατο να αναπτυχθεί με βάση το σύστημα διαχείρισης της κυβερνοασφάλειας, ο κατασκευαστής του οχήματος αποδεικνύει ότι η κυβερνοασφάλεια ελήφθη επαρκώς υπόψη κατά τη διάρκεια του σταδίου ανάπτυξης του οικείου τύπου οχήματος.

7.3.2. Ο κατασκευαστής του οχήματος εντοπίζει και διαχειρίζεται, για τον τύπο οχήματος που εγκρίνεται, κινδύνους που προέρχονται από τους προμηθευτές.

7.3.3. Ο κατασκευαστής του οχήματος εντοπίζει τα κρίσιμα στοιχεία του τύπου οχήματος και διενεργεί ενδελεχή εκτίμηση κινδύνου για τον τύπο οχήματος και αντιμετωπίζει/διαχειρίζεται επαρκώς τους εντοπισθέντες κινδύνους. Στην εκτίμηση κινδύνου εξετάζονται τα επιμέρους στοιχεία του τύπου οχήματος και οι αλληλεξαρτήσεις τους. Στην εκτίμηση κινδύνου λαμβάνονται επίσης υπόψη αλληλεπιδράσεις με εξωτερικά συστήματα. Κατά την εκτίμηση των κινδύνων, ο κατασκευαστής του οχήματος εξετάζει τους κινδύνους που συνδέονται με όλες τις απειλές που αναφέρονται στο παράρτημα 5 μέρος Α, καθώς και οποιονδήποτε άλλο σχετικό κίνδυνο.

7.3.4. Ο κατασκευαστής του οχήματος προστατεύει τον τύπο οχήματος από τους κινδύνους που εντοπίζονται στην εκτίμηση κινδύνου του κατασκευαστή του οχήματος. Για την προστασία του τύπου του οχήματος εφαρμόζονται αναλογικά μέτρα προστασίας. Μεταξύ των μέτρων προστασίας που εφαρμόζονται συγκαταλέγονται όλα τα μέτρα προστασίας του παραρτήματος 5, μέρος Β και Γ που ενδείκνυνται για τους εντοπισθέντες κινδύνους. Ωστόσο, όταν τα μέτρα προστασίας του παραρτήματος 5 μέρος Β ή Γ δεν ενδείκνυνται ή δεν θεωρούνται επαρκή για τον εντοπισθέντα κίνδυνο, ο κατασκευαστής του οχήματος μεριμνά ώστε να εφαρμόζονται άλλα μέτρα προστασίας.

Συγκεκριμένα, όσον αφορά τις εγκρίσεις τύπου που χορηγούνται πριν από την 1η Ιουλίου 2024, ο κατασκευαστής του οχήματος μεριμνά ώστε να εφαρμόζονται άλλα ενδεδειγμένα μέτρα προστασίας, αν το μέτρο προστασίας που αναφέρεται στο παράρτημα 5 μέρος Β ή Γ είναι τεχνικά ανέφικτο να υλοποιηθεί. Η αντίστοιχη εκτίμηση της τεχνικής εφικτότητας προσκομίζεται από τον κατασκευαστή στην αρχή έγκρισης.

7.3.5. Ο κατασκευαστής του οχήματος θέτει σε εφαρμογή κατάλληλα και αναλογικά μέτρα για να θωρακίσει ειδικά περιβάλλοντα στον τύπο οχήματος, τα οποία χρησιμοποιούνται (αν υπάρχουν) για την αποθήκευση και την εκτέλεση λογισμικού, υπηρεσιών, εφαρμογών ή δεδομένων της δευτερογενούς αγοράς.

7.3.6. Ο κατασκευαστής του οχήματος διενεργεί, πριν από την έγκριση, κατάλληλες και επαρκείς δοκιμές για να εξακριβώσει την αποτελεσματικότητα των μέτρων ασφάλειας που εφαρμόζονται.

7.3.7. Ο κατασκευαστής του οχήματος εφαρμόζει μέτρα για τον τύπο οχήματος προκειμένου να:

α) εντοπίζει και να προλαμβάνει κυβερνοεπιθέσεις εναντίον των οχημάτων του τύπου οχήματος·

β) υποστηρίζει την ικανότητα παρακολούθησης του κατασκευαστή του οχήματος στο πλαίσιο της οποίας εντοπίζονται απειλές, ευπάθειες και κυβερνοεπιθέσεις σχετικές με τον τύπο οχήματος·

γ) προσφέρει μέσα για την εγκληματολογική ανάλυση δεδομένων, τα οποία επιτρέπουν στις αρχές να αναλύουν απόπειρες κυβερνοεπιθέσεων ή επιτυχημένες κυβερνοεπιθέσεις.

7.3.8. Οι λειτουργικές μονάδες κρυπτογράφησης που χρησιμοποιούνται για τους σκοπούς του παρόντος κανονισμού εναρμονίζονται με τα πρότυπα κοινής αποδοχής. Αν οι λειτουργικές μονάδες κρυπτογράφησης δεν εναρμονίζονται με τα πρότυπα κοινής αποδοχής, τότε ο κατασκευαστής του οχήματος δικαιολογεί τη χρήση τους.

7.4. Διατάξεις για την υποβολή εκθέσεων

7.4.1. Ο κατασκευαστής του οχήματος υποβάλλει έκθεση τουλάχιστον μία φορά ετησίως, ή συχνότερα αν κρίνεται αναγκαίο, στην αρχή έγκρισης ή στην τεχνική υπηρεσία για το αποτέλεσμα των δραστηριοτήτων παρακολούθησης που υλοποιεί, όπως ορίζεται στην παράγραφο 7.2.2.2 στοιχείο ζ), περιλαμβάνοντας σημαντικές πληροφορίες για νέες κυβερνοεπιθέσεις. Επίσης, ο κατασκευαστής του οχήματος υποβάλλει έκθεση και διαβεβαιώνει την αρχή έγκρισης ή την τεχνική υπηρεσία ότι τα μέτρα προστασίας που εφαρμόζει για την κυβερνοασφάλεια των τύπων των οχημάτων του εξακολουθούν να είναι αποτελεσματικά, αναφέροντας και άλλες ενέργειες στις οποίες έχει ενδεχομένως προβεί.

7.4.2. Η αρχή έγκρισης ή η τεχνική υπηρεσία εξακριβώνει τις πληροφορίες που παρέχονται και, αν κρίνεται αναγκαίο, ζητεί από τον κατασκευαστή του οχήματος να διορθώσει όποιες ατέλειες εντοπίζονται.

Αν η έκθεση ή η απάντηση δεν είναι επαρκής, η αρχή έγκρισης μπορεί να αποφασίσει την απόσυρση του συστήματος διαχείρισης της κυβερνοασφάλειας σύμφωνα με την παράγραφο 6.8.

8. ΤΡΟΠΟΠΟΙΗΣΗ ΤΥΠΟΥ ΟΧΗΜΑΤΟΣ ΚΑΙ ΕΠΕΚΤΑΣΗ ΕΓΚΡΙΣΗΣ ΤΥΠΟΥ

8.1. Κάθε τροποποίηση του τύπου οχήματος που αφορά τις τεχνικές του επιδόσεις όσον αφορά την κυβερνοασφάλεια και/ή τα έγγραφα τεκμηρίωσης που προβλέπονται στον παρόντα κανονισμό κοινοποιείται στην αρχή έγκρισης που ενέκρινε τον τύπο οχήματος. Στην περίπτωση αυτή, η αρχή έγκρισης μπορεί:

8.1.1. να θεωρήσει ότι οι τροποποιήσεις που επήλθαν εξακολουθούν να συμμορφώνονται με τις απαιτήσεις και τα έγγραφα τεκμηρίωσης της υφιστάμενης έγκρισης τύπου· ή

8.1.2. να διενεργήσει την αναγκαία συμπληρωματική αξιολόγηση δυνάμει της παραγράφου 5 και να ζητήσει, κατά περίπτωση, συμπληρωματική έκθεση δοκιμής από την τεχνική υπηρεσία που είναι αρμόδια να διενεργεί τις δοκιμές.

8.1.3. Η επιβεβαίωση ή η επέκταση ή η μη χορήγηση της έγκρισης, με την οποία προσδιορίζονται οι μετατροπές, κοινοποιείται μέσω εντύπου επικοινωνίας που συμφωνεί με το υπόδειγμα του παραρτήματος 2 του παρόντος κανονισμού. Η αρχή έγκρισης που χορηγεί την επέκταση της έγκρισης ορίζει αύξοντα αριθμό για την εν λόγω επέκταση και ενημερώνει σχετικά τα υπόλοιπα συμβαλλόμενα μέρη της συμφωνίας του 1958 που εφαρμόζουν τον παρόντα κανονισμό, μέσω εντύπου κοινοποίησης που συμφωνεί με το υπόδειγμα του παραρτήματος 2 του παρόντος κανονισμού.

9. ΣΥΜΜΟΡΦΩΣΗ ΤΗΣ ΠΑΡΑΓΩΓΗΣ

9.1. Οι διαδικασίες παραγωγής συμφωνούν με τις διαδικασίες που καθορίζονται στη συμφωνία του 1958, πίνακας 1 (E/ECE/TRANS/505/αναθ.3), με τις ακόλουθες προϋποθέσεις:

9.1.1. Ο κάτοχος της έγκρισης μεριμνά για την καταγραφή των αποτελεσμάτων των δοκιμών συμμόρφωσης της παραγωγής και εξασφαλίζει ότι τα συνημμένα έγγραφα παραμένουν διαθέσιμα για χρονική περίοδο που καθορίζεται σε συμφωνία με την αρχή έγκρισης ή την τεχνική της υπηρεσία. Η χρονική αυτή περίοδος δεν υπερβαίνει τα 10 έτη από τη στιγμή της οριστικής διακοπής της παραγωγής.

9.1.2. Η αρχή έγκρισης που έχει χορηγήσει έγκριση τύπου μπορεί ανά πάσα στιγμή να επαληθεύει τις μεθόδους ελέγχου της συμμόρφωσης που εφαρμόζονται σε κάθε μονάδα παραγωγής. Οι εν λόγω επαληθεύσεις διενεργούνται κατά κανόνα ανά τρία έτη.

10. ΚΥΡΩΣΕΙΣ ΣΕ ΠΕΡΙΠΤΩΣΗ ΜΗ ΣΥΜΜΟΡΦΩΣΗΣ ΤΗΣ ΠΑΡΑΓΩΓΗΣ

10.1. Η έγκριση που χορηγείται για τύπο οχήματος δυνάμει του παρόντος κανονισμού μπορεί να ανακληθεί αν δεν εκπληρώνονται οι απαιτήσεις που προβλέπονται στον παρόντα κανονισμό ή αν τα δείγματα αυτοκινήτων δεν εκπληρώνουν τις απαιτήσεις του παρόντος κανονισμού.

10.2. Αν αρχή έγκρισης ανακαλέσει έγκριση που έχει ήδη χορηγήσει, ενημερώνει αμέσως τα συμβαλλόμενα μέρη που εφαρμόζουν τον παρόντα κανονισμό μέσω εντύπου επικοινωνίας που συμφωνεί με το υπόδειγμα του παραρτήματος 2 του παρόντος κανονισμού.

11. ΟΡΙΣΤΙΚΗ ΠΑΥΣΗ ΤΗΣ ΠΑΡΑΓΩΓΗΣ

11.1. Αν ο κάτοχος της έγκρισης διακόψει οριστικά την παραγωγή τύπου οχήματος που έχει εγκριθεί σύμφωνα με τον παρόντα κανονισμό, ενημερώνει σχετικά την αρχή που χορήγησε την έγκριση. Αφού λάβει τη σχετική κοινοποίηση, η εν λόγω αρχή ενημερώνει τα άλλα συμβαλλόμενα μέρη της συμφωνίας που εφαρμόζουν τον παρόντα κανονισμό μέσω αντιγράφου του εντύπου έγκρισης το οποίο στο τέλος φέρει, υπογεγραμμένη και χρονολογημένη, την ένδειξη «ΠΑΥΣΗ ΠΑΡΑΓΩΓΗΣ», με κεφαλαία γράμματα.

12. ΟΝΟΜΑΣΙΕΣ ΚΑΙ ΔΙΕΥΘΥΝΣΕΙΣ ΤΩΝ ΤΕΧΝΙΚΩΝ ΥΠΗΡΕΣΙΩΝ ΠΟΥ ΕΙΝΑΙ ΑΡΜΟΔΙΕΣ ΓΙΑ ΤΗ ΔΙΕΞΑΓΩΓΗ ΔΟΚΙΜΩΝ ΕΓΚΡΙΣΗΣ, ΚΑΘΩΣ ΚΑΙ ΤΩΝ ΑΡΧΩΝ ΕΓΚΡΙΣΗΣ ΤΥΠΟΥ

12.1. Τα συμβαλλόμενα μέρη της συμφωνίας που εφαρμόζουν τον παρόντα κανονισμό γνωστοποιούν στη Γραμματεία των Ηνωμένων Εθνών τις ονομασίες και τις διευθύνσεις των τεχνικών υπηρεσιών που είναι αρμόδιες για τη διεξαγωγή των δοκιμών έγκρισης και των αρχών έγκρισης τύπου που χορηγούν την έγκριση και στις οποίες πρέπει να αποστέλλονται τα έντυπα που εκδίδονται σε άλλες χώρες και πιστοποιούν την έγκριση ή την επέκταση ή την απόρριψη ή την ανάκληση έγκρισης.

ΠΑΡΑΡΤΗΜΑ 1

Έγγραφο πληροφοριών

Οι ακόλουθες πληροφορίες παρέχονται, κατά περίπτωση, εις τριπλούν και περιλαμβάνουν πίνακα περιεχομένων. Τυχόν σχέδια παρέχονται σε κατάλληλη κλίμακα και με επαρκείς λεπτομέρειες σε μέγεθος Α4 ή εντός φακέλου μεγέθους Α4. Οι φωτογραφίες, εάν υπάρχουν, παρουσιάζουν αναλυτικές λεπτομέρειες.

1. Μάρκα (εμπορική επωνυμία του κατασκευαστή): .....

2. Τύπος και γενική/-ές εμπορική/-ές περιγραφή/-ές: .....

3. Μέσα αναγνώρισης τύπου, εφόσον υπάρχει σχετική σήμανση στο όχημα: .....

4. Σημείο τοποθέτησης της εν λόγω σήμανσης: .....

5. Κατηγορία/-ες οχήματος: .....

6. Επωνυμία και διεύθυνση του κατασκευαστή/ του εκπροσώπου του κατασκευαστή: .....

7. Επωνυμία/-ες και διεύθυνση/-εις της/των μονάδας/-ων συναρμολόγησης: .....

8. Φωτογραφία/-ες και/ή σχέδιο/-α αντιπροσωπευτικού οχήματος: .....

9. Κυβερνοασφάλεια

9.1. Γενικά κατασκευαστικά χαρακτηριστικά του τύπου οχήματος, μεταξύ άλλων:

α) τα συστήματα του οχήματος που συνδέονται με την κυβερνοασφάλεια του τύπου οχήματος·

β) τα κατασκευαστικά στοιχεία των εν λόγω συστημάτων που συνδέονται με την κυβερνοασφάλεια·

γ) οι αλληλεπιδράσεις των εν λόγω συστημάτων με άλλα συστήματα του τύπου οχήματος και εξωτερικές διασυνδέσεις.

9.2. Σχηματική αναπαράσταση του τύπου οχήματος

9.3. Ο αριθμός του πιστοποιητικού συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας: .....

9.4. Έγγραφα για τον προς έγκριση τύπο οχήματος στα οποία περιγράφονται το αποτέλεσμα της εκτίμησης κινδύνου και οι εντοπισθέντες κίνδυνοι: .....

9.5. Έγγραφα για τον προς έγκριση τύπο οχήματος στα οποία περιγράφονται τα μέτρα προστασίας που έχουν εφαρμοστεί στα συστήματα που απαριθμούνται ή στον τύπο του οχήματος, και ο τρόπος με τον οποίο τα εν λόγω μέτρα προστατεύουν από τους καταγεγραμμένους κινδύνους: .....

9.6. Έγγραφα για τον προς έγκριση τύπο οχήματος στα οποία περιγράφεται η προστασία των ειδικών περιβαλλόντων που χρησιμοποιούνται για το λογισμικό, τις υπηρεσίες, τις εφαρμογές ή τα δεδομένα της δευτερογενούς αγοράς: .....

9.7. Έγγραφα για τον προς έγκριση τύπο οχήματος στα οποία περιγράφονται οι δοκιμές που έχουν χρησιμοποιηθεί για να εξακριβωθεί η κυβερνοασφάλεια του τύπου οχήματος και των συστημάτων του και το αποτέλεσμα των εν λόγω δοκιμών: .....

9.8. Περιγραφή της παραμέτρου της αλυσίδας εφοδιασμού σε σχέση με την κυβερνοασφάλεια: .....

Προσάρτημα 1 του Παραρτήματος 1

Υπόδειγμα δήλωσης συμμόρφωσης του κατασκευαστή για το σύστημα διαχείρισης της κυβερνοασφάλειας

Δήλωση συμμόρφωσης του κατασκευαστή με τις απαιτήσεις του συστήματος διαχείρισης της κυβερνοασφάλειας

Όνομα κατασκευαστή: .....

Διεύθυνση κατασκευαστή: .....

Ο/Η ..... (*όνομα κατασκευαστή*) βεβαιώνει ότι τα συστήματα που είναι αναγκαία για την εκπλήρωση των απαιτήσεων του συστήματος διαχείρισης της κυβερνοασφάλειας που προβλέπονται στην παράγραφο 7.2 του κανονισμού 155 του ΟΗΕ έχουν εγκατασταθεί και θα διατηρηθούν..... .....

?????: ..... (*τόπος*)

Ημερομηνία: .....

Όνομα του υπογράφοντος: .....

Ιδιότητα του υπογράφοντος: .....

.....

(*Σφραγίδα και υπογραφή του εκπροσώπου του κατασκευαστή*)

ΠΑΡΑΡΤΗΜΑ 2

Επικοινωνία

[Μέγιστες διαστάσεις: A4 (210 × 297 mm)]

Εκδίδεται από: Όνομα υπηρεσίας:
.....
.....
.....

Σχετικά με ([2]): Χορήγηση έγκρισης
Επέκταση έγκρισης
Ανάκληση έγκρισης με ισχύ από την ηη/μμ/εεεε
Απόρριψη έγκρισης
Οριστική παύση της παραγωγής

τύπου οχήματος σύμφωνα με τον κανονισμό αριθ. 155 του ΟΗΕ

Αριθ. έγκρισης: .....

Αριθ. επέκτασης: .....

Λόγος επέκτασης: .....

1. Μάρκα (εμπορική επωνυμία του κατασκευαστή): .....

2. Τύπος και γενική/-ές εμπορική/-ές περιγραφή/-ές .....

3. Μέσα αναγνώρισης τύπου, εφόσον υπάρχει σχετική σήμανση στο όχημα: .....

3.1. Σημείο τοποθέτησης της εν λόγω σήμανσης: .....

4. Κατηγορία/-ες οχήματος: .....

5. Επωνυμία και διεύθυνση του κατασκευαστή/ του αντιπροσώπου του κατασκευαστή: .....

6. Επωνυμία/-ες και διεύθυνση/-εις της/των μονάδας/-ων παραγωγής: .....

7. Αριθμός του πιστοποιητικού συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας: .....

8. Υπεύθυνη τεχνική υπηρεσία για τη διεξαγωγή των δοκιμών: .....

9. Ημερομηνία της έκθεσης δοκιμής: .....

10. Αριθμός της έκθεσης δοκιμής: .....

11. Παρατηρήσεις: (εφόσον υπάρχουν). .....

12. Τόπος: .....

13. Ημερομηνία: .....

14. Υπογραφή: .....

15. Επισυνάπτεται το ευρετήριο του φακέλου πληροφοριών που υποβάλλεται στην αρχή έγκρισης, το οποίο μπορεί να ληφθεί μετά από αίτηση:

([1]) Αναγνωριστικός αριθμός της χώρας που χορήγησε/επέκτεινε/απέρριψε/ανακάλεσε την έγκριση (βλέπε διατάξεις σχετικά με την έγκριση στον κανονισμό).

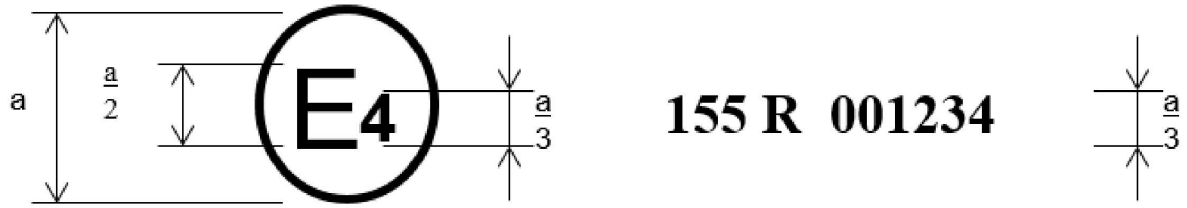
([2]) Διαγράφεται η περιττή ένδειξη.

ΠΑΡΑΡΤΗΜΑ 3

Τρόπος διάταξης σήματος έγκρισης

ΥΠΟΔΕΙΓΜΑ Α

(Βλ. παράγραφο 4.2 του παρόντος κανονισμού)



a = 8 mm τουλάχιστον

Όπως προκύπτει από το ανωτέρω σήμα έγκρισης που έχει επικολληθεί σε όχημα, ο σχετικός τύπος οδικού οχήματος έχει εγκριθεί στις Κάτω Χώρες (E 4), σύμφωνα με τον κανονισμό αριθ. 155 και τον αριθμό έγκρισης 001234. Τα δύο πρώτα ψηφία του αριθμού έγκρισης υποδηλώνουν ότι η έγκριση χορηγήθηκε σύμφωνα με τις απαιτήσεις του κανονισμού υπό την αρχική του μορφή (00).

ΠΑΡΑΡΤΗΜΑ 4

Υπόδειγμα πιστοποιητικού συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας

Πιστοποιητικό συμμόρφωσης για το σύστημα διαχείρισης της κυβερνοασφάλειας

με τον κανονισμό αριθ. 155 του ΟΗΕ

Αριθμός πιστοποιητικού (*αριθμός αναφοράς*)

Ο/Η/Το [……. *Αρχή έγκρισης*]

Πιστοποιεί ότι ο/η

Κατασκευαστής: ……

Διεύθυνση του κατασκευαστή: ……

τηρεί τις διατάξεις της παραγράφου 7.2 του κανονισμού αριθ. 155

Οι έλεγχοι διενεργήθηκαν στις: ……

από (όνομα και διεύθυνση της αρχής έγκρισης ή της τεχνικής υπηρεσίας): ……

Αριθμός έκθεσης: ……

Το πιστοποιητικό ισχύει έως [……*ημερομηνία*]

[…… *Τόπος*]

[……*Ημερομηνία*]

[……*Υπογραφή*]

Συνημμένα: Περιγραφή του συστήματος διαχείρισης της κυβερνοασφάλειας από τον κατασκευαστή.

ΠΑΡΑΡΤΗΜΑ 5

Κατάλογος των απειλών και των αντίστοιχων μέτρων προστασίας

1. Το παρόν παράρτημα αποτελείται από τρία μέρη. Στο μέρος Α του παρόντος παραρτήματος περιγράφεται το σενάριο αναφοράς για τις απειλές, τις ευπάθειες και τις μεθόδους επιθέσεων. Στο μέρος Β του παρόντος παραρτήματος περιγράφονται τα μέτρα προστασίας από τις απειλές, τα οποία σχεδιάστηκαν για τους τύπους οχημάτων. Στο μέρος Γ περιγράφονται τα μέτρα προστασίας από τις απειλές, τα οποία σχεδιάστηκαν για περιβάλλοντα εκτός των οχημάτων, π.χ. για διακομιστές παρασκηνίου ΤΠ.

2. Το μέρος Α, το μέρος Β και το μέρος Γ λαμβάνονται υπόψη στην εκτίμηση κινδύνου και τα μέτρα προστασίας που πρέπει να εφαρμόζουν οι κατασκευαστές των οχημάτων.

3. Οι γενικές κατηγορίες ευπαθειών και τα αντίστοιχα παραδείγματά τους έχουν κωδικοποιηθεί στο μέρος Α. Η ίδια κωδικοποίηση αναφέρεται στους πίνακες των μερών Β και Γ ώστε κάθε επίθεση/ευπάθεια να συνδέεται με τα εκάστοτε μέτρα προστασίας.

4. Κατά την ανάλυση των απειλών λαμβάνονται επίσης υπόψη οι πιθανές επιπτώσεις των επιθέσεων. Με βάση αυτές τις επιπτώσεις αξιολογείται η σοβαρότητα των κινδύνων και εντοπίζονται πρόσθετοι κίνδυνοι. Μεταξύ των πιθανών επιπτώσεων συγκαταλέγονται οι εξής:

   α) επισφαλής λειτουργία του οχήματος που δέχεται την επίθεση·

   β) παύση λειτουργίας του οχήματος·

   γ) τροποποίηση του λογισμικού, αλλοίωση των επιδόσεων·

   δ) αλλοίωση του λογισμικού χωρίς ωστόσο να επηρεαστεί η λειτουργία του·

   ε) παραβίαση της ακεραιότητας των δεδομένων·

   στ) παραβίαση της εμπιστευτικότητας των δεδομένων·

   ζ) περιορισμός της διαθεσιμότητας των δεδομένων·

   η) άλλο, περιλαμβανομένης της εγκληματικότητας.

Μέρος Α. Ευπάθεια ή μέθοδος επίθεσης που συνδέεται με τις απειλές

1. Οι γενικές κατηγορίες απειλών και η σχετική ευπάθεια ή μέθοδος επίθεσης παρατίθενται στον πίνακα Α1.

Πίνακας Α1

Κατάλογος ευπαθειών ή μεθόδων επιθέσεων που συνδέονται με τις απειλές

Γενικές και ειδικές κατηγορίες ευπαθειών/απειλών			Παράδειγμα ευπάθειας ή μεθόδου επίθεσης	
4.3.1. Απειλές σχετικά με διακομιστές παρασκηνίου που συνδέονται με οχήματα σε πραγματικές συνθήκες λειτουργίας	1	Διακομιστές παρασκηνίου χρησιμοποιούνται ως μέσο επίθεσης κατά οχημάτων ή ως μέσο απόσπασης δεδομένων	1.1	Κατάχρηση προνομίων από το προσωπικό (επίθεση εκ των έσω)
			1.2	Μη εξουσιοδοτημένη διαδικτυακή πρόσβαση στον διακομιστή (π.χ. μέσω κακόβουλων λογισμικών που επιτρέπουν σε εισβολείς να έχουν τον απομακρυσμένο έλεγχο υπολογιστών, μέσω μη κατοχυρωμένων λογισμικών, επιθέσεων SQL ή άλλων μεθόδων)
			1.3	Μη εξουσιοδοτημένη φυσική πρόσβαση στον διακομιστή (π.χ. μέσω κλειδιών USB ή άλλων μέσων που συνδέονται με τον διακομιστή)
	2	Διακοπή υπηρεσιών του διακομιστή παρασκηνίου, η οποία επηρεάζει τη λειτουργία του οχήματος	2.1	Επίθεση στον διακομιστή παρασκηνίου έχει ως αποτέλεσμα τη διακοπή της λειτουργίας του διακομιστή, π.χ. ο διακομιστής δεν αλληλεπιδρά με τα οχήματα και δεν παρέχει τις υπηρεσίες που χρησιμοποιούν τα οχήματα

Γενικές και ειδικές κατηγορίες ευπαθειών/απειλών			Παράδειγμα ευπάθειας ή μεθόδου επίθεσης	
	3	Απώλεια ή υπονόμευση των δεδομένων των οχημάτων που φυλάσσονται σε διακομιστές παρασκηνίου («διαρροή δεδομένων»)	3.1	Κατάχρηση προνομίων από το προσωπικό (επίθεση εκ των έσω)
			3.2	Απώλειες πληροφοριών στο υπολογιστικό νέφος. Πιθανότητα απώλειας ευαίσθητων δεδομένων λόγω επιθέσεων ή ατυχημάτων όταν τα δεδομένα αποθηκεύονται από τρίτους παρόχους υπηρεσιών υπολογιστικού νέφους
			3.3	Μη εξουσιοδοτημένη διαδικτυακή πρόσβαση στον διακομιστή (π.χ. μέσω κακόβουλων λογισμικών που επιτρέπουν σε εισβολείς να έχουν τον απομακρυσμένο έλεγχο υπολογιστών, μέσω μη κατοχυρωμένων λογισμικών, επιθέσεων SQL ή άλλων μεθόδων)
			3.4	Μη εξουσιοδοτημένη φυσική πρόσβαση στον διακομιστή (π.χ. μέσω κλειδιών USB ή με τη βοήθεια άλλων μέσων που συνδέονται με τον διακομιστή)
			3.5	Διαρροή πληροφοριών λόγω ακούσιας κοινοποίησης δεδομένων (π.χ. σφάλματα διαχειριστή)
4.3.2. Απειλές κατά οχημάτων που αφορούν τους διαύλους επικοινωνίας τους	4	Πλαστογράφηση μηνυμάτων ή δεδομένων που λαμβάνονται από το όχημα	4.1	Πλαστογράφηση μηνυμάτων με πλαστοπροσωπία (π.χ. όταν κομβόι αυτόνομων οχημάτων επικοινωνεί ασύρματα με αισθητήρες που είναι εγκατεστημένοι στο οδικό δίκτυο με βάση το πρότυπο 802.11p, όταν ανταλλάσσονται μηνύματα μέσω του δικτύου GNSS κ.λπ.).
			4.2	Επίθεση Sybil (ο επιτιθέμενος πλαστογραφεί την ταυτότητά του και δημιουργεί πολλά ψεύτικα οχήματα στον δρόμο)
	5	Δίαυλοι επικοινωνίας χρησιμοποιούνται ως μέσα μη εξουσιοδοτημένου χειρισμού, διαγραφής ή άλλων τροποποιήσεων του κωδικού/των δεδομένων του οχήματος	5.1	Δίαυλοι επικοινωνίας επιτρέπουν επιθέσεις εισαγωγής κώδικα, π.χ. στη ροή επικοινωνίας εισάγεται παραποιημένο λογισμικό δυαδικής μορφής
			5.2	Δίαυλοι επικοινωνίας επιτρέπουν τον χειρισμό των δεδομένων/του κώδικα του οχήματος
			5.3	Δίαυλοι επικοινωνίας επιτρέπουν την αντικατάσταση των δεδομένων/του κώδικα του οχήματος
			5.4	Δίαυλοι επικοινωνίας επιτρέπουν τη διαγραφή των δεδομένων/του κώδικα του οχήματος
			5.5	Δίαυλοι επικοινωνίας επιτρέπουν την εισαγωγή δεδομένων/κώδικα στο όχημα (εγγραφή κώδικα δεδομένων)
	6	Δίαυλοι επικοινωνίας επιτρέπουν την αποδοχή μη αξιόπιστων μηνυμάτων ή είναι ευάλωτοι σε επιθέσεις υφαρπαγής συνόδου/ επαναληπτικής εκτέλεσης	6.1	Αποδοχή πληροφοριών από μη αξιόπιστη πηγή
			6.2	Επίθεση ενδιάμεσου (MITM)/υφαρπαγής συνόδου
			6.3	Επίθεση επαναληπτικής εκτέλεσης, π.χ. η επίθεση σε πύλη επικοινωνίας επιτρέπει στον επιτιθέμενο να υποβαθμίσει το λογισμικό μονάδας ηλεκτρονικού ελέγχου ή το υλικολογισμικό της πύλης

Γενικές και ειδικές κατηγορίες ευπαθειών/απειλών			Παράδειγμα ευπάθειας ή μεθόδου επίθεσης	
	7	Δυνατότητα εύκολης κοινοποίησης πληροφοριών. Παραδείγματος χάρη μέσω υποκλοπής επικοινωνιών ή χορήγησης μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητα αρχεία ή φακέλους	7.1	Υποκλοπή πληροφοριών/ηλεκτρομαγνητικές παρεμβολές/παρακολούθηση επικοινωνιών
			7.2	Απόκτηση μη εξουσιοδοτημένης πρόσβασης σε αρχεία ή δεδομένα
	8	Επιθέσεις άρνησης υπηρεσίας μέσω διαύλων επικοινωνίας με στόχο σκοπό τη διατάραξη των λειτουργιών του οχήματος	8.1	Αποστολή μεγάλου αριθμού απορριφθέντων δεδομένων στο σύστημα πληροφοριών του οχήματος με αποτέλεσμα να είναι αδύνατη η κανονική παροχή υπηρεσιών
			8.2	Επίθεση μαύρης τρύπας με στόχο τη διατάραξη της επικοινωνίας μεταξύ των οχημάτων· ο επιτιθέμενος έχει τη δυνατότητα να εμποδίζει την ανταλλαγή μηνυμάτων μεταξύ των οχημάτων
	9	Μη εξουσιοδοτημένος χρήστης μπορεί να αποκτήσει προνομιακή πρόσβαση στα συστήματα του οχήματος	9.1	Μη εξουσιοδοτημένος χρήστης μπορεί να αποκτήσει προνομιακή πρόσβαση, μεταξύ άλλων και πρόσβαση διαχειριστή (root access)
	10	Ιοί που ενσωματώνονται σε μέσα επικοινωνίας μπορούν να προσβάλλουν τα συστήματα του οχήματος	10.1	Ιός που ενσωματώνεται σε μέσα επικοινωνίας προσβάλλει τα συστήματα του οχήματος
	11	Μηνύματα που λαμβάνονται από το όχημα (π.χ. τα μηνύματα που λαμβάνονται από αισθητήρες του οδικού δικτύου ή τα διαγνωστικά μηνύματα), ή που διαβιβάζονται εντός του οχήματος περιέχουν κακόβουλο περιεχόμενο	11.1	Κακόβουλα εσωτερικά μηνύματα (π.χ. μηνύματα CAN)
			11.2	Κακόβουλα μηνύματα που ανταλλάσσονται μεταξύ οχημάτων και αισθητήρων του οδικού δικτύου, όπως π.χ. τα μηνύματα που αποστέλλονται από οδικές υποδομές στο όχημα ή τα μηνύματα που ανταλλάσσονται μεταξύ οχημάτων (π.χ. μηνύματα CAM, DENM)
			11.3	Κακόβουλα διαγνωστικά μηνύματα
			11.4	Κακόβουλα ιδιόκτητα μηνύματα (π.χ. τα μηνύματα που αποστέλλονται κατά κανόνα από συστήματα OEM ή από προμηθευτές κατασκευαστικών στοιχείων/συστημάτων/λειτουργιών)
4.3.3. Απειλές κατά οχημάτων σχετικά με τις διαδικασίες επικαιροποίησης στα οχήματα	12	Παράνομη χρήση ή υπονόμευση των διαδικασιών επικαιροποίησης	12.1	Υπονόμευση των ασύρματων διαδικασιών επικαιροποίησης λογισμικού. Συμπεριλαμβάνεται η κατασκευή του προγράμματος ή του υλικολογισμικού επικαιροποίησης του συστήματος
			12.2	Υπονόμευση τοπικών/φυσικών διαδικασιών επικαιροποίησης λογισμικού Συμπεριλαμβάνεται η κατασκευή του προγράμματος ή του υλικολογισμικού επικαιροποίησης του συστήματος
			12.3	Το λογισμικό παραποιείται πριν από τη διαδικασία επικαιροποίησης (και επομένως καταστρέφεται) χωρίς ωστόσο να επηρεαστεί η διαδικασία επικαιροποίησης

Γενικές και ειδικές κατηγορίες ευπαθειών/απειλών			Παράδειγμα ευπάθειας ή μεθόδου επίθεσης	
			12.4	Υπονόμευση κλειδιών κρυπτογράφησης του παρόχου του λογισμικού με αποτέλεσμα οι επικαιροποιήσεις να μην είναι έγκυρες
	13	Δυνατότητα απόρριψης κανονικών επικαιροποιήσεων	13.1	Επίθεση άρνησης υπηρεσίας κατά διακομιστή επικαιροποίησης ή δικτύου με αποτέλεσμα να μη διατίθενται κρίσιμης σημασίας επικαιροποιήσεις λογισμικού και/ή να μην ξεκλειδώνονται συγκεκριμένες δυνατότητες για κάθε πελάτη
4.3.4. Απειλές κατά οχημάτων σχετικά με ακούσιες ανθρώπινες ενέργειες που διευκολύνουν κυβερνοεπιθέσεις	15	Νόμιμοι παράγοντες μπορούν να προβαίνουν σε ενέργειες οι οποίες, εν αγνοία τους, διευκολύνουν τη διάπραξη κυβερνοεπιθέσεων	15.1	Αθώο θύμα (π.χ. ιδιοκτήτης, χειριστής ή μηχανικός συντήρησης) εξαπατάται και προβαίνει σε ενέργεια με την οποία εν αγνοία του εισάγει κακόβουλο λογισμικό ή διευκολύνει τη διάπραξη επίθεσης
			15.2	Δεν ακολουθούνται οι καθορισμένες διαδικασίες ασφάλειας
4.3.5. Απειλές κατά οχημάτων σχετικά με την εξωτερική συνδεσιμότητα και τις συνδέσεις των οχημάτων	16	Παραποίηση της συνδεσιμότητας των λειτουργιών του οχήματος επιτρέπει τη διάπραξη κυβερνοεπίθεσης, μεταξύ άλλων μέσω εφαρμογών τηλεματικής· συστημάτων που επιτρέπουν απομακρυσμένες λειτουργίες· και συστημάτων που χρησιμοποιούν ασύρματες επικοινωνίες μικρής εμβέλειας	16.1	Παραποίηση λειτουργιών που υποστηρίζουν την απομακρυσμένη λειτουργία των συστημάτων, όπως π.χ. τα απομακρυσμένα κλειδιά, τα συστήματα ακινητοποίησης και οι σταθμοί φόρτισης
			16.2	Παραποίηση των εφαρμογών τηλεματικής του οχήματος (π.χ. παραποίηση των μετρήσεων της θερμοκρασίας ευαίσθητων προϊόντων, απομακρυσμένο ξεκλείδωμα θυρών του διαμερίσματος του φορτίου)
			16.3	Παρεμβολές σε ασύρματα συστήματα ή αισθητήρες μικρής εμβέλειας
	17	Λογισμικό τρίτων, π.χ, εφαρμογές ψυχαγωγίας, χρησιμοποιείται ως μέσο επίθεσης εναντίον συστημάτων του οχήματος	17.1	Κατεστραμμένες εφαρμογές ή εφαρμογές με ελλιπή ασφάλεια λογισμικού χρησιμοποιούνται ως μέσο επίθεσης εναντίον συστημάτων του οχήματος
	18	Συσκευές που συνδέονται με εξωτερικές διεπαφές, όπως π. χ. οι θύρες USB, η θύρα OBD, χρησιμοποιούνται ως μέσο επίθεσης εναντίον συστημάτων του οχήματος	18.1	Εξωτερικές διεπαφές, όπως π.χ. θύρες USB ή άλλες θύρες, χρησιμοποιούνται ως σημείο επίθεσης, π.χ. για την εισαγωγή κώδικα
			18.2	Μέσα που έχουν προσβληθεί από ιό συνδέονται με σύστημα του οχήματος
			18.3	Η διαγνωστική πρόσβαση [π.χ. κλειδιά υλικού (dongles) στη θύρα OBD] χρησιμοποιείται ως μέσο επίθεσης, π.χ. για τον χειρισμό παραμέτρων του οχήματος (άμεσα ή έμμεσα)
4.3.6. Απειλές κατά των δεδομένων/του κώδικα του οχήματος	19	Εξαγωγή των δεδομένων/του κώδικα του οχήματος	19.1	Εξαγωγή λογισμικού που προστατεύεται από δικαίωμα δημιουργού ή ιδιόκτητου λογισμικού από συστήματα του οχήματος (πειρατεία προϊόντων)
			19.2	Μη εξουσιοδοτημένη πρόσβαση σε προσωπικές πληροφορίες του ιδιοκτήτη, όπως π.χ. σε πληροφορίες για την ατομική του ταυτότητα, τον λογαριασμό πληρωμών, το βιβλίο διευθύνσεων, την τοποθεσία του, την ηλεκτρονική ταυτότητα του οχήματος κ.λπ.
			19.3	Εξαγωγή κλειδιών κρυπτογράφησης

Γενικές και ειδικές κατηγορίες ευπαθειών/απειλών			Παράδειγμα ευπάθειας ή μεθόδου επίθεσης	
	20	Παραποίηση των δεδομένων/του κώδικα του οχήματος	20.1	Παράνομες/μη εξουσιοδοτημένες αλλαγές στην ηλεκτρονική ταυτότητα του οχήματος
			20.2	Απάτη σχετικά με την ταυτότητα. Παραδείγματος χάρη, ο χρήστης επιθυμεί να εμφανίζεται με άλλη ταυτότητα όταν επικοινωνεί με συστήματα διοδίων, το σύστημα διακομιστή του κατασκευαστή
			20.3	Προσπάθειες παράκαμψης συστημάτων παρακολούθησης (π.χ. υποκλοπή/παραποίηση/φραγή μηνυμάτων όπως δεδομένα του ODR Tracker ή ο αριθμός των διαδρομών του οχήματος)
			20.4	Παραποίηση δεδομένων οδήγησης του οχήματος (π.χ. διανυθέντα χιλιόμετρα, ταχύτητα οχήματος, κατεύθυνση οχήματος κ. λπ.)
			20.5	Μη εξουσιοδοτημένες αλλαγές στα διαγνωστικά δεδομένα του συστήματος
	21	Διαγραφή των δεδομένων/του κώδικα	21.1	Μη εξουσιοδοτημένη διαγραφή/παραποίηση αρχείων καταγραφής συμβάντων του συστήματος
	22	Εισαγωγή κακόβουλου λογισμικού	22.2	Εισαγωγή κακόβουλου λογισμικού ή κακόβουλης δραστηριότητας λογισμικού
	23	Εισαγωγή νέου λογισμικού ή αντικατάσταση του υπάρχοντος λογισμικού	23.1	Κατασκευή λογισμικού του συστήματος ελέγχου ή του συστήματος πληροφοριών του οχήματος
	24	Διαταραχή συστημάτων ή δραστηριοτήτων	24.1	Άρνηση υπηρεσίας, η οποία είναι πιθανό να παρουσιαστεί στο εσωτερικό δίκτυο μετά από υπερφόρτωση του διαύλου CAN ή μετά την πρόκληση βλάβης στη μονάδα ελέγχου κινητήρα λόγω εντατικής επεξεργασίας μηνυμάτων
	25	Παραποίηση παραμέτρων οχήματος	25.1	Μη εξουσιοδοτημένη πρόσβαση με σκοπό την παραποίηση των παραμέτρων ρύθμισης των βασικών λειτουργιών του οχήματος, όπως π.χ. τα δεδομένα πέδησης, τα επιτρεπόμενα όρια για την ενεργοποίηση του αερόσακου κ.λπ.
			25.2	Μη εξουσιοδοτημένη πρόσβαση με σκοπό την παραποίηση των παραμέτρων φόρτισης, όπως π. χ. η τάση φόρτισης, η ισχύς φόρτισης, η θερμοκρασία της μπαταρίας κ.λπ.
4.3.7. Πιθανές ευπάθειες που θα μπορούσαν να εκμεταλλευτούν τρίτοι αν το σύστημα δεν είναι επαρκώς προστατευμένο ή ανθεκτικό	26	Εύκολη υπονόμευση ή ανεπαρκής εφαρμογή τεχνολογιών κρυπτογράφησης	26.1	Ο συνδυασμός μικρών κλειδιών κρυπτογράφησης και μεγάλης περιόδου ισχύος επιτρέπει στον επιτιθέμενο να παραβιάσει την κρυπτογράφηση
			26.2	Ανεπαρκής χρήση των αλγορίθμων κρυπτογράφησης που προστατεύουν ευαίσθητα συστήματα
			26.3	Χρήση αλγορίθμων κρυπτογράφησης που έχουν ήδη αποσυρθεί ή που θα αποσυρθούν προσεχώς

Γενικές και ειδικές κατηγορίες ευπαθειών/απειλών			Παράδειγμα ευπάθειας ή μεθόδου επίθεσης	
	27	Παρεμβάσεις σε εξαρτήματα ή υλικά, οι οποίες διευκολύνουν τις επιθέσεις κατά των οχημάτων	27.1	Η κατασκευή του υλισμικού ή του λογισμικού επιτρέπει τη διεξαγωγή επίθεσης ή δεν εκπληρώνει τα κριτήρια σχεδιασμού για την ανάσχεση επίθεσης
	28	Η ανάπτυξη του λογισμικού ή του υλισμικού δημιουργεί ευπάθειες	28.1	Σφάλματα λογισμικού. Η παρουσία σφαλμάτων λογισμικού μπορεί να οδηγήσει σε ευπάθειες που θα μπορούσαν να εκμεταλλευτούν τρίτοι. Αυτό συμβαίνει κυρίως όταν το λογισμικό δεν έχει δοκιμαστεί ώστε να αποδειχθεί ότι δεν περιέχει γνωστό εσφαλμένο κώδικα/σφάλμα και να περιοριστεί ο κίνδυνος παρουσίας άγνωστου εσφαλμένου κωδικού/σφάλματος
			28.2	Η χρήση υπολειμμάτων από την ανάπτυξη του λογισμικού και του υλισμικού (π.χ. θύρες εντοπισμού σφαλμάτων, θύρες JTAG, μικροεπεξεργαστές, πιστοποιητικά επεξεργασίας, κωδικοί πρόσβασης επεξεργαστή...) μπορεί να επιτρέψει την πρόσβαση σε μονάδες ηλεκτρονικού ελέγχου ή να επιτρέψει σε επιτιθέμενους να αποκτήσουν περισσότερα προνόμια
	29	Ο σχεδιασμός του δικτύου δημιουργεί ευπάθειες	29.1	Οι πλεονάζουσες θύρες διαδικτύου έμειναν ανοιχτές, διευκολύνοντας την πρόσβαση σε συστήματα δικτύων
			29.2	Παράκαμψη του διαχωρισμού του δικτύου ώστε να αποκτηθεί ο έλεγχος. Συγκεκριμένο παράδειγμα είναι η χρήση απροστάτευτων πυλών εισόδου ή σημείων πρόσβασης (όπως π.χ. οι πύλες εισόδου φορτηγών-ρυμουλκούμενων) ώστε να παρακαμφθούν τα μέτρα προστασίας και να αποκτηθεί πρόσβαση σε άλλα μέρη του δικτύου με σκοπό την εκτέλεση κακόβουλων πράξεων, όπως π.χ. η αποστολή αυθαίρετων μηνυμάτων διαύλου CAN
	31	Πιθανότητα ακούσιας μεταβίβασης δεδομένων	31.1	Διαρροή πληροφοριών. Πιθανότητα διαρροής δεδομένων προσωπικού χαρακτήρα σε περίπτωση που αλλάξει ο χρήστης αυτοκινήτου (π.χ. αν πωληθεί ή χρησιμοποιηθεί ως μισθωμένο όχημα με νέους μισθωτές)
	32	Η παραποίηση του υλικού των συστημάτων μπορεί να διευκολύνει τη διεξαγωγή επίθεσης	32.1	Παραποίηση ηλεκτρονικού εξοπλισμού, π.χ. προσθήκη μη εξουσιοδοτημένου ηλεκτρονικού εξοπλισμού σε όχημα με σκοπό τη διάπραξη της «επίθεσης του ενδιάμεσου». Αντικατάσταση εξουσιοδοτημένου ηλεκτρονικού εξοπλισμού (π.χ. αισθητήρες) με μη εξουσιοδοτημένο ηλεκτρονικό εξοπλισμό Παραποίηση των πληροφοριών που συλλέγονται από αισθητήρες (π.χ. χρησιμοποιείται μαγνήτης ο οποίος παρεμβαίνει στον αισθητήρα μαγνητικού πεδίου που είναι συνδεδεμένος στο κιβώτιο ταχυτήτων).

Μέρος Β. Μέτρα προστασίας από τις απειλές, τα οποία σχεδιάστηκαν για οχήματα

1. Μέτρα προστασίας για τους «διαύλους επικοινωνίας του οχήματος»

Τα μέτρα προστασίας από τις απειλές που συνδέονται με τους «διαύλους επικοινωνίας του οχήματος» παρατίθενται στον πίνακα Β1.

Πίνακας Β1

Μέτρα προστασίας από τις απειλές που συνδέονται με τους «διαύλους επικοινωνίας του οχήματος»

Παραπομπή στον πίνακα Α1	Απειλές κατά των «διαύλων επικοινωνίας του οχήματος»	Κωδ.	Μέτρο προστασίας
4.1	Πλαστογράφηση μηνυμάτων (π.χ. όταν κομβόι αυτόνομων οχημάτων επικοινωνεί ασύρματα με αισθητήρες που είναι εγκατεστημένοι στο οδικό δίκτυο με βάση το πρότυπο 802.11p, όταν ανταλλάσσονται μηνύματα μέσω του δικτύου GNSS κ.λπ.).	M10	Το όχημα επαληθεύει τη γνησιότητα και την ακεραιότητα των μηνυμάτων που λαμβάνει
4.2	Επίθεση Sybil (ο επιτιθέμενος πλαστογραφεί την ταυτότητά του και δημιουργεί πολλά ψεύτικα οχήματα στον δρόμο)	M11	Διενεργούνται έλεγχοι ασφάλειας για την αποθήκευση κλειδιών κρυπτογράφησης (π.χ. χρήση συστημάτων ασφάλειας υλικού)
5.1	Δίαυλοι επικοινωνίας επιτρέπουν τις επιθέσεις εισαγωγής κώδικα στα δεδομένα/στον κώδικα του οχήματος, π.χ. στη ροή επικοινωνίας εισάγεται παραποιημένο λογισμικό δυαδικής μορφής	M10 M6	Το όχημα επαληθεύει τη γνησιότητα και την ακεραιότητα των μηνυμάτων που λαμβάνει Στα συστήματα ενσωματώνονται δικλείδες ασφάλειας από τον αρχικό τους σχεδιασμό ώστε να περιορίζονται οι κίνδυνοι που τα απειλούν
5.2	Δίαυλοι επικοινωνίας επιτρέπουν τον χειρισμό των δεδομένων/του κώδικα του οχήματος	M7	Εφαρμόζονται τεχνικές και σχεδιασμοί για τον έλεγχο της πρόσβασης ώστε να προστατεύονται τα δεδομένα/ο κώδικας του συστήματος
5.3	Δίαυλοι επικοινωνίας επιτρέπουν την αντικατάσταση των δεδομένων/του κώδικα του οχήματος		
5.4 21.1	Δίαυλοι επικοινωνίας επιτρέπουν τη διαγραφή των δεδομένων/του κώδικα του οχήματος		
5.5	Δίαυλοι επικοινωνίας επιτρέπουν την εισαγωγή δεδομένων/κώδικα στα συστήματα του οχήματος (εγγραφή κώδικα δεδομένων)		
6.1	Αποδοχή πληροφοριών από μη αξιόπιστη πηγή	M10	Το όχημα επαληθεύει τη γνησιότητα και την ακεραιότητα των μηνυμάτων που λαμβάνει
6.2	Επίθεση ενδιάμεσου (MITM)/υφαρπαγής συνόδου	M10	Το όχημα επαληθεύει τη γνησιότητα και την ακεραιότητα των μηνυμάτων που λαμβάνει
6.3	Επίθεση επαναληπτικής εκτέλεσης, π.χ. η επίθεση εναντίον πύλης επικοινωνίας επιτρέπει στον επιτιθέμενο να υποβαθμίσει το λογισμικό της μονάδας ηλεκτρονικού ελέγχου ή το υλικολογισμικό της πύλης εισόδου		
7.1	Υποκλοπή πληροφοριών/ηλεκτρομαγνητικές παρεμβολές/παρακολούθηση επικοινωνιών	M12	Οι εμπιστευτικές πληροφορίες που διαβιβάζονται προς ή από το όχημα προστατεύονται
7.2	Απόκτηση μη εξουσιοδοτημένης πρόσβασης σε αρχεία ή δεδομένα	M8	Χάρη στον σχεδιασμό του συστήματος και στον έλεγχο της πρόσβασης σε αυτό, μη εξουσιοδοτημένο προσωπικό δεν θα έχει τη δυνατότητα πρόσβασης σε προσωπικά ή κρίσιμα για το σύστημα δεδομένα. Παραδείγματα ελέγχων ασφάλειας διατίθενται από την κοινότητα OWASP.

Παραπομπή στον πίνακα Α1	Απειλές κατά των «διαύλων επικοινωνίας του οχήματος»	Κωδ.	Μέτρο προστασίας
8.1	Αποστολή μεγάλου αριθμού απορριφθέντων δεδομένων στο σύστημα πληροφοριών του οχήματος με αποτέλεσμα να είναι αδύνατη η κανονική παροχή υπηρεσιών	M13	Εφαρμόζονται μέτρα για να εντοπίζονται επιθέσεις άρνησης υπηρεσίας και να αποκαθίσταται η λειτουργία του συστήματος μετά τις επιθέσεις
8.2	Επίθεση μαύρης τρύπας, διαταράσσεται η επικοινωνία μεταξύ των οχημάτων και ο επιτιθέμενος έχει τη δυνατότητα να εμποδίζει την ανταλλαγή μηνυμάτων μεταξύ των οχημάτων	M13	Εφαρμόζονται μέτρα για να εντοπίζονται επιθέσεις άρνησης υπηρεσίας και να αποκαθίσταται η λειτουργία του συστήματος μετά τις επιθέσεις
9.1	Μη εξουσιοδοτημένος χρήστης μπορεί να αποκτήσει προνομιακή πρόσβαση, μεταξύ άλλων και πρόσβαση διαχειριστή (root access)	M9	Εφαρμόζονται μέτρα ώστε να αποτρέπονται και να εντοπίζονται περιστατικά μη εξουσιοδοτημένης πρόσβασης
10.1	Ιός που ενσωματώνεται σε μέσα επικοινωνίας προσβάλλει τα συστήματα του οχήματος	M14	Πρέπει να μελετηθούν μέτρα για την προστασία των συστημάτων από ενσωματωμένους ιούς/κακόβουλα λογισμικά
11.1	Κακόβουλα εσωτερικά μηνύματα (π.χ. μηνύματα CAN)	M15	Πρέπει να μελετηθούν μέτρα για τον εντοπισμό κακόβουλων εσωτερικών μηνυμάτων ή δραστηριοτήτων
11.2	Κακόβουλα μηνύματα που ανταλλάσσονται μεταξύ οχημάτων και αισθητήρων του οδικού δικτύου, όπως π.χ. τα μηνύματα που αποστέλλονται από οδικές υποδομές στο όχημα ή τα μηνύματα που ανταλλάσσονται μεταξύ οχημάτων (π.χ. μηνύματα CAM, DENM)	M10	Το όχημα επαληθεύει τη γνησιότητα και την ακεραιότητα των μηνυμάτων που λαμβάνει
11.3	Κακόβουλα διαγνωστικά μηνύματα		
11.4	Κακόβουλα ιδιόκτητα μηνύματα (π.χ. τα μηνύματα που αποστέλλονται συνήθως από συστήματα OEM ή από προμηθευτές κατασκευαστικών στοιχείων/συστημάτων/λειτουργιών)		

2. Μέτρα προστασίας για τη «διαδικασία επικαιροποίησης»

Τα μέτρα προστασίας από τις απειλές που συνδέονται με τη «διαδικασία επικαιροποίησης» παρατίθενται στον πίνακα Β2.

Πίνακας Β2

Μέτρα προστασίας από τις απειλές που συνδέονται με τη «διαδικασία επικαιροποίησης»

Παραπομπή στον πίνακα Α1	Απειλές σχετικά με τη «διαδικασία επικαιροποίησης»	Κωδ.	Μέτρο προστασίας
12.1	Υπονόμευση των ασύρματων διαδικασιών επικαιροποίησης λογισμικού. Συμπεριλαμβάνεται η κατασκευή του προγράμματος ή του υλικολογισμικού επικαιροποίησης του συστήματος	M16	Εφαρμόζονται ασφαλείς διαδικασίες για την επικαιροποίηση του λογισμικού
12.2	Υπονόμευση τοπικών/φυσικών διαδικασιών επικαιροποίησης λογισμικού Συμπεριλαμβάνεται η κατασκευή του προγράμματος ή του υλικολογισμικού επικαιροποίησης του συστήματος		
12.3	Το λογισμικό παραποιείται πριν από τη διαδικασία επικαιροποίησης (και επομένως καταστρέφεται) χωρίς ωστόσο να επηρεαστεί η διαδικασία επικαιροποίησης		

Παραπομπή στον πίνακα A1	Απειλές σχετικά με τη «διαδικασία επικαιροποίησης»	Κωδ.	Μέτρο προστασίας
12.4	Υπονόμευση κλειδιών κρυπτογράφησης του παρόχου του λογισμικού με αποτέλεσμα οι επικαιροποιήσεις να μην είναι έγκυρες	M11	Διενεργούνται έλεγχοι ασφάλειας για την αποθήκευση κλειδιών κρυπτογράφησης
13.1	Επίθεση άρνησης υπηρεσίας κατά διακομιστή επικαιροποίησης ή δικτύου με αποτέλεσμα να μη διατίθενται κρίσιμης σημασίας επικαιροποιήσεις λογισμικού και/ή να μην ξεκλειδώνονται συγκεκριμένες δυνατότητες για κάθε πελάτη	M3	Διενεργούνται έλεγχοι ασφάλειας στα συστήματα παρασκηνίου. Αν οι διακομιστές παρασκηνίου έχουν καίρια σημασία για την παροχή υπηρεσιών, εφαρμόζονται μέτρα αποκατάστασης σε περίπτωση που διακοπεί η λειτουργία του συστήματος. Παραδείγματα ελέγχων ασφάλειας διατίθενται από την κοινότητα OWASP

3. Μέτρα προστασίας για «ακούσιες ανθρώπινες ενέργειες που διευκολύνουν τη διάπραξη κυβερνοεπίθεσης»

Τα μέτρα προστασίας από τις απειλές που συνδέονται με «ακούσιες ανθρώπινες ενέργειες που διευκολύνουν τη διάπραξη κυβερνοεπίθεσης» παρατίθενται στον πίνακα B3.

Πίνακας B3

Μέτρα προστασίας από τις απειλές που συνδέονται με «ακούσιες ανθρώπινες ενέργειες που διευκολύνουν τη διάπραξη κυβερνοεπίθεσης»

Παραπομπή στον πίνακα A1	Απειλές σχετικά με τις «ακούσιες ανθρώπινες ενέργειες»	Κωδ.	Μέτρο προστασίας
15.1	Αθώο θύμα (π.χ. ιδιοκτήτης, χειριστής ή μηχανικός συντήρησης) εξαπατάται και προβαίνει σε ενέργεια με την οποία εν αγνοία του εισάγει κακόβουλο λογισμικό ή διευκολύνει τη διάπραξη επίθεσης	M18	Εφαρμόζονται μέτρα για τον καθορισμό και τον έλεγχο των ρόλων των χρηστών και των δικαιωμάτων πρόσβασης με βάση την αρχή των ελάχιστων δικαιωμάτων πρόσβασης
15.2	Δεν ακολουθούνται οι καθορισμένες διαδικασίες ασφάλειας	M19	Οι οργανισμοί μεριμνούν για τον καθορισμό και την τήρηση των διαδικασιών ασφάλειας, μεταξύ άλλων για την καταγραφή των ενεργειών και των περιπτώσεων πρόσβασης που συνδέονται με τη διαχείριση των λειτουργιών ασφάλειας

4. Μέτρα προστασίας για την «εξωτερική συνδεσιμότητα και τις συνδέσεις»

Τα μέτρα προστασίας από τις απειλές που συνδέονται με την «εξωτερική συνδεσιμότητα και τις συνδέσεις» παρατίθενται στον πίνακα B4.

Πίνακας B4

Μέτρα προστασίας από τις απειλές που συνδέονται με την «εξωτερική συνδεσιμότητα και τις συνδέσεις»

Παραπομπή στον πίνακα A1	Απειλές σχετικά με την «εξωτερική συνδεσιμότητα και τις συνδέσεις»	Κωδ.	Μέτρο προστασίας
16.1	Παραποίηση λειτουργιών που υποστηρίζουν την απομακρυσμένη λειτουργία των συστημάτων του οχήματος, όπως π.χ. τα απομακρυσμένα κλειδιά, τα συστήματα ακινητοποίησης και οι σταθμοί φόρτισης	M20	Διενεργούνται έλεγχοι ασφάλειας στα συστήματα με απομακρυσμένη πρόσβαση
16.2	Παραποίηση των εφαρμογών τηλεματικής του οχήματος (π.χ. παραποίηση των μετρήσεων της θερμοκρασίας ευαίσθητων προϊόντων, απομακρυσμένο ξεκλείδωμα θυρών του διαμερίσματος του φορτίου)		

Παραπομπή στον πίνακα Α1	Απειλές σχετικά με την «εξωτερική συνδεσιμότητα και τις συνδέσεις»	Κωδ.	Μέτρο προστασίας
16.3	Παρεμβολές σε ασύρματα συστήματα ή αισθητήρες μικρής εμβέλειας		
17.1	Κατεστραμμένες εφαρμογές ή εφαρμογές με ελλιπή ασφάλεια λογισμικού χρησιμοποιούνται ως μέσο επίθεσης εναντίον συστημάτων του οχήματος	M21	Αξιολογείται η ασφάλεια, εξακριβώνεται η γνησιότητα και προστατεύεται η ακεραιότητα του λογισμικού. Διενεργούνται έλεγχοι ασφάλειας για να ελαχιστοποιηθεί ο κίνδυνος ο οποίος προέρχεται από λογισμικό τρίτων μερών που πρόκειται ή προβλέπεται να φιλοξενηθεί στο όχημα
18.1	Εξωτερικές διεπαφές, όπως π.χ. θύρες USB ή άλλες θύρες, χρησιμοποιούνται ως σημείο επίθεσης, π.χ. για την εισαγωγή κώδικα	M22	Διενεργούνται έλεγχοι ασφάλειας στις εξωτερικές διεπαφές
18.2	Μέσα που έχουν προσβληθεί από ιούς συνδέονται με το όχημα		
18.3	Η διαγνωστική πρόσβαση [π.χ. κλειδιά υλικού (dongles) στη θύρα OBD] χρησιμοποιείται ως μέσο επίθεσης, π.χ. για τον χειρισμό παραμέτρων του οχήματος (άμεσα ή έμμεσα)	M22	Διενεργούνται έλεγχοι ασφάλειας στις εξωτερικές διεπαφές

5. Μέτρα προστασίας για «πιθανούς στόχους ή κίνητρα επιθέσεων»

Τα μέτρα προστασίας από τις απειλές που συνδέονται με «πιθανούς στόχους ή κίνητρα επιθέσεων» παρατίθενται στον πίνακα Β5.

Πίνακας Β5

Μέτρα προστασίας από τις απειλές που συνδέονται με «πιθανούς στόχους ή κίνητρα επιθέσεων»

Παραπομπή στον πίνακα Α1	Απειλές σχετικά με «πιθανούς στόχους ή κίνητρα επιθέσεων»	Κωδ.	Μέτρο προστασίας
19.1	Απόσπαση λογισμικού που προστατεύεται από δικαίωμα δημιουργού ή ιδιόκτητου λογισμικού από τα συστήματα του οχήματος (πειρατεία προϊόντων/κλεμμένο λογισμικό)	M7	Εφαρμόζονται τεχνικές και σχεδιασμοί για τον έλεγχο της πρόσβασης ώστε να προστατεύονται τα δεδομένα/ο κώδικας του συστήματος. Παραδείγματα ελέγχων ασφάλειας διατίθενται από την κοινότητα OWASP
19.2	Μη εξουσιοδοτημένη πρόσβαση σε προσωπικές πληροφορίες του ιδιοκτήτη, όπως π.χ. σε πληροφορίες για την ατομική του ταυτότητα, τον λογαριασμό πληρωμών, το βιβλίο διευθύνσεων, την τοποθεσία του, την ηλεκτρονική ταυτότητα του οχήματος κ. λπ.	M8	Χάρη στον σχεδιασμό του συστήματος και στον έλεγχο της πρόσβασης σε αυτό, μη εξουσιοδοτημένο προσωπικό δεν θα έχει τη δυνατότητα πρόσβασης σε προσωπικά ή κρίσιμα για το σύστημα δεδομένα. Παραδείγματα ελέγχων ασφάλειας διατίθενται από την κοινότητα OWASP
19.3	Εξαγωγή κλειδιών κρυπτογράφησης	M11	Διενεργούνται έλεγχοι ασφάλειας για την αποθήκευση κλειδιών κρυπτογράφησης, π.χ. συστήματα ασφάλειας υλικού
20.1	Παράνομες/μη εξουσιοδοτημένες αλλαγές στην ηλεκτρονική ταυτότητα του οχήματος	M7	Εφαρμόζονται τεχνικές και σχεδιασμοί για τον έλεγχο της πρόσβασης ώστε να προστατεύονται τα δεδομένα/ο κώδικας του συστήματος. Παραδείγματα ελέγχων ασφάλειας διατίθενται από την κοινότητα OWASP
20.2	Απάτη σχετικά με την ταυτότητα. Παραδείγματος χάρη, ο χρήστης επιθυμεί να εμφανίζεται με άλλη ταυτότητα όταν επικοινωνεί με συστήματα διοδίων, το σύστημα διακομιστή του κατασκευαστή		
20.3	Προσπάθειες παράκαμψης συστημάτων παρακολούθησης (π.χ. υποκλοπή/παραποίηση/φραγή μηνυμάτων όπως δεδομένα του ODR Tracker ή ο αριθμός των διαδρομών του οχήματος)	M7	Εφαρμόζονται τεχνικές και σχεδιασμοί για τον έλεγχο της πρόσβασης ώστε να προστατεύονται τα δεδομένα/ο κώδικας του συστήματος. Παραδείγματα ελέγχων ασφάλειας διατίθενται από την κοινότητα OWASP.

Παραπομπή στον πίνακα A1	Απειλές σχετικά με «πιθανούς στόχους ή κίνητρα επιθέσεων»	Κωδ.	Μέτρο προστασίας
20.4	Παραποίηση δεδομένων οδήγησης του οχήματος (π.χ. διανυθέντα χιλιόμετρα, ταχύτητα οχήματος, κατεύθυνση οχήματος κ.λπ.)		Οι επιθέσεις που στρέφονται κατά των αισθητήρων ή των διαβιβαζόμενων δεδομένων με σκοπό τον χειρισμό των δεδομένων θα μπορούσαν να περιοριστούν μέσω της συσχέτισης των δεδομένων που προέρχονται από διαφορετικές πηγές πληροφοριών
20.5	Μη εξουσιοδοτημένες αλλαγές στα διαγνωστικά δεδομένα του συστήματος		
21.1	Μη εξουσιοδοτημένη διαγραφή/παραποίηση αρχείων καταγραφής συμβάντων του συστήματος	M7	Εφαρμόζονται τεχνικές και σχεδιασμοί για τον έλεγχο της πρόσβασης ώστε να προστατεύονται τα δεδομένα/ο κώδικας του συστήματος. Παραδείγματα ελέγχων ασφάλειας διατίθενται από την κοινότητα OWASP.
22.2	Εισαγωγή κακόβουλου λογισμικού ή κακόβουλης δραστηριότητας λογισμικού	M7	Εφαρμόζονται τεχνικές και σχεδιασμοί για τον έλεγχο της πρόσβασης ώστε να προστατεύονται τα δεδομένα/ο κώδικας του συστήματος. Παραδείγματα ελέγχων ασφάλειας διατίθενται από την κοινότητα OWASP.
23.1	Κατασκευή λογισμικού του συστήματος ελέγχου ή του συστήματος πληροφοριών του οχήματος		
24.1	Άρνηση υπηρεσίας, η οποία είναι πιθανό να παρουσιαστεί στο εσωτερικό δίκτυο μετά από υπερφόρτωση του διαύλου CAN ή μετά την πρόκληση βλάβης στη μονάδα ελέγχου κινητήρα λόγω εντατικής επεξεργασίας μηνυμάτων	M13	Εφαρμόζονται μέτρα για να εντοπίζονται επιθέσεις άρνησης υπηρεσίας και να αποκαθίσταται η λειτουργία του συστήματος μετά τις επιθέσεις
25.1	Μη εξουσιοδοτημένη πρόσβαση με σκοπό την παραποίηση των παραμέτρων ρύθμισης των βασικών λειτουργιών του οχήματος, όπως π. χ. τα δεδομένα πέδησης, τα επιτρεπόμενα όρια για την ενεργοποίηση του αερόσακου κ.λπ.	M7	Εφαρμόζονται τεχνικές και σχεδιασμοί για τον έλεγχο της πρόσβασης ώστε να προστατεύονται τα δεδομένα/ο κώδικας του συστήματος. Παραδείγματα ελέγχων ασφάλειας διατίθενται από την κοινότητα OWASP
25.2	Μη εξουσιοδοτημένη πρόσβαση με σκοπό την παραποίηση των παραμέτρων φόρτισης, όπως π.χ. η τάση φόρτισης, η ισχύς φόρτισης, η θερμοκρασία της μπαταρίας κ.λπ.		

6. Μέτρα προστασίας για «πιθανές ευπάθειες που θα μπορούσαν να εκμεταλλευτούν τρίτοι αν το σύστημα δεν είναι επαρκώς προστατευμένο ή ανθεκτικό»

Τα μέτρα προστασίας από τις απειλές που συνδέονται με «πιθανές ευπάθειες που θα μπορούσαν να εκμεταλλευτούν τρίτοι αν το σύστημα δεν είναι επαρκώς προστατευμένο ή ανθεκτικό» παρατίθενται στον πίνακα B6.

Πίνακας B6

Μέτρα προστασίας από τις απειλές που συνδέονται με «πιθανές ευπάθειες που θα μπορούσαν να εκμεταλλευτούν τρίτοι αν το σύστημα δεν είναι επαρκώς προστατευμένο ή ανθεκτικό»

Παραπομπή στον πίνακα A1	Απειλές σχετικά με «πιθανές ευπάθειες που θα μπορούσαν να εκμεταλλευτούν τρίτοι αν το σύστημα δεν είναι επαρκώς προστατευμένο ή ανθεκτικό»	Κωδ.	Μέτρο προστασίας
26.1	Ο συνδυασμός μικρών κλειδιών κρυπτογράφησης και μεγάλης περιόδου ισχύος επιτρέπει στον επιτιθέμενο να παραβιάσει την κρυπτογράφηση	M23	Ακολουθούνται βέλτιστες πρακτικές κυβερνοασφάλειας κατά την ανάπτυξη του λογισμικού και του υλισμικού

Παρα-πομπή στον πίνακα Α1	Απειλές σχετικά με «πιθανές ευπάθειες που θα μπορούσαν να εκμεταλλευτούν τρίτοι αν το σύστημα δεν είναι επαρκώς προστατευμένο ή ανθεκτικό»	Κωδ.	Μέτρο προστασίας
26.2	Ανεπαρκής χρήση των αλγορίθμων κρυπτογράφησης που προστατεύουν ευαίσθητα συστήματα		
26.3	Χρήση αλγορίθμων κρυπτογράφησης που έχουν αποσυρθεί		
27.1	Η κατασκευή του υλισμικού ή του λογισμικού επιτρέπει τη διεξαγωγή επίθεσης ή δεν εκπληρώνει τα κριτήρια σχεδιασμού για την ανάσχεση επίθεσης	M23	Ακολουθούνται βέλτιστες πρακτικές κυβερνοασφάλειας κατά την ανάπτυξη του λογισμικού και του υλισμικού
28.1	Η παρουσία σφαλμάτων λογισμικού μπορεί να οδηγήσει σε ευπάθειες που θα μπορούσαν να εκμεταλλευτούν τρίτοι. Αυτό συμβαίνει κυρίως όταν το λογισμικό δεν έχει δοκιμαστεί ώστε να αποδειχθεί ότι δεν περιέχει γνωστό εσφαλμένο κώδικα/σφάλμα και να περιοριστεί ο κίνδυνος παρουσίας άγνωστου εσφαλμένου κωδικού/σφάλματος	M23	Ακολουθούνται βέλτιστες πρακτικές κυβερνοασφάλειας κατά την ανάπτυξη του λογισμικού και του υλισμικού. Διενεργούνται αρκετά εκτεταμένες δοκιμές για την κυβερνοασφάλεια
28.2	Η χρήση υπολειμμάτων από την ανάπτυξη του λογισμικού και του υλισμικού (π.χ. θύρες εντοπισμού σφαλμάτων, θύρες JTAG, μικροεπεξεργαστές, πιστοποιητικά επεξεργασίας, κωδικοί πρόσβασης επεξεργαστή...) μπορεί να επιτρέψει στους επιτιθέμενους να αποκτήσουν πρόσβαση σε μονάδες ηλεκτρονικού ελέγχου ή να αποκτήσουν περισσότερα δικαιώματα		
29.1	Οι πλεονάζουσες θύρες διαδικτύου έμειναν ανοιχτές, διευκολύνοντας την πρόσβαση σε συστήματα δικτύων		
29.2	Παράκαμψη του διαχωρισμού του δικτύου για να αποκτηθεί ο έλεγχος. Συγκεκριμένο παράδειγμα είναι η χρήση απροστάτευτων πυλών εισόδου ή σημείων πρόσβασης (όπως π.χ. οι πύλες εισόδου φορτηγών-ρυμουλκούμενων) ώστε να παρακαμφθούν τα μέτρα προστασίας και να αποκτηθεί πρόσβαση σε άλλα μέρη του δικτύου με σκοπό την εκτέλεση κακόβουλων πράξεων, όπως π.χ. η αποστολή αυθαίρετων μηνυμάτων διαύλου CAN	M23	Ακολουθούνται βέλτιστες πρακτικές κυβερνοασφάλειας κατά την ανάπτυξη του λογισμικού και του υλισμικού. Ακολουθούνται βέλτιστες πρακτικές κυβερνοασφάλειας κατά τον σχεδιασμό του συστήματος και την ενοποίηση του συστήματος

7. Μέτρα προστασίας για την «απώλεια δεδομένων/διαρροή δεδομένων από το όχημα»

Τα μέτρα προστασίας από τις απειλές που συνδέονται με την «απώλεια δεδομένων/διαρροή δεδομένων από το όχημα» παρατίθενται στον πίνακα Β7.

Πίνακας Β7

Μέτρα προστασίας από τις απειλές που συνδέονται με την «απώλεια δεδομένων/διαρροή δεδομένων από το όχημα»

Παρα-πομπή στον πίνακα Α1	Απειλές «απώλειας δεδομένων/διαρροής δεδομένων από το όχημα»	Κωδ.	Μέτρο προστασίας
31.1	Διαρροή πληροφοριών. Πιθανότητα διαρροής δεδομένων προσωπικού χαρακτήρα όταν αλλάξει ο χρήστης αυτοκινήτου (π.χ. αν πωληθεί ή χρησιμοποιηθεί ως μισθωμένο όχημα με νέους μισθωτές)	M24	Κατά την αποθήκευση των δεδομένων προσωπικού χαρακτήρα ακολουθούνται βέλτιστες πρακτικές για την προστασία της ακεραιότητας και της εμπιστευτικότητας των δεδομένων.

8. Μέτρα προστασίας για τον «φυσικό χειρισμό των συστημάτων με σκοπό τη διάπραξη επίθεσης»

Τα μέτρα προστασίας από τις απειλές που συνδέονται με τον «φυσικό χειρισμό των συστημάτων με σκοπό τη διάπραξη επίθεσης» παρατίθενται στον πίνακα Β8.

Πίνακας Β8

Μέτρα προστασίας από τις απειλές που συνδέονται με τον «φυσικό χειρισμό των συστημάτων με σκοπό τη διάπραξη επίθεσης»

Παραπομπή στον πίνακα Α1	Απειλές σχετικά με τον «φυσικό χειρισμό των συστημάτων με σκοπό τη διάπραξη επίθεσης»	Κωδ.	Μέτρο προστασίας
32.1	Παραποίηση εξοπλισμού ΟΕΜ, π.χ. προσθήκη μη εξουσιοδοτημένου ηλεκτρονικού εξοπλισμού σε όχημα με σκοπό τη διάπραξη της «επίθεσης του ενδιάμεσου».	M9	Εφαρμόζονται μέτρα ώστε να αποτρέπονται και να εντοπίζονται περιστατικά μη εξουσιοδοτημένης πρόσβασης

Μέρος Γ. Μέτρα προστασίας από τις απειλές εκτός οχημάτων

1. Μέτρα προστασίας για τους «διακομιστές παρασκηνίου»

Τα μέτρα προστασίας από τις απειλές που συνδέονται με τους «διακομιστές παρασκηνίου» παρατίθενται στον πίνακα Γ1.

Πίνακας Γ1

Μέτρα προστασίας από τις απειλές που συνδέονται με τους «διακομιστές παρασκηνίου»

Παραπομπή στον πίνακα Α1	Απειλές σχετικά με τους «διακομιστές παρασκηνίου»	Κωδ.	Μέτρο προστασίας
1.1 & 3.1	Κατάχρηση προνομίων από το προσωπικό (επίθεση εκ των έσω)	M1	Στα συστήματα παρασκηνίου διενεργούνται έλεγχοι ασφάλειας για να ελαχιστοποιηθεί ο κίνδυνος της διάπραξης επίθεσης εκ των έσω
1.2 & 3.3	Μη εξουσιοδοτημένη διαδικτυακή πρόσβαση στον διακομιστή (π.χ. μέσω κακόβουλων λογισμικών που επιτρέπουν σε εισβολείς να έχουν τον απομακρυσμένο έλεγχο υπολογιστών, μέσω μη κατοχυρωμένων λογισμικών, επιθέσεων SQL ή άλλων μεθόδων)	M2	Στα συστήματα παρασκηνίου διενεργούνται έλεγχοι ασφάλειας για να ελαχιστοποιηθούν οι περιπτώσεις μη εξουσιοδοτημένης πρόσβασης Παραδείγματα ελέγχων ασφάλειας διατίθενται από την κοινότητα OWASP
1.3 & 3.4	Μη εξουσιοδοτημένη φυσική πρόσβαση στον διακομιστή (π.χ. μέσω κλειδιών USB ή άλλων μέσων που συνδέονται με τον διακομιστή)	M8	Χάρη στον σχεδιασμό του συστήματος και στον έλεγχο της πρόσβασης σε αυτό, μη εξουσιοδοτημένο προσωπικό δεν θα έχει τη δυνατότητα πρόσβασης σε προσωπικά ή κρίσιμα για το σύστημα δεδομένα
2.1	Επίθεση στον διακομιστή παρασκηνίου έχει ως αποτέλεσμα τη διακοπή της λειτουργίας του διακομιστή, π.χ. ο διακομιστής δεν αλληλεπιδρά με τα οχήματα και δεν παρέχει τις υπηρεσίες που χρησιμοποιούν τα οχήματα	M3	Διενεργούνται έλεγχοι ασφάλειας στα συστήματα παρασκηνίου. Αν οι διακομιστές παρασκηνίου έχουν καίρια σημασία για την παροχή υπηρεσιών, εφαρμόζονται μέτρα αποκατάστασης σε περίπτωση που διακοπεί η λειτουργία του συστήματος. Παραδείγματα ελέγχων ασφάλειας διατίθενται από την κοινότητα OWASP
3.2	Απώλειες πληροφοριών στο υπολογιστικό νέφος. Πιθανότητα απώλειας ευαίσθητων δεδομένων λόγω επιθέσεων ή ατυχημάτων όταν τα δεδομένα αποθηκεύονται από τρίτους παρόχους υπηρεσιών υπολογιστικού νέφους	M4	Διενεργούνται έλεγχοι ασφάλειας για να ελαχιστοποιηθούν οι κίνδυνοι που εγκυμονεί η νεφοϋπολογιστική. Παραδείγματα ελέγχων ασφάλειας διατίθενται από την κοινότητα OWASP και στις οδηγίες για τη νεφοϋπολογιστική που έχει εκδώσει η κεντρική υπηρεσία του Ηνωμένου Βασιλείου για τη νεφοϋπολογιστική (NCSC)
3.5	Διαρροή πληροφοριών λόγω ακούσιας κοινοποίησης δεδομένων (π.χ. σφάλματα διαχειριστή, αποθήκευση δεδομένων σε διακομιστές που βρίσκονται σε κλειστούς χώρους στάθμευσης)	M5	Στα συστήματα παρασκηνίου διενεργούνται έλεγχοι ασφάλειας για να προλαμβάνονται διαρροές δεδομένων. Παραδείγματα ελέγχων ασφάλειας διατίθενται από την κοινότητα OWASP

2. Μέτρα προστασίας για «ακούσιες ανθρώπινες ενέργειες»

Τα μέτρα προστασίας από τις απειλές που συνδέονται με «ακούσιες ανθρώπινες ενέργειες» παρατίθενται στον πίνακα Γ2.

Πίνακας Γ2

Μέτρα προστασίας από τις απειλές που συνδέονται με «ακούσιες ανθρώπινες ενέργειες»

Παραπομπή στον πίνακα Α1	Απειλές σχετικά με τις «ακούσιες ανθρώπινες ενέργειες»	Κωδ.	Μέτρο προστασίας
15.1	Αθώο θύμα (π.χ. ιδιοκτήτης, χειριστής ή μηχανικός συντήρησης) εξαπατάται και προβαίνει σε ενέργεια με την οποία εν αγνοία του εισάγει κακόβουλο λογισμικό ή διευκολύνει τη διάπραξη επίθεσης	M18	Εφαρμόζονται μέτρα για τον καθορισμό και τον έλεγχο των ρόλων των χρηστών και των δικαιωμάτων πρόσβασης με βάση την αρχή των ελάχιστων δικαιωμάτων πρόσβασης
15.2	Δεν ακολουθούνται οι καθορισμένες διαδικασίες ασφάλειας	M19	Οι οργανισμοί μεριμνούν για τον καθορισμό και την τήρηση των διαδικασιών ασφάλειας, μεταξύ άλλων για την καταγραφή των ενεργειών και των περιπτώσεων πρόσβασης που συνδέονται με τη διαχείριση των λειτουργιών ασφάλειας

3. Μέτρα προστασίας για τη «φυσική απώλεια δεδομένων»

Τα μέτρα προστασίας από τις απειλές που συνδέονται με τη «φυσική απώλεια δεδομένων» παρατίθενται στον πίνακα Γ3.

Πίνακας Γ3

Μέτρα προστασίας από τις απειλές που συνδέονται με τη «φυσική απώλεια δεδομένων»

Παραπομπή στον πίνακα Α1	Απειλές σχετικά με τη «φυσική απώλεια δεδομένων»	Κωδ.	Μέτρο προστασίας
30.1	Ζημία που προκαλείται από τρίτους. Ευαίσθητα δεδομένα μπορεί να χαθούν ή να υπονομευθούν λόγω των υλικών ζημιών που προκαλούνται όταν σημειώνονται τροχαία ατυχήματα ή κλοπές	M24	Κατά την αποθήκευση των δεδομένων προσωπικού χαρακτήρα ακολουθούνται βέλτιστες πρακτικές για την προστασία της ακεραιότητας και της εμπιστευτικότητας των δεδομένων. Παραδείγματα ελέγχων ασφάλειας διατίθενται στο πρότυπο ISO/SC27/WG5
30.2	Απώλειες από συγκρούσεις κατά τη ΔΨΔ (διαχείριση ψηφιακών δικαιωμάτων) Τα δεδομένα χρήστη ενδέχεται να διαγραφούν λόγω προβλημάτων που συνδέονται με τη ΔΨΔ		
30.3	Πιθανή απώλεια (ακέραιων) ευαίσθητων δεδομένων λόγω της φυσικής φθοράς των στοιχείων ΤΠ, η οποία μπορεί να προκαλέσει αλυσιδωτές επιπτώσεις (αν π.χ. πρόκειται για πολύ σημαντική αλλοίωση).		