

ΤΕΥΧΟΣ ΠΡΟΔΙΑΓΡΑΦΩΝ 6

(ΤΕΠ-6)

Συστήματα Ηλεκτρονικών Επιτραπέζιων Παιγνίων που Ελέγχονται από Κρουπιέρη
(ΣΗΕΠ-ΕΚ)

Έκδοση: 1.0

ΚΕΦΑΛΑΙΟ 1: ΟΡΙΣΜΟΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΤΡΑΠΕΖΙΩΝ ΠΑΙΓΝΙΩΝ ΠΟΥ ΕΛΕΓΧΟΝΤΑΙ ΑΠΟ ΚΡΟΥΠΙΕΡΗ

1.1.1 Γενική απαίτηση

Τα Ηλεκτρονικά Επιτραπέζια Παιγνία που ελέγχονται από κρουπιέρη αποτελούν τη λειτουργία των επιτραπέζιων παιγνίων τα οποία απαιτούν κρουπιέρη ο οποίος κάνει χρήση ηλεκτρονικών μέσων για τη λειτουργία του παιγνίου (ήτοι έναρξη γύρου παιγνίου, ηλεκτρονική συλλογή, αποθήκευση, επικοινωνία λογιστικών στοιχείων και δεδομένα σημαντικών συμβάντων κλπ.). Το παρόν εφαρμόζεται μόνο σε περιπτώσεις που για τη διεξαγωγή του ηλεκτρονικού επιτραπέζιου παιγνίου απαιτείται κρουπιέρης.

ΣΗΜΕΙΩΣΗ: Στην περίπτωση Συστημάτων Επιτραπέζιων Παιγνίων τα οποία δεν απαιτούν ζωντανό κρουπιέρη, εφαρμόζονται τα προβλεπόμενα στο προηγούμενο τεύχος «Συστήματα Ηλεκτρονικών Επιτραπέζιων Παιγνίων (ΣΗΕΠ)».

ΚΕΦΑΛΑΙΟ 2: ΑΠΑΙΤΗΣΕΙΣ ΣΥΣΤΗΜΑΤΟΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΤΡΑΠΕΖΙΩΝ ΠΑΙΓΝΙΩΝ

2.1 Εισαγωγή

Αυτό το κεφάλαιο ασχολείται με τα ηλεκτρονικά επιτραπέζια παίγνια, ανεξάρτητα από το αν αυτά αποτελούν ή όχι συστατικό ενός συστήματος επιτραπέζιων παιγνίων. Οι απαιτήσεις κάθε υποκεφαλαίου εφαρμόζονται μόνο στις περιπτώσεις που τα ηλεκτρονικά επιτραπέζια παίγνια λειτουργούν ως μέρος ενός «Συστήματος Επιτραπέζιων Παιγνίων» το οποίο είναι ανεξάρτητο από οποιοδήποτε εξωτερικό σύστημα παιγνίων.

2.2 Απαιτήσεις Συστήματος Επιτραπέζιων Παιγνίων

2.2.1 Ρολόι συστήματος

Το Σύστημα πρέπει να διατηρεί ένα εσωτερικό ρολόι που αναπαριστά την τρέχουσα ώρα (μορφή 24 ωρών - η οποία γίνεται κατανοητή με τη μορφή τοπικής

ημερομηνίας/ώρας) και ημερομηνία που πρέπει να χρησιμοποιείται για την παροχή των παρακάτω:

- α) Χρονική σήμανση των Σημαντικών Συμβάντων,
- β) Ρολόι αναφοράς για χρονοσήμανση των αναφορών, και
- γ) Χρονική σήμανση των αλλαγών παραμετροποίησης.

2.2.2 Χαρακτηριστικό συγχρονισμού

Σε περίπτωση υποστήριξης πολλαπλών ρολογιών, το Σύστημα πρέπει να διαθέτει λειτουργία συγχρονισμού των εν λόγω ρολογιών ώστε να μην προκύπτουν αντικρουόμενες πληροφορίες.

2.3 Ασφάλεια Συστήματος

2.3.1 Γενική απαίτηση

Όλοι οι τρόποι επικοινωνίας, συμπεριλαμβανομένης και της απομακρυσμένης πρόσβασης, πρέπει να διέρχονται, σε επίπεδο λογισμικού, από τουλάχιστον ένα εγκεκριμένο τείχος προστασίας και δεν πρέπει να επιτρέπεται να διέλθουν από κάποια άλλη διαδρομή του δικτύου.

2.3.2 Αρχεία Καταγραφής Δεδομένων Τείχους Προστασίας

Το λογισμικό του τείχους προστασίας πρέπει να απενεργοποιεί κάθε επικοινωνία και να παράγει ένα σήμα σφάλματος στην περίπτωση που η μνήμη του αρχείου καταγραφής είναι πλήρης. Επιπλέον, το λογισμικό του τείχους προστασίας πρέπει να διατηρεί ένα αρχείο καταγραφής δεδομένων των κάτωθι πληροφοριών:

- α) Αλλαγές στις ρυθμίσεις του τείχους προστασίας,
- β) Επιτυχημένες και αποτυχημένες προσπάθειες σύνδεσης μέσω του τείχους προστασίας, και
- γ) Τα ηλεκτρονικά πρωτόκολλα (IP), τους αριθμούς των θυρών (Port Numbers) και τις διευθύνσεις προέλευσης και προορισμού (MAC).

2.3.3 Λειτουργία Παρακολούθησης/Ασφάλειας

Το σύστημα πρέπει να παρέχει τη δυνατότητα αναλυτικής αναζήτησης μέσω δικτύου, των σημαντικών στοιχείων του αρχείου καταγραφής.

2.3.4 Έλεγχος πρόσβασης

Το Σύστημα πρέπει να παρέχει διαβαθμισμένη πρόσβαση, η οποία υλοποιείται είτε με όνομα χρήστη και κωδικό πρόσβασης, ή μέσω ενός αποκλειστικού μενού διαχείρισης πρόσβασης, ή μέσω σύνδεσης/συσκευής βασισμένη αυστηρά στο όνομα χρήστη και τον κωδικό πρόσβασης του ή με PIN. Επιπλέον, το Σύστημα δεν πρέπει να επιτρέπει τη μεταβολή τέτοιων σημαντικών πληροφοριών σύνδεσης χωρίς τους απαραίτητους ελέγχους πρόσβασης. Επίσης, μετά από ένα συγκεκριμένο αριθμό αποτυχημένων προσπαθειών σύνδεσης το Σύστημα πρέπει να εμφανίζει στον διαχειριστή του συστήματος σχετικό μήνυμα και να τηρεί αρχείο αποτυχημένων προσβάσεων και αποκλεισμών ανά χρήστη. Το Σύστημα θα πρέπει να καταγράφει τα κάτωθι:

- α) Ημερομηνία και ώρα προσπάθειας (επιτυχημένης/αποτυχημένης) σύνδεσης ανά χρήστη,
- β) Το όνομα χρήστη, και
- γ) Την επιτυχία ή αποτυχία της προσπάθειας αυτής.

Δεν επιτρέπεται η χρήση γενικευμένων (generic) λογαριασμών χρηστών στον εξυπηρετητή.

2.3.5 Τροποποίηση δεδομένων

Το Σύστημα δεν πρέπει να επιτρέπει την τροποποίηση των πληροφοριών του αρχείου καταγραφής των οικονομικών στοιχείων ή σημαντικών συμβάντων χωρίς ελέγχους διαβαθμισμένης πρόσβασης. Σε περίπτωση τροποποίησης των οικονομικών δεδομένων, πρέπει να υφίσταται η δυνατότητα παραγωγής αρχείου καταγραφής ελέγχου για την τεκμηρίωση των εξής:

- α) Των δεδομένων που τροποποιήθηκαν,
- β) Των δεδομένων πριν την τροποποίηση,
- γ) Των δεδομένων μετά την τροποποίηση,
- δ) Της ώρας και της ημερομηνίας τροποποίησης, και
- ε) Τα στοιχεία του προσώπου που πραγματοποίησε την τροποποίηση (σύνδεση χρήστη).

2.4 Απομακρυσμένη πρόσβαση

2.4.1 Ορισμός Απομακρυσμένης Πρόσβασης

Ως απομακρυσμένη πρόσβαση ορίζεται κάθε πρόσβαση στο σύστημα εκτός του «αξιόπιστου» δικτύου.

2.4.2 Γενική απαίτηση

Η απομακρυσμένη πρόσβαση, όπου επιτρέπεται, θα ταυτοποιεί όλα τα συστήματα υπολογιστή με βάση τις ρυθμίσεις εξουσιοδότησης του ηλεκτρονικού επιτραπέζιου παιχνιδιού και του τείχος προστασίας που δημιουργεί σύνδεση με το ΗΕΠ εφόσον τηρούνται τα κάτωθι.

- α) Να υπάρχει καταγραφή της δραστηριότητας του χρήστη απομακρυσμένης πρόσβασης τόσο από την πλευρά του κατασκευαστή όσο και από την πλευρά του ιδιοκτήτη, η οποία να απεικονίζει: το πρόσωπο που έδωσε την εξουσιοδότηση, το όνομα σύνδεσης του χρήστη, την ημερομηνία και ώρα, τη διάρκεια της σύνδεσης και τη δραστηριότητα κατά τη διάρκεια αυτήν,
- β) Δεν επιτρέπεται η μη εξουσιοδοτημένη λειτουργία διαχείρισης απομακρυσμένου χρήστη (προσθήκη χρηστών, αλλαγή αδειών κ.λπ.),
- γ) Δεν επιτρέπεται η μη εξουσιοδοτημένη πρόσβαση σε βάση δεδομένων,
- δ) Δεν επιτρέπεται η μη εξουσιοδοτημένη πρόσβαση στο λειτουργικό σύστημα, και
- ε) Στην περίπτωση που η διαρκής χρήση απομακρυσμένης πρόσβασης είναι απαραίτητη, απαιτείται η εγκατάσταση κάποιου τύπου φίλτρου δικτύου (τείχος προστασίας) για την προστασία της πρόσβασης αυτής.

2.4.3 Αυτο-παρακολούθηση

Το σύστημα πρέπει να εφαρμόζει αυτόματη παρακολούθηση στα σημαντικά στοιχεία διεπαφής (π.χ. κεντρικοί υπολογιστές, συσκευές δικτύου, τείχη προστασίας, σύνδεσμοι σε τρίτα μέρη κ.λπ.). και πρέπει να έχει τη δυνατότητα να ειδοποιεί αποτελεσματικά το διαχειριστή του συστήματος σε κάθε περίπτωση σφάλματος, εάν βέβαια η περίπτωση αυτή δεν είναι καταστροφική. Η λειτουργία αυτή θα πρέπει να επαναλαμβάνεται τουλάχιστον ημερησίως αλλά και σε κάθε έναρξη ή επανεκκίνηση της τάσης τροφοδοσίας.

2.5 Αντίγραφα ασφαλείας και ανάκτηση δεδομένων.

2.5.1 Πόροι, αντίγραφα ασφαλείας και ανάκτηση δεδομένων συστήματος

Το σύστημα πρέπει να έχει επαρκείς πόρους και τέτοια δομή έτσι ώστε στην περίπτωση που κάποιο δομικό του στοιχείο ή τμήμα αυτού πάψει να λειτουργεί, η διεξαγωγή του παιχνιδιού να μπορεί να συνεχιστεί. Στο σύστημα πρέπει να υπάρχουν αρκετά αντίγραφα του κάθε αρχείου καταγραφής ή της βάσης δεδομένων του συστήματος ή και των δύο και ελεύθερη (open) δημιουργία αντιγράφων ασφαλείας και ανάκτησης δεδομένων.

2.5.2 Αντίγραφα ασφαλείας και ανάκτηση δεδομένων

Σε περιπτώσεις καταστροφικής βλάβης, και μόνο όταν δεν είναι δυνατή η επανεκκίνηση του συστήματος με οποιονδήποτε άλλον τρόπο, πρέπει να είναι η δυνατή η εκ νέου φόρτωση των δεδομένων του συστήματος από το τελευταίο λειτουργικό αντίγραφο ασφαλείας το οποίο προτείνεται να περιέχει τα κάτωθι:

- α) Σημαντικά γεγονότα,
- β) Πληροφορίες οικονομικού περιεχομένου,
- γ) Πληροφορίες ελέγχου, και
- δ) Συγκεκριμένες τοπικές πληροφορίες όπως τα αρχεία της συσκευής, το αρχείο με τους εργαζομένους, τα στοιχεία των παιγνίων και άλλα.

2.6 Πρωτόκολλο επικοινωνίας

2.6.1 Γενική απαίτηση

Κάθε στοιχείο του συστήματος ηλεκτρονικών επιτραπέζιων παιχνιδιών πρέπει να λειτουργεί σύμφωνα με τα όσα προβλέπονται από το πρωτόκολλο επικοινωνίας που εφαρμόζεται. Όλα τα πρωτόκολλα πρέπει να χρησιμοποιούν τεχνικές επικοινωνίας οι οποίες περιέχουν κατάλληλους μηχανισμούς εντοπισμού σφαλμάτων ή/και ανάκτησης δεδομένων, οι οποίοι είναι σχεδιασμένοι έτσι ώστε να μην επιτρέπεται η μη εγκεκριμένη πρόσβαση ή αλλοίωση δεδομένων και οι οποίοι μηχανισμοί εφαρμόζουν πρότυπα κρυπτογράφησης δεδομένων ή αντίστοιχη μέθοδο κρυπτογράφησης που χρησιμοποιεί ασφαλείς αλγορίθμους ή φύτρες. Εάν απαιτηθεί η χρήση οποιωνδήποτε εναλλακτικών μέσων, αυτά θα εξετάζονται ανά περίπτωση μετά την έγκριση της ρυθμιστικής αρχής.

2.7 Περιβαλλοντικές επιδράσεις στην ακεραιότητα του συστήματος

2.7.1 Πρότυπο ακεραιότητας

Τα ανεξάρτητα εργαστήρια πιστοποίησης θα πραγματοποιούν συγκεκριμένες δοκιμές για να προσδιορίσουν αν εξωτερικοί παράγοντες μπορούν να επηρεάσουν τη φερεγγυότητα του παιγνίου ή να δημιουργήσουν τη δυνατότητα εξαπάτησης. Τα συστήματα πρέπει να αντεπεξέρχονται στις ακόλουθες δοκιμές, συνεχίζοντας τη λειτουργία τους χωρίς την παρέμβαση του χειριστή:

- α) Γεννήτρια τυχαίων αριθμών. Εφόσον εφαρμόζεται, η γεννήτρια τυχαίων αριθμών και η διαδικασία τυχαίας επιλογής πρέπει να παραμένει ανεπηρέαστη από παράγοντες προερχόμενους από το εξωτερικό περιβάλλον του μηχανήματος, συμπεριλαμβανομένων ενδεικτικά αλλά χωρίς περιορισμό των ηλεκτρομαγνητικών, ηλεκτροστατικών παρεμβολών και των παρεμβολών ραδιοσυχνοτήτων,
- β) Ηλεκτρομαγνητική παρεμβολή. Τα συστήματα δεν πρέπει να προκαλούν ηλεκτρονικό θόρυβο που επηρεάζει την ακεραιότητα ή τη φερεγγυότητα του γειτονικού συνδεδεμένου εξοπλισμού, και
- γ) Ηλεκτροστατική παρεμβολή. Για την προστασία από ηλεκτροστατική εκκένωση απαιτείται γείωση του υλισμικού του συστήματος με τρόπο που η ενέργεια της ηλεκτροστατικής εκκένωσης να μην προκαλεί μόνιμη βλάβη ή να μην αναστέλλει μόνιμα την κανονική λειτουργία των ηλεκτρονικών ή άλλων στοιχείων του συστήματος. Τα συστήματα, ενδέχεται να παρουσιάσουν προσωρινή διακοπή όταν υποβάλλονται σε σημαντική ηλεκτροστατική εκκένωση, μεγαλύτερη από την εκκένωση του ανθρώπινου σώματος, αλλά πρέπει να έχουν τη δυνατότητα να επανέρχονται και να ολοκληρώνουν όλες τις λειτουργίες που διακόπηκαν, χωρίς απώλειες ή αλλοίωση των πληροφοριών που αφορούν τον έλεγχο ή τα σημαντικά δεδομένα που σχετίζονται με το σύστημα. Οι δοκιμές εκκένωσης στον αέρα θα πραγματοποιούνται μέχρι το επίπεδο των 27 kV.

2.7.2 Φυσική Ασφάλεια

Τα στοιχεία του συστήματος ή του εξυπηρετητή πρέπει να είναι τοποθετημένα σε μία ασφαλή περιοχή όπου θα παρέχεται πρόσβαση μόνο σε εξουσιοδοτημένο

προσωπικό. Συνιστάται να καταγράφεται κάθε πρόσβασης στο λογισμικό του παίγνιο είτε στο σύστημα είτε σε υπολογιστή είτε σε άλλη συσκευή καταγραφής που βρίσκεται εκτός της ασφαλούς περιοχής και η πρόσβαση της οποίας δεν είναι δυνατή από τα άτομα που έχουν πρόσβαση στην ασφαλή περιοχή. Τα δεδομένα που καταγράφονται πρέπει να περιλαμβάνουν την ώρα, την ημερομηνία και την ταυτότητα του προσώπου που εισήλθε στην ασφαλή περιοχή. Τα αρχεία καταγραφής πρέπει να φυλάσσονται τουλάχιστον για 90 ημέρες.

2.8 Γεννήτρια Τυχαίων Αριθμών

2.8.1 Γενική Απαίτηση

Η Γεννήτρια Τυχαίων Αριθμών (ΓΤΑ) αποτελεί την επιλογή των συμβόλων του παιχνιδιού ή την παραγωγή των αποτελεσμάτων παιχνιδιού. Οι κανονισμοί της παρούσας ενότητας εφαρμόζονται μόνο σε ηλεκτρονικά επιτραπέζια παίγνια τα οποία κάνουν χρήση ΓΤΑ και η οποία:

- α) Πρέπει να είναι στατιστικά ανεξάρτητη,
- β) Πρέπει να συμμορφώνεται προς την επιθυμητή τυχαία κατανομή,
- γ) Πρέπει να περνά επιτυχώς διάφορες αναγνωρισμένες στατιστικές δοκιμές, και
- δ) Πρέπει να είναι μη προβλέψιμη.

2.8.2 Διαδικασία επιλογής παιχνιδιού

- α) Πρέπει να διατίθενται όλοι οι συνδυασμοί και τα αποτελέσματα. Κάθε πιθανή μετάθεση ή συνδυασμός των στοιχείων του παιχνιδιού που παράγει αποτελέσματα νίκης ή ήττας του παιχνιδιού πρέπει να διατίθεται για τυχαία επιλογή κατά την εκκίνηση κάθε παιχνιδιού, εκτός εάν επισημαίνεται διαφορετικά από το παίγνιο,
- β) Χωρίς παρ' ολίγον ήττα Μετά από την επιλογή του αποτελέσματος του παιχνιδιού, το ηλεκτρονικό επιτραπέζιο παίγνιο δεν πρέπει να προβαίνει σε διαφορετική δευτερεύουσα απόφαση, η οποία επηρεάζει το αποτέλεσμα που εμφανίζεται στον παίκτη. Για παράδειγμα, η γεννήτρια τυχαίων αριθμών επιλέγει ένα αποτέλεσμα στο οποίο το παίγνιο έχει ως αποτέλεσμα την ήττα, και

- γ) Καμία αλλοίωση από τον σχετικό εξοπλισμό. Το ηλεκτρονικό επιτραπέζιο παίγνιο πρέπει να χρησιμοποιεί κατάλληλα πρωτόκολλα προκειμένου να προστατεύει τη γεννήτρια τυχαίων αριθμών και τη διαδικασία τυχαίας επιλογής από τις επιδράσεις σχετικού εξοπλισμού, ο οποίος ενδέχεται να επικοινωνεί με το ηλεκτρονικό επιτραπέζιο παίγνιο.

2.8.3 Εφαρμοσμένες Δοκιμές

Το εργαστήριο αξιολόγησης ενδέχεται να χρησιμοποιεί διάφορες αναγνωρισμένες δοκιμές για να καθορίσει εάν οι τυχαίες τιμές που προέκυψαν από τη γεννήτρια τυχαίων αριθμών περνάνε επιτυχώς ή όχι το επιθυμητό όριο εμπιστοσύνης 99%. Αυτές οι δοκιμές μπορεί να περιλαμβάνουν ενδεικτικά, αλλά χωρίς περιορισμούς, τα εξής:

- α) Δοκιμή χ^2 ,
- β) Δοκιμή ισοκατανομής (συχνότητα),
- γ) Δοκιμή κενού,
- δ) Δοκιμή αλληλοκαλύψεων,
- ε) Δοκιμή πόκερ,
- στ) Δοκιμή συλλέκτη κουπονιών,
- ζ) Δοκιμή αντιμετάθεσης,
- η) Δοκιμή Kolmogorov-Smirnov,
- θ) Δοκιμές κριτηρίου διαδοχικότητας,
- ι) Δοκιμή στατιστικής ακολουθίας,
- ια) Δοκιμές ροών (τα μοτίβα εμφανίσεων δεν πρέπει να είναι επαναλαμβανόμενα),
- ιβ) Δοκιμή διαδραστικής συσχέτισης,
- ιγ) Ισχύς δοκιμής σειριακής συσχέτισης και βαθμός σειριακής συσχέτισης (τα αποτελέσματα πρέπει να είναι ανεξάρτητα από το προηγούμενο παίγνιο),
- ιδ) Δοκιμές ακολουθιών, και
- ιε) Κατανομή Poisson.

2.8.4 Παρασκηνιακή Δραστηριότητα ΓΤΑ

Η ΓΤΑ πρέπει να επαναλαμβάνεται (cycled) συνεχώς στο παρασκήνιο ανάμεσα σε παίγνια και κατά τη διάρκεια παιγνίων με μια ταχύτητα, η οποία δεν μπορεί να

χρονομετρηθεί από τον παίκτη. Αναγνωρίζεται ότι σε κάποια χρονική στιγμή κατά τη διάρκεια του παιγνίου η ΓΤΑ ενδέχεται να μην κυκλωθεί, αλλά η εξαίρεση αυτή πρέπει να διατηρείται στο ελάχιστο επίπεδο.

2.8.5 Παραγωγή φύτρων ΓΤΑ

Το πρώτο φύτρο πρέπει να καθορίζεται τυχαία από ένα μη ελεγχόμενο συμβάν. Μετά από κάθε παίγνιο πρέπει να υπάρχει μια τυχαία αλλαγή στη διαδικασία ΓΤΑ (νέο φύτρο, τυχαίο χρονόμετρο, καθυστέρηση κ.λπ.). Πιστοποιείται ότι η ΓΤΑ δεν ξεκινά με την ίδια τιμή κάθε φορά. Εναλλακτικά, είναι επιτρεπτή η μη χρήση ενός τυχαίου φύτρου. Ωστόσο, ο κατασκευαστής πρέπει να εξασφαλίσει ότι τα παίγνια δεν θα συγχρονίζονται.

2.8.6 Συσχέτιση ζωντανού παιγνίου

Εκτός εάν δηλώνεται διαφορετικά στην οθόνη πληρωμών, όταν στο ηλεκτρονικό επιτραπέζιο παίγνιο διεξάγεται ένα παίγνιο που μπορεί να αναγνωριστεί ως προσομοίωση ενός ζωντανού παιγνίου καζίνο, όπως Πόκερ, Blackjack, Ρουλέτα κ.λπ., πρέπει να είναι ευκρινείς στο προσομοιωμένο παίγνιο οι ίδιες πιθανότητες που σχετίζονται με το ζωντανό παίγνιο. Για παράδειγμα, οι πιθανότητες να επιτύχει κανείς ένα συγκεκριμένο αριθμό στη Ρουλέτα όπου υπάρχει ένα μόνο μηδενικό (0) και ένα διπλό μηδενικό (00) στον τροχό πρέπει να είναι 1 προς 38. Αντίστοιχα, οι πιθανότητες να τραβήξει κανείς ένα συγκεκριμένο φύλλο ή φύλλα στο πόκερ πρέπει να είναι ίδιες με αυτές του ζωντανού παιγνίου.

2.8.7 Χαρτοπαίγνια

Οι απαιτήσεις για παίγνια που απεικονίζουν φύλλα που μοιράζονται από μια τράπουλα είναι οι εξής:

- α) Στην αρχή κάθε γύρου/μοιράσματος, τα φύλλα πρέπει απλώς να μοιράζονται από μια τυχαία ανακατεμένη τράπουλα. Τα φύλλα αντικατάστασης δεν πρέπει να τραβιούνται μέχρι αυτό να καταστεί αναγκαίο και, σύμφωνα με τους κανόνες του παιγνίου, να είναι δυνατή η χρήση πολλαπλών τραπουλών και τραπουλών με μειωμένο αριθμό φύλλων,
- β) Αφού απομακρυνθούν τα φύλλα από την τράπουλα, δεν πρέπει να επιστρέφουν στην τράπουλα, εκτός εάν προβλέπεται κάτι τέτοιο στους κανόνες του απεικονιζόμενου παιγνίου, και

- γ) Μετά την απομάκρυνσή τους από την τράπουλα, τα φύλλα πρέπει να χρησιμοποιούνται αμέσως, όπως καθορίζεται από τους κανόνες του παιχνιδιού (δηλαδή δεν πρέπει να απορρίπτονται λόγω προσαρμοστικής συμπεριφοράς του συστήματος ηλεκτρονικών επιτραπέζιων παιχνιδιών).

ΣΗΜΕΙΩΣΗ: Είναι αποδεκτή η λήψη τυχαίων αριθμών για φύλλα αντικατάστασης κατά τη χρονική στιγμή λήψης του πρώτου τυχαίου αριθμού. Απαραίτητη προϋπόθεση είναι η χρήση των φύλλων να γίνεται διαδοχικά, όπως απαιτείται.

2.9 Διατήρηση κύριας μνήμης

2.9.1 Γενική απαίτηση

Η αποθήκευση της κύριας μνήμης πρέπει να διατηρείται στο τερματικό του παίκτη ή στο σύστημα, εάν αυτό καθίσταται δυνατό. Η διατήρηση των δεδομένων που αποθηκεύονται στην κύρια μνήμη πρέπει να πραγματοποιείται μέσω μιας μεθοδολογίας που καθιστά δυνατή την αναγνώριση σφαλμάτων. Η μεθοδολογία μπορεί να περιλαμβάνει υπογραφές, αθροίσματα ελέγχου, μερικά αθροίσματα ελέγχου, πολλαπλά αντίγραφα, χρονικές σημάνσεις και/ή αποτελεσματική χρήση κωδικών εγκυρότητας.

ΣΗΜΕΙΩΣΗ: Η ενότητα «Διατήρηση κύριας μνήμης» δεν προορίζεται για τον αποκλεισμό της χρήσης εναλλακτικών τύπων μέσων αποθήκευσης, όπως μονάδες σκληρού δίσκου, για τη διατήρηση δεδομένων ζωτικής σημασίας. Τα εν λόγω εναλλακτικά μέσα αποθήκευσης πρέπει επίσης να διατηρούν την ακεραιότητα των δεδομένων ζωτικής σημασίας κατά τρόπο σύμφωνο με τις απαιτήσεις της παρούσας ενότητας, όπως ισχύει για τη συγκεκριμένη εφαρμοζόμενη τεχνολογία αποθήκευσης.

2.9.2 Διεξοδικοί έλεγχοι

Οι διεξοδικοί έλεγχοι της κύριας μνήμης πρέπει να πραγματοποιούνται μετά από την εκκίνηση του παιχνιδιού, αλλά πριν από την προβολή του αποτελέσματος του παιχνιδιού στον παίκτη. Συνιστάται η διαρκής παρακολούθηση της κύριας μνήμης για τυχόν αλλοιώσεις. Η μεθοδολογία πρέπει να ανιχνεύει τις αποτυχίες με εξαιρετικά υψηλό επίπεδο ακρίβειας.

2.9.3 Μη επανορθώσιμο σφάλμα στην κύρια μνήμη

Μια μη επανορθώσιμη αλλοίωση της κύριας μνήμης πρέπει να οδηγεί σε σφάλμα. Το σφάλμα της μνήμης δεν πρέπει να διαγράφεται αυτόματα και πρέπει να οδηγεί σε κατάσταση «tilt», γεγονός που διευκολύνει την αναγνώριση του σφάλματος και οδηγεί στη διακοπή της περαιτέρω λειτουργίας του ηλεκτρονικού επιτραπέζιου παιχνιδιού. Το σφάλμα στην κύρια μνήμη πρέπει επίσης να προκαλεί την άμεση παύση τυχόν επικοινωνιών εκτός του ηλεκτρονικού επιτραπέζιου παιχνιδιού. Σε περίπτωση μη επανορθώσιμου σφάλματος κύριας μνήμης, πρέπει να απαιτείται πλήρης εκκαθάριση της μη μεταβλητής μνήμης (NV), η οποία πραγματοποιείται από εξουσιοδοτημένο άτομο.

2.9.4 Χώρος μη μεταβλητής μνήμης (NV) και συσκευής αποθήκευσης προγράμματος

Ο χώρος της μη μεταβλητής μνήμης (NV) που δεν είναι σημαντικός για την ασφάλεια του ηλεκτρονικού επιτραπέζιου παιχνιδιού δεν χρειάζεται επικύρωση.

2.10 Απαιτήσεις συσκευής αποθήκευσης προγράμματος

2.10.1 Γενική απαίτηση

Ο όρος *Συσκευή Αποθήκευσης Προγράμματος* ορίζεται ως το μέσο ή η ηλεκτρονική συσκευή που περιέχει τα σημαντικά στοιχεία του προγράμματος ελέγχου. Στους τύπους μηχανημάτων περιλαμβάνονται ενδεικτικά αλλά χωρίς περιορισμό EPROM, κάρτες μνήμης τύπου «compact flash», οπτικοί δίσκοι, σκληροί δίσκοι, μονάδες αποθήκευσης σταθερής κατάστασης, μονάδες USB κ.λπ. Αυτή η μερική λίστα ενδέχεται να αλλάζει στην πορεία εξέλιξης της τεχνολογία των μέσων αποθήκευσης. Όλες οι συσκευές αποθήκευσης προγραμμάτων πρέπει:

- α) Να είναι τοποθετημένες μέσα σε ένα πλήρως εσώκλειστο και κλειδωμένο λογικό χώρο/διαμέρισμα,
- β) Να επισημαίνονται εμφανώς με επαρκείς πληροφορίες για να προσδιορίζεται το λογισμικό και το επίπεδο αναθεώρησης των πληροφοριών που είναι αποθηκευμένες στη συσκευή. Σε περίπτωση τύπων μέσων στα οποία ενδέχεται να υπάρχουν πολλά προγράμματα, είναι αποδεκτή η προβολή αυτών των πληροφοριών μέσω του μενού επόπτη,
- γ) Να αυτο-επικυρώνονται κατά τη διάρκεια κάθε επαναφοράς επεξεργαστή,

- δ) Να αυτο-επικυρώνονται κατά την πρώτη φορά χρήσης, και
- ε) Ο δίσκος CD-ROM, DVD και κάθε άλλος χώρος αποθήκευσης προγράμματος που βασίζεται σε οπτικό δίσκο:
 - i. Δεν πρέπει να είναι επανεγγράψιμος, και
 - ii. Η «Συνεδρία Εγγραφής Δίσκου» πρέπει να είναι κλειστή για να αποτραπεί τυχόν περαιτέρω εγγραφή.

2.11 Απαιτήσεις προγράμματος ελέγχου

2.11.1 Επαλήθευση προγράμματος ελέγχου

- α) Χώρος αποθήκευσης προγράμματος με βάση την EPROM:
 - i. Τα ηλεκτρονικά επιτραπέζια παίγνια που έχουν προγράμματα ελέγχου τα οποία βρίσκονται σε ένα ή περισσότερα EPROM πρέπει να διαθέτουν ένα μηχανισμό για την επαλήθευση των προγραμμάτων ελέγχου και των δεδομένων. Ο μηχανισμός πρέπει να χρησιμοποιεί κατ' ελάχιστο ένα άθροισμα ελέγχου (checksum). Ωστόσο, συνιστάται η χρήση των υπολογισμών του Κυκλικού Ελέγχου Πλεονασμού (ΚΕΠ) (16 bit κατ' ελάχιστο),
- β) Ο χώρος αποθήκευσης προγράμματος που δεν βασίζεται σε EPROM πρέπει να τηρεί τους ακόλουθους κανόνες:
 - i. Το λογισμικό πρέπει να διαθέτει ένα μηχανισμό για την ανίχνευση μη εξουσιοδοτημένων και κατεστραμμένων στοιχείων λογισμικού σε κάθε πρόσβαση και, στη συνέχεια, να αποτρέπει την εκτέλεση ή τη χρήση αυτών των στοιχείων από το ηλεκτρονικό επιτραπέζιο παίγνιο. Ο μηχανισμός πρέπει να χρησιμοποιεί έναν αλγόριθμο κλειδώματος, ο οποίος παράγει μία περίληψη του μηνύματος μήκους κατ' ελάχιστο 128 bit, και
 - ii. Σε περίπτωση αποτυχίας του ελέγχου ταυτότητας, αφού τεθεί σε λειτουργία το παίγνιο, το ηλεκτρονικό επιτραπέζιο παίγνιο πρέπει να τίθεται αμέσως σε κατάσταση σφάλματος και να εμφανίζει το κατάλληλο σφάλμα. Αυτό το σφάλμα πρέπει να απαιτεί την επέμβαση του χειριστή για την εκκαθάριση και δεν πρέπει να γίνεται εκκαθάρισή του μέχρι τα

δεδομένα να υποβληθούν σε σωστό έλεγχο ταυτότητας, μετά από την επέμβαση του χειριστή ή κατόπιν αντικατάστασης ή επισκευής του μέσου και εκκαθάρισης της μνήμης του ηλεκτρονικού επιτραπέζιου παίγνιου, και

ΣΗΜΕΙΩΣΗ: Οι Μηχανισμοί Επαλήθευσης του Προγράμματος ελέγχου θα αξιολογούνται κατά περίπτωση και θα εγκρίνονται από την ΕΕΕΠ και το ανεξάρτητο εργαστήριο αξιολόγησης με βάση τις τυπικές βιομηχανικές πρακτικές ασφαλείας.

γ) Τα μεταβλητά μέσα πρέπει να ικανοποιούν τους παρακάτω κανόνες, πέραν των απαιτήσεων που περιγράφονται στην ενότητα 2.11.1(β):

- i. Πρέπει να χρησιμοποιείται ένας μηχανισμός, ο οποίος υποβάλλει σε δοκιμές μη χρησιμοποιημένες ή μη εκχωρημένες περιοχές των μεταβλητών μέσων για ακούσια προγράμματα ή δεδομένα και υποβάλλει σε δοκιμές τη δομή των μέσων για ακεραιότητα. Ο μηχανισμός πρέπει να αποτρέπει το περαιτέρω παίγνιο στο ηλεκτρονικό επιτραπέζιο παίγνιο σε περίπτωση εντοπισμού μη αναμενόμενων ανακολουθιών στα δεδομένα ή τη δομή, και
- ii. Πρέπει να χρησιμοποιείται ένας μηχανισμός για την τήρηση ενός αρχείου κάθε φορά που ένα στοιχείο του προγράμματος ελέγχου προστίθεται, αφαιρείται ή αλλοιώνεται σε κάποιο μεταβλητό μέσο. Το μητρώο αρχείου πρέπει να περιέχει κατ' ελάχιστο τις τελευταίες δέκα (10) τροποποιήσεις στο μέσο και κάθε αρχείο πρέπει να περιέχει την ημέρα και την ώρα της ενέργειας, τα στοιχεία ταυτοποίησης του θιγόμενου στοιχείου, το λόγο της τροποποίησης και κάποιες σχετικές πληροφορίες επικύρωσης.

ΣΗΜΕΙΩΣΗ: Ο χώρος Αποθήκευσης Μεταβλητών Προγραμμάτων δεν περιλαμβάνει συσκευές μνήμης οι οποίες θεωρούνται συνήθως μεταβλητές, οι οποίες έχουν γίνει «μόνο για ανάγνωση» χρησιμοποιώντας είτε το υλικό είτε το λογισμικό.

2.11.2 Ταυτοποίηση προγράμματος

Οι συσκευές αποθήκευσης προγραμμάτων, οι οποίες δεν έχουν τη δυνατότητα να τροποποιηθούν ενώ είναι εγκατεστημένες στο ηλεκτρονικό επιτραπέζιο παίγνιο κατά την κανονική λειτουργία, πρέπει να επισημαίνονται ευκρινώς με επαρκείς πληροφορίες για την ταυτοποίηση του λογισμικού και τις αναθεωρήσεις των πληροφοριών που είναι αποθηκευμένες στις συσκευές.

2.11.3 Ανεξάρτητη επικύρωση του προγράμματος ελέγχου

Ο/Οι εξυπηρετητής/ες του συστήματος καθώς και κάθε στοιχείο του ηλεκτρονικού επιτραπέζιου παιχνιδιού που ενδέχεται να επηρεάζει την αξιοπιστία του ηλεκτρονικού επιτραπέζιου παιχνιδιού, πρέπει να έχει τη δυνατότητα να επιτρέπει την πραγματοποίηση ανεξάρτητου ελέγχου, ως προς την ακεραιότητα του λογισμικού της συσκευής, από κάποια εξωτερική πηγή, και απαιτείται για όλα τα προγράμματα ελέγχου που ενδέχεται να επηρεάζουν την ακεραιότητα του παιχνιδιού. Αυτό πρέπει να διεκπεραιώνεται μέσω ελέγχου ταυτότητας από κάποια τρίτη συσκευή, η οποία ενδέχεται να είναι ενσωματωμένη στο λογισμικό του παιχνιδιού (ανατρέξτε στην παρακάτω ΣΗΜΕΙΩΣΗ), μέσω της ύπαρξης θύρας διεπαφής τρίτων συσκευών για την επαλήθευση των μέσων ή μέσω της δυνατότητας αφαίρεσης των μέσων ώστε να επικυρώνονται εκτός του ηλεκτρονικού επιτραπέζιου παιχνιδιού. Ο έλεγχος ακεραιότητας αποτελεί ένα μέσο επιτόπιας επαλήθευσης του λογισμικού για την ταυτοποίηση και την επικύρωση του προγράμματος. Πριν από την έγκριση των συσκευών, το εργαστήριο αξιολόγησης πρέπει να προβαίνει σε αξιολόγηση της μεθόδου ελέγχου ακεραιότητας.

Σημείωση: Εάν το πρόγραμμα ελέγχου ταυτότητας περιέχεται στο λογισμικό του παιχνιδιού, τότε ο κατασκευαστής πρέπει να λάβει μια γραπτή επιβεβαίωση από το εργαστήριο αξιολόγησης πριν από την υποβολή.

2.12 Απαιτήσεις Τερματικού Διεπαφής Παίκτη

2.12.1 Γενική Απαίτηση

Τα τερματικά διεπαφής παίκτη είτε πρέπει να αποτελούνται από έναν μηχανισμό προβολής όπου το σύστημα πραγματοποιεί όλες τις λειτουργίες του παιχνιδιού (Thin Client), είτε να περιλαμβάνουν τη δική τους λογική συνάρτηση σε συνδυασμό με το σύστημα ηλεκτρονικών επιτραπέζιων παιχνιδιών (Thick Client). Σε κάθε περίπτωση τα τερματικά πρέπει να πληρούν τις απαιτήσεις του τεύχους «Παιγνιομηχανήματα τύπου Καζίνο» του παρόντος.

