Φυσική Κυβερνοασφάλεια Πραγματικού Χρόνου
Μαζικό Ανοικτό Διαδικτυακό Μάθημα MOOC – Εγχειρίδιο Καθηγητή

(Συνοπτική Έκθεση)

Συγγραφείς:

Bahaa Eltahawy, Mike Mekkanen, Tero Vartiainen,
Maria Valliou, Panos Kotsampopoulos, Alexandros Chronis,
Jānis Pekša, Jana Bikovska, Andrejs Romānovs, Rūta Pirta-Dreimane,
Jirapa Kamsamrong, Bjoern Siemers

Προτάσεις προγραμμάτων σπουδών κυβερνοασφάλειας για έξυπνο δίκτυο (CC-RSG)

Έργο στρατηγικής εταιρικής σχέσης Erasmus+

Πνευματική παραγωγή 3

Πανεπιστήμιο της Vaasa, Εθνικό Μετσόβιο Πολυτεχνείο, Τεχνικό Πανεπιστήμιο της Ρίγα, Πανεπιστήμιο του Oldenburg

Το παρόν έργο χρηματοδοτήθηκε από το πρόγραμμα Erasmus+ της Ευρωπαϊκής Ένωσης στο πλαίσιο της συμφωνίας επιχορήγησης με αριθ. 2020-1-FI01-KA203-066624.

Vaasan yliopisto
UNIVERSITY OF VAASA

National Technical University of Athens

1862
RIGA TECHNICAL UNIVERSITY

CARL VON OSSIETZKY universität OLDENBURG

Περιεχόμενα

Περιεχόμενα 3

Ορισμοί, ακρωνύμια και συντομογραφίες 4

1. Εισαγωγή 5

1.1 Στόχοι 6

1.2 Δομή του εγγράφου 6

2. Μεθοδολογία σχεδιασμού του μαθήματος 7

3. Ανασκόπηση των εκπαιδευτικών μεθοδολογιών 7

4. Μοντέλα εκπαιδευτικού σχεδιασμού 8

5. Σχεδιάγραμμα διδασκαλίας μαθήματος 9

6. Περιεχόμενο μαθήματος 10

6.1 Μέρος 1: Έξυπνα δίκτυα, κυβερνοασφάλεια και δίκτυα 10

6.1.1 Κεφάλαιο 1: Βασικές αρχές των συστημάτων έξυπνου δικτύου 10

6.1.2 Κεφάλαιο 2: Κυβερνοασφάλεια και επιχειρησιακή ασφάλεια στα συστήματα έξυπνου δικτύου 10

6.1.3 Κεφάλαιο 3: IEC 61850 και IEC 62351 10

6.2 Μέρος 2: Προσομοίωση σε πραγματικό χρόνο, η θεωρία 11

6.2.1 Κεφάλαιο 4: Βασικές αρχές της προσομοίωσης 11

6.2.2 Κεφάλαιο 5: Προσομοίωση σε πραγματικό χρόνο για το σχεδιασμό συστημάτων 11

6.2.3 Κεφάλαιο 6: Παράλληλη και κατανεμημένη προσομοίωση πραγματικού χρόνου 11

6.2.4 Κεφάλαιο 7: Εργαλεία και εφαρμογές 11

6.3 Μέρος 3: Ασκήσεις και παραδείγματα 11

6.3.1 Άσκηση 1 11

6.3.2 Άσκηση 2 11

6.3.3 Άσκηση 3 12

6.3.4 Άσκηση 4 12

7. Εργαλεία 12

8. Βιβλιογραφία 13

Ορισμοί, ακρωνύμια και συντομογραφίες

ADDIE	Ανάλυση, σχεδιασμός, ανάπτυξη, εφαρμογή και αξιολόγηση
CC-RSG	Προτάσεις προγραμμάτων σπουδών κυβερνοασφάλειας για έξυπνο δίκτυο
CI	Σημαντικές υποδομές
CPS	Κυβερνο-φυσικά συστήματα
DEVS	Προδιαγραφές συστήματος διακριτών γεγονότων
HIL	Hardware in the Loop
ICS	Βιομηχανικά συστήματα ελέγχου
ID	Εκπαιδευτικός σχεδιασμός
IO	Πνευματική παραγωγή
MOOC	Μαζικό Ανοικτό Διαδικτυακό Μάθημα
RCP	Ταχεία προτυποποίηση ελέγχου
RT	Σε πραγματικό χρόνο
SCADA	Εποπτικός έλεγχος και συλλογή δεδομένων
SIL	Software in the Loop
SPSP	Smart Power Security Professional
UML	Ενοποιημένη γλώσσα μοντελοποίησης
WP	Πακέτο εργασίας

1. Εισαγωγή

Πρόσφατα, ο τομέας της ενέργειας υπέστη σημαντικές αλλαγές, οι οποίες οδήγησαν στην εμφάνιση της έννοιας των έξυπνων δικτύων. Ως έξυπνο δίκτυο νοείται ένα δίκτυο ηλεκτρικής ενέργειας που ενσωματώνει τις ενέργειες και τη συμπεριφορά όλων των χρηστών - μεταξύ άλλων των γεννητριών, των καταναλωτών και όσων δρουν και με τις δύο ιδιότητες, με στόχο την αποτελεσματική παροχή βιώσιμης, οικονομικής και ασφαλούς ηλεκτρικής ενέργειας. Η κυβερνοασφάλεια των έξυπνων δικτύων έχει μετατραπεί σε μείζον ζήτημα που πρέπει να αντιμετωπιστεί λόγω του αυξανομένου αριθμού των ευάλωτων σε επιθέσεις σημείων και της κρισιμότητας των συνδεδεμένων στοιχείων. Η κυβερνοασφάλεια αποτελεί μία από τις βασικές ψηφιακές δυνατότητες που επιδιώκει να αναπτύξει η Ευρωπαϊκή Ένωση. Εσωκλείει πολλές πτυχές όπως εργαλεία, πολιτικές, ιδέες ασφαλείας, διασφαλίσεις, κατευθυντήριες γραμμές, προσεγγίσεις διαχείρισης κινδύνου, δράσεις, εκπαίδευση, βέλτιστες πρακτικές, διασφάλιση και τεχνολογίες που μπορούν να χρησιμοποιηθούν για την προστασία των στοιχείων ενός οργανισμού και των χρηστών και του περιβάλλοντος στον κυβερνοχώρο. Παρά τη διαθεσιμότητα πληθώρας εργαλείων και πακέτων λογισμικού από διάφορους προμηθευτές που καλύπτουν τις ανάγκες ασφαλείας και διασφαλίζουν την ευρωστία του δικτύου, η κυβερνοασφάλεια παραμένει ένα σημαντικό ζήτημα.

Το έργο «Προτάσεις προγραμμάτων σπουδών κυβερνοασφάλειας για έξυπνα δίκτυα» (CC-RSG) έχει εμβαθύνει στο θέμα της κυβερνοασφάλειας στα έξυπνα δίκτυα αξιοποιώντας έρευνες, ανασκοπήσεις και εργαστήρια. Από την έρευνα προέκυψαν τα εξής συμπεράσματα:

1. Η τρέχουσα προσέγγιση στην αντιμετώπιση των ζητημάτων κυβερνοασφάλειας στα έξυπνα δίκτυα είναι ελλιπής.
2. Υπάρχει έλλειψη επαγγελματιών κυβερνοασφάλειας στον τομέα των έξυπνων δικτύων λόγω της απουσίας εκπαιδευτικών προγραμμάτων που καλύπτουν σε πρακτικό επίπεδο τον συγκεκριμένο τομέα.
3. Οι υπάρχουσες εκπαιδευτικές προτάσεις δεν ανταποκρίνονται στις απαιτήσεις του Smart Power Security Professional (SPSP).
4. Απουσιάζουν παραδείγματα της πραγματικής ζωής και διασυνδέσεις με τη βιομηχανία.

Η προσφορά εκπαιδευτικών ευκαιριών που μπορούν να ενισχύσουν τις δεξιότητες και να καλύψουν τα κενά που αναφέρθηκαν ανωτέρω αποτελεί μία σημαντική ανάγκη, ιδίως δεδομένων προηγούμενων εκθέσεων που τονίζουν ότι τουλάχιστον το 50% των περιστατικών που αφορούν την κυβερνοασφάλεια προέρχεται από ανθρώπινο λάθος. Για την αντιμετώπιση αυτού του ζητήματος, το έργο CC-RSG επιδιώκει να βοηθήσει τα ιδρύματα μεταδευτεροβάθμιας εκπαίδευσης να ενσωματώσουν στα προγράμματα σπουδών τους μαθησιακά εφόδια που σχετίζονται με την κυβερνοασφάλεια στα έξυπνα δίκτυα. Η παρούσα έκθεση περιέχει το σχεδιάγραμμα του μαθήματος που δημιουργήθηκε για να καλύψει αυτό το θέμα.

Η παρούσα έκθεση παρουσιάζει εν συντομία τα αποτελέσματα του πακέτου εργασίας (WP) 3, «Σχεδιασμός, ανάπτυξη και πιλοτική εφαρμογή» - Πνευματικό αποτέλεσμα (IO) 3 - του έργου CC-RSG. Ως εκ τούτου, η έκθεση βασίζεται στα αποτελέσματα προηγούμενων εκθέσεων και IO για να παρέχει ένα μαζικό ανοικτό διαδικτυακό μάθημα (MOOC) για φυσικά συστήματα κυβερνοασφάλειας σε πραγματικό χρόνο. Στόχος του μαθήματος είναι να καλύψει τα κενά που διαπιστώθηκαν στα κυβερνο-φυσικά συστήματα (CPS), καθώς και να αναπτύξει δεξιότητες γύρω από τα συστήματα προσομοίωσης πραγματικού χρόνου που χρησιμοποιούνται για προσομοιώσεις υψηλής ταχύτητας, δοκιμές κρίσιμων υποδομών (CI) και αξιολόγηση των διαδικασιών και λειτουργιών ασφαλείας. Για το σχεδιασμό του μαθήματος εξετάστηκαν και δοκιμάστηκαν διάφορες προσεγγίσεις, ώστε να βρεθούν οι καταλληλότερες μέθοδοι που

εξυπηρετούν τον σκοπό της δημιουργίας του μαθήματος και της κάλυψης των ελλείψεων που εντοπίστηκαν στο κομμάτι των δεξιοτήτων. Συνεπώς, το μάθημα πρόκειται να χρησιμοποιήσει τις ακόλουθες προσεγγίσεις: Ανεστραμμένη μάθηση, Προσομοιώσεις και Εικονικά και απομακρυσμένα εργαστήρια. Οι προσεγγίσεις αυτές επιλέχθηκαν προσεκτικά με γνώμονα την ικανότητά τους να παρέχουν μέσα αλληλεπίδρασης, να αναπτύσσουν δεξιότητες ανάλυσης και επίλυσης προβλημάτων, καθώς και να προωθούν πρακτικές δεξιότητες.

Οι βασικές εισηγήσεις της έκθεσης IO3 του μαθήματος είναι:

1. Παροχή του θεωρητικού υποβάθρου σχετικά με τα συστήματα προσομοίωσης πραγματικού χρόνου
2. Ανάπτυξη πρακτικών δεξιοτήτων σχετικά με τη χρήση προσομοίωσης πραγματικού χρόνου
3. Παρουσίαση και εφαρμογή παραδειγμάτων, σεναρίων και ασκήσεων χρήσης για σκοπούς πρακτικής εξάσκησης και εκπαίδευσης.

Στην έκθεση IO3 του μαθήματος «Φυσική Κυβερνοασφάλεια Πραγματικού Χρόνου Μαζικό Ανοικτό Διαδικτυακό Μάθημα MOOC – Εγχειρίδιο Καθηγητή», έχει ληφθεί μέριμνα για τις θεωρητικές και θεμελιώδεις γνώσεις, με τη δημιουργία ισχυρών βάσεων και παρέχοντας τη βάση για τη γνώση σχετικά με τα έξυπνα δίκτυα, τα πρωτόκολλα επικοινωνίας έξυπνων δικτύων και την κυβερνοασφάλεια στα έξυπνα δίκτυα. Επιπλέον, έχει δοθεί ιδιαίτερη προσοχή στα συστήματα προσομοίωσης πραγματικού χρόνου, δεδομένου ότι έχουν αναγνωριστεί ως ένα από τα πιο εξειδικευμένα και αποτελεσματικά εργαλεία για τον πειραματισμό, τη δοκιμή και τη εκμάθηση σχετικά με τις κρίσιμες υποδομές και τα έξυπνα δίκτυα. Κατά συνέπεια, έχουν παρουσιαστεί πολλές ιδέες γύρω από την προσομοίωση σε πραγματικό χρόνο. Εξάλλου, το μάθημα δεν περιορίζεται μόνο σε θεωρητικές γνώσεις αλλά υπερκαλύπτει και τις πρακτικές δεξιότητες που απαιτούνται από τη βιομηχανία. Έτσι, δημιουργήθηκαν τέσσερις ασκήσεις γύρω από επιλεγμένα βιομηχανικά σενάρια και υλοποιήθηκαν μέσω ενός φυσικού συστήματος προσομοίωσης πραγματικού χρόνου.

Τέλος, η έκθεση IO3 του μαθήματος αποτελεί το εγχειρίδιο του καθηγητή. Συνεπώς, κατά το σχεδιασμό του μαθήματος, προσπαθήσαμε να συγκεντρώσουμε όλες τις πληροφορίες που απαιτούνται για τη σφαιρική κάλυψη του ζητήματος της κυβερνοασφάλειας στα έξυπνα δίκτυα. Για τη χρήση αυτής της έκθεσης, συνιστάται στους καθηγητές/εκπαιδευτές να χρησιμοποιήσουν το παρόν υλικό για τον σχεδιασμό παρουσιάσεων και φυλλαδίων, και δεδομένου ότι δίνεται έμφαση στην ανεστραμμένη μάθηση και στα MOOC, συνιστάται ιδιαίτερα η εκ των προτέρων δημιουργία ηχογραφημένων βίντεο και αυτοματοποιημένων δραστηριοτήτων.

1.1 Στόχοι

Βασικός στόχος της IO3 είναι ο σχεδιασμός ενός μαθήματος που θα εφοδιάσει τους συμμετέχοντες με τις απαραίτητες γνώσεις προκειμένου να δραστηριοποιηθούν στον τομέα των CPS, και ειδικότερα γνώσεις αναφορικά με την κυβερνοασφάλεια στα έξυπνα δίκτυα.

1.2 Δομή του εγγράφου

- Η ενότητα 2 περιλαμβάνει τη μεθοδολογία σχεδιασμού του μαθήματος
- Η ενότητα 3 εξετάζει τις εκπαιδευτικές μεθοδολογίες και τις διδακτικές προσεγγίσεις που χρησιμοποιούνται
- Η ενότητα 4 περιλαμβάνει τα γενικά μοντέλα εκπαιδευτικού σχεδιασμού (ID)
- Η ενότητα 5 περιλαμβάνει το σχεδιάγραμμα του μαθήματος

- Η ενότητα 6 παραθέτει συνοπτικά το περιεχόμενο του μαθήματος και τα θέματα που καλύπτονται.
- Τέλος, η ενότητα 7 παραθέτει τα εργαλεία που χρησιμοποιήθηκαν

2. Μεθοδολογία σχεδιασμού του μαθήματος

Για τον αποτελεσματικό σχεδιασμό του μαθήματος εφαρμόστηκαν οι ακόλουθες διαδικασίες:

1. Έμφαση στην ανάγκη σχεδιασμού του μαθήματος
2. Προσδιορισμός της κατάστασης και του πλαισίου του μαθήματος
3. Καθορισμός των στόχων και του επιθυμητού αποτελέσματος
4. Καθορισμός των εκπαιδευτικών μεθοδολογιών και δραστηριοτήτων
5. Καθορισμός του περιεχομένου του μαθήματος
6. Επιλογή κριτηρίων αξιολόγησης
7. Ανάπτυξη και υλοποίηση

3. Ανασκόπηση των εκπαιδευτικών μεθοδολογιών

Δεν μπορεί να παραγνωριστεί η σημασία της εκπαιδευτικής μεθοδολογίας, καθώς καθορίζει τους τρόπους με τους οποίους επιτυγχάνονται και αξιολογούνται οι μαθησιακοί στόχοι. Καταρχάς, υπάρχουν διάφορες εκπαιδευτικές μεθοδολογίες και τεχνικές ανάλογα με το επιθυμητό επίπεδο εμπέδωσης της γνώσης. Αυτές περιλαμβάνουν τη διδασκαλία με διαλέξεις, τη βιωματική μάθηση, την ενεργητική μάθηση, τη συνεργατική μάθηση, την ανεστραμμένη μάθηση, τη διερευνητική μάθηση, τη μάθηση βάσει προβλήματος και έργου και την παιχνιδοποίηση, ως εξής:

1. Η συμβατική μέθοδος μάθησης, δηλαδή η μάθηση με βάση τη διάλεξη, προϋποθέτει ότι ο εκπαιδευτής παραδίδει το υλικό του μαθήματος, διενεργεί αξιολογήσεις και αναλαμβάνει την πλήρη ευθύνη για την εκπαιδευτική εμπειρία. Ωστόσο, αυτή η μέθοδος είναι κατά κύριο λόγο παθητική και βασίζεται σε μεγάλο βαθμό στην απομνημόνευση. Με την ενσωμάτωση δραστηριοτήτων όπως η απευθείας επιλογή ενός μαθητή (cold calling), οι συζητήσεις, οι κάρτες μάθησης και άλλα διαδραστικά στοιχεία, η μάθηση με βάση τη διάλεξη μπορεί να μετατραπεί σε μια ενεργητική και πιο αποτελεσματική προσέγγιση.
2. Η βιωματική μάθηση είναι μια ενεργητική προσέγγιση μάθησης που απαιτεί από τους μαθητές να συμμετέχουν στη μαθησιακή διαδικασία και να αποκτούν εμπειρίες καθώς μαθαίνουν. Η ενεργητική μάθηση από την άλλη, δεν αφορά μόνο την ενσωμάτωση δραστηριοτήτων και την ενθάρρυνση της συμμετοχής, αλλά συνεπάγεται επίσης την ανάλυση των απαντήσεων όλων των μαθητών πριν από την παράθεση νέων πληροφοριών.
3. Η συνεργατική μάθηση είναι μια ομαδική προσέγγιση στην οποία οι συμμετέχοντες συνεργάζονται για την επίτευξη συγκεκριμένων στόχων και αναλαμβάνουν πλήρως την ευθύνη για την ολοκλήρωση μιας δραστηριότητας. Η ανεστραμμένη μάθηση αποτελεί μια σύγχρονη προσέγγιση που δίνει τη δυνατότητα στους μαθητές να αναλάβουν την ευθύνη της μάθησής τους, παρέχοντας εκ των προτέρων το εκπαιδευτικό υλικό, συμβάλλοντας σε μια πιο δυναμική και διαδραστική εμπειρία στην τάξη.
4. Η διερευνητική μάθηση είναι μια προσέγγιση που προϋποθέτει ότι οι μαθητές ακολουθούν τις ίδιες πρακτικές με τους εξειδικευμένους επιστήμονες για την απόκτηση γνώσης και εμπειρίας. Η μάθηση βάσει προβλήματος και έργου εμπλέκει ενεργά τους

συμμετέχοντες στη μαθησιακή διαδικασία διερευνώντας ένα συγκεκριμένο πρόβλημα ή ερώτημα με στόχο την εξεύρεση απαντήσεων ή λύσεων.

5. Τέλος, η παιχνιδοποίηση χρησιμοποιεί στοιχεία που προσομοιάζουν παιχνίδια, όπως η αφήγηση ιστοριών, η εναλλαγή επιπέδων και τα εμβλήματα, για να ενθαρρύνει τη συμμετοχή και να κάνει τη μαθησιακή διαδικασία πιο ενδιαφέρουσα. Με την αξιοποίηση αυτών των διαφορετικών προσεγγίσεων, οι εκπαιδευτικοί μπορούν να δημιουργήσουν ένα πιο αποδοτικό και ενδιαφέρον περιβάλλον εκμάθησης για τους μαθητές τους.

Δεύτερον, οι προαναφερθείσες εκπαιδευτικές μεθοδολογίες χρησιμοποιούνται συνήθως για να αντικατοπτρίζουν το ποσοστό συγκράτησης της γνώσης που καθορίζεται από τους στόχους του μαθήματος και τους διαθέσιμους πόρους. Σημειώνεται ότι όσο μεγαλύτερη είναι η συμμετοχή στη μαθησιακή διαδικασία, τόσο υψηλότερο είναι το ποσοστό συγκράτησης- ωστόσο, τόσο περισσότεροι πόροι απαιτούνται. Στη συνέχεια παρατίθεται το ποσοστό συγκράτησης των διαφόρων μαθησιακών δραστηριοτήτων:

1. Συμβατική μέθοδος και διαλέξεις: 5%
2. Ανάγνωση και αυτομελέτη: 10%
3. Οπτικοακουστικές απεικονίσεις: 20%
4. Επίδειξη και ημιενεργός συμμετοχή: 30%
5. Σχεδιασμός, συζητήσεις και ενεργός συμμετοχή: 50%
6. Μάθηση μέσω της πράξης: 75%
7. Διδάσκοντας άλλους: 90%

Κατά το σχεδιασμό ενός μαθήματος, είναι ζωτικής σημασίας να καθοριστεί πρώτα το επίπεδο συγκράτησης που επιδιώκεται και, συνεπώς, να προσαρμοστούν ο φόρτος μελέτης και οι πόροι ώστε να ανταποκρίνονται σε αυτό το κριτήριο.

4. Μοντέλα εκπαιδευτικού σχεδιασμού

Δεδομένου ότι η IO3 αφορά το σχεδιασμό μαθημάτων, τα γενικά μοντέλα ID που αναφέρονται παρακάτω χρησιμοποιήθηκαν για να βοηθήσουν στη διαδικασία καθορισμού στόχων, επιλογής δραστηριοτήτων και επιλογής υλικού του μαθήματος.

1. Η ταξινομία Bloom είναι ένα ιεραρχικό μοντέλο που χρησιμοποιείται για την αξιολόγηση της μαθησιακής προόδου. Περιλαμβάνει διάφορα επίπεδα μάθησης, με την απομνημόνευση στη βάση και τη δημιουργία στην κορυφή. Ανάλογα με το επιθυμητό αποτέλεσμα, οι δραστηριότητες μπορούν να διαμορφώνονται κατά τέτοιο τρόπο ώστε να διασφαλίζεται ότι οι μαθητές επιτυγχάνουν τους μαθησιακούς τους στόχους.
2. Το μοντέλο των εννέα γεγονότων του Gagne είναι ένα πλήρες πλαίσιο διδακτικών γεγονότων που πρέπει να ληφθούν υπόψη για να εξασφαλιστεί η αποτελεσματική μάθηση. Τα γεγονότα αυτά περιλαμβάνουν την προσέλκυση της προσοχής, την ενημέρωση για τους στόχους, την αναδρομή σε προηγούμενες γνώσεις, την παρουσίαση του περιεχομένου, την παροχή καθοδήγησης, τη διευκόλυνση της εξάσκησης, την παροχή ανατροφοδότησης, την αξιολόγηση της επίδοσης και την ενίσχυση της συγκράτησης και της μεταφοράς.
3. Το μοντέλο ADDIE είναι ένα δομημένο πλαίσιο για το σχεδιασμό και την ανάπτυξη μαθημάτων, το οποίο αποτελείται από πέντε φάσεις: ανάλυση, σχεδιασμός, ανάπτυξη, υλοποίηση και αξιολόγηση. Το μοντέλο τονίζει τη σημασία της συνεχούς διόρθωσης και βελτίωσης καθ' όλη τη διάρκεια της διαδικασίας ανάπτυξης μαθημάτων.
4. Οι αρχές της Merrill προσδιορίζουν διάφορες αρχές που είναι κοινές στα αποτελεσματικά μοντέλα σχεδιασμού διδασκαλίας. Αυτές περιλαμβάνουν σχεδιασμό

με επίκεντρο το έργο/πρόβλημα, ενεργοποίηση προηγούμενων γνώσεων, επίδειξη νέων γνώσεων, εφαρμογή νέων γνώσεων και ενθάρρυνση της ενσωμάτωσης νέων γνώσεων.

5. Το μοντέλο των Dick και Carey, γνωστό και ως Μοντέλο Συστημικής Προσέγγισης, είναι ένα μοντέλο σχεδιασμού για την ανάπτυξη μαθημάτων. Καλύπτει τον καθορισμό διδακτικών στόχων, την εκπόνηση διδακτικής ανάλυσης, τον καθορισμό απαιτήσεων εισδοχής, τον καθορισμό στόχων επίδοσης και μέσων εξέτασης, την ανάπτυξη διδακτικής στρατηγικής και διδακτικών υλικών και τη διεξαγωγή διαμορφωτικών και αθροιστικών αξιολογήσεων. Το μοντέλο αυτό διασφαλίζει ότι το πλάνο του μαθήματος είναι περιεκτικό και καλύπτει όλες τις πτυχές της διδακτικής διαδικασίας.

Είναι σημαντικό να σημειωθεί ότι ενώ αυτές οι μεθοδολογίες παρέχουν ένα ολοκληρωμένο πλαίσιο για το σχεδιασμό και την ανάπτυξη μαθημάτων, μπορεί να μην ευθυγραμμίζονται πάντα απόλυτα με τους ειδικούς στόχους και πόρους ενός συγκεκριμένου μαθήματος. Στην πράξη, ίσως χρειαστεί να γίνουν τροποποιήσεις των καθορισμένων χαρακτηριστικών για να διασφαλιστεί ότι το μάθημα ανταποκρίνεται στους επιδιωκόμενους στόχους του. Οι εν λόγω μεθοδολογίες έχουν σχεδιαστεί για να λειτουργούν ως οδηγός και θα πρέπει να προσαρμόζονται ανάλογα με τις ιδιαίτερες ανάγκες και συνθήκες του μαθήματος. Απώτερος στόχος είναι η χρήση αυτών των μεθοδολογιών για τη δημιουργία αποδοτικών και ευχάριστων μαθησιακών εμπειριών για τους μαθητές. Παρόλο που παρέχουν μια στέρεη βάση για την ανάπτυξη μαθημάτων, θα πρέπει να εναρμονίζονται με τις ξεχωριστές ανάγκες κάθε μαθήματος, λαμβάνοντας υπόψη παράγοντες όπως το ακροατήριο, το αντικείμενο και τους διαθέσιμους πόρους.

5. Σχεδιάγραμμα διδασκαλίας μαθήματος

Λαμβάνοντας υπόψη τους καθορισμένους στόχους και πόρους για το σχεδιασμό του μαθήματος, υιοθετείται το ακόλουθο περίγραμμα:

1. Μαθησιακοί στόχοι: Να καλυφθεί το γνωστικό έλλειμμα της κυβερνοασφάλειας στα έξυπνα δίκτυα.
2. Προαπαιτούμενα: Το μάθημα απευθύνεται μόνο σε φοιτητές και επαγγελματίες με σχετικές γνώσεις στους τομείς της κυβερνοασφάλειας και των έξυπνων δικτύων.
3. Επίπεδο συγκράτησης που προβλέπεται από αυτό το μάθημα: 60% έως 75%, με στόχο την ενεργή συζήτηση και την απλή εξάσκηση με την πραγματοποίηση δραστηριοτήτων
4. Μεθοδολογίες εκπαιδευτικού σχεδιασμού που ακολουθούνται: Τα μοντέλα ADDIE και Dick και Carey για το σχεδιασμό και στόχευση στο τρίτο επίπεδο - εφαρμογή - της ταξινόμησης του Bloom για τη συγκράτηση.
5. Προσεγγίσεις που χρησιμοποιούνται: Κυρίως ανεστραμμένη μάθηση και παιχνιδοποίηση, με δραστηριότητες που προάγουν τη συνεργατική μάθηση
6. Μέθοδος παράδοσης: Εποπτευόμενες μαγνητοσκοπημένες συνεδρίες
7. Κριτήρια για την ενίσχυση της συγκέντρωσης και της συμμετοχής: Επιβραβεύσεις, χρήση παιχνιδιών και φόρουμ συζητήσεων
8. Αξιολόγηση και μέτρηση: Τακτικά κουίζ και τελική εξέταση, κατά προτίμηση αυτοματοποιημένη αυτοαξιολόγηση.
9. Φόρτος μαθήματος: 125-140 ώρες διαλέξεων, ασκήσεων και υλικού αυτομελέτης

6. Περιεχόμενο μαθήματος

Το μάθημα αποτελείται από τρία μέρη. Το πρώτο μέρος καλύπτει τα έξυπνα δίκτυα, την κυβερνοασφάλεια και τα δίκτυα. Το δεύτερο μέρος καλύπτει την προσομοίωση πραγματικού χρόνου, τη θεωρία. Τέλος, το τρίτο μέρος αφορά την ανάπτυξη πρακτικών δεξιοτήτων με την παροχή ασκήσεων και παραδειγμάτωνν. Τα εν λόγω τρία μέρη περιλαμβάνουν επτά κεφάλαια και τέσσερις πρακτικές ασκήσεις εξάσκησης. Στις επόμενες υποενότητες παρατίθενται συνοπτικά τα βασικά σημεία κάθε κεφαλαίου.

6.1 Μέρος 1: Έξυπνα δίκτυα, κυβερνοασφάλεια και δίκτυα

6.1.1 Κεφάλαιο 1: Βασικές αρχές των συστημάτων έξυπνου δικτύου

Το παρόν κεφάλαιο καλύπτει τις κύριες έννοιες των συστημάτων έξυπνων δικτύων, όπως: τα στοιχεία του έξυπνου δικτύου, τους οδηγούς συσκευής (drivers) των έξυπνων δικτύων, τα κύρια οφέλη και τις προκλήσεις που αντιμετωπίζει η εφαρμογή και η υλοποίηση του έξυπνου δικτύου, καθώς και το μοντέλο αρχιτεκτονικής ενός έξυπνου δικτύου. Το κεφάλαιο ξεκινά με παρουσίαση των τεχνολογιών έξυπνων δικτύων όσον αφορά το πλαίσιο, τις λειτουργίες και τις δυνατότητες, τους πόρους και τα συστήματα αποθήκευσης ενέργειας, τα μικροδίκτυα, τους έξυπνους υποσταθμούς και το πρωτόκολλο επικοινωνίας IEC 61850. Στη συνέχεια, αναφέρονται οι προκλήσεις και οι παράγοντες επιτυχίας του δικτύου, όπου παρουσιάζονται έξι προκλήσεις που περιλαμβάνουν τον επιχειρηματικό μετασχηματισμό, τη σύγκλιση των λειτουργιών, την προσέγγιση του ολοκληρωμένου συστήματος, την πολυπλοκότητα ενός ετερογενούς συστήματος, την κυβερνοασφάλεια και, τέλος, την προστασία της ιδιωτικής ζωής, ενώ έπονται οι βασικοί παράγοντες επιτυχίας του δικτύου. Οι τελευταίες ενότητες του κεφαλαίου περιλαμβάνουν τις παγκόσμιες πρωτοβουλίες για τα έξυπνα δίκτυα, ειδικά στην ευρωπαϊκή αγορά, και το μέλλον των έξυπνων δικτύων.

6.1.2 Κεφάλαιο 2: Κυβερνοασφάλεια και επιχειρησιακή ασφάλεια στα συστήματα έξυπνου δικτύου

Αυτό το κεφάλαιο καλύπτει πτυχές της ασφάλειας του δικτύου, συμπεριλαμβανομένης της πειρατείας δικτύου και των κύριων μεθόδων επίθεσης, των μοντέλων ασφάλειας για το σύστημα εποπτικού ελέγχου και συλλογής δεδομένων (SCADA), τα βιομηχανικά συστήματα ελέγχου (ICS) και το έξυπνο δίκτυο και, τέλος, καταλήγει στις μεθόδους ασφαλείας του έξυπνου δικτύου, συμπεριλαμβανομένης της διενέργειας ελέγχων ασφαλείας, της προστασίας των ζωνών πεδίου, της προστασίας των ζωνών ελέγχου, της προστασίας των ζωνών εξυπηρέτησης, της θέσπισης ισχυρών ορίων και διαχωρισμού ζωνών, της προηγμένης καθοδήγησης δικτύου, της προστασίας δεδομένων και εφαρμογών και της επίγνωσης της κατάστασης.

6.1.3 Κεφάλαιο 3: IEC 61850 και IEC 62351

Το IEC 61850 χρησιμοποιείται εδώ και πολύ καιρό ως το πρότυπο πρωτόκολλο για την επικοινωνία έξυπνων δικτύων. Το κεφάλαιο 3 καλύπτει τις κύριες πτυχές και την αρχιτεκτονική του εν λόγω προτύπου και εισάγει το συμπληρωματικό πρωτόκολλο ασφαλείας IEC 62351 που χρησιμοποιείται για τη δημιουργία ενός ακόμη επιπέδου ασφαλείας πέραν του IEC 61850.

6.2 Μέρος 2: Προσομοίωση σε πραγματικό χρόνο, η θεωρία

6.2.1 Κεφάλαιο 4: Βασικές αρχές της προσομοίωσης

Το παρόν κεφάλαιο καλύπτει τις βασικές έννοιες σχετικά με τις τεχνολογίες προσομοίωσης. Αυτό περιλαμβάνει διακριτά, συνεχή και υβριδικά μοντέλα, υβριδική προσομοίωση υψηλής ταχύτητας σε πραγματικό χρόνο, τυποποιημένη προσέγγιση για τη σχεδίαση κατανεμημένων συστημάτων, μοντελοποίηση με χρήση των γλωσσών Discrete Event System Specification (DEVS) και Unified Modeling Language (UML), καθώς και εργαλεία για την ενσωμάτωση με MATLAB και Simulink.

6.2.2 Κεφάλαιο 5: Προσομοίωση σε πραγματικό χρόνο για το σχεδιασμό συστημάτων

Αυτό το κεφάλαιο καλύπτει τις έννοιες του σχεδιασμού συστήματος, συμπεριλαμβανομένης της προοδευτικής προσομοίωσης, των εννοιών Hardware in the Loop (HIL) και Software in the Loop (SIL), της επικύρωσης και των εργαλείων επικύρωσης, και τέλος την έννοια της χρήσης ταχείας προτυποποίησης ελέγχου (RCP) για τη διευκόλυνση του σχεδιασμού και της δοκιμής του συστήματος.

6.2.3 Κεφάλαιο 6: Παράλληλη και κατανεμημένη προσομοίωση πραγματικού χρόνου

Στο κεφάλαιο αυτό παρουσιάζεται ένα περιβάλλον δοκιμών που χρησιμοποιεί το πρωτόκολλο DNP3 και στη συνέχεια δίνεται έμφαση στη χρήση της συστημικής προσέγγισης στην προσομοίωση για την εκπαίδευση.

6.2.4 Κεφάλαιο 7: Εργαλεία και εφαρμογές

Στο κεφάλαιο αυτό παρουσιάζεται η έννοια της διαστολής του χρόνου, με την οποία μπορεί να επιτευχθεί ακριβής προσομοίωση σε συστήματα μεγάλης κλίμακας. Εισάγονται επίσης συναφείς έννοιες όπως τα εικονικά συστήματα, ο χρονοπρογραμματισμός της CPU, η προσομοίωση δικτύου και η εξομοίωση μνήμης.

6.3 Μέρος 3: Ασκήσεις και παραδείγματα

6.3.1 Άσκηση 1

Εγχειρίδιο για την έναρξη χρήσης του προσομοιωτή πραγματικού χρόνου EXATA CPS και HYPERSIM OPAL-RT

6.3.2 Άσκηση 2

Προσομοιώσεις σε πραγματικό χρόνο ενός μικροδικτύου ενεργού διαχείρισης ισχύος έναντι επίθεσης καθυστέρησης

6.3.3 Άσκηση 3

Προσομοιώσεις σε πραγματικό χρόνο ενός μικροδικτύου ενεργού διαχείρισης ισχύος έναντι επίθεσης τροποποίησης πακέτων δεδομένων

6.3.4 Άσκηση 4

Προσομοιώσεις σε πραγματικό χρόνο ενός μικροδικτύου με βάση το Hardware in the Loop HIL του ελεγκτή

7. Εργαλεία

Τα εργαλεία που χρησιμοποιήθηκαν κατά τη διάρκεια αυτού του μαθήματος περιλαμβάνουν υποστηρικτικά εκπαιδευτικά εργαλεία και εργαλεία για ασκήσεις και πρακτικές δεξιότητες, ως εξής:

1. Υποστηρικτικά εκπαιδευτικά εργαλεία: Πρόκειται για τα εργαλεία που χρησιμοποιούνται για την υποστήριξη της εκπαιδευτικής διαδικασίας. Εν προκειμένω, δεδομένου ότι το προσφερόμενο μάθημα έχει τη μορφή MOOC, χρησιμοποιείται ένα ειδικό αποθετήριο (MOODLE) για τη διατήρηση του μαθησιακού υλικού, των φόρουμ συζητήσεων, των κουίζ και των διαδικτυακών εξετάσεων. Άλλα εργαλεία που μπορούν να χρησιμοποιούνται περιλαμβάνουν διαθέσιμα εργαλεία επικοινωνίας και μετάδοσης βίντεο, καθώς και εργαλεία για το σχεδιασμό παρουσιάσεων και την επεξεργασία βίντεο.
2. Εργαλεία πρακτικών δεξιοτήτων: Στο συγκεκριμένο μάθημα, το σύστημα OPAL-RT, το οποίο είναι ένας προσομοιωτής πραγματικού χρόνου, χρησιμοποιείται για τη διενέργεια εκπαιδευτικών συνεδριών και την εκμάθηση των δεξιοτήτων που αναφέρονται στους στόχους του μαθήματος.

8. Βιβλιογραφία

[1] Ευρωπαϊκή Τεχνολογική Πλατφόρμα, Ευρωπαϊκή Επιτροπή, “Strategic deployment document for Europe electricity networks of the future” (Στρατηγικό έγγραφο ανάπτυξης για την Ευρώπη των δικτύων ηλεκτρικής ενέργειας του μέλλοντος), Απρίλιος του 2010.

[2] Elzinga, David. "Electricity system development: A focus on smart grids. overview of activities and players in smart grids." (Ανάπτυξη του συστήματος ηλεκτρικής ενεργείας: Έμφαση στα έξυπνα δίκτυα. Επισκόπηση των δραστηριοτήτων και των φορέων στα έξυπνα δίκτυα.) UNECE. www. unece. org/fileadmin/DAM/energy/se/pdfs/eneff/eneff_h. news/Smart. Δίκτυα. Επισκόπηση. pdf, (2015).

[3] Ευρωπαϊκή Επιτροπή (2020). Η Ευρώπη επενδύει στην ψηφιακή τεχνολογία: το πρόγραμμα «Ψηφιακή Ευρώπη». https://digital-strategy.ec.europa.eu/el/activities/digital-programme

[4] ITU. 2009. Επισκόπηση της κυβερνοασφάλειας. Σύσταση ITU-T X.1205. Γενεύη: Διεθνής Ένωση Τηλεπικοινωνιών (ITU). https://www.itu.int/rec/T-REC-X.1205-200804-I/en

[5] Young, Susan, και Dave Aitel. The hacker's handbook: the strategy behind breaking into and defending networks. (Το εγχειρίδιο του χάκερ: η στρατηγική της παραβίασης και υπεράσπισης δικτύων.) Εκδόσεις Auerbach, 2003.

[6] Vacca, John R., ed. Managing information security. Elsevier, 2013.

[7] Romanovs, Andrejs, et al. "State of the Art in Cybersecurity and Smart Grid Education.'' (Η εξέλιξη της τεχνολογίας στην εκπαίδευση για την κυβερνοασφάλεια και το έξυπνο δίκτυο.) IEEE EUROCON 2021-19ο Διεθνές Συνέδριο για τις Έξυπνες Τεχνολογίες. IEEE, 2021.

[8] Valliou, Maria, et al. "Strategy for Cybersecurity Education in Smart Grids.'' (Στρατηγική για την εκπαίδευση στον τομέα της κυβερνοασφάλειας στα έξυπνα δίκτυα.) (2022).

[9] González-Manzano, Lorena, και Jose M. de Fuentes. "Design recommendations for online cybersecurity courses.'' (Συστάσεις σχεδιασμού για διαδικτυακά μαθήματα κυβερνοασφάλειας.) Computers & Security 80 (2019): 238-256.

[10] Scott, Bernard, και Chunyu Cong. "Knowledge and task analysis methods for course design.'' (Μέθοδοι ανάλυσης γνώσεων και δραστηριοτήτων για το σχεδιασμό μαθημάτων.) Readings in Technology in Education: Proceedings of the International Conference on Information Communications Technologies in Education. 2007.

[11] Arora, Bela. "Teaching cyber security to non-tech students.» (Διδασκαλία της κυβερνοασφάλειας σε άτομα που δεν είναι φοιτητές τεχνολογικών σπουδών.) Politics 39.2 (2019): 252-265.

[12] A comprehensive guide. John Wiley & Sons, 2020.

[13] Becker, S. Adams, et al. NMC horizon report: 2017 higher education edition. The New Media Consortium, 2017.

[14] Shi, Yinghui, et al. "Examining interactive whiteboard-based instruction on the academic self-efficacy, academic press and achievement of college students.» (Εξέταση της διδασκαλίας με διαδραστικό πίνακα στην ακαδημαϊκή αυτεπάρκεια, τον ακαδημαϊκό τύπο και την επίδοση των φοιτητών.) Open Learning: The Journal of Open, Distance and e-Learning 33.2 (2018): 115-130.

[15] Hall, Steven R., et al. "Adoption of active learning in a lecture-based engineering class.» (Υιοθέτηση ενεργητικής μάθησης σε ένα μάθημα μηχανικής με διαλέξεις.) 32nd Annual frontiers in education. Vol. 1. IEEE, 2002.

[16] Kolb, David A. Experiential learning: Experience as the source of learning and development. FT press, 2014.

[17] Felder, Richard M., and Rebecca Brent. "Active learning: An introduction.'' (Ενεργητική μάθηση:
Εισαγωγή.) ASQ higher education brief 2.4 (2009): 1-5.

[18] Felder, Richard M., and Rebecca Brent. "Cooperative learning.'' (Συνεργατική μάθηση.) Active learning: Models from the analytical sciences 970 (2007): 34-53.

[19] Bergmann, Jonathan, and Aaron Sams. Flipped learning: Gateway to student engagement. International Society for Technology in Education, 2014.
[20] Keselman, Alla. "Supporting inquiry learning by promoting normative understanding of multivariable causality.'' (Υποστήριξη της διερευνητικής μάθησης με την προώθηση της νοερής κατανόησης της πολυπαραγοντικής αιτιότητας.) Journal of Research in Science Teaching 40.9 (2003): 898-921.
[21] English, Mary C., and Anastasia Kitsantas. "Supporting student self-regulated learning in problem-and project-based learning.'' (Υποστήριξη της αυτοελεγχόμενης μάθησης στη μάθηση που βασίζεται σε προβλήματα και έργα.) Interdisciplinary journal of problem-based learning 7.2 (2013): 6.
[22] Deterding, Sebastian, et al. "From game design elements to gamefulness: defining" gamification". (Από τα στοιχεία σχεδιασμού παιχνιδιών στην παιχνιδιάρικη διάθεση: ο ορισμός της «παιχνιδοποίησης».) Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments. 2011.
[23] Lalley, J., and R. Miller. "The learning pyramid: Does it point teachers in the right direction." (Η πυραμίδα της μάθησης: Δείχνει στους εκπαιδευτικούς τη σωστή κατεύθυνση;) Education 128.1 (2007): 16.
[24] Reigeluth, Charles M. "Instructional design: What is it and why is it.» (Εκπαιδευτικός σχεδιασμός:
Τι είναι και γιατί είναι.) Instructional-design theories and models: An overview of their current status 1 (1983): 3-36.
[25] Spector, J. Michael. Foundations of educational technology: Integrative approaches and interdisciplinary perspectives. Routledge, 2015.
[26] Huang, Ronghuai, J. Michael Spector, και Junfeng Yang. Educational technology a primer for the 21st century. Springer, 2019.
[27] Brown, Abbie H., and και D. Green. The essentials of instructional design: Connecting fundamental principles with process and practice. Routledge, 2015.
[28] Faruque, MD Omar, et al. "Real-time simulation technologies for power systems design, testing, and analysis.» (Τεχνολογίες προσομοίωσης σε πραγματικό χρόνο για το σχεδιασμό, τη δοκιμή και την ανάλυση συστημάτων ηλεκτρικής ενέργειας.) IEEE Power and Energy Technology Systems Journal 2.2 (2015): 63-73.
[29] Popovici, Katalin, και Pieter J. Mosterman, eds. Real-time simulation technologies: Principles, methodologies, and applications. CRC Press, 2017.
[30] Poudel, Shiva, Zhen Ni, και Naresh Malla. "Real-time cyber physical system testbed for power system security and control.'' (Δοκιμαστικό περιβάλλον φυσικού συστήματος στον κυβερνοχώρο σε πραγματικό χρόνο για την ασφάλεια και τον έλεγχο του συστήματος ηλεκτρικής ενέργειας.) International Journal of Electrical Power & Energy Systems 90 (2017): 124-133.
[31] "SCALABLE and OPAL-RT Innovate Cyber-Physical Solution." (SCALABLE και OPAL-RT καινοτομούν στη δημιουργία λύσης κυβερνο-φυσικής.) Scalable Network Technologies, 5 July 2017, www.scalable-networks.com/news/scalable-and-opal-rt-innovate-cyber-physical-solution.