Reāllaika fiziskā kiberdrošība
Plašs atvērtais tiešsaistes kurss MOOC – skolotāja rokasgrāmata

(Izpildpārskats)

Autori:

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

Kiberdrošības mācību programmu ieteikumi viedtīkliem (CC-RSG)

Erasmus+ stratēģiskās partnerības projekts

Intellectual Output 3

Vāsas Universitāte, Atēnu Nacionālā tehniskā universitāte, Rīgas Tehniskā universitāte, Oldenburgas Universitāte

Šis projekts ir saņēmis Eiropas Savienības Erasmus+ programmas finansējumu dotāciju līguma № 2020-1-FI01-KA203-066624 ietvaros.

Saturs

Saturs 2
Definīcijas, akronīmi un saīsinājumi 3
1. Ievads 4
1.1 Mērķi 5
1.2 Dokumenta uzbūve 5
2. Kursa dizaina metodoloģija 5
3. Izglītības metodoloģiju pārskats 5
4. Mācību dizaina modeļi 6
5. Kursu dizaina izklāsts 7
6. Kursa saturs 8
6.1 1. daļa: Viedtīkli, kiberdrošība un tīkli 8
6.1.1 1. nodaļa: Viedtīklu sistēmu pamati 8
6.1.2 2. nodaļa: Kiberdrošība un darbības drošība viedtīklu sistēmās 8
6.1.3 3. nodaļa: IEC 61850 un IEC 62351 8
6.2 2. daļa: Reāllaika simulācija, teorija 8
6.2.1 4. nodaļa: Simulācijas pamati 8
6.2.2 5. nodaļa: Sistēmas dizaina reāllaika simulācija 9
6.2.3 6. nodaļa: Paralēla un sadalīta reāllaika simulācija 9
6.2.4 7. nodaļa: Rīki un pielietošanas jomas 9
6.3 3. daļa: Uzdevumi un gadījumu scenāriji 9
6.3.1 1. uzdevums 9
6.3.2 2. uzdevums 9
6.3.3 3. uzdevums 9
6.3.4 4. uzdevums 9
7. Rīki 10
8. Bibliogrāfija 10

Definīcijas, akronīmi un saīsinājumi

ADDIE Analyze, Design, Develop, Implement, and Evaluate (Analizēt, projektēt, attīstīt, ieviest un izvērtēt)

CC-RSG Cybersecurity Curricula Recommendations for Smart Grid (Kiberdrošības mācību programmu ieteikumi viedtīkliem)

CI Critical Infrastructure (Kritiskā infrastruktūra)

CPS Cyber-physical Systems (Kiberfiziskās sistēmas)

DEVS Discrete Event System Specification (Diskrētas notikumu sistēmas specifikācija)

HIL Hardware in the Loop (Aparatūra cilpā)

ICS Industrial Control Systems (Industriālās vadības sistēmas)

ID Instructional Design (Mācību dizains)

IO Intellectual Output (Intelektuālais rezultāts)

MOOC Massive Open Online Course (Plašs atvērtais tiešsaistes kurss)

RCP Rapid Control Prototyping (Ātrās kontroles prototipēšana)

RT Real-time (Reāllaika)

SCADA Supervisory Control and Data Acquisition (Uzraudzības kontrole un datu iegūšana)

SIL Software in the Loop (Programmatūra cilpā)

SPSP Smart Power Security Professional

UML Unified Modeling Language (Vienotā modelēšanas valoda)

WP Work Package (Darba kopa)

1. Ievads

Pēdējā laikā enerģētikas sektorā ir notikušas būtiskas pārmaiņas, kas novedušas pie viedtīklu koncepcijas rašanās. Viedtīkls attiecas uz elektrotīklu, kas integrē visu lietotāju, tostarp radītāju, patērētāju un abu, darbības un uzvedību ar mērķi efektīvi nodrošināt ilgtspējīgu, ekonomisku un drošu elektrības padevi. Viedtīklu kiberdrošība ir kļuvusi par kritisku problēmu, kura ir jārisina pieaugošās uzbrukuma virsmas un saistīto līdzekļu kritiskuma dēļ. Kiberdrošība ir viena no svarīgākajām digitālajām spējām, ko Eiropas Savienība vēlas sasniegt. Tā ietver vairākus aspektus, piemēram, rīkus, politikas, drošības koncepcijas, drošības pasākumus, vadlīnijas, riska pārvaldības metodes, darbības, apmācību, labāko praksi, garantijas un tehnoloģijas, ko var izmantot, lai aizsargātu organizāciju un lietotāja īpašumus un kibervidi. Neskatoties uz to, ka ir pieejami daudzi dažādu nodrošinātāju rīki un programmatūras pakotnes, kas nodrošina drošības vajadzības un tīkla noturību, kiberdrošība joprojām ir svarīga problēma.

Kiberdrošības mācību programmu ieteikumi viedtīkliem (CC-RSG) ir projekts, kas iedziļinājās viedtīklu kiberdrošības problēmā, izmantojot aptaujas, recenzijas un seminārus. Pētījuma rezultātā ir izdarīti tālāk minētie secinājumi.

1. Pašreizējā pieeja kiberdrošības jautājumu risināšanai viedtīklos ir nepietiekama.
2. Viedtīklu jomā trūkst kiberdrošības speciālistu, jo trūkst izglītības programmu, kas praktiski aptver šo specifisko jomu.
3. Esošie izglītības piedāvājumi neatbilst Smart Power Security Professional (SPSP) prasībām.
4. Trūkst reālu scenāriju un saistības ar industriju.

Svarīga nepieciešamība ir nodrošināt izglītības iespējas, kas var uzlabot prasmes un novērst iepriekš minētās nepilnības, jo īpaši ņemot vērā iepriekšējos pārskatus, kuros uzsvērts, ka vismaz 50 % kiberdrošības incidentu izraisa cilvēku kļūdas. Lai risinātu šo problēmu, CC-RSG projekts cenšas palīdzēt augstākās izglītības iestādēm integrēt ar viedtīklu kiberdrošību saistītus mācību rezultātus savās mācību programmās. Šajā pārskatā ir sniegts kursa izklāsts, kas tika izstrādāts, lai risinātu šo problēmu.

Šajā pārskatā ir sniegti īsi CC-RSG projekta 3. darba kopas (WP) “Projektēšana, izstrāde un pilotēšana” – Intelektuālais rezultāts (IO) 3 – rezultāti. Tādējādi pārskats ir balstīts uz iepriekšējo pārskatu un IO rezultātiem, lai nodrošinātu plašu atvērto tiešsaistes kursu (MOOC) reāllaika fiziskās kiberdrošības sistēmām. Kursa mērķis ir novērst atklātās nepilnības kiberfizikālajās sistēmās (CPS), kā arī attīstīt prasmes reāllaika simulācijas sistēmās, kuras tiek izmantotas ātrgaitas simulācijām, kritiskās infrastruktūras (CI) testēšanai, un drošības darbību un funkciju izvērtēšanai. Lai izstrādātu kursu, ir izpētītas un pārbaudītas dažādas pieejas, lai atrastu vispiemērotākās metodes, kas kalpo kursa izveides mērķim un izcelto prasmju nepilnību novēršanai. Tādēļ kursā ir jāizmanto šādas pieejas: apgriezta mācīšanās, simulācijas un virtuālās un attālinātās laboratorijas. Šīs pieejas tika rūpīgi atlasītas, pamatojoties uz to spējām nodrošināt mijiedarbības līdzekļus, attīstīt analītiskās un problēmu risināšanas prasmes, kā arī veicināt praktiskās prasmes.

IO3 kursa pārskata galvenie ieguldījumi ir:

1. Sniegt teorētisku pamatinformāciju par reāllaika simulācijas sistēmām.
2. Veidot praktiskas prasmes izmantot reāllaika simulāciju.
3. Ieviest un izmantot pielietošanas gadījumus, scenārijus un treniņu un apmācību uzdevumus.

IO3 kursa pārskatā “Reāllaika fiziskās kiberdrošības plašs atvērtais tiešsaistes kurss MOOC – skolotāja rokasgrāmata” ir apskatītas teorētiskās un pamatzināšanas, radot spēcīgu pamatu un sniedzot svarīgākās zināšanas par viedtīkliem, viedtīklu komunikācijas protokoliem un viedtīklu kiberdrošību. Turklāt īpaša uzmanība ir pievērsta reāllaika simulācijas sistēmām, jo tās ir atzītas par vienu no nišas līderiem un efektīvākajiem instrumentiem kritiskās infrastruktūras un viedtīklu eksperimentēšanai, testēšanai un apguvei. Attiecīgi ir prezentētas daudzas reāllaika simulācijas koncepcijas. Turklāt kurss koncentrējas ne tikai uz teorētiskajām zināšanām, bet arī apskata nozarē nepieciešamās praktiskās prasmes. Tādēļ tika izveidoti četri vingrinājumi, pamatojoties uz izvēlētiem industrijas scenārijiem, un tika īstenoti, izmantojot fizisku reāllaika simulatora sistēmu.

Visbeidzot, IO3 kursa dizaina pārskats kalpo kā skolotāja rokasgrāmata. Tādējādi, veidojot kursu, mēs centāmies apkopot visu nepieciešamo informāciju, lai vispusīgi aptvertu viedtīklu kiberdrošības tēmu. Lai izmantotu šo pārskatu, skolotājiem/instruktoriem ir ieteicams izmantot šeit pieejamo materiālu, veidojot prezentācijas un izdales materiālus, kā arī, tā kā uzsvars tiek likts uz apgriezto mācīšanos un MOOC, ir ieteicams izveidot iepriekš ierakstītus videoklipus un automatizētus uzdevumus.

1.1 Mērķi

IO3 galvenais mērķis ir radīt kursu, kas sniedz dalībniekiem zināšanas, kas nepieciešamas, lai uzsāktu darbību CPS jomā, jo īpaši viedtīklu kiberdrošībā.

1.2 Dokumenta uzbūve

- 2. sadaļā ir pieejama kursa dizaina metodoloģija
- 3. sadaļā ir pārskats par izglītības metodoloģiju un izmantotajām mācību pieejām
- 4. sadaļā ir uzskaitīti vispārīgie mācību dizaina (ID) modeļi
- 5. sadaļā ir pieejama kursa dizaina izklāsts
- 6. sadaļā ir pieejams kursa saturs un īsumā apskatīti temati
- Noslēdzošajā 7. sadaļā ir uzskaitīti izmantotie rīki

2. Kursa dizaina metodoloģija

Lai efektīvi izstrādātu kursu, tika izmantoti šādi procesi:

1. Uzsvara likšana uz kursa dizaina nepieciešamību
2. Gadījuma un kursa konteksta noteikšana
3. Mērķu un vēlamā rezultāta noteikšana
4. Mācību metodoloģijas un aktivitāšu noteikšana
5. Kursa satura noteikšana
6. Izvērtēšanas kritēriju izvēle
7. Izstrādāšana un ieviešana

3. Izglītības metodoloģiju pārskats

Izglītības metodoloģijas nozīmi nedrīkst novērtēt par zemu, jo tā nosaka veidus, kā tiek sasniegti un novērtēti mācību mērķi. Pirmkārt, ir pieejamas dažādas izglītības metodoloģijas

un tehnikas atkarībā no vēlamā zināšanu uzturēšanas līmeņa. Tās ietver uz lekcijām balstītas mācības, mācīšanos ar pieredzes gūšanu, aktīvu mācīšanos, kooperatīvu mācīšanos, apgrieztu mācīšanos, uz vaicājumiem balstītu mācīšanos, uz problēmām un projektiem balstītu mācīšanos un spēļu izmantošanu, kā norādīts tālāk.

1. Parastā mācīšanās metode – uz lekcijām balstīta mācīšanās – paredz, ka pasniedzējs nodrošina kursa materiālu, veic novērtējumus un uzņemas pilnu atbildību par izglītības pieredzi. Tomēr šī metode pamatā ir pasīva un lielā mērā balstās uz informācijas atcerēšanos. Iekļaujot tādas aktivitātes kā zvanīšana, diskusijas, mācību kartes un citus interaktīvus elementus, uz lekcijām balstītu mācīšanos var pārvērst par aktīvu un efektīvāku pieeju.
2. Mācīšanās no pieredzes ir aktīva pieeja mācībām, kas prasa studentiem iesaistīties mācību procesā un mācoties attīstīt pieredzi. No otras puses, aktīvā mācīšanās ir ne tikai aktivitāšu iekļaušana un līdzdalības veicināšana, bet arī visu izglītojamo reakciju apstrāde pirms jaunas informācijas sniegšanas.
3. Kooperatīvā mācīšanās ir uz grupu balstīta pieeja, kurā dalībnieki sadarbojas, lai sasniegtu konkrētus mērķus un uzņemtos pilnu atbildību par uzdevuma izpildi. Apgrieztā mācīšanās ir mūsdienīga pieeja, kas ļauj apmācāmajiem uzņemties atbildību par savu mācīšanos, viņiem iepriekš nodrošinot izglītojošus materiālus, tādējādi nodrošinot dinamiskāku un interaktīvāku mācību pieredzi.
4. Uz vaicājumiem balstīta mācīšanās ir pieeja, kurā studenti izmanto tādu pašu praksi kā profesionāli zinātnieki, lai iegūtu zināšanas un pieredzi. Uz problēmām un projektiem balstītā mācīšanās aktīvi iesaista dalībniekus mācību procesā, izpētot konkrētu problēmu vai jautājumu ar mērķi rast atbildes vai izstrādāt risinājumu.
5. Visbeidzot, spēļu izmantošana izmanto spēlei līdzīgas funkcijas, piemēram, stāstu stāstīšanu, līmeņa pārsniegšanu un nozīmītes, lai veicinātu līdzdalību un padarītu mācību procesu saistošāku. Izmantojot šīs dažādās pieejas, pedagogi var radīt efektīvāku un saistošāku mācību vidi saviem studentiem.

Otrkārt, iepriekš minētās izglītības metodoloģijas parasti tiek izmantotas, lai atspoguļotu zināšanu uzturēšanas līmeni, ko nosaka kursa mērķi un pieejamie resursi. Jāņem vērā, ka, jo lielāka ir iesaistīšanās mācību procesā, jo augstāks ir uzturēšanas līmenis; tomēr ir nepieciešams arī vairāk resursu. Tālāk ir norādīts dažādu mācību aktivitāšu uzturēšanas līmenis:

1. Parastā metode un lekcijas: 5%
2. Lasīšana un neatkarīga mācīšanās: 10%
3. Audiovizuālās ilustrācijas: 20%
4. Demonstrēšana un daļēji aktīva dalība: 30%
5. Plānošana, diskusijas un aktīva dalība: 50%
6. Mācīšanās darot: 75%
7. Citu mācīšana: 90%

Veidojot kursu, ir svarīgi vispirms definēt, kurš uzturēšanas līmenis ir vēlams, un tādējādi pielāgot darba apjomu un resursus, lai tie atbilstu šim kritērijam.

4. Mācību dizaina modeļi

Tā kā IO3 ir par kursu dizainu, tālāk minētie vispārīgie ID modeļi tika izmantoti, lai palīdzētu definēt mērķus, izvēlēties aktivitātes un kursa materiālu.

1. Blūma Taksonomija ir hierarhisks modelis, ko izmanto mācību progresa novērtēšanai. Tā ietver dažādus mācīšanās līmeņus, kuru apakšdaļā ir atcerēšanās, bet augšdaļā – radīšana. Atkarībā no vēlamā rezultāta aktivitātes var attiecīgi pielāgot, lai nodrošinātu, ka studenti sasniedz savus mācību mērķus.
2. Gaņjē Deviņu mācību notikumu modelis ir visaptverošs mācību pasākumu ietvars, kas jāņem vērā, lai nodrošinātu efektīvu mācīšanos. Šie notikumi ietver uzmanības piesaistīšanu, mērķu paziņošanu, iepriekšējo zināšanu atsaukšanu, satura prezentēšanu, norādījumu sniegšanu, prakses veicināšanu, atgriezeniskās saites sniegšanu, snieguma novērtēšanu un saglabāšanas un nodošanas uzlabošanu.
3. ADDIE modelis ir strukturēts ietvars kursu izstrādei un radīšanai, kas sastāv no pieciem posmiem: Analizēt, projektēt, attīstīt, ieviest un izvērtēt. Šis modelis uzsver nepārtrauktas pārskatīšanas un uzlabošanas nozīmi visā kursa izstrādes procesā.
4. Merila principi nosaka vairākus principus, kas kopīgi efektīviem mācību dizaina modeļiem. Tie ietver uz uzdevumu/problēmu vērstu dizainu, iepriekšējo zināšanu aktivizēšanu, jaunu zināšanu demonstrēšanu, jaunu zināšanu pielietošanu un jaunu zināšanu integrācijas veicināšanu.
5. Dika un Kerija modelis, kas pazīstams arī kā Sistēmu pieejas modelis, ir plānošanas modelis mācību stundu izstrādei. Tas ietver mācību mērķu noteikšanu, mācības analīzes veikšanu, sākuma prasību noteikšanu, snieguma mērķu un testa priekšmetu norādīšanu, apmācības stratēģijas un materiālu izstrādi, kā arī veidojošo un apkopojošo novērtējumu veikšanu. Šis modelis nodrošina, ka mācību stundu plāns ir visaptverošs un aptver visus mācības procesa aspektus.

Ir svarīgi atzīmēt, ka, lai gan šīs metodoloģijas nodrošina visaptverošu sistēmu kursu izstrādei un izveidei, tās ne vienmēr var pilnībā saskaņot ar konkrēta kursu piedāvājuma specifiskajiem mērķiem un resursiem. Praksē var būt nepieciešams veikt noteikto atribūtu korekcijas, lai nodrošinātu, ka kurss atbilst paredzētajiem mērķiem. Šīs metodoloģijas ir paredzētas kā ceļvedis, un tās ir jāpielāgo, lai tās atbilstu kursa unikālajām vajadzībām un apstākļiem. Galīgais mērķis ir izmantot šīs metodoloģijas, lai studentiem sniegtu efektīvu un saistošu mācību pieredzi. Lai gan tās nodrošina stabilu pamatu kursu izstrādei, tās ir jāpielāgo katra kursa īpašajām vajadzībām, ņemot vērā tādus faktorus kā auditorija, priekšmets un pieejamie resursi.

5. Kursu dizaina izklāsts

Balstoties uz kursa izstrādes noteiktajiem mērķiem un resursiem, tiek pieņemts šāds izklāsts:

1. Mācību mērķi: Nosegt zināšanu trūkumus par kiberdrošību viedtīklu jomā.
2. Priekšnoteikumi: Kursam ir jābūt pieejamam tikai studentiem un profesionāļiem ar priekšzināšanām kiberdrošības un viedtīklu jomā.
3. Šī kursa prognozētais uzturēšanas līmenis: 60% līdz 75%, tiecoties uz aktīvām diskusijām un vienkāršu praksi, veicot uzdevumus.
4. Pieņemtās mācību dizaina metodoloģijas: ADDIE un Dika un Kerija dizina modeļi, un mērķēšana uz trešo līmeni – uzturēšanai izmantot Blūma Taksonomiju.
5. Izmantotās pieejas: Galvenokārt apgrieztā mācīšanās un spēļu izmantošana ar uzdevumiem, kas veicina kooperatīvu mācīšanos.
6. Mācību nodrošināšanas metode: Uzraudzītas ierakstītas sesijas
7. Kritēriji, lai veicinātu uzmanību un iesaistīšanos: Bonusa punkti, spēļu izmantošana un diskusiju forumi.
8. Novērtēšana un mērīšana: Regulāri pārbaudes darbi un gala eksāmens; vēlams automatizēti pašvērtējuma.

9. Kursa slodze: 125 līdz 140 lekciju stundas, uzdevumi un individuālu mācību materiāls.

6. Kursa saturs

Izveidotais kurss ir iedalīts trīs daļās. Pirmā daļa aplūko viedtīklus, kiberdrošību un tīklus. Otrajā daļā ietverta reāllaika simulācija un teorija. Un trešā daļa ir veltīta praktisko prasmju veidošanai, nodrošinot uzdevumus uzdevumi un gadījumu scenārijus. Minētās trīs daļas ietver septiņas nodaļas un četrus praktiskus treniņuzdevumus. Nākamajās apakšsadaļās īsumā ir izklāstīti katras nodaļas galvenie punkti.

6.1 1. daļa: Viedtīkli, kiberdrošība un tīkli

6.1.1 1. nodaļa: Viedtīklu sistēmu pamati

Šajā nodaļā ir apskatīti viedtīklu sistēmu galvenie jēdzieni, tostarp: viedtīklu komponenti, viedtīklu draiveri, galvenie ieguvumi un izaicinājumi, ar kuriem saskaras viedtīkla ieviešana un realizācija, un viedtīkla arhitektūras modelis. Nodaļa turpinās ar viedtīklu tehnoloģiju ieviešanu attiecībā uz struktūru, funkcionalitāti un iespējām, resursiem un enerģijas uzglabāšanas sistēmām, mikrotīkliem, viedajām apakšstacijām un sakaru protokolu IEC 61850. Tālāk aplūkoti ar tīklu saistītie izaicinājumi un veiksmes faktori, kuros tiek ieviesti 6 izaicinājumi, kas ietver biznesa transformāciju, darbību konverģenci, integrētu sistēmu pieeju, heterogēnas sistēmas sarežģītību, kiberdrošību un visbeidzot privātumu, kam seko galvenie tīkla veiksmes faktori. Visbeidzot, nodaļas pēdējās sadaļās ir iekļautas globālās iniciatīvas saistībā ar viedtīkliem, jo īpaši Eiropas tirgū, un viedtīklu nākotne.

6.1.2 2. nodaļa: Kiberdrošība un darbības drošība viedtīklu sistēmās

Šajā nodaļā ir apskatīti tīkla drošības aspekti, tostarp tīkla uzlaušana un galvenās uzbrukuma metodes, uzraudzības kontroles un datu iegūšanas (SCADA), industriālās vadības sistēmas (ICS) un viedtīkla drošības modeļi, un visbeidzot ir norādītas viedtīkla drošības metodes, tostarp drošības kontroles ieviešana, lauka zonu aizsardzība, kontroles zonu aizsardzība, apkalpošanas zonu aizsardzība, stingru robežu noteikšana un zonu atdalīšana, progresīvs tīkla mentorings, datu un lietojumprogrammu aizsardzība un situācijas apzināšanās.

6.1.3 3. nodaļa: IEC 61850 un IEC 62351

IEC 61850 jau ilgu laiku izmanto kā standartizētu protokolu viedtīklu komunikācijai. Šajā nodaļā ir apskatīti šī standarta galvenie aspekti un arhitektūra, kā arī sniegts ievads papildu drošības protokolam IEC 62351, kuru izmanto, lai izveidotu drošības slāni papildus IEC 61850.

6.2 2. daļa: Reāllaika simulācija, teorija

6.2.1 4. nodaļa: Simulācijas pamati

Šajā nodaļā aplūkoti galvenie koncepcijas saistībā ar simulācijas tehnoloģijām. Tas ietver diskrētus, nepārtrauktus un hibrīdus modeļus, liela ātruma reāllaika hibrīda simulāciju,

formalizētu pieeju sadalīto sistēmu projektēšanai, modelēšanu, izmantojot diskrētās notikumu sistēmas specifikācijas (DEVS) un vienotās modelēšanas valodas (UML), kā arī rīkus integrācijai ar MATLAB un Simulink.

6.2.2 5. nodaļa: Sistēmas dizaina reāllaika simulācija

Šajā nodaļā ir apskatīti sistēmas dizaina jēdzieni, tostarp progresīvā simulācija, aparatūra cilpā (HIL) un programmatūra cilpā (SIL) koncepcijas, validācijas un validētāja rīki un visbeidzot ātrās kontroles prototipēšanas (RCP) izmantošanas koncepcija, lai atvieglotu sistēmas dizainu un testēšanu.

6.2.3 6. nodaļa: Paralēla un sadalīta reāllaika simulācija

Šī nodaļa iepazīstina ar testa platformu, kurā tiek izmantots DNP3 protokols, un pēc tam tiek uzsvērta sistēmas pieejas izmantošana mācību simulācijā.

6.2.4 7. nodaļa: Rīki un pielietošanas jomas

Šajā nodaļā ir izklāstīta laika dilatācijas koncepcija, tādējādi var panākt precīzu simulāciju lielizmēra sistēmās. Tiek ieviesti arī ar to saistītie jēdzieni, piemēram, virtualizētas sistēmas, CPU plānošana, tīkla emulācija un atmiņas emulācija.

6.3 3. daļa: Uzdevumi un gadījumu scenāriji

6.3.1 1. uzdevums

Rokasgrāmata darba sākšanai ar reāllaika simulatoru EXATA CPS un HYPERSIM OPAL-RT

6.3.2 2. uzdevums

Mikrotīkla aktīvās jaudas pārvaldības reāllaika simulācijas pret aizkavētu uzbrukumu

6.3.3 3. uzdevums

Mikrotīkla aktīvās jaudas pārvaldības reāllaika simulācijas pret modificētu datu pakešu uzbrukumu

6.3.4 4. uzdevums

Mikrotīkla kontrollera aparatūras cilpā HIL reāllaika simulācijas

7. Rīki

Šajā kursā izmantotie rīki ietver mācīšanās palīgrīkus un rīkus uzdevumiem un praktiskām prasmēm, kā norādīts tālāk.

1. Mācīšanās palīgrīki: Šie ir rīki, ko izmanto mācību procesa atvieglošanai. Tā kā piedāvātais kurss ir MOOC formātā, mācību materiālu, diskusiju forumu, viktorīnu un tiešsaistes eksāmenu izvietošanai izmanto īpašu krātuvi (MOODLE). Citi rīki, ko varētu izmantot, ir pieejamie saziņas un video straumēšanas rīki, kā arī prezentāciju izstrādes un video rediģēšanas rīki.
2. Praktisko prasmju rīki: Šajā kursā OPAL-RT sistēma, kas ir reāllaika simulators, tiek izmantota, lai vadītu mācību sesijas un sniegtu dalībniekiem prasmes, kas tika noteiktas kursa mērķos.

8. Bibliogrāfija

[1] Eiropas Tehnoloģiju platforma, Eiropas Komisija, “Strategic deployment document for Europe electricity networks of the future”, 2010. gada aprīlis.

[2] Elzinga, David. "Electricity system development: A focus on smart grids. overview of activities and players in smart grids." UNECE. www. unece. org/fileadmin/DAM/energy/se/pdfs/eneff/eneff_h. news/Smart. Grids. Overview. pdf, (2015).

[3] European Commission (2020). Europe investing in digital: the Digital Europe Programme. https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[4] ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). https://www.itu.int/rec/T-REC-X.1205-200804-I/en

[5] Young, Susan un Dave Aitel. The hacker's handbook: the strategy behind breaking into and defending networks. Auerbach publications, 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." IEEE EUROCON 2021-19th International Conference on Smart Technologies. IEEE, 2021.

[8] Valliou, Maria, et al. "Strategy for Cybersecurity Education in Smart Grids." (2022).

[9] González-Manzano, Lorena un Jose M. de Fuentes. "Design recommendations for online cybersecurity courses." Computers & Security 80 (2019): 238-256.
[10] Scott, Bernard un Chunyu Cong. "Knowledge and task analysis methods for course design." 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." 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." 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." 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. un Rebecca Brent. "Active learning: An introduction." ASQ higher education brief 2.4 (2009): 1-5.
[18] Felder, Richard M. un Rebecca Brent. "Cooperative learning." Active learning: Models from the analytical sciences 970 (2007): 34-53.
[19] Bergmann, Jonathan un 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." Journal of Research in Science Teaching 40.9 (2003): 898-921.
[21] English, Mary C. un Anastasia Kitsantas. "Supporting student self-regulated learning in problem-and project-based learning." Interdisciplinary journal of problem-based learning 7.2 (2013): 6.
[22] Deterding, Sebastian, et al. "From game design elements to gamefulness: defining" gamification"." Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments. 2011.
[23] Lalley, J. un R. Miller. "The learning pyramid: Does it point teachers in the right direction." Education 128.1 (2007): 16.
[24] Reigeluth, Charles M. "Instructional design: What is it and why is it." 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 un Junfeng Yang. Educational technology a primer for the 21st century. Springer, 2019.
[27] Brown, Abbie H. un Timothy 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." IEEE Power and Energy Technology Systems Journal 2.2 (2015): 63-73.
[29] Popovici, Katalin un Pieter J. Mosterman, eds. Real-time simulation technologies: Principles, methodologies, and applications. CRC Press, 2017.
[30] Poudel, Shiva, Zhen Ni un Naresh Malla. "Real-time cyber physical system testbed for power system security and control." International Journal of Electrical Power & Energy Systems 90 (2017): 124-133.
[31] "SCALABLE and OPAL-RT Innovate Cyber-Physical Solution." Scalable Network Technologies, 2017. gada 5. jūlijs, www.scalable-networks.com/news/scalable-and-opal-rt-innovate-cyber-physical-solution.