Physische Cybersicherheit in Echtzeit Massive Open Online Course MOOC – Lehrerhandbuch

(Kurzbericht)

Verfasser:

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

Empfehlungen für Cyberssicherheits-Lehrpläne für intelligente Stromnetze (CC-RSG)

Erasmus+ Strategisches Partnerschaftsprojekt

Intellektuelle Leistung 3

Universität Vaasa, Nationale Technische Universität Athen, Technische Universität Riga, Universität Oldenburg

Dieses Projekt hat Mittel von dem Programm Erasmus+ der Europäischen Union im Rahmen der Finanzhilfevereinbarung Nr. 2020-1-FI01-KA203-066624 erhalten.

Inhalt

Inhalt 2

Definitionen, Akronyme und Abkürzungen 3

1. Einführung 4

1.1 Ziele 5

1.2 Struktur des Dokuments 5

2. Methodologie des Kursdesigns 6

3. Eine Besprechung der Bildungsmethodologien 6

4. Instruktionsdesignmodelle 7

5. Umriss des Kursdesigns 8

6. Kursinhalt 8

6.1 Teil 1: Intelligente Stromnetze, Cybersicherheit und Stromnetze 8

6.1.1 Kapitel 1: Grundlagen intelligenter Stromnetzsysteme 9

6.1.2 Kapitel 2: Cybersicherheit und Betriebssicherheit in intelligenten Stromnetzsystemen 9

6.1.3 Kapitel 3: IEC 61850 und IEC 62351 9

6.2 Teil 2: Echtzeit-Simulation, die Theorie 9

6.2.1 Kapitel 4: Grundlagen der Simulation 9

6.2.2 Kapitel 5: Echtzeit-Simulation für das Systemdesign 10

6.2.3 Kapitel 6: Parallele und verteilte Echtzeit-Simulation 10

6.2.4 Kapitel 7: Tools und Anwendungen 10

6.3 Teil 3: Übungen und Fallszenarien 10

6.3.1 Übung 1 10

6.3.2 Übung 2 10

6.3.3 Übung 3 10

6.3.4 Übung 4 10

7. Tools 10

8. Bibliografie 11

Definitionen, Akronyme und Abkürzungen

ADDIE Analyze (analysieren), Design (konzipieren), Develop (entwickeln), Implement (umsetzen) und Evaluate (evaluieren)

CC-RSG Cybersecurity Curricula Recommendations for Smart Grid (Empfehlungen für Cyberssicherheits-Lehrpläne für intelligente Stromnetze)

CI Kritische Infrastruktur

CPS Cyber-physische Systeme

DEVS Discrete Event System Specification (ereignisdiskrete Systemspezifikation)

HIL Hardware in the Loop

ICS Industrielle Steuerungssysteme

ID Instruktionsdesign

IO Intellektuelle Leistung

MOOC Massive Open Online Course (massiver offener Onlinekurs)

RCP Rapid Control Prototyping

RT Real-time (Echtzeit)

SCADA Supervisory Control and Data Acquisition

SIL Software in the Loop

SPSP Smart Power Sicherheitsprofi

UML Unified Modeling Language (Vereinheitlichte Modellierungssprache)

WP Arbeitspaket

1. Einführung

In jüngster Zeit ist es im Energiesektor zu erheblichen Änderungen gekommen, was zu dem Entstehen des Konzepts intelligenter Stromnetze geführt hat. Ein intelligentes Stromnetz bezieht sich auf ein Stromnetz, das die Tätigkeiten und das Verhalten aller Benutzer integriert, einschließlich der Erzeuger, der Verbraucher und derjenigen, die beide Funktionen umfassen, mit dem Ziel einer effizienten Bereitstellung einer nachhaltigen, wirtschaftlichen und sicheren Stromversorgung. Die Cybersicherheit von intelligenten Stromnetzen ist zu einem kritischen Thema geworden, das aufgrund der größer werden Angriffsfläche und der Bedeutung der verbundenen Vermögenswerte unbedingt angegangen werden muss. Cybersicherheit ist eine der wesentlichen digitalen Fähigkeiten, deren Erwerb die Europäische Union anstrebt. Sie umfasst mehrere Aspekte wie Tools, Richtlinien, Sicherheitskonzepte, Sicherungen, Leitlinien, Risikomanagementansätze, Aktionen, Schulung, Best Practices, Versicherung und Technologien, die eingesetzt werden können, um eine Organisation und Vermögenswerte von Benutzern und die Cyberumgebung zu schützen. Trotz der Verfügbarkeit zahlreicher Tools und Softwarepakete von verschiedenen Anbietern, die Sicherheitsbedürfnisse abdecken und die Robustheit des Netzes sicherstellen, bleibt Cybersicherheit ein wichtiges Thema.

Das Projekt Empfehlungen für Cyberssicherheits-Lehrpläne für intelligente Stromnetze (CC-RSG) ist mithilfe von Umfragen, Überprüfungen und Workshops tiefer in das Thema der Cybersicherheit in Stromnetzen eingetaucht. Die Untersuchung hat die folgenden Ergebnisse gezeitigt:

1. Der derzeitige Ansatz für die Bewältigung von Cybersicherheitsthemen in intelligenten Stromnetzen ist ungenügend.
2. Es gibt einen Mangel an Fachleuten für Cybersicherheit im Bereich intelligente Stromnetze aufgrund der wenigen Ausbildungsprogramme, die dieses spezifische Feld in der Praxis abdecken.
3. Die vorhandenen Ausbildungsangebote entsprechen nicht den Anforderungen eines Smart Power Sicherheitsprofis (SPSP).
4. Reale Szenarien und Verbindungen zur Branche fehlen.

Die Bereitstellung von Ausbildungsgelegenheiten, die die Fähigkeiten verbessern und die aufgezählten Lücken angehen, ist eine wichtige Notwendigkeit, vor allem wenn man bedenkt, dass frühere Berichte hervorheben, dass mindestens 50% aller Cybersicherheitsvorfälle auf menschliches Versagen zurückzuführen sind. Um dieses Problem anzugehen, will das CC-RSG-Projekt postsekundären Institutionen dabei helfen, Lernergebnisse im Zusammenhang mit der Cybersicherheit in intelligenten Stromnetzen in ihre Lehrpläne aufzunehmen. Dieser Bericht bietet einen Umriss des Kurses, der zu diesem Thema entwickelt wurde.

Dieser Bericht stellt das Ergebnis des Arbeitspakets (WP) 3, “Designing, Developing, and Piloting” – Intellectual Output (IO) 3 (Konzipieren, Entwickeln und Pilotieren“ - Intellektuelle Leistung) – des CC-RSG-Projekts in Kürze dar. Daher baut der Bericht auf den Ergebnissen früherer Berichte und IOs auf, um einen Massive Open Online Course (MOOC) für physische Cybersicherheitssysteme in Echtzeit zu bieten. Der Kurs strebt an, die gefundenen Lücken in cyber-physischen Systemen (CPS) zu füllen und Fähigkeiten rund um Echtzeit-Simulationssysteme aufzubauen, die für Hochgeschwindigkeitssimulationen verwendet werden, wobei die kritische Infrastruktur (CI) getestet und Sicherheitsvorgänge und -funktionen evaluiert werden. Für die Entwicklung des Kurses wurden unterschiedliche Ansätze untersucht und getestet, um die am besten geeigneten Methoden zu finden, die dem Zweck der Erschaffung eines Kurses dienen und die hervorgehobenen Kompetenzlücken zu schließen. Daher nutzt der Kurs die folgenden Ansätze: Flipped Learning („auf den Kopf gestelltes Lernen“), Simulationen und virtuelle und ferngesteuerte Labore. Diese Ansätze wurden

sorgfältig aufgrund ihrer Fähigkeit ausgewählt, Mittel für die Interaktion bereitzustellen, analytische und Problemlösungsfähigkeiten aufzubauen und praktische Fähigkeiten zu fördern.

Die Hauptbeiträge des IO3-Kursberichts sind:

1. Bereitstellung des theoretischen Hintergrunds für Echtzeit-Simulationssysteme
2. Aufbau von praktischen Fähigkeiten durch Verwendung einer Echtzeit-Simulation
3. Einführung und Anwendung von Nutzungsfällen, Szenarien und Übungen für Praxis- und Schulungszwecke.

In dem IO3-Kursbericht „Physische Cybersicherheit in Echtzeit, Massive Open Online Course MOOC – Lehrerhandbuch“ („Real-Time Physical Cybersecurity Massive Open Online Course MOOC – Teacher's Handbook”) werden die Grundlagen theoretischer Kenntnisse durch Bereitstellung starker Grundkenntnisse über intelligente Stromnetze, Kommunikationsprotokolle und Cybersicherheit in intelligenten Stromnetzen gelegt. Außerdem wurde besonderen Wert auf Echtzeit-Simulationssysteme gelegt, da diese als eines der besonders wirksamen Nischen-Tools für das Experimentieren mit, Testen von und Lernen über kritische Infrastruktur and intelligente Stromnetze erkannt wurden. Dementsprechend wurden viele Konzepte rund um die Echtzeit-Simulation präsentiert. Außerdem konzentriert sich der Kurs nicht nur auf theoretische Kenntnisse, sondern geht weiter, um auch die für die Branche erforderlichen praktischen Fähigkeiten zu umfassen. Daher wurden vier Übungen rund um ausgewählte industrielle Szenarien ausgewählt und durch ein physisches Echtzeit-Simulatorsystem umgesetzt.

Und zum Schluss dient der IO3-Kursbericht als ein Lehrerhandbuch. Daher haben wir bei der Gestaltung des Kurses versucht, alle Informationen zusammenzutragen, die notwendig sind, um das Thema der Cybersicherheit in intelligenten Stromnetzen umfassend abzudecken. Um diesen Bericht zu verwenden, wird Lehrern/Ausbildern empfohlen, das Material zu verwenden, um Präsentationen und Informationsblätter zu erstellen. Es wird auch dringend empfohlen, da der Schwerpunkt auf ‚Flipped Learning‘ und MOOC liegt, zuvor aufgezeichnete Videos und automatisierte Aufgaben zu erstellen.

1.1 Ziele

Das Hauptziel des IO3 ist es, den Teilnehmern Kenntnisse zu vermitteln, die notwendig sind, damit sie im Bereich CPS tätig sein können, vor allem im Bereich Cybersicherheit in intelligenten Stromnetzen.

1.2 Struktur des Dokuments

- Abschnitt 2 präsentiert die Methologie des Kursdesigns
- Abschnitt 3 bespricht Lehrmethodologien und genutzte Lernansätze
- Abschnitt 4 präsentiert die allgemeinen Instruktionsdesign- (ID) Modelle
- Abschnitt 5 präsentiert den Umriss des Kursdesigns
- Abschnitt 6 präsentiert den Inhalt des Kurses und die behandelten Themen in Kürze.
- Und Abschnitt 7 präsentiert schließlich die verwendeten Tools

2. Methodologie des Kursdesigns

Um den Kurs effektiv zu konzipieren, wurden die folgenden Verfahren angewandt:

1. Betonung der Notwendigkeit des Kursdesigns
2. Definition des Falls und Kontexts des Kurses
3. Angabe der Ziele und des gewünschten Ergebnisses
4. Angabe der Lernmethodologien und Aktivitäten
5. Angabe des Kursinhalts
6. Wahl der Evaluierungskriterien
7. Entwicklung und Umsetzung

3. Eine Besprechung der Bildungsmethodologien

Die Bedeutung der Bildungsmethodologie kann nicht genug betont werden, da sie die Art definiert, in der Lernziele erreicht und bewertet werden. Zuerst einmal sind verschiedene Bildungsmethodologien und Lerntechniken verfügbar, je nachdem, was das gewünschte Niveau an Wissenserhalt ist. Diese umfassen eine vortragsbasierte Unterrichtung, empirisches Lernen, aktives Lernen, kooperatives Lernen, ‚Flipped Learning', fragenbasiertes Lernen und projektbasiertes Lernen sowie Gamifizierung, und zwar folgendermaßen:

1. Die konventionelle Lernmethode, vortragsbasiertes Lernen, beinhaltet, dass ein Lehrer das Kursmaterial bereitstellt, Beurteilungen durchführt und die volle Verantwortung für die Lernerfahrung übernimmt. Jedoch ist diese Methode in erster Linie passiv und verlässt sich sehr stark auf Auswendiglernen. Durch Einbeziehung von Aktivitäten wie unaufgeforderte Anrufe, Diskussionen, Lernkarten und andere interaktive Elemente kann das vortragsbasierte Lernen in einen aktiven und effektiveren Ansatz umgewandelt werden.
2. Empirisches Lernen ist ein aktiver Ansatz zum Lernen, bei dem sich die Studenten aktiv am Lernprozess beteiligen müssen und beim Lernen Erfahrungen sammeln. Bei dem aktiven Lernen geht es jedoch nicht nur um die Einbeziehung von Aktivitäten und die Ermutigung zur Teilnahme, sondern es schließt auch die Verarbeitung aller Antworten der Lernenden ein, bevor neue Informationen präsentiert werden.
3. Kooperatives Lernen ist ein teambasierter Ansatz, bei dem die Teilnehmer zusammenarbeiten, um spezifische Ziele zu erreichen, und die volle Verantwortung für die Ausführung einer Aufgabe übernehmen. ‚Flipped Learning' (‚auf den Kopf gestelltes Lernen') ist ein moderner Ansatz, der die Lernenden befähigt, Verantwortung für ihr Lernen zu übernehmen, indem ihnen im Voraus Lernmaterialien bereitgestellt werden, was eine dynamischere und interaktive Erfahrung im Klassenzimmer ermöglicht.
4. Anfragenbasiertes Lernen ist ein Ansatz, bei dem die Studenten dieselben Praktiken befolgen wie professionelle Wissenschaftler, um Kenntnisse und Erfahrungen zu gewinnen. Problem- und projektbasiertes Lernen bezieht die Teilnehmer aktiv in den Lernprozess ein, indem ein spezifisches Problem oder eine Frage mit dem Ziel untersucht wird, Antworten zu finden oder eine Lösung zu entwickeln.
5. Und schließlich wendet die Gamifizierung spielähnliche Merkmale an, wie Geschichtenerzählen, verschiedene Stufen und Abzeichen, um zur Teilnahme zu ermutigen und den Lernprozess spannender zu gestalten. Durch Nutzung dieser verschiedenen Ansätze können Ausbilder eine effektivere und interessantere Lernumgebung für ihre Studenten schaffen.

Zweitens werden die vorstehend aufgeführten Lehrmethodologien typischerweise verwendet, um das Lernen und Behalten widerzuspiegeln, das durch die Kursziele und die verfügbaren

Ressourcen definiert wird. Es ist festzustellen, dass je höher die Einbeziehung in den Lernprozess ist, desto höher ist auch das Ausmaß des Lernens und Behaltens: allerdings werden auch mehr Ressourcen benötigt. Das Ausmaß des Lernens und Behaltens der unterschiedlichen Lernaktivitäten:

1. Konventionelle Methode und Vorlesungen: 5%
2. Lesen und Selbststudium: 10%
3. Audiovisuelle Illustrationen: 20%
4. Vorführung und semiaktive Teilnahme: 30%
5. Planung, Diskussionen und aktive Teilnahme: 50%
6. Lernen durch Handeln: 75%
7. Andere unterrichten: 90%

Bei der Konzipierung eines Kurses ist es wesentlich, zuerst zu definieren, welches Ausmaß des Lernens und Behaltens angestrebt wird, und dann die Arbeitsbelastung und die Ressourcen an diese Kriterien anzupassen

4. Instruktionsdesignmodelle

Da es beim IO3 um das Kursdesign geht, wurden die nachstehend aufgeführten allgemeinen ID-Modelle verwendet, um bei dem Prozess der Definition von Zielen, der Auswahl von Aktivitäten und der Auswahl des Kursmaterials zu helfen.

1. Die Lernzieltaxonomie (Bloom's Taxonomy) ist ein hierarchisches Modell, das zur Bewertung des Lernprozesses verwendet wird. Sie schließt verschiedene Lernstufen ein, wobei das Erinnern ganz unten und das Erschaffen oben stehen. Je nach dem gewünschten Ergebnis können Aktivitäten zugeschnitten werden um sicherzustellen, dass die Studenten ihre Lernziele erreichen.
2. Gagnes Neun-Ereignisse-Modell ist ein umfassender Rahmen für Lehrereignisse, die beachtet werden müssen, um ein effektives Lernen zu gewährleisten. Diese Ereignisse umfassen Aufmerksamkeit erzielen, Ziele mitteilen, frühere Kenntnisse abrufen, Inhalt präsentieren, Anleitungen bieten, die Praxis erleichtern, Feedback bereitstellen, die Leistung bewerten und das Behalten und die Umsetzung verbessern.
3. Das ADDIE-Modell ist ein strukturierter Rahmen für die Konzipierung und Entwicklung von Kursen, der aus fünf Stadien besteht: Analyze (analysieren), Design (konzipieren), Develop (entwickeln), Implement (umsetzen) und Evaluate (evaluieren) Das Modell betont die Wichtigkeit der ständigen Überarbeitung und Verbesserung während des Kursentwicklungsprozesses.
4. Merrills Prinzipien identifizieren mehrere Prinzipien, die effektiven Instruktionsdesignmodellen gemein sind. Diese schließen das aufgaben-/problembasierte Design, die Aktivierung früherer Kenntnisse, das Demonstrieren neuer Kenntnisse, die Anwendung neuer Kenntnisse und die Ermutigung zur Integration neuer Kenntnisse ein.
5. Das Dick- und Carey-Modell, auch als Systemansatzmodell bekannt, ist ein Planungsmodell für die Entwicklung von Lektionen. Es schließt die Definition der Lehrziele, die Durchführung einer Instruktionsanalyse, die Definition von Eingangsanforderungen, die Festlegung von Leistungszielen und Testpunkten, die Entwicklung einer Lehrstrategie und von Lehrmaterialien und die Durchführung formativer und zusammenfassender Auswertungen ein. Dieses Modell stellt sicher, dass der Lehrplan umfassend ist und alle Aspekte des Instruktionsprozesses umfasst.

Es ist wichtig festzustellen, dass diese Methodologien zwar einen umfassenden Rahmen für die Konzipierung und Entwicklung von Kursen darstellen, aber nicht unbedingt immer perfekt zu den spezifischen Zielen und Ressourcen eines bestimmten Kursangebots passen. In der Praxis ist es vielleicht notwendig, Anpassungen an den definierten Attributen vorzunehmen um sicherzustellen, dass der Kurs zu seinen beabsichtigten Zielen passt. Diese Methodologien dienen als Leitfaden und sollten angepasst werden, um den einzigartigen Bedürfnissen und Umständen des Kurses zu entsprechen. Ultimativ besteht das Ziel darin, diese Methodologien zu verwenden, um eine effektive und interessante Lernerfahrung für die Studenten zu schaffen. Sie bieten zwar eine solide Grundlage für die Kursentwicklung, aber sie sollten an die spezifischen Bedürfnisse jedes Kurses angepasst werden, wobei Faktoren wie das Publikum, das Thema des Kurses und die verfügbaren Ressourcen berücksichtigt werden sollten.

5. Umriss des Kursdesigns

Auf der Grundlage der spezifischen Ziele und Ressourcen für das Kursdesign wird der folgende Umriss übernommen:

1. Lernziele: Die Lücke der Cybersicherheitskenntnisse im Bereich intelligente Stromnetze füllen
2. Voraussetzungen: Der Kurs steht nur Studenten und Fachleuten offen, die vorherige Kenntnisse in den Bereichen Cybersicherheit und intelligente Stromnetze haben
3. Vorhergesehenes Ausmaß des Lernens und Behaltens für diesen Kurs: 60% bis 75%, das Ziel sind aktive Diskussionen und einfache Praxis durch Ausführung von Aufgaben
4. Angewandte Instruktionsdesignmethodologien: ADDIE und Dick- und Carey-Modelle für das Design und Anstreben der dritten Stufe – Anwendung – der Lernzieltaxonomie für das Behalten.
5. Verwendete Ansätze: Hauptsächlich ‚Flipped Learning' und Gamifizierung, mit Aufgaben, die ein kooperatives Lernen fördern
6. Bereitstellungsmethode: Beaufsichtigte aufgenommene Sitzungen
7. Kriterien, um die Aufmerksamkeit und das Engagement zu erhöhen: Bonuspunkte, Nutzung von Spiele und Diskussionsforen
8. Bewertung und Messung: Regelmäßige Tests und ein Schlussexamen, vorzugsweise automatische selbstausgewertete Tests.
9. Studienpensum:125-140 Stunden Vorlesungen, Übungen und Material zum Selbststudium

6. Kursinhalt

Der konzipierte Kurs in in drei Teile unterteilt. Teil Eins deckt intelligente Stromnetze, Cybersicherheit und Stromnetze ab. Teil Zwei deckt Echtzeit-Simulation ab, die Theorie. Und schließlich betrifft Teil Drei den Aufbau praktischer Fähigkeiten, indem Übungen und Fallszenarien bereitgestellt werden. Die besagten drei Teile schließen sieben Kapitel und vier praktische Übungen ein. In den nächsten Unterabschnitten werden die Hauptpunkte jedes Kapitels noch kurz präsentiert.

6.1 Teil 1: Intelligente Stromnetze, Cybersicherheit und Stromnetze

6.1.1 Kapitel 1: Grundlagen intelligenter Stromnetzsysteme

Dieses Kapitel deckt die Hauptkonzepte intelligenter Stromnetzsysteme ab, einschließlich: Komponenten des intelligenten Stromnetzes, Hauptvorteile und Herausforderungen bei der Implementierung und Umsetzung eines intelligenten Stromnetzes und das Architekturmodell eines intelligenten Stromnetzes. Das Kapitel stellt Technologien für intelligente Stromnetze in Bezug auf Rahmen, Funktionen und Fähigkeiten, Ressourcen und Energiespeichersysteme, Mikronetze, kleine Umspannwerke und das Kommunikationsprotokoll IEC 61850 vor. Als Nächstes kommen die Herausforderungen und Erfolgsfaktoren des Netzes, in dem 6 Herausforderungen eingeführt werden, darunter Geschäftsumwandlung, Annäherung der Abläufe, integrierter Systemansatz, die Komplexität eines heterogenen Systems, Cybersicherheit und schließlich Datenschutz. Im Anschluss werden dann die Haupterfolgsfaktoren des Netzes erklärt. In den letzten Abschnitten des Kapitels werden globale Initiativen zu intelligenten Stromnetzen, vor allem auf dem europäischen Markt, und die Zukunft des intelligenten Stromnetzes eingeführt.

6.1.2 Kapitel 2: Cybersicherheit und Betriebssicherheit in intelligenten Stromnetzsystemen

Dieses Kapitel deckt die Sicherheitsaspekte des Netzes, einschließlich Hacking des Netzes und die Hauptangriffsmethoden, Sicherheitsmodelle für die Supervisory Control and Data Acquisition (SCADA), industrielle Steuerungssysteme (ICS) und das intelligente Netz, und zum Schluss werden Methoden für die Sicherheit des intelligenten Netzes beschrieben, einschließlich der Implementierung von Sicherheitskontrollen, Feldzonenschutz, Steuerungszonenschutz, Servicezonenschutz, die Einrichtung starker Abgrenzungen und Zonentrennung, fortschrittliches Netzwerk-Mentoring, Schutz von Daten und Anwendungen und Situationsbewusstsein.

6.1.3 Kapitel 3: IEC 61850 und IEC 62351

IEC 61850 wird bereits seit langem als standardisiertes Protokoll für die Kommunikation in intelligenten Netzen verwendet. Dieses Kapitel deckt die Hauptaspekte und Architektur dieser Norm ab und führt auch das komplementäre Sicherheitsprotokoll IEC 62351 ein, das für die Einrichtung einer Sicherheitsschicht zusätzlich zu IEC 61850 verwendet wird.

6.2 Teil 2: Echtzeit-Simulation, die Theorie

6.2.1 Kapitel 4: Grundlagen der Simulation

Dieses Kapitel deckt die Hauptkonzepte der Simulationstechnologien ab. Dazu gehören Auflösen, kontinuierliche und Hybridmodelle, Hochgeschwindigkeits-Echtzeit-Hybridsimulation, ein formalisierter Ansatz für das Design verteilter Systeme, Modellierung unter Verwendung der ereignisdiskreten Systemspezifikation (DEVS) und Vereinheitlichte Modellierungssprachen (UML) sowie Tools für die Integration mit MATLAB und Simulink.

6.2.2 Kapitel 5: Echtzeit-Simulation für das Systemdesign

Dieses Kapitel deckt die Konzepte des Systemdesigns ab, einschließlich progressiver Simulation, der Konzepte Hardware in the Loop (HIL) und Software in the Loop (SIL), Validierung und Validator-Tools und schließlich das Konzept der Nutzung des Rapid Control Prototyping (RCP), um die Konzipierung und das Testen des Systemdesigns zu erleichtern.

6.2.3 Kapitel 6: Parallele und verteilte Echtzeit-Simulation

Dieses Kapitel führt ein Testbed unter Verwendung des DNP3-Protokolls ein und betont dann die Nutzung des Systemansatzes für die Simulation für die Schulung.

6.2.4 Kapitel 7: Tools und Anwendungen

Dieses Kapitel präsentiert das Konzept der Zeitdilation, daher kann eine präzise Simulation in Systemen in großem Maßstab erreicht werden. Es werden auch damit verbundene Konzepte wie virtualisierte Systeme, CPU-Planung, Netzwerkemulation und Speicheremulation eingeführt.

6.3 Teil 3: Übungen und Fallszenarien

6.3.1 Übung 1

Ein Leitfaden für die Einführung in die Bedienung des Echtzeit-Simulators EXATA CPS und HYPERSIM OPAL-RT

6.3.2 Übung 2

Echtzeit-Kosimulationen eines aktiven Energiemanagements im Mikronetz gegen Verzögerungsangriffe

6.3.3 Übung 3

Echtzeit-Kosimulationen eines aktiven Energiemanagements im Mikronetz gegen einen Angriff Änderung des Datenpakets

6.3.4 Übung 4

Echtzeit-Kosimulationen eines Mikronetzes basierend auf Controller Hardware in the Loop HIL

7. Tools

Tools, die im gesamten Kurs verwendet werden, schließen folgende Tools für Lernhilfen und Tools für Übungen und praktische Fähigkeiten ein:

1. Lernhilfe-Tools: Diese Tools sollen beim Lernprozess helfen. Da der Kurs in der Form eines MOOC angeboten wird, wird ein eigener Speicher (MOODLE) als Host für das Lernmaterial, Diskussionsforen, Tests und Online-Prüfungen verwendet. Weitere Tools, die verwendet werden können, schließen verfügbare Kommunikations- und Video-Streaming-Tools sowie Tools für das Design von Präsentationen und das Bearbeiten von Videos ein.
2. Tools für praktische Fähigkeiten: In diesem Kurs wird das OPAL-RT-System, ein Echtzeit-Simulator, verwendet, um Schulungseinheiten auszuführen und den Teilnehmern die Fähigkeiten bereitzustellen, die in den Kurszielen identifiziert wurden.

8. Bibliografie

[1] Europäische Technologieplattform, Europäische Kommission, “Strategic deployment document for Europe electricity networks of the future”, April 2010.

[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] Europäische Kommission (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. Genf: International Telecommunication Union (ITU). https://www.itu.int/rec/T-REC-X.1205-200804-I/en

[5] Young, Susan und 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 2021-19. International Conference on Smart Technologies. IEEE, 2021.

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

[9] González-Manzano, Lorena und Jose M. de Fuentes. "Design recommendations for online cybersecurity courses." Computers & Security 80 (2019): 238-256.

[10] Scott, Bernard und 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.und Rebecca Brent. "Active learning: An introduction." ASQ higher education brief 2.4 (2009): 1-5.
[18] Felder, Richard M.und Rebecca Brent. "Cooperative learning." Active learning: Models from the analytical sciences 970 (2007): 34-53.
[19] Bergmann, Jonathan und 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. und 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. und 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 und Junfeng Yang. Educational technology a primer for the 21st century. Springer, 2019.
[27] Brown, Abbie H. und 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 und Pieter J. Mosterman, eds. Real-time simulation technologies: Principles, methodologies, and applications. CRC Press, 2017.
[30] Poudel, Shiva, Zhen Ni, und 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, 5. Juli 2017, www.scalable-networks.com/news/scalable-and-opal-rt-innovate-cyber-physical-solution.