Fysisk cybersäkerhet i realtid
Lärarhandbok i storskaliga öppna nätkurser (MOOC)

(Verkställande rapport)

Författare:

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

Kursplansrekommendationer för cybersäkerhet i smarta nät (CC-RSG)

Strategiskt partnerskapsprojekt inom Erasmus+

Kunskapsproduktion 3

University of Vaasa, National Technical University of Athens, Riga Technical University, University of Oldenburg

Detta projekt har fått finansiering från Europeiska unionens Erasmus+program inom ramen för bidragsavtal nr 2020-1-FI01-KA203-066624.

Innehåll

Innehåll ... 2

Definitioner, akronymer och förkortningar ... 3

1. Inledning ... 4

1.1 Mål ... 5

1.2 Dokumentets struktur ... 5

2. Metod för kursutformning ... 5

3. Översikt av utbildningsmetoder ... 6

4. Modeller för instruktionsdesign ... 7

5. Ram för kursutformningen ... 7

6. Kursinnehåll ... 8

6.1 Del 1: Smarta nät, cybersäkerhet och elnät ... 8

6.1.1 Kapitel 1: Grunderna i smarta nätsystem ... 8

6.1.2 Kapitel 2: Cybersäkerhet och driftsäkerhet i smarta nät ... 8

6.1.3 Kapitel 3: IEC 61850 och IEC 62351 ... 9

6.2 Del 2: Realtidssimulering, teori ... 9

6.2.1 Kapitel 4: Grundprinciper för simulering ... 9

6.2.2 Kapitel 5: Realtidssimulering för systemdesign ... 9

6.2.3 Kapitel 6: Parallell och distribuerad realtidssimulering ... 9

6.2.4 Kapitel 7: Verktyg och applikationer ... 9

6.3 Del 3: Övningar och case-scenarier ... 9

6.3.1 Övning 1 ... 9

6.3.2 Övning 2 ... 10

6.3.3 Övning 3 ... 10

6.3.4 Övning 4 ... 10

7. Verktyg ... 10

8. Litteraturförteckning ... 11

Definitioner, akronymer och förkortningar

ADDIE	Analys Design Utveckling Genomförande Utvärdering
CC-RSG	Kursplansrekommendationer för cybersäkerhet i smarta nät
CI	Kritisk infrastruktur
CPS	Cyberfysiskt system
DEVS	Discrete Event System Specification
HIL	Hardware in the Loop
ICS	Industriella styrsystem
ID	Instruktionsdesign
IO	Kunskapsproduktion
MOOC	Storskaliga öppna nätkurser
RCP	Rapid Control Prototyping
RT	Realtid
SCADA	Supervisory Control and Data Acquisition
SIL	Software in the Loop
SPSP	Smart Power Security Professional
UML	Unified Modeling Language
WP	Arbetspaket

1. Inledning

På senare tid har energisektorn genomgått betydande förändringar, vilket lett till uppkomsten av begreppet smarta nät. Ett smart nät avser ett elnät som integrerar alla användares handlingar och beteenden, inklusive producenter, konsumenter och de som fungerar som båda, i syfte att leverera hållbar, ekonomisk och säker elförsörjning på ett effektivt sätt. Cybersäkerhet för smarta nät har blivit en avgörande fråga som måste lösas på grund av den ökande attackytan och den kritiska karaktären hos anslutna tillgångar. Cybersäkerhet är en av de grundläggande digitala kapaciteter som Europeiska unionen strävar efter att uppnå. Det omfattar flera aspekter som verktyg, policyer, säkerhetskoncept, skyddsåtgärder, riktlinjer, riskhanteringsmetoder, åtgärder, utbildning, bästa praxis, säkerhet och teknik som kan användas för att skydda en organisation och användarnas tillgångar och cybermiljön. Trots att det finns många verktyg och programvarupaket från olika leverantörer som täcker säkerhetsbehov och säkerställer nätets robusthet är cybersäkerhet fortfarande en viktig fråga.

Cybersecurity Curricula Recommendations for Smart Grid (CC-RSG)-projektet har fördjupat sig i frågan om cybersäkerhet i smarta nät med hjälp av enkäter, översikter och workshops. Undersökningen gav följande resultat:

1. Den nuvarande strategin för att ta itu med cybersäkerhetsfrågor i smarta nät är otillräcklig.
2. Det råder brist på yrkesverksamma proffs på cybersäkerhet inom området smarta nät på grund av bristen på utbildningsprogram som täcker detta specifika område i praktiken.
3. De befintliga utbildningsprogrammen uppfyller inte kraven för Smart Power Security Professional (SPSP).
4. Verkliga scenarier och kopplingar till industrin saknas.

Det är viktigt att tillhandahålla utbildningsmöjligheter som kan förbättra kompetensen och åtgärda de brister som nämns ovan, särskilt med tanke på tidigare rapporter som framhåller att minst 50 % av cybersäkerhetsincidenterna beror på mänskliga fel. För att ta itu med denna fråga vill CC-RSG-projektet hjälpa eftergymnasiala institutioner att integrera lärandemål relaterade till cybersäkerhet i smarta nät i sina kursplaner. Den här rapporten ger en översikt över den kurs som utformades för att täcka frågan.

Denna rapport presenterar i korthet resultatet av arbetspaketet (WP) 3, ”Design, Utveckling, och Testning” och Kunskapsproduktion (IO) 3 av CC-RSG-projektet. Rapporten bygger på resultat från tidigare rapporter och kunskapsproduktion, för att tillhandahålla en storskalig öppen nätkurs (MOOC) för fysiska cybersäkerhetssystem i realtid. Kursen syftar till att åtgärda de konstaterade luckorna i cyberfysiska system (CPS) samt bygga upp färdigheter kring realtidssimuleringssystem som används för höghastighetssimuleringar, testning av kritisk infrastruktur (CI) och utvärdering av säkerhetsoperationer och säkerhetsfunktioner. För att utforma kursen har man undersökt och testat olika tillvägagångssätt för att hitta de lämpligaste metoderna som tjänar till att skapa kursen och fylla de kunskapsluckor som lyfts fram. Kursen kommer därför använda sig av följande metoder: omvänt lärande, simuleringar och virtuella labb och fjärrlabb. Dessa metoder valdes noggrant ut på grundval av deras förmåga att tillhandahålla medel för interaktion, bygga upp analytiska färdigheter och problemlösningsfärdigheter samt främja praktiska färdigheter.

De viktigaste bidragen i IO3-kursrapporten är följande:

1. Tillhandahållande av den teoretiska bakgrunden avseende system för realtidssimulering

2. Uppbyggande av praktiska färdigheter för att använda realtidssimulering
3. Introducering och tillämpning av användningsfall, scenarier och övningar i övningssyfte.

I IO3-kursrapporten ”Real-Time Physical Cybersecurity Massive Open Online Course MOOC – Teacher’s Handbook” har man beaktat både teoretisk och grundläggande kunskap genom att tillhandahålla starka grunder och en bas för kunskap om smarta nät, kommunikationsprotokoll för smarta nät och cybersäkerhet i smarta nät. Dessutom har man tagit särskild hänsyn till system för realtidssimulering, eftersom de har identifierats som en nisch och ett av de mest effektiva verktygen för experimentering, testning och lärande om kritisk infrastruktur och smarta nät. Därför presenterar vi många begrepp kring realtidssimulering. Dessutom fokuserar kursen inte bara på teoretiska kunskaper, utan den inbegriper också praktiska färdigheter som industrin behöver. Fyra övningar byggdes alltså upp kring utvalda industriscenarier och genomfördes genom ett fysiskt system för realtidssimulation.

Slutligen fungerar IO3-kursutformningsrapporten som en lärarhandbok. När vi utformade kursen försökte vi därför samla in all information som behövs för att på ett heltäckande sätt ta upp frågan om cybersäkerhet i smarta nät. För att utnyttja den här rapporten rekommenderas lärare/lektorer att använda materialet för att utforma presentationer och kopior. Även eftersom betoningen ligger på omvänt lärande och MOOC, rekommenderar vi att utforma förinspelade videor och automatiska uppgifter.

1.1 Mål

Huvudsyftet med IO3 är att utforma en kurs som ger deltagarna den kunskap som krävs för att få in en fot på CPS-området, särskilt cybersäkerhet i smarta nät.

1.2 Dokumentets struktur

- I avsnitt 2 presenteras kursutformningsmetoden
- I avsnitt 3 granskas de utbildningsmetoder och inlärningsmetoder som används
- I avsnitt 4 presenteras modeller för allmän instruktionsdesign (ID)
- I avsnitt 5 presenteras ramarna för kursutformningen
- I avsnitt 6 beskrivs innehållet i kursen och de ämnen som behandlas kortfattat.
- Slutligen, i avsnitt 7 presenteras de verktyg som används.

2. Metod för kursutformning

För att utforma kursen på ett effektivt sätt antogs följande processer:

1. Betoning av behovet av kursutformning
2. Definiera kursens case och sammanhang
3. Ange mål och önskat resultat
4. Ange inlärningsmetoder och -aktiviteter
5. Specificera kursinnehåll
6. Välj utvärderingskriterier
7. Utveckling och genomförande

3. Översikt av utbildningsmetoder

Utbildningsmetodens betydelse ska inte underskattas eftersom den definierar hur lärandemålen ska uppnås och bedömas. För det första finns det olika utbildningsmetoder och tekniker beroende på vilken nivå av kunskapsbehållning som önskas. Dessa omfattar föreläsningsbaserad undervisning, erfarenhetsinlärning, aktivt lärande, samarbetsinriktat lärande, omvänt lärande, forskningsbaserat lärande, problembaserat och projektbaserat lärande samt spel:

1. Den konventionella inlärningsmetoden, föreläsningsbaserat lärande, innebär att en lektor presenterar kursmaterialet, gör bedömningar och tar fullt ansvar för utbildningserfarenheten. Denna metod är dock i första hand passiv och är starkt beroende av memorering. Genom att inkludera aktiviteter som cold calling, diskussioner, inlärningskort och andra interaktiva element kan föreläsningsbaserat lärande omvandlas till en aktiv och mer effektiv metod.
2. Experimentellt lärande är en aktiv inlärningsmetod som kräver att studenterna deltar i inlärningsprocessen och utvecklar sina erfarenheter när de lär sig. Aktivt lärande handlar däremot inte bara om att inkludera aktiviteter och uppmuntra deltagande, utan även om att behandla alla studenters svar innan ny information läggs fram.
3. Samarbetsinriktat lärande är en gruppbaserad metod där deltagarna samarbetar för att uppnå specifika mål och tar fullt ansvar för att slutföra en uppgift. Omvänt lärande är en modern metod som ger eleverna möjlighet att ta ansvar för sitt lärande genom att tillhandahålla utbildningsmaterial i förväg, vilket möjliggör en mer dynamisk och interaktiv klassrumserfarenhet.
4. Forskningsbaserat lärande är en metod som involverar studenterna att följa samma praxis som professionella forskare för att få kunskap och erfarenhet. Problem- och projektbaserat lärande engagerar aktivt deltagarna i lärandeprocessen genom att utforska ett specifikt problem eller en specifik fråga i syfte att hitta svar eller utveckla en lösning.
5. Slutligen, gamification (spelifiering) använder spelliknande funktioner som t.ex. storytelling, att klara nivåer och märken för att uppmuntra deltagande och göra inlärningsprocessen mer engagerad. Genom att använda dessa olika metoder kan utbildare skapa en mer effektiv och engagerande inlärningsmiljö för sina studenter.

För det andra används de ovannämnda utbildningsmetoderna vanligen för att reflektera över den behållningsgrad för lärande som definieras av kursmålen och tillgängliga resurser. Det bör noteras att ju större engagemang för lärandeprocessen som det finns, desto högre är behållningsgraden, men då behövs också mer resurser. Här är behållningsgraden för olika inlärningsaktiviteter:

1. Konventionell metod och föreläsningar: 5 %
2. Läsning och självstudier: 10 %
3. Audiovisuella illustrationer: 20 %
4. Demonstrering och semi-aktivt deltagande: 30 %
5. Planering, diskussioner och aktivt deltagande: 50 %
6. Lär dig genom att göra: 75 %
7. Att lära andra: 90 %

När du utformar en kurs är det viktigt att först definiera vilken behållningsnivå som ska användas och på så sätt justera arbetsbelastningen och resurserna så att de motsvarar detta kriterium.

4. Modeller för instruktionsdesign

Eftersom IO3 handlar om kursutformning användes de allmänna ID-modeller som nämns nedan för att hjälpa till att definiera mål, välja aktiviteter och välja kursmaterial.

1. Blooms taxonomi är en hierarkisk modell som används för att bedöma inlärningsförlopp. Det omfattar olika nivåer av inlärning, med att komma ihåg längst ned och skapa högst upp. Beroende på det önskade resultatet kan aktiviteterna skräddarsys i enlighet med detta för att säkerställa att eleverna uppnår sina inlärningsmål.
2. Gagne's Nine Events Model är ett omfattande ramverk av undervisningsaktiviteter som måste övervägas för att säkerställa ett effektivt lärande. Dessa aktiviteter omfattar att få uppmärksamhet, informera om mål, påminna sig själv om tidigare kunskap, presentera innehåll, tillhandahålla vägledning, facilitera praktik, ge återkoppling, utvärdering av prestationer och förbättra behållningen och överföringen.
3. ADDIE-modellen är en strukturerad ram för utformning och utveckling av kurser som består av fem steg: Analys, Design, Utveckling, Implementering och Utvärdering. Modellen betonar vikten av kontinuerlig översyn och förbättring under hela kursutformningsprocessen.
4. Merrills principer identifierar flera principer som är gemensamma för effektiva modeller för instruktionsdesign. Dessa omfattar uppgifts-/problemcentrerad design, aktivering av tidigare kunskap, demonstration av ny kunskap, tillämpning av ny kunskap och uppmuntran till integrering av ny kunskap.
5. Dick- och Carey-modellen, även känd som Systems Approach-modellen, är en planeringsmodell för utveckling av lektioner. Den omfattar att definiera instruktionsmål, utföra instruktionsanalys, fastställa inmatningskrav, specificera prestandamål och testobjekt, utveckla instruktionsstrategi och instruktionsmaterial samt genomföra formativa och sammanfattande utvärderingar. Denna modell säkerställer att lektionsplanen är heltäckande och täcker alla aspekter av instruktionsprocessen.

Det är viktigt att notera att även om dessa metoder utgör en heltäckande ram för utformning och utveckling av kurser kanske de inte alltid är perfekt anpassade till de specifika målen och resurserna för ett visst kursutbud. I praktiken kan det vara nödvändigt att justera de definierade attributen för att säkerställa att kursen uppfyller de avsedda målen. Dessa metoder är avsedda att fungera som vägledning och bör anpassas till kursens unika behov och omständigheter. I slutändan är målet att använda dessa metoder för att skapa effektiva och engagerande lärandeupplevelser för studenter. Även om de utgör en solid grund för kursutformning bör de anpassas till varje kurs särskilda behov, med beaktande av faktorer som publiken, ämnet och tillgängliga resurser.

5. Ram för kursutformningen

På grundval av de angivna målen och resurserna för kursutformningen antas följande ram:

1. Lärandemål: Att täcka bristen på cybersäkerhetskunskaper i smarta nät
2. Förutsättningar: Kursen ska endast vara öppen för studenter och yrkesverksamma med förhandskunskap på områdena cybersäkerhet och smarta nät.
3. Behållningsnivå som planeras av den här kursen: 60–75 %, genom aktiva diskussioner och enkel praktik genom att utföra uppgifter

4. Antagna instruktiondesignmetoder: ADDIE- och Dick- och Carey-modeller för design och som är inriktade på den tredje nivån – tillämpning – av Blooms taxonomi för behållning.
5. Metoder som används: I huvudsak omvänt lärande och gamification (spelifiering), med uppgifter som främjar samarbetsinriktat lärande
6. Genomförandemetod: Övervakade inspelade sessioner
7. Kriterier för att öka uppmärksamhet och engagemang: Bonuspoäng, användning av spel och diskussionsforum
8. Bedömning och mätning: Regelbundna frågesporter och en slutexamen, helst automatiserade självutvärderade.
9. Kursbelastning: 125–140 timmar föreläsningar, övningar och självstudiematerial

6. Kursinnehåll

Den designade kursen är indelad i tre delar. Del ett omfattar smarta elnät, cybersäkerhet och elnät. Del två täcker realtidssimulering, teori. Slutligen, del tre handlar om att bygga upp praktiska färdigheter genom att tillhandahålla övningar och case-scenarier. Dessa tre delar omfattar sju kapitel och fyra praktiska övningar på området. I nästa underavsnitt presenteras huvudpunkterna i varje kapitel kortfattat.

6.1 Del 1: Smarta nät, cybersäkerhet och elnät

6.1.1 Kapitel 1: Grunderna i smarta nätsystem

Detta kapitel innehåller huvudkoncept för smarta nätsystem, inklusive komponenter i det smarta nätet, drivkrafter för smarta nät, de viktigaste fördelarna och utmaningarna som genomförandet och förverkligandet av det smarta nätet och modellen för smart nätarkitektur. Kapitlet fortsätter med att introducera teknik för smarta nät vad gäller ramverk, funktioner och kapacitet, resurser och energilagringssystem, mikronät, smarta understationer och kommunikationsprotokollet IEC 61850. Sedan kommer utmaningarna och framgångsfaktorerna i nätet, där sex utmaningar som omfattar affärsomvandling, konvergens av verksamhet, integrerad systemstrategi, komplexiteten i att ha ett heterogent system, cybersäkerhet och slutligen integritet, införs, följt av de viktigaste framgångsfaktorerna i nätet. Slutligen innehåller de sista avsnitten i kapitlet de globala initiativen om smarta nät, särskilt på den europeiska marknaden, och framtiden för smarta nät.

6.1.2 Kapitel 2: Cybersäkerhet och driftsäkerhet i smarta nät

Detta kapitel behandlar nätets säkerhetsaspekter, inklusive hackning av nätet och de huvudsakliga attackmetoderna, säkerhetsmodeller för SCADA (Supporty Control and Data Acquisition), industriella kontrollsystem (ICS) och smarta nät, och avslutar med metoder för säkerhet för det smarta nätet, inklusive införande av säkerhetskontroller, skydd av fältzoner, skydd av kontrollzoner, skydd av tjänstezoner, upprättande av starka gränser och zonseparering, avancerad nätmentoring, skydd av data och applikationer samt situationsmedvetenhet.

6.1.3 Kapitel 3: IEC 61850 och IEC 62351

IEC 61850 har länge använts som standardprotokoll för smart nätkommunikation. Detta kapitel behandlar de viktigaste aspekterna och arkitekturen i denna standard och ger också introduktion till det kompletterande säkerhetsprotokollet IEC 62351 som används för att upprätta ett säkerhetsskikt utöver IEC 61850.

6.2 Del 2: Realtidssimulering, teori

6.2.1 Kapitel 4: Grundprinciper för simulering

Detta kapitel behandlar huvudkoncepten för simuleringsteknologi. Detta omfattar diskreta, kontinuerliga modeller och hybridmodeller, höghastighetshybridsimulering i realtid, formaliserad metod för utformning av distribuerade system, modellering med hjälp av DEVS (Dicrete Event System Specification) och UML-språk (Unified Modeling Language) och verktyg för integrering med MATLAB och Simulink.

6.2.2 Kapitel 5: Realtidssimulering för systemdesign

Detta kapitel behandlar koncepten systemutformning, inklusive progressiv simulering, Hardware in the Loop (HIL) och Software in the Loop (SIL), validering och valideringsverktyg, och slutligen konceptet användning av Rapid Control Prototyping (RCP) för att underlätta systemdesign och testning.

6.2.3 Kapitel 6: Parallell och distribuerad realtidssimulering

I detta kapitel introduceras en testbädd med hjälp av DNP3-protokollet. Därefter betonas användningen av systemmetoden för simulering för utbildning.

6.2.4 Kapitel 7: Verktyg och applikationer

I detta kapitel presenteras konceptet tidsdilatation, vilket innebär att korrekt simulering i storskaliga system kan uppnås. Relaterade begrepp som virtualiserade system, CPU-schemaläggning, nätverksemulering och minnesemulation, introduceras också.

6.3 Del 3: Övningar och case-scenarier

6.3.1 Övning 1

En guide för att komma igång med realtidssimulator EXATA CPS och HYPERSIM OPAL-RT

6.3.2 Övning 2

Samordnade realtidssimuleringar i Microgrid Active Power Management mot fördröjningsattacker

6.3.3 Övning 3

Samordnade realtidssimuleringar av en Microgrid Active Power Management mot ändring av datapaketattack

6.3.4 Övning 4

Samordnade realtidssimuleringar i Microgrid-baserade on Controller Hardware in the Loop HIL

7. Verktyg

Verktyg som används under hela kursen inkluderar verktyg för inlärningsstöd och verktyg för övningar och praktiska färdigheter, enligt följande:

1. Verktyg för inlärningsstöd: Dessa är de verktyg som används för att hjälpa till i inlärningsprocessen. Eftersom den kurs som erbjuds är i form av en MOOC används en särskild databas (MOODLE) där lärandematerial, diskussionsforum, frågesporter och onlineundersökningar finns samlat. Andra verktyg som kan användas är kommunikations- och videostreamingverktyg samt verktyg för att utforma presentationer och videoredigering.
2. Verktyg för praktiska färdigheter: I denna kurs används OPAL-RT-systemet, som är en realtidssimulator, för att genomföra utbildningstillfällen och för att förse deltagarna med de färdigheter som identifierades i kursmålen.

8. Litteraturförteckning

[1] European Technology Platform, European Commission, “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] Europeiska kommissionen(2020). Europa som investerar i digitalisering: programmet för ett digitalt Europa. 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, och 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, and Jose M. de Fuentes. "Design recommendations for online cybersecurity courses." Computers & Security 80 (2019): 238-256.

[10] Scott, Bernard, and 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. och Rebecca Brent. ”Active learning: An introduction.” ASQ higher education brief 2.4 (2009): 1-5.

[18] Felder, Richard M. och Rebecca Brent. ”Cooperative learning.” Active learning: Models from the analytical sciences 970 (2007): 34–53.

[19] Bergmann, Jonathan och 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] Engelska, Mary C. och 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. och 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 och Junfeng Yang. Educational technology a primer for the 21st century. Springer, 2019.
[27] Brown, Abbie H., och 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 och Pieter J. Mosterman, red. Real-time simulation technologies: Principles, methodologies, and applications. CRC Press, 2017.
[30] Poudel, Shiva, Zhen Ni och 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.