Die Schulung Cybersicherheit in intelligenten Stromnetzen Wissensfundus Roadmap für Entwicklung und Umsetzung (Kurzbericht)

Verfasser:

Rūta Pirta-Dreimane, Jana Bikovska, Andrejs Romānovs, Maria Valliou, Bahaa Eltahawy, Jānis Pekša

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

Erasmus+ Strategisches Partnerschaftsprojekt

Intellektuelle Leistung 4

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

Abkürzungen 3

1. Einführung 4

2. Modell für Lehrpläne 4

2.1 Modell für den Inhalt der Lehrpläne 5

2.2 Entwicklungsmethologie für Schulungsprogramme 7

2.3 Methoden- und Tool-Bank 9

3. Empfehlungen für Schulungslehrpläne 10

3.1 Profile der Lernenden 10

3.2. Arbeitsrollen und Aufgaben 10

3.3. Wissensbereiche und Wissenseinheiten 11

3.4. Methoden- und Tool-Bank 11

Referenzen 13

Abkürzungen

ACM Association for Computing Machinery (Verband für Rechenmaschinen)
NICE Nationale Initiative für Schulungen im Bereich Cybersicherheit
CC-RSG Cybersecurity Curricula Recommendations for Smart Grids (Empfehlungen für Cyberssicherheits-Lehrpläne für intelligente Stromnetze)
CPES Center for Power Electronics Systems (Center für Leistungselektroniksysteme)
ENISA Europäische Agentur für Netz- und

Informationssicherheit
EU Europäische Union
JTF Gemeinsame Task Force
IT Informationstechnologie
IO Intellektuelle Leistung
MOOC Massive Open Online Course (massiver offener Onlinekurs)
NIST National Institut für Normen und Technologie
PMU Phasenmessgeräte
OT Betriebstechnologie
SCADA Supervisory Control and Data Acquisition
KMU Kleine und mittelständische Unternehmen
VET Berufsausbildung
WP Arbeitspaket

1. Einführung

Cybersicherheit wird als eine der europäischen strategischen Fähigkeiten definiert, und es wurde anerkannt, dass die EU ihre digitalen Fähigkeiten im Bereich Cybersicherheit erheblich verbessern muss [1]. Dies schließt den Einsatz digitaler Technologien sowie die notwendigen digitalen Fähigkeiten für EU-Arbeitskräfte ein. Cybersicherheit ist ein interdisziplinäres Fach [2]- [3], um alle wesentlichen Kompetenzen sicherzustellen, müssen mehrere Dimensionen und Disziplinen in Schulungsprogramme integriert werden, wie Informatik, Maschinenbau, Psychologie, Soziologie und Recht. Cybersicherheitsspezialisten müssen ein tiefgehendes technisches Verständnis haben, aber auch allgemeine Fähigkeiten sind wesentlich, vor allem in Krisensituationen.

Das Umfeld intelligenter Stromnetze beinhaltet eine zusätzliche Komplexität in Bezug auf die Cybersicherheit. Ein intelligentes Stromnetz integriert eine Vielzahl von Sensoren, Steuersystemen und Kommunikationsnetzwerken, was die Angriffsfläche für einen Cyberangriff erhöht. Cybersicherheitspezialisten, die im Umfeld intelligenter Stromnetze arbeiten, müssen eine breite Vielfalt an Kompetenzen haben, um die Infrastruktur zu schützen, wobei Cybersicherheit und Elektrotechnikkompetenzen sowie auch soziale Kompetenzen ausgewogen sein müssen.

Dieses Dokument repräsentiert die WP4-Ergebnisse des Projekts „Empfehlungen für Cyberssicherheits-Lehrpläne für intelligente Stromnetze (CC-RSG) Cybersicherheit Curricula Recommendations for Smart Grids (CC-RSG)". Mit dieser Arbeitsaktivität wird die Konzipierung der bei dem Projekt gewonnenen Erkenntnisse und die Bereitstellung von Empfehlungen für die Entwicklung eines Lehrplans zum Thema Cybersicherheit für intelligente Stromnetze angestrebt.

Das Hauptziel des Dokuments ist die Bereitstellung von Empfehlungen für Ausbilder und sonstige relevante Parteien für die Entwicklung von Schulungsprogrammen unter Berücksichtigung des Bedarfs der Industrie, den Anforderungen der Arbeitskräfte, studentenzentrierter Schulungsmethoden und auftretender Support-Tools.

2. Modell für Lehrpläne

Das Ziel des Modells ist die Bereitstellung von Leitfäden für kompetenzorientierte Cybersicherheit-Schulungsprogramme für die Entwicklung, die Ausführung und die Bewertung von intelligenten Stromnetzen. Das Modell erklärt, wie ein Wissensfundus (z.B. dieses Dokument) genutzt werden sollte, um die Integration von Arbeitskraft- und Schulungsdimensionen zu integrieren.

Das Modell basiert auf der der in [4] vorgeschlagenen Methodologie und besteht aus drei Bausteinen (Abbildung 1):

1. **Der Inhalt von Lehrplänen** definiert Rollen und aufgabenspezifische Kompetenzen und verbundene Wissensbereiche, Wissenseinheiten, Lernthemen und Lernergebnisse.
2. **Die Designmethodologie von Schulungsprogrammen** schlägt Prinzipien und Verfahren für die Entwicklung, die Ausführung und die Bewertung von Studienprogrammen und Kursen vor.
3. **Die Tools- und Methodenbank** schließt eine Listen mit Methoden und Tools ein und Anleitungen (Muster) für ihre Nutzung. Die Listen können bei der Entwicklung, Ausführung und Bewertung von Cybersicherheits-Schulungsprogrammen für intelligente Stromnetze verwendet werden.

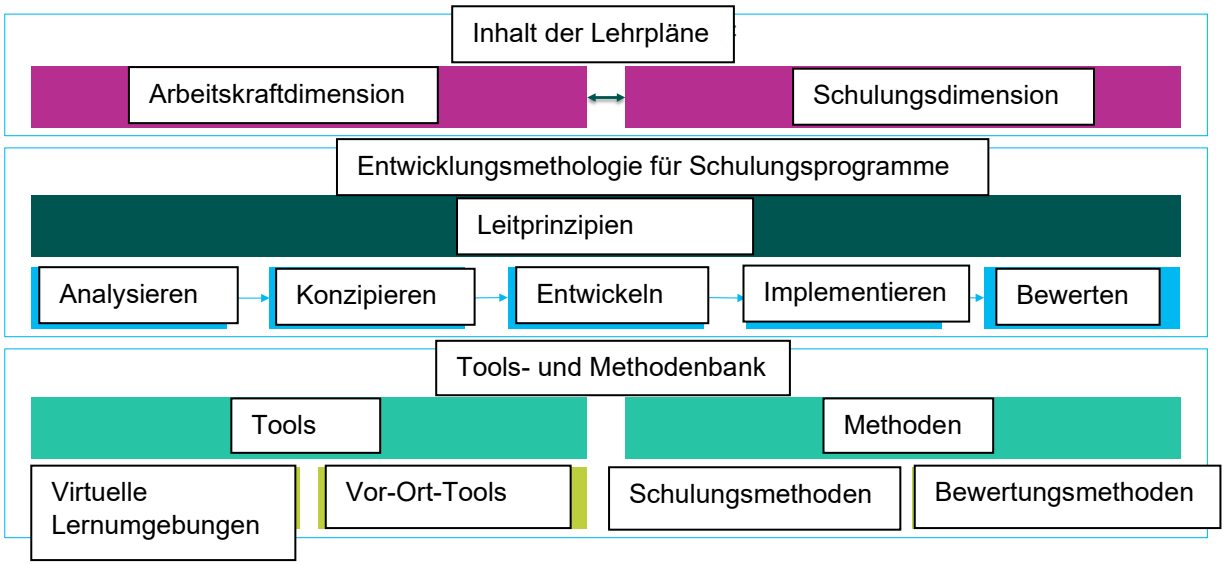

Abbildung 1 Übersicht über das Modell für Lehrpläne

2.1 Modell für den Inhalt der Lehrpläne

Lehrpläne müssen auf der Grundlage der Arbeitskraftanforderungen konzipiert werden, um sicherzustellen, dass die Kompetenzen der Cybersicherheitsspezialisten der Nachfrage der Branche entsprechen, einschließlich Fähigkeiten, die gelehrt werden müssen, und Kompetenzfelder, die abgedeckt werden müssen [2].

Das vorgeschlagene Modell für Lehrpläne umfasst zwei Dimensionen – die Arbeitskraftdimension und die Schulungsdimension (Abbildung 2).

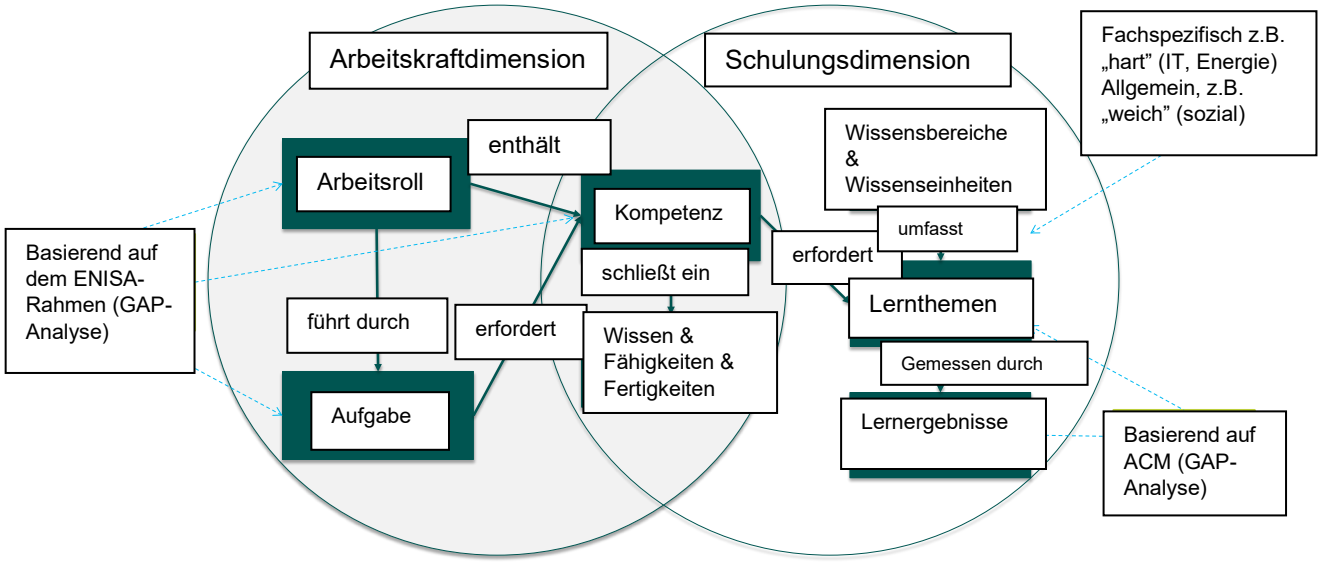

Abbildung 2 Übersicht über das Modell für Lehrpläne

Die Arbeitskraftdimension schließt die folgenden wesentlichen Konzepte ein [5]:

- **Arbeitsrollen** sind die detailliertesten Gruppierungen der mit der Cybersicherheit verbundenen Arbeit, einschließlich einer Liste der Eigenschaften, z.B. Kenntnisse, Fähigkeiten und Fertigkeiten, die notwendig sind, um die mit der Rolle verbundenen Aufgaben auszuführen.
- **Aufgaben** repräsentieren spezifische Arbeiten, die in Kombination mit anderen identifizierten Aufgaben den Umfang der Arbeit in einem spezifischen Fachgebiet oder einer bestimmten Arbeitsrolle ausmachen.
- **Kompetenzen** beschreiben die Fähigkeiten der Anwendung und Nutzung von Wissen, Fähigkeiten, Fertigkeiten, Verhalten und persönliche Eigenschaften, die notwendig sind, um wesentliche Arbeitsaufgaben, spezifische Funktionen erfolgreich auszuführen oder in einer bestimmten Rolle oder Position tätig zu sein. Bei den Fähigkeiten ist es wichtig, zwischen fachspezifischen (z.B. „harten Fähigkeiten") und allgemeinen (z.B. „sozialen Kompetenzen") zu unterscheiden. Zu den harten Fähigkeiten gehören technische oder administrative Kompetenz. Soziale Kompetenzen sind eine Reihe produktiver Charaktereigenschaften, die die eigenen Beziehungen in einer sozialen Umgebung charakterisieren. Dazu können gesellschaftliche Umgangsformen, Kommunikationsfähigkeiten, Sprachkenntnisse, kognitive oder emotionale Empathie, Zeitmanagement, Teamarbeit und Führungskompetenzen gehören.

Mehrere Rahmen definieren mit der Cybersicherheit verbundene Rollen, verbundene Aufgaben und erforderliche Kompetenzen, zum Beispiel Nationale Initiative für Cybersicherheitsausbildung (NICE) Arbeitskraftrahmen (NIST-NICE-Rahmen) [5] und der Fähigkeitenrahmen der Agentur der Europäischen Union für Cybersicherheit (ENISA) (ENISA-Rahmen) [6].

Für die Schulung zur Cybersicherheit in intelligenten Stromnetzen wird vorgeschlagen, das ENISA-Kompetenzmodell als Basis für das Konzept von Schulungsprogrammen zu verwenden, weil es eine einfachere Arbeitsrollenstruktur im Vergleich zum NIST hat. Die NIST-Rollen wurden hauptsächlich für große Unternehmen konzipiert, daher repräsentieren sie isolierte Cybersicherheitfähigkeiten, die über Organisationen hinweg verteilt sind. Empirische Beobachtungen zeigen, dass Unternehmen typischerweise ähnliche Rollen kombinieren und „T-förmige" Kompetenzen und multi-funktionelle Teams ermöglichen.

Vorhandene Cybersicherheits-Kompetenzmodelle konzentrieren sich auf Cybersicherheit-Governance und IT-spezifische Cybersicherheitsaspekte, aber die gehen nicht auf Cybersicherheitsrollen, Aufgaben und Kompetenzen in intelligenten Stromnetzen ein. Daher sind spezifische Cybersicherheitsaufgaben für intelligente Stromnetze in das ENISA-Modell (Abschnitt 3.2.) eingebaut. Aufgaben und Kompetenzen werden von dem Expertenteam des Projekts (Abschnitt 3) vorgeschlagen. Daher definiert dieses Dokument das Referenzmodell für Cybersicherheitsrollen und Aufgaben für intelligente Stromnetze, die die Basis für relevante Schulungsprogrammdesigns sind.

Die Arbeitskraftdimension hängt über die Kompetenzen, die Wissen, Fähigkeiten und Fertigkeiten einschließen, mit der Schulungsdimension zusammen. Die Schulungsdimension schließt die folgenden wesentlichen Konzepte ein [7]:

- **Wissensbereiche** und **Wissenseinheiten** sind thematische Gruppierungen, die zahlreiche miteinander verbindende **Lernthemen einschließen**.

- **Lernergebnisse** repräsentieren detailliertere Ergebnisse als die Kompetenzen und können als die Ergebnisse der gelernten Lektionen betrachtet werden. Lernergebnisse betonen, was die Studenten tun können im Vergleich dazu, was die Studenten nur wissen.

Mehrere Empfehlungen für Cybersicherheitslehrpläne schlagen wichtige Wissensbereiche, Wissenseinheiten, Lernthemen und Lernergebnisse vor. Beispielsweise der Leitfaden für Cybersicherheitlehrpläne für Associate-Degree-Programme (Cyber2yr2020), der von dem Ausschuss für Computerschulung in Community Colleges des Verbandes für Rechenmaschinen vorbereitet wurde, in [7] und die globalen Empfehlungen für Cybersicherheitslehrpläne der CSEC2017 Gemeinsame Task Force für die Cybersicherheitsschulung (JTF) [3].

Für die Schulung zur Cybersicherheit in intelligenten Stromnetzen wird vorgeschlagen, die Cyber2yr2020-Leitlinien für die Definition von IT-spezifischen Cybersicherheit-Wissenseinheiten, Wissensbereichen, Themen und Lernergebnissen anzuwenden. Eine Cybersicherheitsschulung spezifisch für intelligente Stromnetze wird in begrenztem Umfang in bestehenden Rahmen angesprochen, daher werden spezifische Cybersicherheitskompetenzen, Lernthemen und Lernergebnisse für intelligente Stromnetze in das Modell Cyber2yr2020 aufgenommen. Spezifische Cybersicherheitskompetenzen, Lernthemen und Lernergebnisse für intelligente Stromnetze werden von dem Expertenteam des Projekts vorgeschlagen (Abschnitt 3.3.).

In diesem Dokument werden die Kompetenzen in vier Gruppen unterteilt:

- IT-spezifische Kompetenzen definieren das Wissen, die Fähigkeiten und die Fertigkeiten, die notwendig sind, um IT-spezifische Cybersicherheitausaufgaben auszuführen. Diese Kompetenzen basieren auf den Leitlinien Cyber2yr2020 (nur wesentliche Kompetenzen). Diese Kompetenzen definieren ‚was-ist-zu-tun'_Aspekte [7].
- Kompetenzen, die für intelligente Stromnetze spezifisch sind, definieren das Wissen, die Fähigkeiten und die Fertigkeiten, die notwendig sind, um für intelligente Stromnetze spezifische Cybersicherheitausaufgaben auszuführen. Diese Kompetenzen werden von dem Expertenteam des Projekts vorbereitet und von Experten der Branche validiert. Diese Kompetenzen definieren ‚was-ist-zu-tun'_Aspekte [7].
- Betriebliche Kompetenzen umfassen Führungs- und betriebliche Kompetenzen, die definieren, ‚wie Aktivitäten ausgeführt werden sollten', und zwar sowohl in IT-spezifischen als auch für intelligente Stromnetze spezifischen Bereichen.
- Allgemeine Kompetenzen definieren erwartete ‚soziale Kompetenzen'.

2.2 Entwicklungsmethologie für Schulungsprogramme

Die Entwicklungsmethologie für Schulungsprogramme definiert allgemeine Prinzipien, die eingehalten werden müssen, und wichtige Schritte, wie Schulungsprogramme definiert werden sollten (Abbildung 2). Bei der Definition, Ausführung und Bewertung des Programms können Ausbilder das Kompetenzmodell für intelligente Stromnetze und die in diesem Dokument beschriebenen Lehrplanempfehlungen verwenden. Der präzise Inhalt muss jedoch auf die Profile der Lernenden des Programms und ihre Bedürfnisse (Zielrollen usw.) ausgerichtet werden.

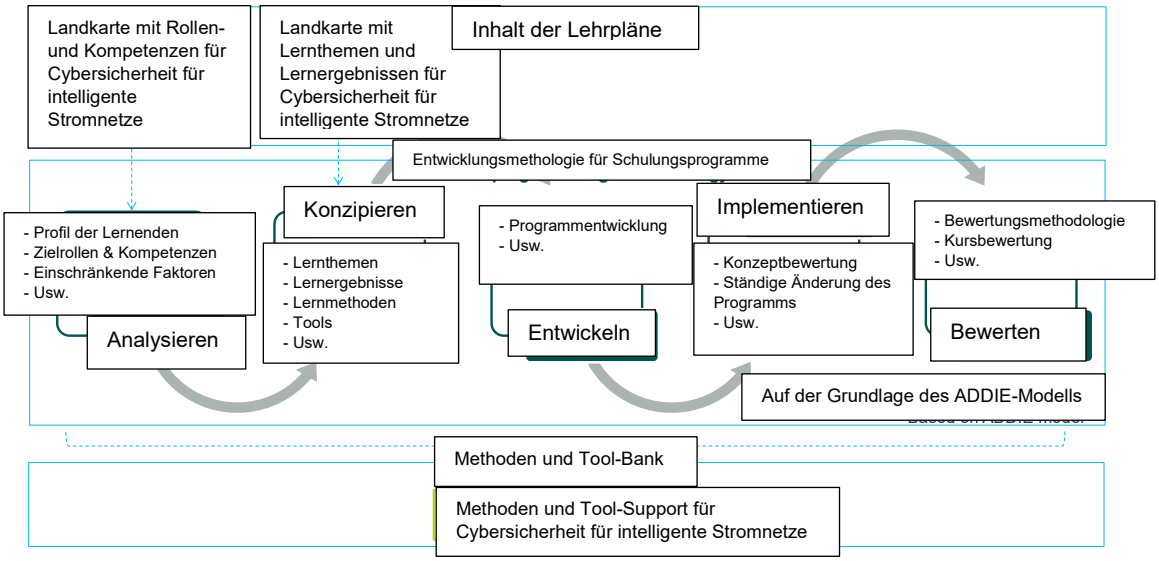

Abbildung 3 Entwicklungsmethologie für Schulungsprogramme

Schulungsprogramme sollten unter Einhaltung mehrerer Leitprinzipien vorbereitet werden. Nach dem Design-Thinking-Ansatz über die Nutzung in der Schulungskonzipierung [8], [9] werden Designprinzipien häufig verwendet, um die Hauptrichtung festzulegen, die bei der Konzipierung und Ausführung von Programmen befolgt werden müssen [10]. Die Designprinzipien werden definiert als [9]: "...Ein Zwischenschritt zwischen wissenschaftlichen Ergebnissen, die generalisiert und wiederholbar sein müssen, und lokalen Erfahrungen oder Beispielen, die in der Praxis auftreten. Wegen der Notwendigkeit, Designprinzipien zu interpretieren, lassen sie sich nicht so einfach verfälschen wie wissenschaftliche Gesetze. Die Prinzipien werden induktiv von früheren Erfolgsbeispielen erzeugt und unterliegen einer Verfeinerung im Laufe der Zeit, wenn andere versuchen, sie an ihre eigenen Erfahrungen anzupassen". Designprinzipien eruieren Designwissen aus erfolgreichen Lernumgebungen [10] und fassen wieder verwendbare Best Practices zusammen.

Für Schulungen zur Cybersicherheit in intelligenten Stromnetzen wird die Einhaltung der folgenden Kernprinzipien vorgeschlagen:

1) **Zielrollen und aufgabenorientiertes Kompetenzdesign** - Kompetenzen müssen auf der Basis der Zielrollen der Lernenden definiert werden, um eine Integration der Arbeitskraft- und Schulungsdimensionen zu ermöglichen.
2) **Orientierung an den Lernenden und Personalisierung** – Studienprogramme müssen sich auf die Bedürfnisse der Studenten konzentrieren und eine profilspezifische Kompetenzentwicklung bieten.
3) **Synergie zwischen fachspezifischen und allgemeinen Kompetenzen** – allgemeine Kompetenzen müssen zusammen mit fachspezifischen Kompetenzen in jedes Lernfach integriert werden.
4) **Integration von Erfahrungen aus der echten Welt** – Studienprogramme und Kursinhalte müssen Herausforderungen aus der echten Welt widerspiegeln und sich im Laufe der Zeit anpassen.

5) **Vertikale Integration** – Cybersicherheit ist ein multidisziplinäres Fach; Programme müssen Sozialwissenschaften (wie Psychologie) integrieren, um die Entwicklung allgemeiner Kompetenzen zu ermöglichen.
6) **Ständige Verbesserung auf der Basis von Feedback** – eine ständige Verbesserung aufgrund des Feedback von Lernenden und Arbeitskräften muss geplant werden.

Der vorgeschlagene Designprozess für das Schulungsprogramm basiert auf dem ADDIE-Modell [11]. Das ADDIE-Modell ist der generische Prozess, der herkömmlich von Instruktionsdesignern und Schulungsentwicklern verwendet wird. Das Modell schließt fünf Phasen ein:

1. **Analyse** - die Analyse des Profils der Lernenden (einschließlich ihrer Eigenschaften, vorhandener Kompetenz, erwarteter Zielrollen und ihres Schulungsbedarfs), Definition der Lehrziele und der sonstigen Ziele. Das Programm muss so konzipiert werden, dass es Kompetenzen einschließt, die für die Zielrollen der Lernenden erforderlich sind. Dieses Dokument schließt typische Cybersicherheitsrollen ein, die durch für intelligente Stromnetze spezifische Cybersicherheitsaufgaben und Kompetenzen bereichert werden (Abschnitt 3.2.). Dieses Dokument kann als Referenzmodell für die Kartierung der Zielrollen der Lernenden verwendet werden. Die Rollen werden auf der Basis typischer Profile der Lernenden für die Cybersicherheit in intelligenten Stromnetzen konzipiert (Abschnitt 3.1.), die auf der Grundlage der Erfahrung der Projektexperten definiert werden.
2. **Konzipierung –** Ziele des Studienprogramms, Definition der Lernthemen, Lernergebnisse und Lehrmethoden. Dieses Dokument definiert die Reihe der Lernthemen und Lernergebnisse, die definierte Rollen benötigen (Abschnitt 3.3.). Diese Themen sind eingekapselt in Wissenbereiche und -einheiten. Eine Karte mit Arbeitsrollen, Aufgaben, Kompetenzen und Lernthemen wird in Anhang 1 hinzugefügt. Die Themen müssen auf der Basis der Zielrollen ermittelter Lernender ausgewählt werden. Lernende können auf der Basis vorhandener Kompetenzen individuelle Pläne haben (wenn z.B. ein Lernender eine Ausbildung in IT-spezifischer Cybersicherheit und anstrebt, ein Sicherheitsarchitekt in einer Institution des Energiesektors zu werden, muss er spezifische Cybersicherskompetenzen für intelligente Stromnetze erwerben). Das Dokument schließt eine Methodenbank (Abschnitt 4) und eine Tool-Bank (Abschnitt 5) ein, die zur Unterstützung des Schulungsprogrammdesigns verwendet werden können.
3. **Entwicklung** – Entwicklung der Studienprogrammmaterialien und Hochladen in E-Learning-Systeme (falls zutreffend).
4. **Implementierung – tatsächliche Bereitstellung des Programms und der Kurse.**
5. **Bewertung –** Erfassung von Feedback und Daten für die Ermittlung von Verbesserungsbereichen. Das Dokument schließt eine Methodenbank (Abschnitt 4) und eine Tool-Bank (Abschnitt 5) ein, die zur Unterstützung der Bewertung des Schulungsprogramms verwendet werden können.

2.3 Methoden- und Tool-Bank

Die Methodenbank und die Tool-Bank (Abschnitt 4) schlagen die Methoden und Tools vor, die die Designer und Lehrkräfte des Studienprogramms bei allen Prozessphasen der Schulungsentwicklung verwenden können (Analyse, Konzipierung, Entwicklung,

Implementierung und Bewertung). Methoden und Tools werden in der Form wiederverwerndbarer Muster definiert, die eine Wissensbasis für das Kursdesign und die Ausführungsunterstützung verwendet werden können. Die Verknüpfung der Methoden und Tools mit den Phasen des Schulungsdesigns und des Ausführungsprozesses werden auf jeder Methoden- /Tool-Karte beschrieben.

3. Empfehlungen für Schulungslehrpläne

Die Empfehlungen für Schulungslehrpläne bilden das Referenzmodell für die Integration von Arbeitskräften und Schulung. Sie enthalten folgende Hauptkonzepte:

- **Die Profile der Lernenden** – typische Profile der Lernenden für Cybersicherheit in intelligenten Stromnetzen bilden die Grundlage für die Definition der Zielarbeitsrollen;
- **Arbeitsrollen und Aufgaben** repräsentieren die Zielrollen der Lernenden, die Aufgaben und die erforderlichen Kompetenzen (einschließlich IT-spezifischer Cybersicherheitskompetenzen, für intelligente Stromnetze spezifische Cybersicherheitskompetenzen, betriebliche und allgemeine Kompetenzen);
- **Wissenseinheiten und Wissensbereiche** definieren die **Lernthemen und Lernergebnisse,** die notwendig sind, um Kompetenz zu erlangen.

3.1 Profile der Lernenden

Der Zweck des Studentenprofils besteht darin, die Gruppen von Studenten hervorzuheben, auf die das Lehrplanmodell angewandt werden kann.

Hier sind zwei Gruppen von Absolventen, die daran interessiert sein könnten, ihre Schulung im Bereich Cybersicherheit für intelligente Stromnetze fortzusetzen: Absolventen der Bereiche Informatik und Stromsysteme. Die anderen beiden Gruppen mit Fachleuten sind entweder in den Bereichen IT und OT oder im Management von intelligenten Stromnetzen tätig. Sie haben Arbeitserfahrung in Stromsystemen und intelligenten Stromnetzen, aber sie benötigen mehr Fortgeschrittenenwissen im Bereich Cybersicherheit für intelligente Stromnetze.

Die folgenden Attribute werden für das Profil in Erwägung gezogen:

- Der Hintergrund bezieht sich auf die absolvierte Ausbildung oder die beruflichen Fähigkeiten eines Lernenden;
- Der Schulungsbedarf ist die Lücke zwischen dem derzeitigen Wissen, den Fähigkeiten und der Haltung des Lernenden und den gewünschten, damit er sich an eine neue Situation anpassen kann, was durch eine Schulung erreicht werden kann.
- Die Erwartungen beschreiben das Wissen und die Fähigkeiten, von denen erwartet wird, dass die Studenten sie am Ende ihrer Schulung beherrschen.

Die Energiebranche benötigt Arbeitskräfte, die sich mit Cybersicherheit auskennen, und eine höhere Ausbildung könnte eine wichtige Rolle dabei spielen, diese Lücke zu füllen.

3.2. Arbeitsrollen und Aufgaben

Die Arbeitsrollen für Cybersicherheit in intelligenten Stromnetzen wurden im gemäß den von ENISA vorgeschlagenen Rollen aufgebaut: Chief Information Security Officer (CISO), Reaktionsverantwortlicher für Cybervorfälle, Cybersicherheitsjurist, Policy & Compliance Officer, Cybersicherheitsarchitekt, Cybersicherheitsprüfer, Cybersicherheitsumsetzer und Cybersicherheits-Risikomanager. Die Rollen,

Aufgaben und Kompetenzen wurden gemäß den spezifischen Angaben des intelligenten Stromnetzes ergänzt.

Die ENISA-Rollen wurde durch neue Rollen ergänzt, bei denen die Spezifikationen von intelligenten Stromnetzen berücksichtigt wurden – Energy Citizen, Netzanlagenmanager und Netzkommunikationsingenieur. Die gemeinsamen Geschäftsziele für die spezifischen Rollen für intelligente Stromnetze sind [12]: Aufrechterhaltung der Sicherheit, Aufrechterhaltung der Zuverlässigkeit des Stromnetzes, Aufrechterhaltung der Resilienz des Stromnetzes und Modernisierung des Unterstützungsnetzes.

3.3. Wissensbereiche und Wissenseinheiten

Wissensbereiche und -einheiten basieren auf dem „Leitfaden für Cybersicherheitlehrpläne für Associate-Degree-Programme (Cyber2yr2020), der von dem Ausschuss für ComputerSchulung in Community Colleges (CCECC) des Verbandes für Rechenmaschinen (ACM) erstellt wurde: Datensicherheit, Softwaresicherheit, Komponentensicherheit, Verbindungssicherheit, Systemsicherheit, menschliche Sicherheit, Organisationssicherheit, gesellschaftliche Sicherheit. Sie werden bereichert durch für intelligente Stromnetze spezifische Kompetenzen, die für definierte Arbeitsrollen erforderlich sind (3.2. Abschnitt). Der neue Wissensbereich „Sicherheit in intelligenten Stromnetzen" ergänzt den ACM-Rahmen.

3.4. Methoden- und Tool-Bank

Die Methoden und Tool-Bank schlägt Methoden und Tools vor, die für die Schulung zur Cybersicherheit in intelligenten Stromnetzen verwendet werden können: Simulationstools, CPES-Laboratorien und Testbeds, die Gamifizierung, das problem- und projektbasierte Lernen und das „Flipped Learning". Eine schnelle Art für die Lehrer/Ausbilder, die einen Lehrplan formulieren wollen, um die Basiselemente der Methode und die gewöhnlichen Nutzungsfälle zum Thema Cybersicherheit und/oder intelligente Stromnetze zu sehen. Mit den Schulungsmethoden wird auch das Tool der Simulations-Testbeds mit Nutzungsfällen beschrieben.

Testbeds werden verwendet, um in realen Systemen in verschiedenem Ausmaß zu simulieren. Einige Testbeds verwenden Software-Simulation für Teile des Systems, anderen nutzen nur Hardwarekomponenten. Außerdem gibt es Testbeds, die nur eine Komponente des Systems simulieren, andere simulieren das gesamte System. Die Verwendung eines Echtzeitsimulators in Kombination mit realer Hardware (wie Wechselrichter und PMUs), um ein gesamten Mikronetz zu simulieren, ist die realistischste und vollständigste Weise, um das Verhalten eines Stromnetzes bei einem Cyberangriff zu studieren.

Die Gamifizierung ist eine Lehrmethode, bei der Elemente und Mechanismen des Spieldesigns verwendet werden, um die Motivation der Studenten zu erhöhen [13]. Solche Elemente und Mechanismen können beispielsweise eine Erzählung sein, die auf die Ausführung einer Aufgabe beschränkt ist, Punkte, Abzeichen und das Erreichen verschiedener Levels.

Bei dem problembasierten Lernen (PBL) untersucht eine Gruppe von Studenten ein Problem der realen Welt mit einem offenen Ende und versucht, die geeignetstes Lösung zu finden, die die Gruppe dann ihren Mitstudenten präsentiert. Das projektbasierte Lernen basiert auf derselben Idee, dauert aber im Allgemeinen länger, und es wird ein konkretes Ergebnis anstelle einer theoretischen Lösung bereitgestellt.

Die Haupteigenschaften des Flipped Learning sind, dass die Studenten das Material, dass im Allgemeinen im Unterricht studiert wird, selber zu Hause studieren. Auf diese Weise haben sie im Unterricht die Gelegenheit, über das studierte Material nachzudenken, und sie haben Zeit für Experimente.

Referenzen

[1] Europäische Kommission, „Die Cybersicherheitsstrategie der EU für das digitale Jahrzehnt," 2020. [Online]. Verfügbar: https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta, and R. De Nicola, "Framework, Tools and Good Practices for Cybersicherheit Curricula," *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3093952.

[3] Joint Task Force on Cybersicherheit Education, *Curricula 2017 Cybersecurity Curriculum - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*, Vol. Version 1., Nr. Dezember. 2017.

[4] R. Pirta-Dreimane, A. Brilingaite, E. Roponena, and K. Parish, "Multi-dimensional Cybersecurity Education Design: A Case Study," in *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, IEEE, Sep. 2022, S. 1–8. doi: 10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927931.

[5] D. S. M. C. S. K. A. W. and G. W. R. Petersen, "Workforce Framework for Cybersecurity (NICE Framework)," 2020.

[6] E. Agentur der Europäischen Union für Cybersicherheit , „Rahmen für europäsche Cybersicherheitsfähigkeiten," *https://www.enisa.europa.eu/publications/european-Cybersicherheit-skills-framework-role-profiles*, 2022.

[7] Cyber2yr2020 Task Group, *Cybersecurity Curricular Guidance for Associate-Degree Programs*. 2020. doi: 10.1145/3381686.

[8] I. Wrogemann, L. Sarp, N. Susser, and J. Falk, "D-Learning – Design Thinking as a means to innovative product development in adult learning," *https://cesie.org/media/ d-learning-manual-en.pdf,* 2021.

[9] S. Panke, "Design Thinking in Education: Perspectives, Opportunities and Challenges," *Open Education Studies*, vol. 1, no. 1. 2019. doi: 10.1515/edu-2019-0022.

[10] Y. Kali, R. Levin-Peled, and Y. Dori, "The role of design-principles in designing courses that promote collaborative learning in higher-education. Computers in Human Behavior," *Comput Human Behav*, vol. 25, 2009.

[11] G. Morrison and S. Ross, *Designing Effective Instruction, 7th Edition*. 2013.

[12] J. Marron, A. Gopstein, N. Bartol, and V. Feldman, "Cybersecurity framework smart grid profile," Gaithersburg, MD, Jul. 2019. doi: 10.6028/NIST.TN.2051.

[13] S. Deterding, K. O'Hara, M. Sicart, D. Dixon, and L. Nacke, "Gamification: Using game design elements in non-gaming contexts," in *Conference on Human Factors in Computing Systems - Proceedings*, 2011. doi: 10.1145/1979742,1979575.