F I Ş A D I S C I P L I N E I

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea Petrol-Gaze din Ploiești
1.2. Facultatea	Inginerie Mecanică și Electrică
1.3. Departamentul	Automatică, Calculatoare și Electronică
1.4. Domeniul de studii universitare	Ingineria sistemelor
1.5. Ciclul de studii universitare	Master
1.6. Programul de studii universitare	Automatizări Avansate

2. Date despre disciplină

2.1. Denumirea disciplinei	Securitatea sistemelor de automatizare
2.2. Titularul activităților de curs	Conf. dr. ing. PRICOP Emil
2.3. Titularul activităților laborator	Conf. dr. ing. PRICOP Emil
2.4. Titularul activității proiect	-
2.5. Anul de studiu	II
2.6. Semestrul *	1
2.7. Tipul de evaluare	Verificare
2.8. Categoria formativă** / regimul*** disciplinei	DF/DFA

* numărul semestrului este conform planului de învățământ;

** DF - Discipline fundamentale; DS - discipline de specializare; DC - discipline complementare

*** obligatorie/impusă = DOB; opțională = DOP; facultativă = DFA

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1. Număr de ore pe săptămână	2	din care: 3.2. curs	1	3.3. Laborator	1	3.4. Proiect	-
3.5. Total ore din planul de învățământ	28	din care: 3.6. curs	14	3.7. Laborator	14	3.8. Proiect	-
3. 9. Total ore studiu individual (studiu după suport de curs, bibliografie și notițe, documentare suplimentară în bibliotecă, pe platformele electronice de specialitate, pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri)							92
3.10. Total ore pe semestru							120
3.11. Numărul de credite							4

4. Condiții (acolo unde este cazul)

4.1. de curriculum	➢ Cunoștințe de bază referitoare la rețelele de calculatoare, adresarea IP și serviciile de rețea. ➢ Cunoștințe de bază privind utilizarea calculatorului și a serviciilor Internet, precum și a diverselor aplicații specializate pentru rețele de calculatoare.
4.2. de desfășurare a cursului	➢ Sala de curs dotată cu videoproiector / tablă inteligentă și conexiune la Internet
4.3. de desfășurare a laboratorului	➢ Laborator dotat cu sisteme PC și conexiune la Internet. ➢ Existența unui software de virtualizare (VMware Fusion / Oracle VirtualBox) și a mașinilor virtuale cu Kali Linux.

5. Competențe specifice acumulate și rezultatele învățării* care stau la baza acestora

Competențe profesionale	Rezultatele învățării*
Cp3. Utilizarea sistemelor de conducere avansate adaptive, optimale, robuste, distribuite și ierarhizate și utilizarea sistemelor de comunicații în mediul industrial.	**C1** - Studentul/absolventul descrie, identifică și sumarizează concepte și metode de securitate cibernetică aplicabile sistemelor de comunicații și sistemelor de conducere din mediul industrial (arhitecturi ierarhizate, modelul Purdue, diferențe între securitatea IT și OT). **A2** - Studentul/absolventul utilizează instrumente specifice (Kali Linux, scannere de vulnerabilități, firewall-uri, honeypot-uri) pentru evaluarea și creșterea securității rețelelor și sistemelor de comunicații din mediul industrial, în mediu virtualizat de laborator. **RA2** - Studentul/absolventul selectează și utilizează surse bibliografice specifice domeniului.
Cp5. Proiectarea, monitorizarea, diagnoza și asigurarea siguranței în funcționare a sistemelor automate complexe prin utilizarea tehnicilor și metodelor inteligenței artificiale.	**C1** - Studentul/absolventul identifică și sumarizează concepte și metode de monitorizare, diagnoză și asigurare a siguranței în funcționare și a securității fizice și cibernetice a sistemelor automate complexe. **A1** - Studentul/absolventul specifică cerințe de securitate, elaborează scenarii de testare, propune soluții de rezolvare a unor probleme de securitate și siguranță în funcționare, analizează și evaluează riscurile și vulnerabilitățile sistemelor automate. **RA1** - Studentul/absolventul arată spirit de inițiativă și acțiune pentru actualizarea cunoștințelor profesionale, economice și de cultură organizațională.
Competențe transversale	**Rezultatele învățării***
Ct1. Aplicarea autonomă, în contextul respectării legislației, a principiilor, normelor și valorilor codului de etică profesională în cadrul propriei strategii de muncă riguroasă, eficientă și responsabilă.	**C1** - Studentul/absolventul descrie, identifică și sumarizează principiile de etică profesională și reglementările din domeniul securității cibernetice a sistemelor de automatizare (NIS2, Cyber Resilience Act). **A1** - Studentul/absolventul aplică normele de etică profesională și legislația din domeniu în evaluarea și securizarea sistemelor de automatizare. **RA2** - Studentul/absolventul demonstrează autonomie în învățare pe probleme specifice domeniului ingineria sistemelor.
Ct2. Definirea și asumarea responsabilă a rolurilor și responsabilităților într-o echipă plurispecializată sau în context instituțional și aplicarea de tehnici de relaționare și muncă eficientă în cadrul echipei sau în context instituțional.	**A1** - Studentul/absolventul aplică tehnici de relaționare și muncă eficientă în echipă în derularea lucrărilor de laborator și în analiza scenariilor de securitate. **RA2** - Studentul/absolventul lucrează eficient ca membru în echipă sau ca lider al acesteia.
Ct3. Identificarea autonomă a oportunităților de formare continuă și valorificarea eficientă a resurselor informaționale și tehnicilor de dezvoltare pentru propria dezvoltare, atât în limba română, cât și într-o limbă de circulație internațională.	**C1** - Studentul/absolventul descrie, identifică și sumarizează resursele de informare (standarde, ghiduri, documentații tehnice) utile pentru actualizarea competențelor în domeniul securității cibernetice a sistemelor de automatizare. **A1** - Studentul/absolventul valorifică eficient resursele informaționale, atât în limba română, cât și într-o limbă de circulație internațională, pentru propria dezvoltare profesională. **RA3** - Studentul/absolventul este angajat în învățarea pe tot parcursul vieții pentru dobândirea și implementarea cunoștințelor, după cum este necesar, folosind metode și strategii de învățare adecvate.

* C – cunoștințe; A – aptitudini; RA – responsabilitate și autonomie.

6. Obiectivele disciplinei (reieșind din grila competențelor specifice acumulate)

6.1. Obiectivul general al disciplinei	➢ La sfârșitul cursului studentul va fi familiarizat, prin cunoștințele dobândite, cu problematica evaluării și asigurării securității fizice și cibernetice a sistemelor de automatizare.
6.2. Obiectivele specifice	La sfârșitul cursului, studentul va fi capabil: ➢ să înțeleagă conceptele fundamentale specifice securității cibernetice a sistemelor informatice și a sistemelor de automatizare; ➢ să înțeleagă diferențele fundamentale între securitatea sistemelor IT și a celor de automatizare; ➢ să caracterizeze din perspectiva modelului Purdue și a reglementărilor în domeniu securitatea sistemelor de automatizare; ➢ să cunoască măsurile fundamentale necesare pentru asigurarea securității fizice și a securității cibernetice a sistemelor de automatizare; ➢ să utilizeze, în mediu de laborator controlat, instrumente specifice pentru identificarea vulnerabilităților și creșterea securității (Kali Linux, scannere de vulnerabilități, firewall-uri, honeypot-uri).

7. Conținuturi

7.1. Curs	Nr. ore	Metode de predare	Observații
Concepte generale de securitate a datelor. Principii de asigurare a confidențialității, integrității, autenticității și disponibilității datelor.	3	Interactivă și convențională, centrată pe student.	
Analiza comparativă a conceptului de securitate cibernetică IT vs. OT. Amenințări și vulnerabilități specifice.	2		
Aspecte referitoare la securitatea fizică a sistemelor de automatizare.	3		
Modelul Purdue pentru securitatea sistemelor de automatizare.	2		
Metode de creștere a securității sistemelor de automatizare.	2		
Reglementări europene în domeniul securității cibernetice a sistemelor de automatizare – Directiva NIS2 și Cyber Resilience Act (CRA).	2		

Bibliografie

1. Dutta, N., Jadav, N., Tanwar, S., Sarma, H.K.D., Pricop, E., Cyber Security: Issues and Current Trends. Studies in Computational Intelligence, vol 995. Springer, Singapore, 2022
2. Mihalache, S.F., Pricop, E., Fattahi, J., Resilience Enhancement of Cyber-Physical Systems: A Review. In: Mahdavi Tabatabaei, N., Najafi Ravadanegh, S., Bizon, N. (eds) Power Systems Resilience. Power Systems. Springer, Cham, 2019
3. Bîrleanu, F.G., Anghelescu, P., Bizon, N., Pricop, E., Cyber Security Objectives and Requirements for Smart Grid. In: Kabalci, E., Kabalci, Y. (eds) Smart Grids and Their Communication Systems. Energy Systems in Electrical Engineering. Springer, Singapore, 2019

<table>
<tr><td colspan="4">
4. Ackerman, P., Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment. Packt Publishing Ltd, 2021
5. Brooks, C.J., Craig Jr., P.A., Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT. John Wiley & Sons, 2022
6. NIST Special Publication 800-82r3, Guide to Operational Technology (OT) Security, septembrie 2023. Disponibil on-line: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf
7. Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS2)
8. Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale de securitate cibernetică pentru produsele cu elemente digitale (Cyber Resilience Act)
</td></tr>
<tr><td>7.2. Laborator</td><td>Nr. ore</td><td>Metode de predare</td><td>Observații</td></tr>
<tr><td>Descrierea și caracterizarea riscurilor de securitate specifice sistemelor de automatizare. Exemple de vulnerabilități.</td><td>2</td><td rowspan="8">Interactivă și convențională, centrată pe student. Teme pentru verificarea gradului de înțelegere a noțiunilor predate.</td><td></td></tr>
<tr><td>Configurarea și utilizarea Kali Linux. Identificarea instrumentelor disponibile.</td><td>2</td><td></td></tr>
<tr><td>Instrumente din Kali Linux pentru reconnaissance (descoperire activă și pasivă).</td><td>2</td><td></td></tr>
<tr><td>Scannere de vulnerabilități.</td><td>2</td><td></td></tr>
<tr><td>Tehnici de hacking web. Securitatea parolelor și a rețelelor wireless. Atacuri de tip SQL-injection.</td><td>2</td><td></td></tr>
<tr><td>Firewall-uri. Configurare și operare.</td><td>2</td><td></td></tr>
<tr><td>Honeypot-uri. Testarea interesului atacatorilor.</td><td>2</td><td></td></tr>
<tr><td colspan="4">Bibliografie
KALI Linux, Kali Docs – Official Documentation. Disponibil on-line: https://www.kali.org/docs/
Dutta, N., Jadav, N., Tanwar, S., Sarma, H.K.D., Pricop, E., Cyber Security: Issues and Current Trends. Studies in Computational Intelligence, vol 995. Springer, Singapore, 2022</td></tr>
<tr><td>7.3. Proiect</td><td>Nr. ore</td><td>Metode de predare</td><td>Observații</td></tr>
<tr><td colspan="4">Nu este cazul</td></tr>
<tr><td colspan="4">Bibliografie
Nu este cazul</td></tr>
</table>

8. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

- Conținuturile disciplinei sunt specifice domeniului, fiind coroborate cu așteptările comunității epistemice, ale asociațiilor profesionale și ale angajatorilor ce activează în acest domeniu.
- Prin studiul disciplinei se asigură o abordare inginerească, sistematică a modalităților de evaluare și asigurare a securității sistemelor de automatizare.

9. Evaluare

Tip activitate	9.1. Criterii de evaluare	9.2. Metode de evaluare	9.3. Pondere din nota finală
9.4. Curs	Verificare finală	Lucrare scrisă cu 25 de întrebări cu răspuns rapid sau grilă.	50%
	Verificarea cunoștințelor pe parcursul semestrului	Activitate la curs, participarea activă la discuții	10%
9.5. Laborator	Activitate laborator și verificări periodice	Verificare pe parcursul lucrărilor și la încheierea activității de laborator.	40%
9.6. Proiect	-		
9.7. Standard minim de performanță			
➢ Realizarea tuturor lucrărilor de laborator. ➢ Studentul trebuie să demonstreze cunoașterea noțiunilor de bază privind securitatea sistemelor de automatizare (definirea conceptelor triadei CIA, menționarea diferențelor între securitatea IT/OT, cunoașterea unor exemple relevante de atacuri care au vizat sisteme de automatizare, cunoașterea a cel puțin trei metode de creștere a securității cibernetice a sistemelor de automatizare, cunoașterea domeniului de aplicabilitate al Directivei NIS2).			

Data completării	Semnătura titularului de curs	Semnătura titularului de laborator	Semnătura titularului de proiect
18.09.2026	*Conf. dr. ing. Pricop Emil*	*Conf. dr. ing. Pricop Emil*	

Data avizării în departament	Director de departament	Decan
25.09.2026	*Conf. dr. ing. Pricop Emil*	*Conf. dr. ing. Bădicioiu Marius*