



Universitatea Națională de Știință și Tehnologie Politehnica București
Facultatea de Electronică, Telecomunicații și
Tehnologia Informației



FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Națională de Știință și Tehnologie Politehnica București
1.2 Facultatea	Electronică, Telecomunicații și Tehnologia Informației
1.3 Departamentul	Tehnologie Electronică și Fiabilitate
1.4 Domeniul de studii	Inginerie Electronică, Telecomunicații și Tehnologii Informaționale
1.5 Ciclul de studii	Masterat
1.6 Specializarea	Ingineria Calității și Siguranței în Funcționare în Electronică și Telecomunicații

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)				Tehnici avansate în siguranța în funcționare a sistemelor Advanced techniques in the safe operation of systems			
2.2 Titularul activităților de curs				Dr. ing. Sabina Axinte			
2.3 Titularul activităților de seminar / laborator				Dr. ing. Sabina Axinte			
2.4 Anul de studiu	2	2.5 Semestrul	I	2.6. Tipul de evaluare	E	2.7 Regimul disciplinei	Ob
2.8 Tipul disciplinei	DA	2.9 Codul disciplinei	UPB.04.M3.O.14-08	2.10 Tipul de notare	Nota		

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

3.1 Număr de ore pe săptămână	3	Din care: 3.2 curs	1.00	3.3 seminar/laborator	2
3.4 Total ore din planul de învățământ	42.00	Din care: 3.5 curs	14	3.6 seminar/laborator	28
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie și notițe Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate Pregătire seminarii/ laboratoare/proiecte, teme, referate, portofolii și eseuri					52
Tutorat					0
Examinări					6
Alte activități (dacă există):					0
3.7 Total ore studiu individual	58.00				
3.8 Total ore pe semestru	100				
3.9 Numărul de credite	4				

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Nu este cazul
4.2 de rezultate ale învățării	Acumularea unor cunoștințe de bază din domeniile: calitate / fiabilitate / mentenabilitate, standardizare și legislație în calitate și siguranță în funcționare, programare Web



5. Condiții necesare pentru desfășurarea optimă a activităților didactice (acolo unde este cazul)

5.1 Curs	Cursul se va desfășura într-o sală dotată cu videoproiector și computer
5.2 Seminar/ Laborator/Proiect	Participarea activă atât în cadrul laboratoarelor, cât și la ședințele de elaborare a proiectului (conform regulamentului studiilor universitare de masterat în POLITEHNICA București).

6. Obiectiv general *(Se referă la intențiile profesorilor pentru studenți, la ceea ce studenții vor fi învățați în timpul cursului. Oferă o orientare cu privire la locul cursului în cadrul domeniului științific abordat, precum și la rolul pe care acesta îl are în cadrul specializării studiate. Vor fi descrise de o manieră generală tematicile abordate, justificarea includerii cursului în planul de învățământ al specializării studiate etc.)*

Acest curs este proiectat cu scopul de a oferi o aprofundare a cunoștințelor de fiabilitate și siguranță în funcționare acumulate de cursanți în timpul masterului ICSFET. În consecință, se analizează o serie de metode avansate utilizate în evaluarea siguranței în funcționare a sistemelor informatice complexe. În plus, se detaliază conceptele fundamentale necesare stabilirii nivelului de siguranță în funcționare, modelarea securității sistemelor informatice în cadrul ciclului de dezvoltare software (SDLC) și îmbunătățirea utilizabilității aplicațiilor software. Cunoștințele acumulate în cadrul acestui curs creează o bază de solidă de informații, esențială pentru orice analist de fiabilitate software.

7. Competențe *(Capacitatea dovedită de a utiliza cunoștințe, aptitudini și abilități personale, sociale și/sau metodologice în situații de muncă sau de studiu și pentru dezvoltarea profesională și personală. Reflectă cerințele angajatorilor.)*

Specifice	Demonstrează că deține cunoștințe de bază / avansate privind evaluarea siguranței în funcționare a sistemelor informatice complexe. Corelează cunoștințele din domeniul securității sistemelor informatice în cadrul ciclului de dezvoltare software (SDLC). Aplică în practică cunoștințele corelate cu îmbunătățirea aplicațiilor software la nivelul siguranței în funcționare. Aplică metode și instrumente standardizate, specifice domeniului, pentru realizarea procesului de evaluare și diagnoză a unei situații, în funcție de problemele identificate/raportate, și identifică soluții. Argumentează și analizează coerent și corect contextul de aplicare a cunoștințelor de bază ale domeniului, utilizând concepte cheie ale disciplinei și metodologia specifică. Utilizează vocabularul științific specific domeniului, în vederea comunicării eficiente, în scris și oral.
Transversale (generale)	Lucrează în echipă și comunică eficient, coordonându-și eforturile cu ceilalți pentru rezolvarea de situații problemă de complexitate medie. Autonomie și gândire critică: abilitatea de a gândi în termeni științifici, de a căuta și analiza date în mod independent, precum și de a desprinde și prezenta concluzii / identifica soluții. Capacitate de analiză și sinteză: prezintă în mod sintetic cunoștințele dobândite, ca urmare a unui proces de analiză sistematică. Respectă principiile de etică academică: în activitatea de documentare citează corect sursele bibliografice utilizate. Pune în practică elemente de inteligență emoțională în gestionarea socio-emoțională adecvată a unor situații din viața reală/academică/profesională, demonstrând stăpânire de sine și obiectivitate în luarea deciziilor sau în situații de stres.

8. Rezultatele învățării (Sunt enunțuri sintetice referitoare la ceea ce un student va fi capabil să facă sau să demonstreze la finalizarea unui curs. Rezultatele învățării reflectă realizările studentului și mai puțin intențiile profesorului. Rezultatele învățării informează studenții despre ceea ce se așteaptă de la ei din punct de vedere al performanței, pentru a obține notele și creditele dorite. Sunt definite în termeni concreți, folosind verbe similare exemplurilor de mai jos și indică ceea ce se va urmări prin evaluare. Rezultatele învățării vor fi astfel redactate încât să fie evidențiată clar relația față de competențele definite la punctul 7.)

Cunoștințe	Rezultatul asimilării de informații prin învățare. Cunoștințele reprezintă ansamblul de fapte, principii, teorii și practici legate de un anumit domeniu de muncă sau de studiu. Pot fi teoretice și/sau faptice. • Enumeră etape principale care marchează evoluția software-ului și a sistemelor informatice complexe. • Definește noțiuni specifice asigurării fiabilității și securității sistemelor informatice. • Descrie/clasifică noțiuni/procese/fenomene/structuri. • Evidențiază consecințe și relații.
Aptitudini	Capacitatea de a aplica cunoștințe și de a utiliza know-how pentru a duce la îndeplinire sarcini și a rezolva probleme. Aptitudinile sunt descrise ca fiind cognitive (implicând utilizarea gândirii logice, intuitive și creative) sau practice (implicând dexteritate manuală și utilizarea de metode, materiale, unelte și instrumente). • Selectează și grupează informații relevante într-un context dat. • Utilizează argumentat principii specifice în vederea asigurării fiabilității și securității software-ului. • Lucrează productiv în echipă. • Elaborează un text științific. • Verifică experimental soluții identificate. • Rezolvă aplicații practice. • Interpretează adecvat relații de cauzalitate. • Analizează și compară standarde, regulamente și documentații referitoare la ciclul de dezvoltare software (SDLC). • Identifică soluții și elaborează planuri de rezolvare/proiecte. • Formulează concluzii la experimentele realizate. • Argumentează soluțiile identificate/modurile de rezolvare.
Responsabilitate și autonomie	Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale. • Selectează surse bibliografice potrivite și le analizează, respectând principiile de etică academică și citând corect sursele bibliografice utilizate. • Demonstrează receptivitate pentru contexte noi de învățare. • Manifestă colaborare cu ceilalți colegi și cadre didactice în desfășurarea activităților didactice. • Demonstrează autonomie în organizarea contextului de învățare sau a situației de rezolvat. • Manifestă responsabilitate socială prin implicarea activă în viața socială studentască/implicare în evenimentele din comunitatea academică. • Promovează/contribuie prin soluții noi, aferente domeniului de specialitate pentru a îmbunătăți calitatea vieții sociale. • Conștientizează valoarea contribuției sale în domeniul ingineriei la identificarea de soluții viabile/sustenabile care să rezolve probleme din viața socială (responsabilitate socială). • Aplică principii de etică/deontologie profesională în analiza impactului tehnologic al soluțiilor propuse în domeniul de specialitate asupra mediului înconjurător. • Analizează și valorifică oportunități de dezvoltare antreprenorială în domeniul de specialitate. • Demonstrează abilități de management al situațiilor din viața reală (gestionarea timpului, colaborare și soluționarea ipoteticilor situații conflictuale).



9. Metode de predare (Se vor avea în vedere metode care să asigure predarea centrată pe student. Se va descrie modul în care se asigură participarea studenților la stabilirea propriului parcurs de învățare, cum se identifică eventualele rămânări în urmă și ce măsuri remediale se adoptă în astfel de cazuri.)

Pornind de la analiza caracteristicilor de învățare și de la nevoile specifice ale studenților, procesul de predare va explora atât metode expositive (prelegerea, expunerea), cât și conversative-interactive, bazate pe modele de învățare prin descoperire, facilitate de explorarea directă și indirectă a realității (experimentul, demonstrația, modelarea), dar și pe metode bazate pe acțiune, precum exercițiul, activitățile practice și rezolvarea de probleme întâmpinate. În activitatea de predare vor fi utilizate prelegeri, în forma unor prezentări PowerPoint. Fiecare curs va debuta cu recapitularea capitolelor deja parcurse, cu accent asupra noțiunilor parcurse la ultimul curs pentru validarea și facilitarea însușirii noțiunilor. Prezentările utilizează suport vizual auxiliar (imagini, grafice, scheme, filmulețe), astfel încât informațiile prezentate să fie ușor de înțeles și asimilat. Această disciplină acoperă informații și activități practice menite să-i sprijine pe studenți în eforturile de învățare și de dezvoltare a unor relații optime de colaborare și comunicare într-un climat favorabil învățării prin descoperire. Se va avea în vedere exersarea abilităților de ascultare activă și de comunicare asertivă, precum și a mecanismelor de construcție a feedback-ului, ca modalități de reglare comportamentală în situații diverse și de adaptare a demersului pedagogic la nevoile de învățare ale studenților. Se va exersa abilitatea de lucru în echipă pentru rezolvarea diferitelor sarcini de învățare.

10. Conținuturi

CURS		
Capitolul	Conținutul	Nr. ore
1	Noțiuni introductive	2
2	Metodologii de management al proiectelor software. Metode și niveluri de testare.	4
3	Vulnerabilități de securitate și riscurile asociate. Tipuri de atacuri și atacatori.	4
4	Modelarea calității produsului în SDLC. Modelarea securității, utilizabilității, performanței și mentenabilității	4
Total:		14



Bibliografie:

Fenton, N., Bieman, J., "Software Metrics: A Rigorous and Practical Approach" (2014)
Martin, R.C., "Functional Design: Principles, Patterns, and Practices" (2023)
Humble, J., Farley, D., "Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation" (2010)
Martin, R.C., "Clean Code: A Handbook of Agile Software Craftsmanship" (2008)
Pullum, L., "Software Fault Tolerance Techniques and Implementation" (2001)
Smith, D.J., "Reliability, Maintainability and Risk: Practical Methods for Engineers" (2005)
Shaw, M., Garlan D., "Software Design for Resilient Computer Systems" (2000)
Smith, D.J., Simpson, K.G.L., "Safety Critical Systems Handbook: A Guide to Functional Safety" (2016)
Herrmann, D.S., "Software Safety and Reliability: Techniques, Approaches, and Standards of Key Industrial Sectors" (2000)
Kuzmiakova, A., "Security Designs for the Cloud, IoT, and Social Networking" (2022)
Kofler, M., Gebeshuber, K., Kloep, P., et al., "Hacking and Security: The Comprehensive Guide to Penetration Testing and Cybersecurity" (2023)
Steirer, T., "Test Automation Fundamentals" (2022)
Yorkston, K., "Performance Testing" (2021)
Newbould, C., "Software Testing Security Tester Guide for ISTQB certification" (2023)
Yorkston, K., "Improving the Test Process: Implementing Improvement and Change" (2013)
Black, R., "Mobile testing" (2018)
ISO/IEC 25000:2014, "Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE)"
ISO/IEC 27001:2022, "Information technology - Security techniques - ISMS"
ISO/IEC 31000:2018, "Risk management"
ISO/IEC 33000:2015, "Systems and software engineering"
Verizon, „Yearly Data Breach Investigations Report"
OWASP, Top 10 (riscuri de securitate), definirea și combaterea acestora
Suport în platforma Moodle - <https://curs.upb.ro/2023/course/view.php?id=9654>

LABORATOR

Nr. crt.	Conținutul	Nr. ore
1	Proiectarea securității și utilizabilității în SDLC	4
2	Testarea utilizabilității	4
3	Testarea securității	4
4	Colocviu laborator	2
Total:		14

PROIECT

Nr. crt.	Conținutul	Nr. ore
1	Definirea proiectelor și a metodologiei de documentare în baze de date naționale / internaționale pentru tema aleasă	2
2	Stabilirea temelor individuale și a metodologiei de cercetare	2
3	Stabilirea abordărilor și a pachetelor software necesare pentru analiza asistată de calculator a fiabilității și mentenabilității unor sisteme complexe	2
4	Stabilirea matricii proiectului și a planului de monitorizare	2



5	Gestionarea proiectului	2
6	Analiza riscurilor legate de proiect	2
7	Susținere proiecte	2
Total:		14

Bibliografie:

Fenton, N., Bieman, J., "Software Metrics: A Rigorous and Practical Approach" (2014)
Martin, R.C., "Functional Design: Principles, Patterns, and Practices" (2023)
Humble, J., Farley, D., "Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation" (2010)
Martin, R.C., "Clean Code: A Handbook of Agile Software Craftsmanship" (2008)
Pullum, L., "Software Fault Tolerance Techniques and Implementation" (2001)
Smith, D.J., "Reliability, Maintainability and Risk: Practical Methods for Engineers" (2005)
Shaw, M., Garlan D., "Software Design for Resilient Computer Systems" (2000)
Smith, D.J., Simpson, K.G.L., "Safety Critical Systems Handbook: A Guide to Functional Safety" (2016)
Herrmann, D.S., "Software Safety and Reliability: Techniques, Approaches, and Standards of Key Industrial Sectors" (2000)
Kuzmiakova, A., "Security Designs for the Cloud, IoT, and Social Networking" (2022)
Kofler, M., Gebeshuber, K., Kloepe, P., et al., "Hacking and Security: The Comprehensive Guide to Penetration Testing and Cybersecurity" (2023)
Steirer, T., "Test Automation Fundamentals" (2022)
Yorkston, K., "Performance Testing" (2021)
Newbould, C., "Software Testing Security Tester Guide for ISTQB certification" (2023)
Yorkston, K., "Improving the Test Process: Implementing Improvement and Change" (2013)
Black, R., "Mobile testing" (2018)
ISO/IEC 25000:2014, "Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE)"
ISO/IEC 27001:2022, "Information technology - Security techniques - ISMS"
ISO/IEC 31000:2018, "Risk management"
ISO/IEC 33000:2015, "Systems and software engineering"
Verizon, „Yearly Data Breach Investigations Report"
OWASP, Top 10 (riscuri de securitate), definirea și combaterea acestora
Suport în platforma Moodle - <https://curs.upb.ro/2023/course/view.php?id=9654>

11. Evaluare

Tip activitate	11.1 Criterii de evaluare	11.2 Metode de evaluare	11.3 Pondere din nota finală
11.4 Curs	Analiza diferențială a tehnicilor și metodelor teoretice	- lucrare de verificare	10%
	Cunoașterea noțiunilor teoretice fundamentale	- examen final (scris)	40%
11.5 Seminar/laborator/proiect	Aprecierea activității la laborator	- colocviu laborator	20%
	Finalizarea unui proiect cu temă predefinită	- prezentare proiecte	30%
11.6 Condiții de promovare			
Obținerea unui punctaj peste 50%, prezență la evaluarea finală și activitate constantă în cadrul laboratoarelor (conform regulamentului studiilor universitare de masterat în POLITEHNICA București).			



12. Coroborarea conținutului disciplinei cu așteptările reprezentanților angajatorilor și asociațiilor profesionale reprezentative din domeniul aferent programului, precum și cu stadiul actual al cunoașterii în domeniul științific abordat și practicile în instituții de învățământ superior din Spațiul European al Învățământului Superior (SEİS)

- Prin activitățile desfășurate, studenții dezvoltă abilități de a oferi soluții unor probleme și de a propune idei de îmbunătățire a situației existente în domeniul siguranței în funcționare a sistemelor informatice complexe, în modelarea securității sistemelor informatice și îmbunătățirea utilizabilității aplicațiilor software
- În dezvoltarea conținutului disciplinei s-au avut în vedere cunoștințe / aspecte / fenomene descrise de literatura de specialitate / cercetările proprii publicate / prezentate în jurnale și conferințe științifice
- Prin activitățile practice în cadrul ședințelor de laborator / proiect se are în vedere dezvoltarea abilităților studentului de a gestiona situații practice cu care se poate confrunța în viața reală în scopul creșterii contribuției acestuia la îmbunătățirea mediului socio-economic.

Data completării

Titular de curs

Titular(i) de aplicații

14.10.2024

Dr. ing. Sabina AXINTE

Dr. ing. Sabina AXINTE

Data avizării în departament

Director de departament

Conf. dr. ing. Marian VLĂDESCU

Data aprobării în Consiliul Facultății

Decan

01.11.2024

Prof. Dr. Mihnea Udrea