Sorin TOPOR

INIȚIERE ÎN SISTEME CIBER-FIZICE (CPS)

Curs introductiv în CYBER-PHYSICAL SYSTEMS (CPS)

EDITURA

INIȚIERE ÎN SISTEME CIBER-FIZICE (CPS)

Curs introductiv în CYBER-PHYSICAL SYSTEMS (CPS)

Sorin TOPOR

INIȚIERE ÎN SISTEME CIBER-FIZICE (CPS)

Curs introductiv în CYBER-PHYSICAL SYSTEMS (CPS)

EDITURA IC

București, 2023

INSTITUTUL NAȚIONAL DE CERCETARE - DEZVOLTARE
ÎN INFORMATICĂ - ICI BUCUREȘTI

Procesare PC - Alexandru Mihai Manolescu
Layout & Prepress - Iuliana Panciu
Copertă - Andrei Victor Moldoveanu

ISBN 978-606-94606-9-6

CUPRINS

TEMA 1: INTRODUCERE ÎN CURS. CONCEPT ȘI DEFINIȚII

Scopul acestui program de pregătire este de a oferi claritate cu privire la unele aspecte de conținut pentru orientarea utilizatorului potențial, aflat la început de drum în utilizarea Sistemelor ciber-fizice (CPS).

Acest curs se adresează celor care au interacționat foarte puțin sau deloc cu domeniile securității cibernetice aplicate sistemelor mecanice și doresc să înțeleagă ce schimbări pot produce CPS-urile în activitățile domestice și profesionale. Dacă nu sunteți decișsi cu privire la curiculla educațională pe care doriți să o urmați, acest curs vă va ajuta să înțelegeți locul pe care îl va ocupa omul în viitoarele tehnologii informaționale și, probabil, vă va ajuta să identificați o direcție de evoluție pe care să o urmați.

Alături de traineri, vă veți familiariza cu domeniul și veți afla care sunt principiile asigurării cerințelor minimale pentru securitatea cibernetică a unui model CPS, din funcția de utilizator.

1.1. Contextul general al organizării cursului Inițiere în CPS

Cursul Inițiere în sisteme CSP se încadrează în viziunea pentru transformare digitală a Europei până în 2030 (viziune pentru deceniul digital al UE), inițiativă care se încadrează pe patru direcții cardinale și anume:

1. Digitizarea serviciilor publice;
2. Competențe;
3. Infrastructuri digitale sigure și durabile;
4. Transformarea digitală a întreprinderilor.

Până în 2030, este de așteptat ca tehnologiile digitale să devină esențiale pentru majoritatea întreprinderilor. Multe dintre acestea vor fi mai simple și vor încorpora noi produse în procesele de fabricație și în noile modele de afaceri, bazate pe schimbul echitabil de date în economia datelor. În acest context, este de presupus că adoptarea și punerea rapidă în aplicare a propunerilor Comisiei privind piața

unică digitală și a strategiilor incluse în comunicarea „Conturarea viitorului digital al Europei" vor consolida transformarea digitală a întreprinderilor și vor asigura o economie digitală echitabilă și competitivă.

Cursul *Inițiere în sisteme CPS* este creat pentru a răspunde Metodologiei de selectare a partenerilor în proiectul finanțat din PNRR, componenta 7 „Transformare digitală", operațiunea D. „Competențe digitale, capital uman și utilizarea internetului", investiția I19, din cadrul competiției ADR pentru sprijin al IMM-urilor pentru îmbunătățirea competențelor în rândul angajaților cu aplicabilitate în cele 9 tehnologii emergente, respectiv:

1. Internet of things,
2. Big data,
3. Cloud techologies,
4. Învățare automată,
5. Inteligența artificială,
6. Automatizarea proceselor robotice,
7. Blockchain,
8. Cyber-Physical Systems,
9. Additive manufacturing.

Toate acestea se vor desfășura în cadrul platformei puse la dispoziție de către ADR.

Activitatea de formare se va finaliza prin acordarea, pe baza unei testări, a unei diplome de absolvire pentru fiecare angajat care participă în activitatea de formare. Testarea în vederea obținerii diplomei la finalul sesiunii de formare va asigura și posibilitatea de reexaminare în situația angajaților care nu au putut finaliza formarea, din motive obiective.

Diploma nominală va atesta absolvirea, în format electronic și va fi acordată fiecărui participant.

Cursurile propuse vor include aplicații practice, exemple, studii de caz, exerciții, simulări, tutoriale etc. adaptate grupului țintă vizat și specificului cursului pentru tehnologia emergentă respectivă.

Durata programului de formare profesională, pentru pregătirea teoretică și practică, este de minim 40 ore, pentru corelarea cu Ordinul nr. 2228/2022-3025/2023 pentru modificarea și completarea Metodologiei de autorizare a furnizorilor de formare profesională a adulților.

Cerințele minime privind desfășurarea formarii și evaluării competențelor angajaților din IMM-uri, în cadrul platformei pentru schema dedicată perfecționării angajaților din IMM-uri, stabilite de ADR, sunt detaliate mai jos:

- Conținutul digital va fi interactiv, optimizat pentru a rula atât pe echipamente tip laptop/PC, cât și pe dispozitive mobile precum telefoane și tablete;

- Conținutul va fi centrat pe utilizator, luând în calcul nevoile și obiectivele acestuia și oferind o experiență personalizată și relevantă;

- Conținutul va avea o funcție de căutare clară și eficientă, care să permită utilizatorilor să găsească cu ușurință informațiile;

- Parcursul educațional va fi ghidat în așa fel încât la orice pas, utilizatorul să aibă posibilitatea de a identifica unde se află în cadrul conținutului, care este nivelul său din acel moment și ce mai are de parcurs în continuare;

- Interactivitatea conținutului digital va fi exprimată atât la nivel de interfață (ex. butoane de navigare), cât și în interiorul elementelor componente;

- Conținutul trebuie să ofere utilizatorilor posibilitatea de a primi feedback în diferite moduri (ex.: text, grafică și sunet). Mesajele de tip text, vizual și/sau sonor vor fi adecvate nivelului cursanților;

- Resursele multimedia folosite (sunet, imagine, animație) trebuie să aibă o calitate video ridicată de minim 1080 p și calitatea audio trebuie să fie înaltă. De asemenea, resursele ar trebui să aibă un design atractiv și atrăgător, cu un stil vizual consistent și coerent;

- Structura grafică a paginilor trebuie să fie funcțională și să permită posibilitatea de revenire la ecranul precedent. În egală măsură, ar trebui

să aibă un design minimalist, cu accent pe simplitate și un aspect curat, neaglomerat, care să asigure o vizibilă sporită informațiilor relevante;

- Conținutul trebuie să asigure o navigare ușoară (cuprins, instrumente de navigare accesibile, acces la meniurile de opțiuni și la harta cursului);
- Instrucțiunile de parcurgere trebuie să fie concise, clare, inteligibile și relevante pentru utilizator;
- Fiecare conținut digital trebuie să fie structurat sub forma unor capitole/ secțiuni sau alte tipuri de împărțire adecvate;
- Mărimea textului trebuie să fie suficient de mare pentru ca textul să fie ușor de citit;
- Combinația de culoare dintre text și fundalul acestuia trebuie să fie astfel aleasă încât să nu obosească ochii, dar să existe și un contrast suficient pentru a asigura lizibilitatea textului;
- Paragrafele de text prea lungi pentru a încăpea în interiorul unui singur ecran trebuie să poată fi accesate prin folosirea barei verticale de defilare (scrolling);
- Conținutul dezvoltat va conține și elemente de fixare a cunoștințelor;
- Conținutul digital va fi personalizat pentru a reflecta identitatea vizuală a Beneficiarului, proiectului și finanțatorului, conform manualului de identitate vizuală PNRR.

Scopul și obiectivele cursului *Inițiere în sisteme CPS*:

Cursul urmărește integrarea cunoștințelor provenite din domenii separate, care au fost predate în mod tradițional în discipline distincte, într-un mod eficient și creativ pentru a forma o bază a culturii de securitate în domeniul CPS. Cursanții provin, în general, din medii educaționale diverse. Prin acest curs se dorește realizarea unui transfer de cunoștințe interdisciplinare pentru a se forma premisele unei bune educații în domeniul CPS.

Scopul principal al acestui curs este familiarizarea cursanților cu conceptele de bază ale sistemelor ciber-fizice (CPS). În plus, cursul ilustrează sfera și impactul potențial al utilizării CPS și identifică modalități de participare la asigurarea securității acestora.

Cursul poate fi văzut ca o inițiativă educațională bazată pe trei întrebări cheie:

1. Care sunt conceptele de bază pentru CPS?

2. Cum pot fi integrate aceste concepte în proiectarea unui sistem CPS?

3. Ce metode pot ajuta la proiectarea securității cibernetice a unui CPS?

Inovația în cazul CPS necesită buna înțelegere și cunoaștere a conceptelor și a funcțiilor acestui tip de sisteme, particularități care sunt atribuite, în mod tradițional, altor discipline din mediile educaționale. Această situație face dificilă asimilarea cunoștințelor fără o aliniere conceptuală și fără însușirea definițiilor specifice.

Pentru a putea realiza o comunicare cu experții și specialiștii în proiectarea sistemelor CPS, pentru a avea un dialog cu alți operatori/utilizatori privind componentele și funcțiile specifice, este benefic ca aceste concepte să fie înțelese corect pe baza definițiilor consacrate.

Obiectivele cursului pentru inițiere în CPS sunt:

- Recunoașterea sferei și amplorii impactului potențial al tehnologiei CPS;

- Înțelegerea realității privind integrarea sporită a inovațiilor în CPS;

- Înțelegerea referințelor de comunicare care pot sprijini inovarea în CPS;

- Dezvoltarea gândirii critice pentru analiza unor evenimente și susținerea unui dialog pe baza informațiilor cumulative din știință, inginerie și comunicare socială despre sistemele hibride care înglobează tehnologii emergente.

Cursul urmărește realizarea obiectivelor educaționale prin abordarea subiectelor descrise anterior. Discuțiile din cadrul seminarelor precum și feedback-ul din partea cursanților vor ajuta la corectarea unor aspecte organizatorice și formale în activitatea de învățare și în conținutul temelor.

1.2. Concept și definiții

Sistemele ciber-fizice(CPS), alături de celelalte tehnologii emergente, joacă un rol tot mai important în infrastructura critică, în sistemele de guvernare și chiar în viața cotidiană a cetățenilor. Automobilele, dispozitivele medicale, sistemele de

control a securității clădirilor, a rețelelor inteligente de senzori etc., toate sunt toate exemple de CPS-uri. Fiecare dintre acestea încorporează dispozitive inteligente, rețelele de senzori, procesoare și alte dispozitive de acționare care detectează și interacționează cu lumea fizică și susțin performanța garantată, în timp real, în aplicații critice și în servicii pentru securitate.

Dispozitivele fizice, rețele, algoritmi de procesare etc., strâns legate de așa numitele tehnologii emergente, continuă să apară și să se extindă într-un ritm exponențial, invers proporțional raportat la costurile producerii lor. Fie că se referă la capacitatea de prevenire asupra coliziunii frontale a unei mașini, la capacitatea unui dispozitiv medical de a se adapta circumstanțelor în timp real sau la cea mai recentă inovație în IoT, aceste sisteme sunt o sursă care asigură avantaj competitiv în economia inovatoare (Industria 4.0), de astăzi, precum și oportunități vaste pentru activități de securitate internă.

În același timp, utilizarea CPS-urilor, în mod similar tuturor tehnologiilor emergente, crește riscurile de securitate cibernetică și creează oportunități pentru apariția de noi tipuri de vulnerabilități. Consecințele greșelilor neintenționate sau ale atacurilor rău intenționate ar putea avea un impact grav asupra calității vieții umane și asupra mediului. Pentru aceasta, fiecare cetățean, alături de structurile specializate, trebuie să depună eforturi proactive, coordonate prin măsuri și proceduri, pentru a consolida cultura de securitatea și încrederea în CPS-uri și în celelalte tehnologii emergente.

Etapa istorică pe care o parcurgem reprezintă un moment critic în proiectarea și implementarea CPS-urilor. Progresele în sistemele de computing, IT și comunicații au permis apariția unei game largi de dispozitive noi. Concentrarea pe această direcție a determinat, în unele situații, apariția unei incoerențe sau a unei inadaptări a securității cibernetice. Spre exemplu, sistemele economice ale unui stat sunt guvernate de cerințele funcționale și de piețele aflate în mișcare rapidă. Designurile operaționale și ale produselor evoluează rapid. Apar noi standarde. Multe dispozitive care sunt deja implementate, dețin durate de viață limitate, măsurate în ani calendaristici.

De aceea, alegerile actuale de proiectare vor avea un impact deosebit asupra deceniilor viitoare în domenii diverse precum transport, asistență medicală, controlul clădirilor, răspuns în situații de urgență, energie, în alte sectoare. Pentru a înțelege amploarea acestor provocării, putem face un exercițiu imaginar, analizând progresele actuale în industria auto pentru autoturismele pe care le conducem. În mod similar,

putem observa evoluția dispozitivelor medicale de care depindem sau a sistemelor care operează în clădirile unde ne desfășurăm mare parte a activităților cotidiene. Autovehiculele moderne, pentru a evita o coliziune, pot frâna automat, dispozitivele medicale pot monitoriza, în timp real, condițiile din mediu ambiant și se pot adapta la schimbările identificate, clădirile și rețeaua energetică sunt îmbunătățite cu o serie de servicii inteligente etc. De fapt, miliarde de noi dispozitive CPS sunt de așteptat să fie conectate la diverse sisteme și rețele.

De aceea, dacă nu sunt respectate normele și procedurile de securitate stabilite sau, mai mult, dacă acestea sunt eludate în mod voit, se riscă inițierea unor erori de funcționare care vor facilita executarea de atacuri care vor schimba modul în care o mașină frânează, modul în care dispozitivele medicale se adaptează la mediu și a modurilor în care clădirile și rețelele inteligente de securitate răspund la evenimente.

Se poate înțelege că în viitor, starea de securitatea (cibernetică dar și fizică) devine tot mai dificil de asigurat, pe măsură ce se adaugă conexiuni cu alte miliarde de dispozitive care vin cu propriile vulnerabilități de securitate.

De aceea, abordarea problemelor de securitate prin fixarea soluțiilor la nivelul sistemelor implementate pe scară largă nu reprezintă o soluție globală viabilă. Problemele de securitate cibernetică trebuie analizate, înțelese și rezolvate în permanență, încă din primele etape de proiectare și de implementare a sistemelor. Concluziile rezultate trebuie comunicate către cei care proiectează atât sisteme cât și îmbunătățesc soluțiile existente prin pachete de programe de securitate de tip up-date.

Cadrul european al dezvoltării conceptuale pentru sistemele CPS

În general, sistemele CPS combină rețele de senzori cu sistemele informaționale încorporate pentru a monitoriza și controla mediul fizic, cu bucle de feedback care le permit să auto-activeze fie comunicarea, fie controlul, fie o acțiune aflată sub controlul unui computer astfel încât, să răspundă în timp real la o serie de stimuli externi. Sistemele CPS cuprind dispozitive digitale și analogice, interfețe, rețele de comunicații, sisteme informatice și altele componente a căror funcționare depinde de lumea fizică, naturală și/sau creată de om. Această combinare interconectată și eterogenă, determină ca analiza și proiectarea unui CPS să fie o sarcină interesantă și provocatoare pentru oricare ecosistem digitalizat, actual.

Conceptul CPS a fost creat și promovat pentru a caracteriza noile tipuri de sisteme ale unui ecosistem cibernetic. În anul 2018, la Luxemburg, la nivelul

Uniunii Europene a fost înființată așa numita întreprindere comună European High Performance Computing Joint (EuroHPC JU)[1] care reprezintă o inițiativă comunitară pentru a dezvolta un ecosistem de supercomputing de clasă mondială, în Europa, în scopul îmbunătățirii calității vieții cetățenilor europeni, promovării științei și stimulării competivității industriale, concomitent cu asigurarea autonomiei tehnologice a Europei. Aceasta este o entitate juridică care are ca obiectiv principal reunirea resurselor UE a 32 de țări europene și trei parteneri privați cu ambiția de a face din Europa un lider mondial în supercomputing. Beneficiile implementării acestui concept permit țărilor europene să-și coordoneze strategiile și investițiile în domeniul digitalizării, să dezvolte un ecosistem HPC competitiv, care să asigure menținerea poziției de lider în economia digitală și o consolidare a autonomiei tehnologice și de date a Europei, precum și o consolidare a bazei de cunoștințe în domeniul tehnologiilor HPC prin îmbunătățirea rețelei centrelor naționale de competență HPC. Aceste centre naționale vor acționa local pentru a facilita accesul la oportunitățile europene HPC, în diferite sectoare industriale, oferind soluții personalizate pentru o mare varietate de utilizatori.

România, a ales să fie membru al întreprinderii comune, alături de alte state membre și țări asociate precum: Austria, Belgia, Bulgaria, Croația, Cipru, Republica Cehă, Danemarca, Estonia, Finlanda, Franța, Germania, Grecia, Ungaria, Islanda, Irlanda, Italia, Letonia, Lituania, Luxemburg, Malta, Muntenegru, Țările de Jos, Macedonia de Nord, Norvegia, Polonia, Portugalia, Serbia, Slovacia, Slovenia, Spania, Suedia și Turcia. Membri privați sunt: reprezentanți ai Platformei tehnologice europene pentru calculul de înaltă performanță (ETP4HPC), asociației Big Data Value (BDVA) și a Consorțiului European Quantum Industry (QuIC). De asemenea, întreprinderea comună se bazează și pe colaborarea cu actori europeni cheie, cum ar fi PRACE (Parteneriatul pentru calcul avansat în Europa) și GEANT (rețeaua paneuropeană de mare viteză pentru cercetare și educație).

În orice moment, se pot alătura alte state membre și state asociate la programul Europa Orizont 2020 sau Europa digitală.

EuroHPC JU echipează deja UE cu o infrastructură de clasă mondială de supercomputing pre-exascale și petascale și dezvoltă tehnologiile, aplicațiile și performanțele necesare pentru atingerea capabilităților complete exascale (nivel de

[1] UE, Întreprindere comună pentru calcul european de înaltă performanță (EuroHPC), https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-high-performance-computing-joint-undertaking-eurohpc-ju_ro visited at 19.06.2023

performanță capabil să execute de la 10 până la o putere de 18 operații pe secundă), până la finalul anului 2023.

Până în prezent, sunt deplin operaționale opt supercomputere și anume: LUMI în Finlanda (care ocupă locul 3 în lume), LEONARDO în Italia (care ocupă locul 4 în lume), Vega în Slovenia, MeluXina în Luxemburg, Discoverer în Bulgaria, Karolina în Republica Cehă, Deucalion în Portugalia și MareNostrum5 în Spania.

De asemenea, EuroHPC JU a anunțat cinci noi site-uri de găzduire pentru o nouă generație de supercomputere europene în Germania, Grecia, Ungaria, Irlanda și Polonia, unul dintre ele fiind primul supercomputer exascale din Europa: JUPITER, care va fi găzduit în Centrul de supercalculare Jülich, în Germania. La fel ca supercomputerele EuroHPC existente, noile locații vor fi conectate și disponibile pentru a servi o gamă largă de utilizatori europeni, din comunitatea științifică și din industrie, în special întreprinderile mici și mijlocii, precum și organizații din sectorul public din UE și din țările participante.

În plus, EuroHPC JU a anunțat că șase site-uri vor găzdui computere cuantice. Acestea sunt în Cehia, Germania, Spania, Franța, Italia și Polonia. Calculatoarele cuantice vor fi integrate cu supercomputere existente.

Știința și cercetarea se va concentra pe transformarea digitală a societății și a economiilor digitale pe baza supercalculului în știință, care să permită înțelegerea științifică aprofundată și progresul în aproape toate domeniile științifice, precum:

- **fizica fundamentală** (extinderea frontierelor cunoașterii în domeniu, explorarea universului);
- **științele materialelor** (de exemplu, proiectarea de noi componente critice pentru sectorul farmaceutic sau cel energetic)
- **științele pământului** (modelarea fenomenelor atmosferice și oceanice la nivel planetar).

Cine vor fi beneficiarii?

Cetățenii prin exploatarea numeroaselor aplicații utile:

- **cercetarea medicală**, descoperirea de **noi medicamente**, dezvoltarea și orientarea terapiilor medicale în funcție de nevoile și de afecțiunile individuale ale pacienților;

- anticiparea **condițiilor meteorologice** severe și monitorizarea **schimbărilor climatice**;
- combaterea **criminalității cibernetice** (phishing, furt de identitate etc.);
- sporirea **securității cibernetice**, în special, pentru protejarea infrastructurii critice (utilități etc.).

În industrie se estimează o creștere a inovării și dezvoltarea de produse și servicii cu valoare mai mare în sectoarele industriale, care să reducă, în același timp, costurile și ciclurile de producție, îmbunătățind eficiența lor. Acest lucru pregătește terenul pentru tehnologii mai sigure și mai ecologice în industrie, conform modelului Industria 4.0.

DEFINIȚIE

Sistemele CPS sunt sisteme informaționale bazate pe AI care integrează computere, mașini de calcul, sisteme de comunicații și sisteme automatizate de control pentru obținerea performanței dorite a proceselor fizice.

Definiția ENISA elaborată de un colectiv de autori acreditați este:" Sistemele Cyber-Fizice (CPS) sunt integrări de calcul, comunicare și control care realizează performanța dorită a proceselor fizice. "

În România conceptul de Cyber-Physical Systems este reglementat sub conținutul de *„sisteme integrate în care părţi şi procese fizice sunt controlate de algoritmi sau software"* în Anexa nr. 3, Acronime și abrevieri/ Anexa la Hotărârea Guvernului nr. 429/2019 pentru aprobarea Strategiei 5G pentru România, din 20.06.2019.

Acest document prevede la capitolul 5.3.1. Industrii 4.0 că:

> *„Creșterea productivității prin digitalizarea industriei manufacturiere, cunoscută și sub numele de a patra revoluție industrială (sau Industriile 4.0) este alimentată de dezvoltarea sistemelor cyber fizice (CPS) și de internetul lucrurilor (IoT). Creșterea semnificației CPS implică în mod necesar și obiectiv îmbunătățirea substanțială a conectivității, dar și comunicarea și schimbul rapid de informații între un număr mare de aparate diferite, situații care potențează în mod evident rolul 5G în lanțurile creatoare de valoare adăugată."*

Convenție! În curs, pentru a identificat aceste sisteme vom folosi denumirea de

„Sisteme ciber-fizice”.

Terminologie specifică:

Acuator	Dispozitiv care face ca o mașină sau alt dispozitiv să funcționeze.
Algoritm Support Vector Machine (SVM)	Un algoritm SVM (Support Vector Machine) este un algoritm de învățare supravegheat utilizat în clasificarea seturilor de date de antrenament.
Învățarea bazată pe arbori de decizie (DT)	Învățarea bazată pe arbori de decizie (Decision Tree) este o formă de învățare automată supravegheată
Cloud computing	Furnizare de servicii informatice – inclusiv servere, stocare, baze de date, rețele, software, analiză și informații – prin Internet. Este o infrastructură mult mai facilă decât calculatorul personal sau server, oferind servicii de rețea mai rapide, resurse flexibile și economii remarcabile de timp.
Cluster K-means	Clusterul K-means este unul dintre cei mai simpli și mai populari algoritmi de învățare automată nesupravegheată.
Fog computing	O infrastructură distribuită de calculatoare care aduce datele, procesarea și stocarea lor mai aproape de marginea rețelei, unde sunt amplasate multe dispozitive IoT. Aceasta facilitează operarea între centralele de date și dispozitivele finale prin reducerea dependenței de cloud pentru sarcinile mari consumatoare de resurse, îmbunătățind performanța și reducând latența. Mai este cunoscută și sub denumirea de „edge computing”.
Industry 4.0	A patra revoluție industrială numită și 4IR, este următoarea fază în digitalizarea sectorului de producție, condusă de tendințe disruptive, care includ creșterea datelor și a conectivității, analize, interacțiune om-mașină și îmbunătățiri în robotică.
Inteligența artificială (AI)	Nu există o definiție unanim recunoscută pentru AI. Deși lipsește o definiție comună, majoritatea definițiilor au următoarele părți comune(cf. JRC5) care pot fi considerate principalele caracteristici ale IA: (i) percepția mediului, inclusiv luarea în considerare a complexității lumii reale. (ii) prelucrarea informațiilor (colectarea și interpretarea intrărilor sub formă de date); (iii) luarea deciziilor (inclusiv procese de raționament și de învățare) precum: executare de acțiuni, îndeplinirea sarcinilor (inclusiv adaptarea și reacția la schimbările din mediu) cu un anumit nivelul de autonomie; (iv) realizarea unor obiective specifice.

Internet industrial	O infrastructură de organizații care furnizează o mare varietate de produse și servicii, în primul rând online, prin intermediul site-urilor web.
Internet of Everything	Internet of Everything (IoE) se referă la o rețea de conexiuni între oameni, lucruri, date și procese care oferă intelligence general și cunoaștere îmbunătățită în mediul determinat de un spațiu cibernetic. IoE este un sistem coerent care îmbunătățește capacitățile entităților participante și aduce informații de rețea pentru a facilita luarea deciziilor mai informat concomitent cu un schimb facil de date.
Învățare automată (ML)	Învățarea automată (Machine Learning) este o secvență a IA care utilizează în esență statistici avansate pentru a organiza cadrul de referință și are capacitatea de a învăța din datele disponibile, de a identifica tipare și de a face predicții fără a necesita intervenția umană.
Învățare ML nesupervizată	Una dintre cele trei paradigme de bază ale învățării automate, împreună cu învățarea prin consolidare și învățarea supervizată, care se ocupă cu procesul de deducere a tiparelor pe baza dateleor istorice
Învățare profundă (DL)	Învățarea profundă (Deep Learning) face parte dintr-o familie mai largă de metode de învățare automată bazate pe rețele neuronale artificiale (ANN).
Învățarea prin consolidare (RL)	Învățarea prin consolidare (reinforcement learning) este o zonă a învățării automate care se preocupă de modul în care agenții inteligenți selectează acțiunile într-un mediu în condițiile de maximalizare a noțiunii de recompensă cumulativă. Învățarea prin consolidare este una dintre cele trei paradigme de bază ale învățării automate, alături de învățarea supravegheată și de învățarea nesupravegheată.
Machine-to-Machine (M2M),	M2M este o infrastructură de comunicare directă între dispozitive folosind orice canal de comunicații, pe cablu sau Wi-Fi. Comunicarea mașină la mașină poate include instrumente industriale, permițând unui senzor sau contor să comunice informațiile pe care le înregistrează (cum ar fi temperatura, nivelul de inventar etc.) unui software de aplicație care o poate folosi (de exemplu, ajustarea unui proces industrial bazat pe temperatură sau plasarea comenzilor pentru completarea stocurilor). Inițial, o astfel de comunicare a fost realizată pentru a optimiza comunicarea pe rețelele distribuite de mașini, prin transmiterea informațiile de feedback la un hub central în vederea analizei și redirecționării lor într-un sistem unic, ca un computer personal.

Metode de ansamblu (Ensemble methods)	Tehnici care vizează îmbunătățirea acurateței rezultatelor prin modelare rezultată prin combinarea mai multor modele, în loc de utilizarea unui model unic.
Model Hidden Markov (HMM)	Modelul Hidden Markov (HMM) este un model statistic care este folosit și în învățarea automată. Poate fi folosit pentru a descrie evoluția evenimentelor observabile care depind de factori interni ce nu sunt observabili în mod direct. Modelele HMM au apărut inițial în domeniul recunoașterii vorbirii. În ultimii ani, acestea au atras un interes tot mai mare și în zona vizuală computerizată.
Naive Bayes (NB)	Naive Bayes este un algoritm popular de învățare automată supravegheată
Rețele neuronale artificiale (ANN) sau Rețele neuronale (NN)	Rețelele neuronale artificiale (artificial neural network), numite de obicei pur și simplu rețele neuronale (neural networks), sunt sisteme de calcul bazate pe o colecție de unități sau noduri conectate numite neuroni artificiali, care modelează vag neuronii dintr-un creier biologic.
Securitate prin design	Un concept în inginerie software și de design de produs care ia în considerare considerentele de securitate din primele etape ale dezvoltării produsului.
Sistem de inteligență artificială (AIs)	Sistemele AI reprezintă o serie de software (care sunt dezvoltate prin abordări ale învățării automate și abordări bazate pe logică și cunoaștere). În plus, acestea pot, pentru un set date pentru obiective definite de om, să genereze rezultate precum conținut, predicții, recomandări sau decizii care influențează mediile cu care interacționează. Sistemele de inteligență artificială pot include, eventual, sisteme hardware concepute de oameni care, au un scop complex, acționează în dimensiunea fizică sau digitală prin perceperea mediului ambiental prin achiziția de date, prin interpretarea datelor structurate sau nestructurate culese, prin raționament asupra cunoștințelor sau prin procesarea informațiilor derivate din aceste date și adoptarea unei decizii pentru cea mai bună acțiune(i) de executat, pentru a atinge un obiectiv clar definit.
Supervizare ML	Învățarea supravegheată este o subcategorie a învățării automate definită prin utilizarea seturilor de date etichetate pentru a antrena algoritmi pentru a clasifica datele sau pentru a prezice rezultatele cu precizie.
Syber	Ecosistem certificat pentru transferul și gestionarea datelor în siguranță și confidențialitate.
TSensor	Dispozitivele TSensor scanează senzorii de temperatură bluetooth din apropiere și analizează temperatura, umiditatea, presiunea aerului, altitudinea, afișează datele mod listă și grafic.

Wireless sensor network (WSN)	Rețelele de senzori fără fir (WSNs) se referă la rețele de senzori dedicați și distribuiți spațial care monitorizează și înregistrează condițiile fizice ale mediului și transmit datele colectate către o locație centrală (centrală de date). WSN-urile pot măsura condițiile de mediu, cum ar fi temperatura, sunetul, nivelurile de poluare, de umiditate și puterea vântului. Acestea sunt similare rețelelor wireless ad-hoc, în sensul că se bazează pe conectivitate fără fir și pe formarea spontană a rețelelor, astfel încât datele senzorilor să poată fi transmise pe conexiuni fără fir.

*

* *

Apreciem că interesul pentru a înțelege corect conținutul conceptului derivă din realitatea plasării întregii omeniri în fața celei de-a patra revoluții industrială caracterizată prin utilizarea pe scară largă a sistemelor CPS. Efectele economice și de producție face ca tot mai mulți lucrători să fie disponibilizați pe piața muncii.

Totuși, *frica pierderii locului de muncă reprezintă o provocare majoră* care poate fi transformată în oportunitate. Este evident că Internetul, digitalizarea, automatizarea proceselor de tot felul etc., au un impact semnificativ asupra pieței muncii în special prin generarea următoarelor oportunități:

1. Creșterea cererii de specialiști în tehnologie cibernetică: dintre aceste profesii enumerăm ingineri/specialiști/experți de software, hardware, în rețele de comunicații și în securitate cibernetică;

2. Crearea de noi locuri de muncă în domenii emergente precum Internet of Things (IoT), industria 4.0, mobilitate autonomă, sănătate digitală, alte profesii care necesită cunoștințe și abilități specifice noilor relații economice;

3. Eficiență și productivitate crescută în diverse sectoare industriale, inclusiv producție, transport, energie și sănătate. Această creștere a eficienței poate duce la crearea de noi oportunități de muncă sau la reorientarea forței de muncă către alte domenii;

4. Dezvoltarea industriei manufacturiere prin facilitarea automatizării și optimizarea proceselor de producție. Utilizarea roboților autonomi, a

sistemelor de monitorizare și control, a sistemelor de analiză a bazelor mari de date etc., în timp real poate crește eficiența, reduce erorile și costurile de producție. Pentru toate acestea este nevoie de specialiști în domeniul automatizării industriale și de producție, capabili să lucreze cu sisteme integrate;

5. Dezvoltarea transporturilor și a sistemelor logistice pentru adaptarea la mobilitatea integrată și transportul autonom. Această evoluție deschide oportunități de muncă în domeniul dezvoltării software, al analizei datelor, a securității cibernetice și a ingineriei mecanice pentru îmbunătățirea eficienței și siguranței mijloacelor de transport;

6. Inovarea sănătății și asistenței medicale prin integrarea dispozitivelor inteligente și a sistemelor de monitorizare a sănătății. Pentru aceasta este nevoie de specialiști în domeniul tehnologiei medicale, programatori în domeniul sănătății și în domenii conexe care contribuie la îmbunătățirea îngrijirii pacienților și la gestionarea eficientă a resurselor medicale;

7. Optimizarea consumului de energie și gestionarea eficientă a resurselor naturale poate fi abordată ca o oportunitate pentru viitoarele piețe a muncii. Prin intermediul senzorilor și a sistemelor de control inteligent, se poate realiza monitorizarea și ajustarea eficientă a consumului de energie și a resurselor în diverse medii, precum în clădirile inteligente și în rețelele de distribuție;

Apreciem că implementarea CPS poate aduce și alte provocări în piața muncii precum:

8. Necesitatea de recalificare și de adaptare determină modificări majore în cerințele specifice posturilor și în abilitățile angajaților. Lucrătorii trebuie să fie pregătiți să se recalifice și să se adapteze continuu pentru a rămâne relevanți pe piața muncii;

9. Securitatea cibernetică și confidențialitatea datelor culese, stocate și procesate de bazele mari de date determină noi abordări în comunicare, pentru stimularea încrederii și formarea de percepții. Protejarea datelor personale și asigurarea securității cibernetice devin aspecte critice într-un mediu interconectat. Este necesară o abordare mai atentă a securității și a protecției datelor pentru a asigura încrederea utilizatorilor și a angajaților.

De altfel, interesul pentru conceptul de sistem CPS a reprezentat o serie de suișuri și coborâșuri în diverse perioade, menținând totuși o tendință crescătoare conform figurii 1.1.

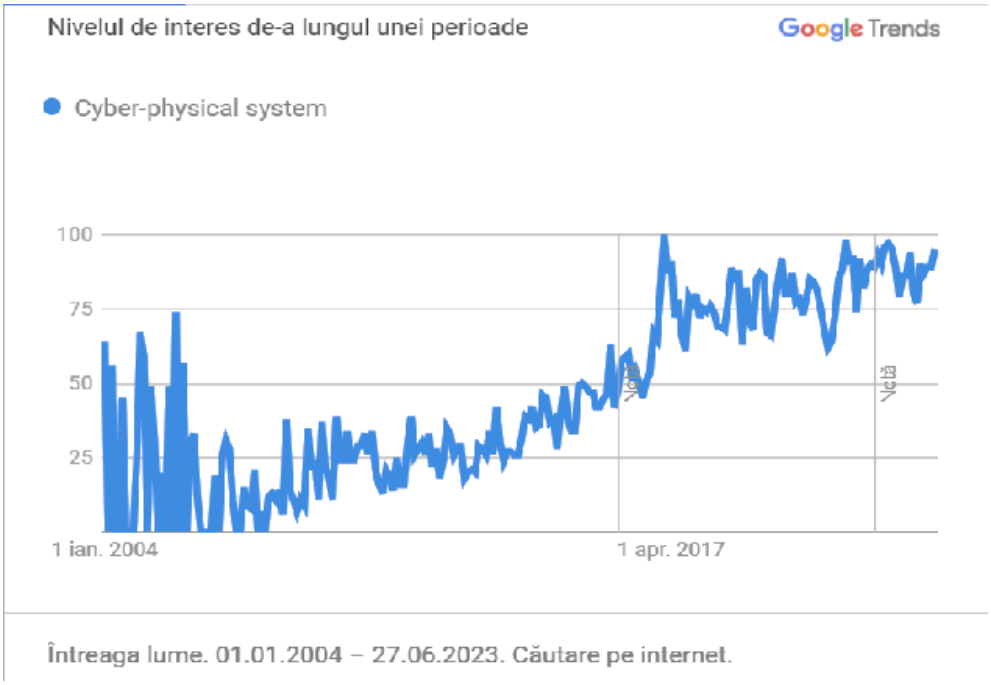

Figura 1.1. Nivelul de interes determinat prin numărul de căutări pentru CPS în Internet.

Din 253 de țări care au interese de căutare și de studiere a acestui concept, România ocupă locul 96. Primele țări sunt: Coreea de Sud, Japonia, Taiwan, Singapore, China, urmate de prima țară europeană Germania. Căutarea a fost efectuată cu Google Trends, la data de 27.06.2023, pentru conceptul *Cyber-physical system*.

Este de remarcat că acest concept a atras o atenție sporită mediilor academice și guvernelor asiatice în comparație cu restul lumii. Aceste țări exploatează potențialul tehnologiilor cibernetice dincolo de jocuri, fiind cunoscută eficiența modului de utilizare în industrie și în administrația publică.

În acest context, apreciem că acest material suport având ca temă CPS-urile aduce nenumărate beneficii de dezvoltare atât la nivelul personalului întreprinderilor cât și a altor structuri organizaționale de producție, ori la nivel de individ, pentru organizarea activităților și prioritizarea intereselor personale.

Rezumat

Pentru întărirea cunoștințelor dobândite în urma studierii definițiilor trebuie înțeles că un sistem CPS este rezultatul interacțiunii domeniilor cibernetică și fizică.

10. Domeniul cibernetic cuprinde funcții și relații de calcul, de comunicare și control care sunt discrete, logice și optimizate (automatizate).

11. Domeniul fizic cuprinde funcții și relații specifice sistemelor naturale și a celor create de om. Acestea sunt guvernate de legile fizicii și funcționează în mod continuu.

Sistemele ciber-fizice sunt sistemele în care cibernetica și fizica sunt strâns integrate la toate nivelurile. Modificările aplicațiilor (funcțiile, algoritmii, formulele etc.) cibernetice sunt aplicate mediului fizic. Schimbările din mediul fizic determină modificări ale aplicațiilor cibernetice. Toate componentele sistemului sunt guvernate de un computer. Un sistem CPS reprezintă un nou mod de gândire a relațiilor într-un ecosistem reprezentând trecerea de la reacțiile ad-hoc (de tip acțiune-reacțiune) la inteligență artificială.

CPS-urile vor schimba interacțiunea cu lumea fizică în mod similar Internetului care a schimbat modul de comunicare între oameni.

Probleme de reflecție:

1. Identificați cadrul general al dezvoltării conceptului CPS în România?

2. În ce domenii cunoașteți sau ați identifcat aplicații CPS în viața cotidiană?

3. Ce înțelegeți că este un sistem CPS?

4. Cum puteți să diferențiați conceptul de sistem CPS de dispozitivele cu AI și ML?

5. Dați exemple de interacțiuni ale domeniilor cibernetic și fizic pentru un CPS.

TEMA 2: EVOLUȚIA CPS - ORIGINEA, EVOLUȚIA ȘI IMPACTUL CPS ÎN VIAȚA COTIDIANĂ

În această temă urmărim să ne familiarizăm cu locul și rolul CPS-urilor în viața cotidiană. Pornind de la originea conceptului urmărind, într-un fir logic, evoluția și impactul CPS-urilor asupra evoluției societăților umane moderne și a schimbărilor rapide în modul de gândire spre guvernanța asigurată de inteligența artificial vom înțelege rolul acestora și faptul că, deja, tehnologia speciică își face loc rapid în viața nastră cotidiană.

2.1. Originea conceptului de sistem fizico - cibernetic

Conceptul de sistem ciber-fizic reprezintă traducerea din limba engleză a termenului Cyber-Physiscal System (CPS). Acesta a apărut în domeniul ingineriei și tehnologiei, ca o continuare a conceptului de sistem informațional, prin integrarea unei serii de tehnologii cibernetice. Prin urmare, originea acestui concept poate fi atribuită dezvoltării tehnologiei și a necesității integrării sistemelor informatice în mediul fizic.

Autorul acestui concept este cercetătorul Helen Gill (Fundația Națională de Științe, SUA), care, în anul 2006, a publicat o lucrare prin care dezvolta conceptul de „spațiu cibernetic", previzionat de neoromancierului William Gibson. Gibson dezvolta conceptul de cyberpunk în cartea Neuromantul[1] (Neuromancer-lb.engl. - este un roman science-fiction, publicat în 1984), fiind considerat unul dintre cele mai vechi și mai cunoscute lucrări din genul cyberpunk. Acesta a câștigat Premiul Nebula, Premiul Philip K. Dick și Premiul Hugo, constituind romanul de debut al său și începutul trilogiei Sprawl. Acțiunea romanului se petrece în viitor, urmărindu-l pe Henry Case, un expert în cibernetică, discreditat la ultimul său serviciu, pus în contact cu o inteligență artificială extrem de puternică.

Astfel, Gill înțelese, în 2006, necesitatea desprinderii unui cadru academic al unei noi discipline emergente care să integreze procesarea datelor cu procesele naturale fizice, chiar dacă rădăcinile conceptuale sunt mult mai vechi și mai profunde.

[1] Lee, E.A.,(2015) *The Past, Present and Future of Cyber-Physical Systems: A Focus on Models*, Sensors (Basel), 2015 Mar; 15(3): 4837-4869, PMC4435108, MDPI, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4435108/ visited at 27.06.2023

Pe baza teoriei lui a apărut o comunitate de cercetare, în curs de dezvoltare, care se bazează pe o abordare transversală a mai multor domenii precum: sisteme încorporate, sisteme în timp real, sisteme hibride, teoria controlului, rețele de senzori și metode formale. Totodată, s-a generat o curriculă pentru formarea studenților care erau interesați să lucreze în domeniul CPS.

În prezent, proiectul general pentru CPS-uri angajează la nivel global foarte mulți cercetătorii din diverse domenii conexe. Pentru aceasta, încă de la început, Fundația Națională pentru Știință (NSF) din SUA a alocat sume fabuloase unui proiect de cercetare pentru CPS. Multe universități și institute de cercetare (cum ar fi: UCB, Vanderbilt, Memphis, Michigan, Notre Dame, Maryland și Centrul de Cercetare și Dezvoltare GeneralMotors etc.) s-au alăturat proiectului de cercetare[2]. În plus, au devenit interesați și cercetătorii din numeroase țări, fiind conștienți de importanța cercetării pentru CPS în fundamentarea teoretică, pentru proiectare și implementare de sisteme, în alte aplicații, dar și în domeniul educației. În ansamblu, deși cercetătorii au înregistrat progrese în modelarea sistemelor, în controlul energiei, în securitate, în proiectare de software etc., CPS-urile sunt, încă, doar într-un stadiu incipient de dezvoltare.

2.2. Structura de principiu a sistemelor CPS

În esență, CPS-urile caracterizează acele sisteme cibernetice cu legături în procesele fizice cu funcții de confidențialitate, integritate și disponibilitate a datelor. Chiar dacă conceptul este apărut relativ recent, așa cum am precizat, a stârnit interesul multor cercetători pentru dezvoltarea unor viziuni moderne de abordare a serviciilor sociale care transcend timpul și spațiul la dimensiuni nemaiîntâlnite[3].

Termenul CPS este frecvent confundat cu securitatea cibernetică. De reținut este diferența că securitatea cibernetică, nu are nicio legătură cu procesele fizice, chiar dacă sistemele CPS au legături strânse cu securitatea cibernetică și cu protecția datelor. Acesta se referă doar la securitatea spațiului cibernetic. Conceptul CPS implică multe probleme de securitate și de confidențialitate a datelor ce pot fi regăsite

[2] Shi, J., Wan, J., Hui Suo, H.Y., (2011) *A Survey of Cyber Physical Systems*, 2011 IEEE, DOI: 10.1109/WCSP.2011.6096958, https://www.researchgate.net/publication/228934884_A_Survey_of_Cyber_Physical_Systems visited at 28.06.2023

[3] Sanislav, T., Miclea, L., (2012) *Cyber Physical Systems – Concept, Challenge and Research Areas*, CEAI, Vol14, No.2, pp. 28-33, 2012, https://www.researchgate.net/publication/289701937_Cyber-physical_systems_-_Concept_challenges_and_research_areas#fullTextFileContent visited at 27.06.2023

și în securitatea cibernetică dar și în alte aplicații cibernetice precum Internet of Things (IoT), Industry 4.0, Internet industrial, Machine-to-Machine (M2M), Internet of Everything, TSensors și fog computing (un cloud computing care implică și procese fizice). Mai degrabă, CPS reflectă preocupările academice ale cercetătorilor în îmbinarea ingineriei tradiționale fizice în lumea cibernetică.

Ca și teorie a sistemelor liniare, CPS-urile se referă la modele. Modelarea joacă un rol central în toate disciplinele științifice și de inginerie. Cu toate acestea, deoarece CSP-urile conectează discipline distincte, modelele predominante nu se combină, cele mai populare fiind cele din industrie, din transporturi, din sănătate, din infrastructura urbană și din energie, domenii unde sistemele CPS sunt capabile să colecteze date și să le proceseze în timp real, să ia decizii autonome și să acționeze în mediul fizic. În viitor, este posibil ca acestea să depășească barierele autodeterminate și să își găsească aplicabilitate și în alte ramuri economice, aplicațiile CPS contribuind astfel la dezvoltarea tehnologică și la îmbunătățirea eficienței și a performanței sistemelor fizice.

CPS-urile integrează dinamica proceselor fizice cu cea a software-ului și a comunicării, oferind abstractizări și tehnici de modelare, de proiectare și de analiză pentru întregul spațiu integrat. Interacțiunea dinamică dintre computere, rețele și sistemele fizice necesită tehnologii de design fundamental noi. Tehnologia depinde de abordări multidisciplinare, cum ar fi: în sistemele încorporate, în computere, în comunicații etc., precum și software încorporat, în dispozitive ale căror principiu nu este doar de calculul. De exemplu în mașini industriale și în autovehicule, în dispozitive medicale, în unele instrumente științifice, în sistemele inteligente de transport etc.

2.2.1. Caracteristicile CPS

Platformele industriale emergente așa cum este Internetul obiectelor (IoT), Internetul industrial și Industria 4.0, au accelerat enorm dezvoltarea de noi generații de CPS. Acestea integrează oameni și organizații umane (H-CPS) cu sisteme fizice și procese de calcul și se extind la sisteme mari, la scară societală, precum rețelele de trafic, rețelele electrice sau rețelele de sisteme autonome (autovehicule cu conducere autonomă, vehicule autonome aeriene fără pilot etc.) unde datele și controlul relațiilor între oameni și mașini este dinamic.

Este evident că tendința evoluțiilor și implementarea extrem de rapidă a CPS-urilor determină o creștere a tensiunilor societale cu privire la evoluția noilor tendințe tehnologice și la impactul lor asupra modului în care trăim. În plus, această stare determină și tensiunile emergente care apar și se extind asupra reglementărilor legislative, asupra certificărilor, asigurărilor și a altor relații societale, care sunt necesare în vederea adoptării pe scară largă a acestor tehnologii.

Pentru înțelegerea interacțiunii dintre oameni și dispozitivele care integrează CPS-uri prezentăm în figura 2.1 un model de structură schematică.

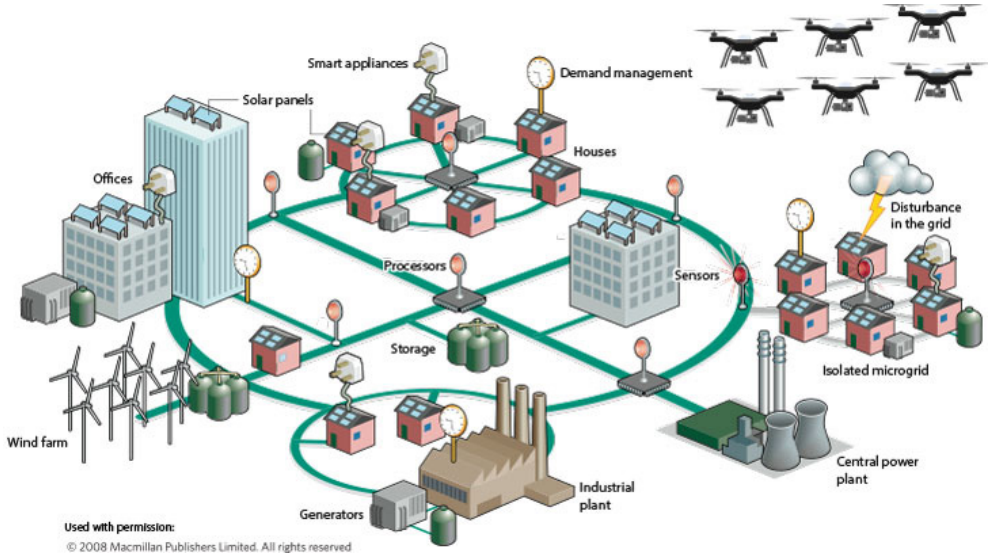

Figura 2.1. – Ecosistem societal bazat pe CPS-uri[4]

Prin modelul ipotetic prezentat, în cadrul Institutului pentru sisteme CPS a Universității Vanderbilt, a fost rezolvată problema ambuteiajelor rutiere cu autovehicule autonome. Astfel seturile mari de date au fost folosite pentru a înțelege congestionarea traficului urban, la scara orașului și a traficului feroviar de marfă, pentru o scară regională. Optimizarea acestuia s-a realizat prin modele matematice și instrumente din Teoria Sistemelor, pentru a înțelege comportamentul de bază a fluxurilor de trafic. Acest proiect de pionierat în metodele de monitorizare și de control al traficului rutier a folosit autovehicule, pentru detectarea și controlul aglomerației rutiere, în defavoarea infrastructurii fixe. În 2015, aceste modele au

[4] CPS-VO, *Science of Design for Societal-Scale Cyber-Physical Systems (CPS)*, https://cps-vo.org/group/sdss-cps visited at 28.06.2023

fost testate pe tehnologii ale autovehiculelor comerciale disponibile ale firmei Ford și mediatizate prin emisiunea Good Morning America, difuzată la postul american ABC, în conformitate cu pagina Internet a proiectului de cercetare științifică[5]. Prin acest experiment s-a demonstrat că ambuteiajele „fantomă", care par să apară fără o cauză evidentă și care se datorează comportamentului uman în condus, pot fi eliminate prin controlul unei mici secvențe de autovehicule automatizate, din flux.

Trebuie bine înțeles că CPS-urile nu sunt sisteme informatice tradiționale, încorporate sau independente, destinate pentru a executa una sau mai multe funcții, în timp real, prin conexiune la rețele de senzori și la aplicații, pe dispozitive desktop. Ele depășesc aceste cerințe contemporane prezentând unele caracteristici particulare precum:

1. CPS-urile sunt integrări ale proceselor de calcul și fizice;

2. Prezintă capabilități și resurse cibernetice limitate, în fiecare componentă fizică;

3. Rețeaua este multiplă și cu o scalabilitate extremă. CPS-urile, ale căror rețele includ rețea cu fir/wireless, WLAN, Bluetooth, GSM etc. sunt sisteme distribuite;

4. Permit reconfigurare/reorganizare dinamică, complicată, pentru realizarea capacităților optime de adaptare;

5. Au un grad ridicate de automatizare, iar relațiile de feedback trebuie să se închidă;

6. Funcționarea lor trebuie să fie fiabilă și certificată, în unele cazuri;

7. Componentele cibernetice și fizice sunt integrate pentru învățare în secvențe de timp și de spațiu. Infrastructura se poate raporta la mai multe scale temporale și spațiale.

[5] Institute for Software Integrated Systems, *Work research group*, https://lab-work.github.io/ visited at 28.06.2023

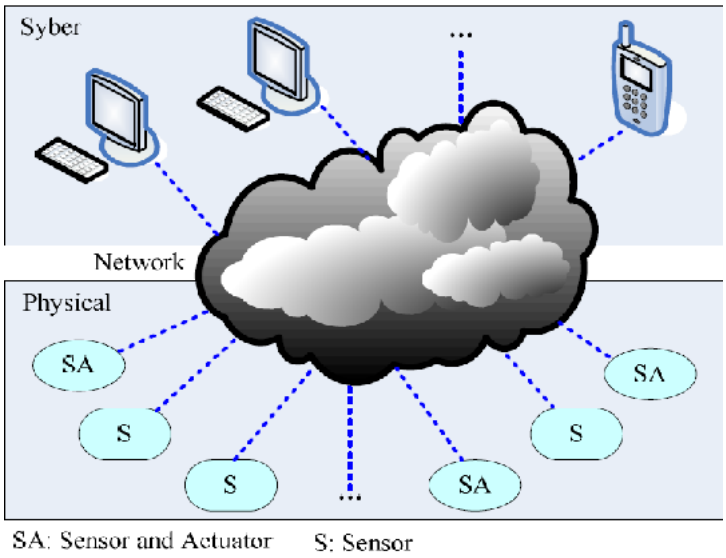

Figura 2.2. – Schemă generală pentru CPS

2.2.2. Aplicații CPS în viața cotidiană

Principalele aplicații CPS contemporane includ dispozitive și sisteme medicale, aplicații de tip locuințe inteligente, sisteme de control și siguranță în trafic, sisteme auto avansate, sisteme de control al proceselor, sisteme de conservare a energiei, de control a mediului și software pentru aviație, instrumente pentru infrastructura critică (în special pentru energie și apă), robotică distribuită, sisteme de arme, sisteme de producție, comenzi de detectare distribuită și de control, structuri inteligente, biosisteme, sisteme de comunicații etc.

Prezentăm trei exemple de aplicații pe bază de CPS estimate pentru următoarele domenii:

A. Asistență medicală și medicină

Domeniul asistenței medicale și a medicinei include rețeaua națională de informații privind sănătatea, instrumente de înregistrare electronică a pacientului, instrumente de îngrijire la domiciliu, instrumente medicale din sălile de operație etc. Toate sunt din ce în ce mai mult controlate de sisteme informatice cu componente hardware și software, formând un sistem sigur și sincronizat, care funcționează în timp real. Un caz de CPS pentru o sală de operație este prezentat în Figura 2.3.

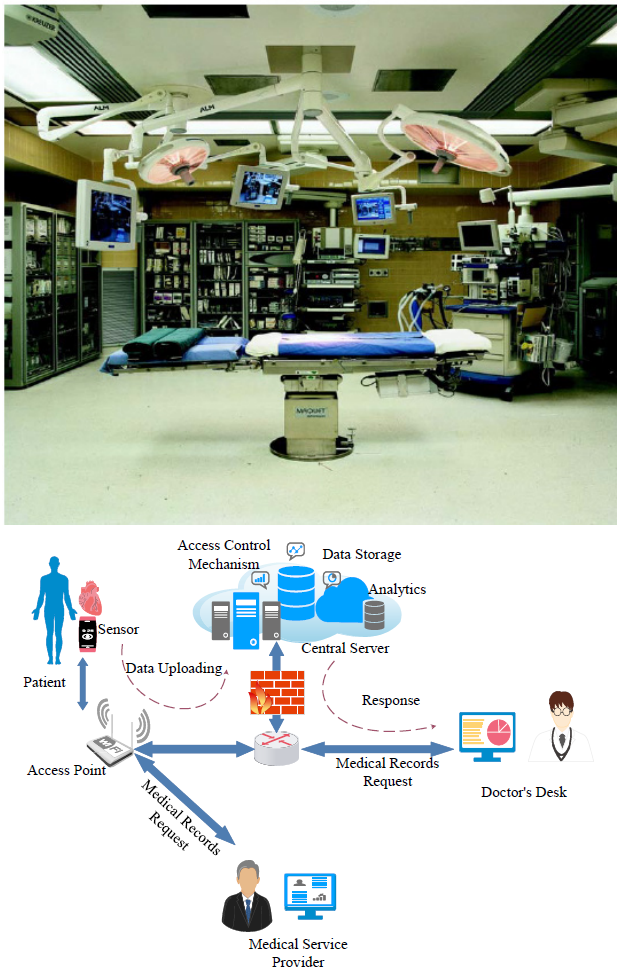

Figura 2.3 – Modelul unei săli de operație bazată pe CPS[6]

B. Rețea de alimentare și transport a energiei electrice

Energia electrică de putere ori rețeaua de alimentare și de control includ dispozitive care încorporează software. Infrastructura lor reprezintă un CPS al cărui design este puternic influențat de toleranța la erori, de securitate, de control

[6] Santhosh, E.B., Pradhan, A.K., Badarla, V.R., Mohanty, S.P. (2021) Fortified-Chain: A Blockchai-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control, IEEE Internet of Things Journal PP(99):1-1, DOI:10.1109/JIOT.2021.3058946, Lab: Ashok Kumar Pradhan's Lab, https://www.researchgate.net/publication/349284375_Fortified-Chain_A_Blockchain-Based_Framework_for_Security_and_Privacy-Assured_Internet_of_Medical_Things_With_Effective_Access_Control visited at 28.06.2023

descentralizat, de mediul economic și de aspecte etice sociale. În Figura 2.4 prezentăm un CPS specific.

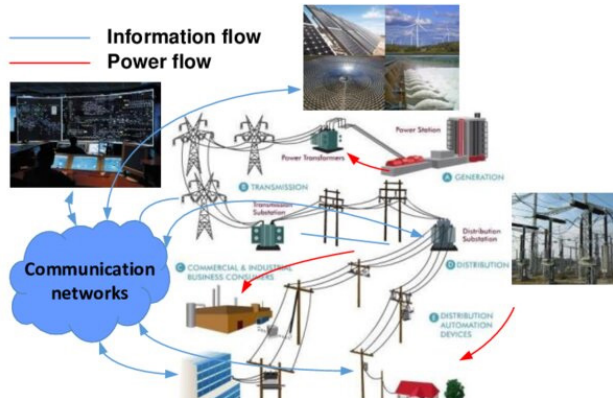

Figura 2.4.- Rețea de energie electrică bazată pe CPS[7]

C. Integrarea drumurilor inteligente cu vehiculul fără pilot

Odată cu dezvoltarea rețelei de senzori încorporate în sisteme, unele soluții noi pot fi aplicate vehiculelor fără pilot uman la bord, fie ele aeriene, terestre și submersibile. Modelul unui drum inteligent pentru vehicule fără pilot uman la bord, reprezintă o formă de CPS. Figura 2.5 prezintă un astfel de model bazat pe CPS.

Figura 2.5 – Model de drum rutier bazat pe CPS[8]

[7] Yang, Q. & other (2017) PMU Placement in Electric Transmission Networks for Reliable State Estimation Against False Data Injection Attacks, IEEE Internet of Things Journal PP(99)1-1, DOI: 10.1109/JIOT.2017.2769134, https://www.researchgate.net/publication/320827505_PMU_Placement_in_Electric_Transmission_Networks_for_Reliable_State_Estimation_Against_False_Data_Injection_Attacks visited at 28.06.2023

[8] Dey, K., Fries, R., Ahmed, S., (2018) Future of Transportation Cyber-Physical Systems – Smart Cities/

Devine tot mai clar că domeniul dezvoltării CPS-urilor dezvoltă noi provocări în cercetarea aplicată care trebuie să găsească răspunsuri pentru o varietate de întrebări, pentru diverse tipuri de arhitecturii și infrastructuri, sub aspectul proiectării sistemelor, în vederea convergenței și integrării lumii fizice cu spațiul cibernetic.

Cele mai relevante provocări analizate în mediile științifice sunt:

1. Sisteme hibride de control

Trebuie identificate și dezvoltate noi teorii de modelare matematică care să îmbine sistemele bazate pe evenimente cu sisteme bazate pe timp, pentru controlul feedback-ului. Aceasta trebuie, de asemenea, să fie potrivite pentru ierarhii care implică dinamica asincronă în momente scalare diferite și în medii geografice.

2. Senzori și rețele mobile

Nevoia de autonomie sporită a sistemelor necesită aplicații practice de autoorganizare și/sau reorganizarea rețelelor mobile de comunicații pentru CPS-uri. Pentru acestea sunt esențiale aplicații de colectare și de rafinare a datelor și informațiilor critice, dintr-o cantitate mare de date brute.

3. Robustețe, fiabilitate, siguranță și securitate

Aceasta reprezintă o provocare critică deoarece incertitudinea mediului. Apărarea contra atacurilor și erorile în dispozitivele fizice fac ca asigurarea generală a robusteții, a securității și siguranței sistemului să fie cerințe prioritare. Exploatarea mediului fizic determină ca natura CPS să sporească valorificarea sistemelor a căror funcții se bazează pe locație, pe timp și pe mecanisme de etichetare (tag-based mechanism) pentru a stabili soluții de securitate.

4. Abstractizare

Acest aspect include încorporarea, în timp real, a sistemelor abstracte și a abstracțiilor informaționale care au nevoie de o nouă schemă de alocare a resurselor. Pentru asigurarea acestei cerințe trebuie create noi sisteme de toleranță, de scalabilitate, de optimizare etc. Pentru noile formule de optimizare distribuită și

Regions, Transportation Cyber-Physical Systems, doi.org/10.1016/B978-0-12-814295-0.00011-3, Ed: Deka L. & Chowdhury M., Elsevier Inc. Public House, 2019, pp. 267-307, https://www.sciencedirect.com/science/article/abs/pii/B9780128142950000113 visited at 28.06.2023

noile metode de comunicare, inter și intra grup, în timp real, sunt necesare programe și algoritmi capabili să modeleze proprietățile mediului fizic.

5. Dezvoltare bazată pe modele

Deși știința modelării sistemelor are puternice rădăcini în trecut, multe din metodele de dezvoltare bazate pe modele nu corespund cerințelor CPS-urilor. Calculatoarele, comunicațiile și dinamica fizică trebuie să fie abstractizată și modelată pe diferite niveluri, determinate de volum, de locație și de puterea de rezoluție a calificărilor temporare.

Furnizarea unui formalism a conceptului de granulitate a timpului face posibilă modelarea datelor bazate pe timp (time-series data) în raport cu domenii temporare diferite.

6. Verificare, validare și certificare

Trebuie stabilită o interacțiune între metodele formale și testarea lor. Aceasta este necesară identificării posibilităților de aplicare a naturii eterogene a modelelor CPS la metodele de verificare și de testare a compoziției lor.

2.3. Rolul și principiile utilizării infrastructurilor bazate pe CPS pe tot parcursul vieții

În prezent, digitalizarea permite identificarea unor game variate de soluții de optimizare a activităților cotidiene. În funcție de felul muncii sau a modului de petrecere a timpului liber oricare individ poate identifica efectele digitalizării. Întregi comunități sociale și profesionale sunt digitalizate, mai mult sau mai puțin, în funcție de interesul acordat și de percepția elementelor de guvernare față de avalanșa noului.

Privind percepția cetățenilor față de aceste tendințe, opiniile diferă în funcție de nivelul de educație și de interesul acordat pentru învățare profesională, într-o piață extrem de flexibilă și de mobilă. Conceptul de „învățare pe tot parcursul vieții" (lb.eng. „lifelong learning") a căpătat noi valori, trecând de la o linie strategică a politicilor liberale la o necesitate reală, pentru adaptarea vieții umane la modelele societății viitorului. Acesta, include toată învățarea care se desfășoară în școală dar și în afara acesteia. Prin intermediul formelor de pregătire continuă, un individ dobândește noi abilități cu care se poate adapta la viitoarele provocări, pe de o parte, dar mai poate colabora și contribui în mod activ la dezvoltarea altor domenii sociale.

Nu este un concept nou, fiind asociat cu accesul la educație pentru toată populația, fără discriminări, pe tot parcursul vieții, apărut în anii 1960 și 1970. Acesta este urmare a perspectivei conform căreia educația, în întregimea ei, ar fi putut sau ar fi trebuit să nu fie limitată la perioada învățământului formal pentru copii, adolescenți și tineri. Prin reîmprospătarea cunoștințelor și dezvoltarea aptitudinilor/competențelor oamenii devin buni cetățeni și angajați. Aceste direcții de evoluție a societății, de la acea vreme, au fost influențate de ONU care, în anul 1972, a elaborat și publicat raportul Organizației Națiunilor Unite pentru Educație, Știință și Cultură (UNESCO), Learning to Be (A învăța să fii) (raportul Faure, 1972) și raportul Organizației pentru Cooperare și Dezvoltare Economică (OCDE), Recurrent Education: A Strategy for Lifelong learning (Educaţia recurentă: o strategie de învățare pe tot parcursul vieții, 1973). Aspectele subliniate întăreau preocupările UNESCO pentru diverse aspecte culturale și ale OCDE pe linii economice și care țineau de piața muncii, având raționamente similare.

Dezvoltarea tehnologică, în mod firesc, a determinat schimbări în sistemele de educație care pot fi identificate de oricine. Chiar și în prezent actualele schimbări ale programelor de învățământ și a altor forme de pregătire profesională sunt rezultatul evoluției tehnologice și a încercărilor de adaptare a lor pentru direcțiile viitoare, estimate că ar putea fi în viitor. Cert este că actualele infrastructuri inovatoare de comunicații și IT precum și platformele digitale vor oferi noi servicii tuturor comunităților, majoritatea fiind deja interconectate prin Internet. În viitor, interconectarea în rețele de tot felul va reprezenta o condiție de normalitate a mediului social, cu infrastructuri digitale care vor asigura servicii sustenabile și de regenerare, toate fiind destinate folosirii soluțiilor de îmbunătățire a nivelului de trai.

Pentru acesta fiecare cetățean trebuie să înțeleagă că sprijinul pe care îl poate acorda dezvoltării comunității se poate manifesta prin comunicarea nevoilor și a cerințelor sale. Există numeroși factori din administrațiile locale și din alte organizații care știu și au responsabilități față de mediul și față de comunitate. De altfel, avantajele implementării noilor tehnologii reprezintă esența evoluției comunității respective.

Privind CPS-urile, ele nu trebuie privite ca ceva pe care nu are rost să le înțelegi și să le folosești. Chiar și în prezent tot mai multe CPS-uri sunt implementate sub formă de dispozitiv încorporat sau independent și fac parte din viața noastră, fără a le numi așa.

Încă din anul 2005, au fost încorporate o serie de procesoare pe mașinile personale, identificate sub diferite firme și mărci de producție. Astfel, sistemele de control al motorului, sistemele de asistare la impact, modalitatea de declanșare a airbag-urilor, sistemele inteligente a ștergătoarelor de parbriz, a celor de închidere și de încuiere a ușilor, unele sisteme de divertisment etc., toate cuprind procesoare, sisteme de operare (în principal Windows CE OS), posibilități de conectare la rețele multiple etc., autoturismele fiind senzori și actuatori în rețelele V2V, putând emite alerte active de siguranță în rețea și informații pentru navigația autonomă.

Rețeaua Națională de Informații în Sănătate, prin inițiativa numită Fișa electronică a pacientului asigură fișe medicale în orice punct de urgență, spital, unitate de terapie intensivă, de intervenție de pe salvări și chiar paramedicilor aflați în misiune. CPS-urile de acest tip sunt integrate în dispozitive destinate îngrijirii la domiciliu a pacienților, pentru servicii de monitorizare și control precum: pulsoximetre (saturația în oxigen), monitorizarea glicemiei, pompe de perfuzie (cu insulină), accelerometre (cădere, imobilitate), rețele portabile pentru analiza mersului etc. În viitor, sălile de operație vor avea monitorizare și controlul în buclă închisă, direct conectate cu stații de tratament multiplu, cu dispozitive plug and play, cu echipamente de microchirurgie robotică (controlată de la distanță sau autonome) etc.

Căderile de tensiune și alte defecțiuni din rețelele de alimentare cu energie electrică sau din rețele de comunicații sunt monitorizate și remediate cu ajutorul CPS-urilor. O rețea modernă de comunicații cuprinde dispozitive de rețea (routere), medii de comunicare (cu și fără fir, Wi-Fi), senzori și controlele. O rețea electrică cuprinde magistrale/linii de transport/distribuție, magistrale de încărcare, transformatoare, centre de control, senzori și routere, legături de comunicație etc. Cu aceste echipamente se formează căi active care permit ca la apariția unei defecțiuni traficul fluxurilor respective să fie redistribuit către alte căi active, fără a fi influențați beneficiarii.

CPS-uri pentru domeniul militar sunt cuprinse în capitolul tehnologii disruptive și pot fi găsite în sistemele contemporane de arme și pe diverse platforme de luptă. Dintre acestea, cele mai frecvente sunt la rachetele de croazieră și cele din sistemele antirachetă (de tip Patriot) precum și în unele sisteme autonome, fără pilot uman la bord.

În concluzie, întreaga activitate umană este sprijinită de CSP-uri. Înțelegerea interacțiunii dintre oameni și sistemele digitale va reduce frica firească a cetățenilor față de digitalizare și de implementarea masivă a platformelor specifice. Aceste

tendințe obligă atât la o pregătire continuă profesională cât și la adoptarea unei viziuni flexibile față de educația continuă. Acestea vor contribui esențial la adaptarea condițiilor impuse de piața muncii, care depind de cerințele unei economii digitale dar și de cerințele sociale ale unui ecosistem digitalizat. De aceea, identificarea clară a obiectivelor de realizat, raportate la perioade scurte de timp pentru a fi reanalizate, va permite creatorilor de sisteme CPS să realizeze o trecere facilă și rapidă către un viitor pe care, în prezent, doar creatorii de conținut science fiction îl pot anticipa.

Propunem o serie de criterii care să permită implementarea eficientă, sigură și fiabilă a infrastructurilor CPS:

1. Să se urmărească obiective care să permită proiectarea unei infrastructuri ce se poate extinde și poate fi scalată pe măsură ce crește numărul de componente și dispozitive interconectate. Astfel, poate fi asigurată adaptabilitatea sistemului la noile schimbări de mediu și permite adăugarea de noi funcții și operații;

2. Securitatea sistemului și a datelor reprezintă o prioritate în inovarea CPS. Având în vedere interconectarea dispozitivelor și schimbul de date, infrastructura trebuie să conțină mecanisme puternice de securitate care să permită autentificarea și autorizarea dispozitivelor, criptarea datelor, protecția sistemelor la atacuri cibernetice etc.

3. Componentele CPS trebuie să comunice între ele. Stabilirea unor servicii eficiente și interoperabile bazate pe diverse tehnologii, care să respecte standarde și protocoalele propuse, poate reprezenta o direcție inovativă pentru CPS;

4. Sistemele CPS pot fi critice din punct de vedere al funcționării. De aceea, ele trebuie să fie rezistente la eșecuri și erori, să conțină mecanisme de redundanță și de recuperare în caz de defecțiuni majore apărute la dispozitivele sistemului sau în cadrul liniilor de conectivitate;

5. Soluțiile de management și de stocare a datelor pot reprezenta direcții de inovare pentru CPS. Gestionarea volumelor mari de date, în timp real, pe fondul menținerii unei eficiențe sporite face ca infrastructura să includă baze de date distribuite, tehnologii de stocare în cloud sau alte soluții adecvate;

6. Soluții de monitorizare și de analiză a datelor. Infrastructura ar trebui să permită monitorizarea și analiza în timp real a datelor colectate de senzori. Acestea presupun instrumente de analiză performate, algoritmi de învățare automată, sisteme de gestionare a evenimentelor, alte soluții de analiză, în timp real, a datelor;

7. Identificarea și actualizarea mecanismelor și soluțiilor de actualizare software și de întreținere a dispozitivelor reprezintă o cerință permanentă a CPS. Accentul se pune pe realizarea unei actualizări și a întreținerii sistemelor de la distanță;

8. Nu în ultimul rând identificarea unor programe educaționale pentru populație, programe care să nu depindă de mediul educațional formal (școală) pot reprezenta soluții pentru modificarea percepțiilor și a unor mentalități privind rolul și locul CPS în viața noastră. Cursul de față este o formă care se încadrează pe această direcție.

Privind implicațiile utilizării CPS-urilor în cadrul activității cotidiene a oamenilor, trebuie să înțelegem că pentru un CPS mediul său este lumea reală. Aceasta poate fi un mediu social uman (pentru aplicațiile de roboții sociali), o stradă a orașului (pentru un vehiculele autonome), un spațiu de îngrijire a sănătății sau un spital (pentru o îngrijirea asistată) sau oricare loc de muncă (ca instrument de optimizare a muncii).

„Mediul" unui CPS poate fi clinic (pentru stabilirea unui diagnostic medical), public – de exemplu, pentru analiza datelor și recunoașterea facială în aeroporturi sau virtual pentru culegerea și procesarea datelor din rețelele sociale. Ar putea fi asimilat unui robot fizic care interacționează cu oamenii, mașinile și cu alți roboți. De altfel, interacțiunea cu oamenii dă naștere la ample probleme de ordin etic.

Toate CPS-urile îndeplinesc funcții clare pentru sarcini specializate, așa cum au fost ele proiectate. Chiar dacă obiectivele pentru CPS-urile multirol sunt încă în studiu, este important de înțeles că unele componente există și sunt deja implementate în diverse tehnologii contemporane. Învățarea automată este termenul folosit pentru AI pe care se bazează un CPS al viitorului, pentru a se adapta mai bine la mediul lor.

Există o gamă largă de abordări ale învățării automate, dar acestea se încadrează de obicei în două categorii: învățarea supravegheată și cea nesupravegheată.

Sistemele de învățare supravegheată folosesc, în general, rețelele neuronale artificiale (ANN), care sunt antrenate prin furnizarea de intrări (de exemplu, imagini cu animale), fiecare dintre acestea fiind etichetate (de către oameni) cu o ieșire (adică identificarea tipului animalului adică un câine, o pisică, un cal, o vacă etc.). Acest set de intrări și de ieșiri potrivite se numesc seturi de date de antrenament. După antrenament, un ANN ar trebui să fie capabil să identifice ce animal se află într-o imagine prezentată (adică un câine), chiar dacă acea imagine cu un câine nu a fost prezentă în setul de date de antrenament. În schimb, învățarea nesupravegheată nu are date de instruire. AI (sau CPS-ul) trebuie să descopere singur cum să rezolve o anumită sarcină (adică cum să navigheze cu succes dintr-o rețea de străzi), în general prin încercare și eroare.

Atât învățarea supravegheată, cât și cea nesupravegheată au limitările lor. Dintre acestea amintim: apariția unor potriviri prin identificarea de imagini neconcludente, limitarea doar la imaginile prevăzute de designerii umani, învățare lentă din foarte multe evenimente etc.

Sub aceste premise, pentru societatea umană o mare problemă ține de aspecte de etică pentru CPS. Acesta se concentrează pe modului în care dezvoltatorii și producătorii umani ar trebui să minimalizeze daunele etice care pot apărea din utilizarea CPS-urilor în societate, fie ca urmare a unui design slab (neetic), a unei aplicări inadecvate sau a unei utilizări greșite. Domeniul de aplicare al eticii CPS-urilor cuprinde preocupări imediate, așa cum sunt asigurarea confidențialității datelor și comunicarea între sistemele actuale, impactul tehnologiilor bazate pe CPS-uri asupra locurilor de muncă, gradul de inteligență maxim al AI din CPS-uri.

Este cunoscut că aspectele care țin de etica AI a trecut de la o preocupare academică la o problemă de dezbatere publică. Omniprezența tot mai mare a telefoanelor inteligente și a aplicațiilor bazate pe inteligență artificială, pe care mulți dintre noi se bazează acum în fiecare zi, faptul că inteligența artificială are un impact din ce în ce mai mare asupra tuturor sectoarelor socio-economice (industrie, sănătatea, transporturi, securitate națională și justiție, finanțe, divertisment etc.), a determinat apariția unui număr extraordinar de inițiative naționale și internaționale, din partea ONG-urilor, grupărilor academice și industriale, a structurilor profesionale și de guverne, care au condus la publicarea unui număr mare de seturi de principii etice, în special pentru robotică și AI. Astfel, din ianuarie 2017 au fost publicate cel puțin 22 de seturi diferite de principii etice pentru AI, sunt noi standarde etice precum IEEE Standards, iar un număr tot mai mare de țări și alianțe politico-

militare propun strategii de AI, asigurând fondurile necesare înființării de structuri naționale de consiliere sau politici noi. Acestea își propun identificarea și înlăturarea posibilelor prejudicii etice care, în general, pot afecta respectarea drepturile omului și bunăstarea socială, pot conduce la vătămare emoțională, la afectarea securității, confidențialității, accesibilității, încrederii în tehnologiile digitale, pot produce prejudicii sociale, juridice, financiare, de legalitate și dreptate, pot crea abuzuri prin utilizarea excesivă a resurselor mediului și pot genera riscuri existențiale asupra infrastructurilor critice.

De aceea, implicarea oricărui cetățean și nu numai a specialiștilor IT în identificarea acelor aspecte care pot afecta etica socială îi va ajuta pe designerii CPS-urilor să caute soluții adecvate care să apere confortul societal și să îi descurajeze pe cei care doresc să utilizeze tehnologiile digitale în scopuri malițioase, în mod individual sau grupați în structuri de crimă organizată și terorism. Aceasta trebuie să devină o activitate benevolă și asumată de comunicare a incidentelor de securitate cibernetică către structurile special destinate în vederea combaterii lor. Din punct de vedere instituțional lărgirea cadrului de informare și de colaborare interinstituțională reprezintă esența stabilirii de noi politici de securitate adaptate la mediul social pentru oricare societate modernă.

TEMA 3: ELEMENTELE DE BAZA ALE UNUI CPS ȘI INTERACȚIUNEA DINTRE ACESTEA

Din cele prezentate în tema anterioară observăm că sistemele CPS integrează o serie de proprietăți specifice dispozitivelor electronice (senzori, rețele și computing) în scopul de a le face cât mai atractive prin adaptabilitatea lor la mediu, prin autonomie, eficiență, funcționalitate, fiabilitate, siguranță și optimizarea utilizării lor. Aceste noi proprietăți sunt generate de aplicațiile și de resursele utilizate pentru rezolvarea sarcinilor proiectate, fiind prioritizate pe grade și niveluri de execuție diferite. De exemplu, în infrastructurile critice, fiabilitatea și siguranța sunt însușiri cu importanță primordială. În schimb, pentru producția industrială principala funcție a unui astfel de sistem poate fi funcționalitatea.

Integrarea într-un sistem a componentelor cibernetice cu cele fizice în scopul îndeplinirii a cel puțin o sarcină este principalul scop al proiectării unui CPS. Anterior apariției acestui concept un astfel de sistem era cunoscut sub denumirea generică de sistem informațional. Și atunci, în mod firesc ne întrebăm de ce a trebuit să se creeze un nou concept? Ce aduce nou? Care este plus valoarea? Un CPS se limitează doar la optimizare funcțională?

În tema următoare vom căuta să identificăm răspunsul aceste întrebări și a altora care pot apărea pe parcursul înțelegerii modului de organizare și de funcționare a unui CPS generic, urmând ca particularitățile utilizării lui în aplicații specifice să fie dezvoltate de fiecare cursant, în funcție de interesul profesional sau particular al său.

3.1. Elementele de bază ale unui CPS

Figura 3.1 propune un model de asociere a unor componente cibernetice și fizice uzuale. Subsistemul fizic este compus din componente care sunt corelate în mod natural prin relații fizice. Adesea, ele pot fi considerate componentele sistemului fizic original, înainte de a fi „activate cibernetic”. Subsistemul cibernetic este compus din elemente care sunt conectate între ele în scopul informării curente. Acestă funcție ar putea fi realizată prin mijloace fizice, precum doi senzori conectați printr-o legătură de comunicații în vederea stabilirii unei comunicări fizice, ori a unei comunicări virtuale, printr-un canal cu sau fără fir. În subsistemele fizice și cibernetice, fiecare dintre elemente sunt cuplate individual, în mod funcțional, așa cum se poate vedea

în imagine. De obicei, schema legăturilor de comunicații se proiectează, printr-un model grafic, anterior proiectării sistemului.

Integrarea elementelor cibernetice și cu cele fizice are loc într-un mediu fizic și cibernetic, prin echipamente specifice. Aici, legătura fizico-cibernetică se realizează la nivelul senzorilor, care convertesc observațiile sesizate în mediu în date, cumulate în cantități fizice măsurabile (baze mari de date – Big data). Legătura fizico-ciberentică are loc la nivelul interfeței de acționare, prin care datele sunt procesate în vederea luării unei decizii în scopul determinării unor schimbări fizice în sistemul fizic. De exemplu, dispozitivul de stocare a datelor dintr-un sistem de alimentare cu energie electrică, care utilizează informații pentru a decide dacă puterea energetică trebui să fie absorbită sau remisă pentru a menține stabilitatea rețelei electrice.

CPS-urile specifice pot varia semnificativ, în funcție de locul și rolul utilizării lor în întreaga rețea energetică. Tendința emergentă este în dezvoltare a distribuției de energie electrică pe o plajă largă, în subsisteme de rețea.

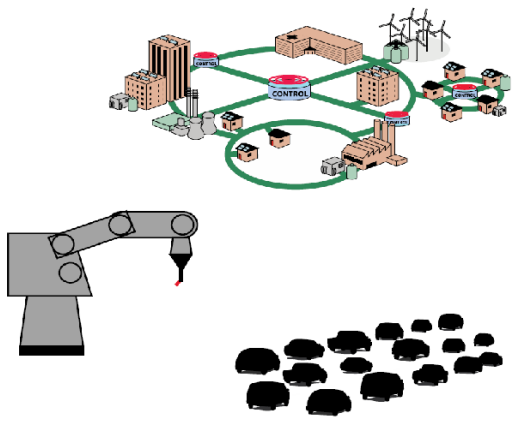

Figura 3.1 – Model de sistem fizico-cibernetic (CPS) pentru o rețea energetică

Elementele de bază ale unui sistem fizico-cibernetic (CPS) includ componente cibernetice și fizice care interacționează între ele pentru a realiza o funcție comună. Acestea, în principal, includ (sub rezerva diversității și a gamei variate de echipamente):

- Sisteme informatice: componente hardware și software utilizate pentru a controla și monitoriza componentele fizice. Sistemele informatice pot include calculatoare, servere, dispozitive de rețea, alte componente

similare. Monitorizarea și analiza datelor în timp real pot implica utilizarea senzorilor interni și a algoritmilor de analiză pentru a detecta anomalii, a anticipa defecțiuni și a optimiza performanța sistemului. CPS-urile pot genera cantități mari de date provenite de la diverse componente și senzori. Tehnologiile Big Data și de analiză avansată pot fi utilizate pentru a extrage cunoștințe valoroase din aceste date, pentru a identifica modele complexe și pentru a oferi informații utile în vederea stabilirii unei decizii;

- Sisteme fizice: acestea sunt componentele cu cea mai largă gamă de utilizare determinată de destinația și de modul de utilizare pentru a controla mașini industriale, roboți, vehicule autonome, senzori, actuatori, alte dispozitive care interacționează cu lumea fizică;

- Rețele de comunicație: acestea permit transmiterea datelor și informațiilor între componentele cibernetice și cele fizice. Rețelele de comunicației pot fi realizate prin cabluri sau Wi-Fi, ori cordless, Bluetooth, Zigbee etc,. și pot include protocoale și tehnologii specifice pentru transferul datelor. Unele CPS-uri pot fi conectate la rețele IoT, pentru comunicarea și schimbul de informații cu alte dispozitive și sisteme asociate. Această tehnică permite monitorizarea și controlul CPS-urilor de la distanță, colectarea datelor suplimentare și realizarea rețelelor extinse;

- Senzori și actuatori: senzorii detectează schimbările din mediul fizic, în conformitate cu destinația lor, convertind informațiile în semnale digitale. Actuatorii acționează asupra mediului fizic prin instrucțiunile primite de la componente cibernetice. Atât senzorii cât și actuatorii permit CPS-ului să obțină date din mediul fizic și să acționeze în cel mai bun mod. În plus, gestionarea eficientă a resurselor se realizează prin tehnici de optimizare energetică, precum gestionarea puterii, gestionarea sarcinii, utilizarea surselor de energie regenerabilă pentru a reduce impactul asupra mediului și a îmbunătăți eficiența energetică. În plus, având în vedere complexitatea CPS-urilor este important de asigurat o toleranță mare la erori și un nivel ridicat de reziliență a sistemului. Acest lucru implică capacitatea de a detecta și de a se adapta la eșecuri, de a lua măsuri de corectare și de menținere a funcționalității esențiale, în ciuda problemelor și avariilor;

- Algoritmi și software: aceste sunt programe informatice responsabile pentru procesarea datelor și pentru adoptarea deciziilor într-un CPS. Algoritmii pot fi utilizați pentru controlul și monitorizarea sistemelor fizice, pentru analiza datelor, pentru optimizarea performanței și în multe

alte scopuri. Software-ul este responsabil de implementarea acestor algoritmi și de gestionarea resurselor de comunicații (linii și interfețe) cu componentele fizice. Unele programe software fac parte din sistemele de învățare automată a CPS-urilor. Acestea implică schimb autonom de informații, coordonarea acțiunilor și realizarea de obiective comune prin intermediul protocoalelor și algoritmilor specializați în modelare și simulare.

- Dispozitive de interacțiune de tip om-mașină: Un CPS poate interacționa cu utilizatorul uman. Pentru aceasta trebuie să conțină echipamente care-i permit utilizatorului să monitorizeze și să controleze un CPS, primește informații și ia decizii în funcție de datele furnizate de sistem. Unele CPS-uri pot facilita interacțiunea și colaborarea între oameni într-un mediu fizic și cibernetic. Acest lucru poate include interacțiunea socială mediată de tehnologie, colaborarea în timp real și partajarea informațiilor între utilizatori, prin intermediul sistemului CPS.

În mod ***suplimentar***, în funcție de rolul și de destinația CPS-ului, sistemul mai poate conține:

- *Echipamente cloud computing*: Unele CPS-uri pot utiliza servicii de cloud computing pentru a stoca și procesa datele colectate de la componentele fizice. Această funcție permite accesul rapid și scalabil la resursele de calcul și de stocare, precum și realizarea analizelor avansate prin algoritmi complexi.

- *Echipamente de securitate cibernetică*: Deoarece CPS-ul implică interacțiunea între componentele cibernetice cu cele fizice, un accent deosebit se pune pe securitatea cibernetică. Este crucial să se protejeze împotriva atacurilor cibernetice toate componentele cibernetice, precum rețelele, sistemele informatice și datele, scopul final fiind de asigurare a integrității, confidențialității și disponibilității sistemului.

- *Sisteme suplimentare de gestionare a datelor*: Unele CPS-uri generează și culeg o cantitatea imensă de date provenite de la senzori, de la alte dispozitive și componente. Sistemele de gestionare a datelor permit stocarea, prelucrarea, organizarea și analiza acestor date, pentru a obține informații valoroase și a lua decizii în timp real.

- *Sisteme de realitate virtuală (VR) și augmentată (AR)*: CPS-urile pot beneficia de tehnologii specifice realității virtuale și augmentate pentru a spori interacțiunea și înțelegerea comunicării cu utilizatorul uman.

Aceste tehnologii pot fi utilizate pentru a oferi vizualizări avansate, instrucțiuni sau asistență, în timp real, pentru optimizarea acțiunii în mediul fizic. În plus, prin aceste componente se poate crea un mediu virtual în care pot fi simulate diverse scenarii și condiții de operare, pentru evaluarea performanței sistemului și pentru a identifica posibile probleme înainte de implementarea proceselor în sistemul fizic.

- *Sisteme de inteligență artificială (AI) și machine-learning (ML)*: pentru a îmbunătăți funcționarea sistemului, CPS-urile pot utiliza tehnici de inteligență artificială și de învățare automată. Aceste tehnologii pot fi utilizate pentru a realiza analize avansate de date, pentru identificarea modelelor și tendințelor, pentru optimizarea operațiunilor și pentru a lua decizii autonome, în funcție de datele colectate.

- *Standarde și protocoale de interoperabilitate*: CPS-urile pot implica diverse componente și tehnologii care provin de la furnizori și dezvoltatori diverși. Pentru a facilita interoperabilitatea și integrarea funcționării, standardizarea este crucială. Există eforturi de dezvoltare a standardelor comune și a protocoalelor de comunicare pentru a asigura compatibilitatea și interoperabilitatea între componente și sisteme diferite.

- *Norme de securitate a datelor personale și etice*: utilizarea CPS-urilor implică adesea colectarea și procesarea datelor personale și a altor informații sensibile. Asigurarea confidențialității datelor și respectarea principiilor etice sunt elemente esențiale în proiectarea și utilizarea CPS-urilor. De aceea, este important să se acorde atenție protecției datelor pe fondul asigurării respectării drepturilor utilizatorilor.

- *Proceduri de actualizare și de mentenanță*: CPS poate necesita actualizări și mentenanță periodică pentru a asigura funcționalitatea optimă și securitatea continuă. Aceste reglementări pot include standarde de securitate cibernetică, norme de protecție a datelor personale, cerințe privind calitatea și fiabilitatea sistemului etc. Îmbunătățirile software, actualizările de securitate și remedierea problemelor tehnice sunt aspecte importante pentru menținerea unui CPS într-o stare eficientă și fiabilă.

Acestea sunt câteva elemente suplimentare care pot fi prezente într-un CPS. Este important de amintit că CPS-urile variază în funcție de domeniul de aplicare și de specificațiile sistemului în sine.

Lista componentelor suplimentare poate continua cu:

- *Roboți și sisteme autonome*: CPS-urile pot implica utilizarea roboților și a sistemelor autonome care interacționează cu mediul fizic. Acestea pot fi responsabile de sarcini diverse precum: manipularea obiectelor, navigare autonomă, asamblarea unor componente, monitorizarea mediului etc. Integrarea roboților și a sistemelor autonome implică sincronizarea funcționării unor componente cibernetice și furnizare de date, în timp real.

- *Edge computing*: Un CPS poate beneficia de capacitate sporită de prelucrare și de stocare a datelor la nivelul dispozitivelor periferice sau a celor aflate la marginea rețelei (edge). Acestea tehnici permit luarea deciziilor și realizarea prelucrării datelor la nivel local, pot reduce dependența de transfer de date la nivel central, pot permite o reacție mai rapidă și o mai mare eficiență a sistemului, mai ales la nivelul terminalelor din zona resurselor fizice sau zona utilizatorilor finali.

- *Sisteme locale de reprezentare bazate pe realitate artificială și realitate virtuală*. Aceste tehnologii pot fi interfețe pentru utilizatori, mai imersive și mai interactive. Prin acestea se pot simula scenarii complexe, se pot vizualiza seturi de date variabile, precum și informații relevante, în moduri mult mai intuitive și atractive. Pot include și diverse dispozitive utilizate pentru proceduri de mentenanță sau de întreținere.

- *Blockchain*: tehnologia blockchain poate fi integrată în CPS pentru a asigura securitatea, autenticitatea și transparența datelor. Prin blockchain se poate înregistra, distribui și verifica o serie de evenimente și se pot transfera date, oferind astfel, un înalt nivel de încredere și de integralitate.

- *Interfețe de interoperabilitate cu sisteme externe*. Un CPS poate interacționa și colabora cu alte sisteme externe, infrastructuri digitale sau sisteme IoT care permit automatizarea și optimizarea proceselor, dezvoltarea de noi interfețe și protocoale de comunicare, interoperabilitate, tehnici avansate de control etc., toate în scopul îmbunătățirii eficienței și performanței operațiunilor, reducerii erorilor umane și maximalizării utilizării resurselor disponibile.

- *Interfețe pentru extragerea datelor pentru inovare* în scopul asigurării evoluției CPS. Inovarea și menținerea evoluției sistemului reprezintă un rol cheie în îmbunătățirea permanentă a lor. Aceasta pot implica dezvoltare de noi tehnologii, algoritmi și modele de optimizare, exploatarea de noi

aplicații și îmbunătățirea performanțelor și funcționalității sistemelor existente. Din acest punct de vedere informațiile din cadrul relațiilor feedback sunt extrem de importante și implică, în mod deosebit, rapoarte din partea utilizatorilor.

După cum se observă, intersecția dintre lumea digitală și mediul fizic este extrem de complexă, având potențialul de a transforma multe domenii dintre care amintim, transporturile, liniile tehnologice și producția, sănătatea, securitatea cibernetică, integrarea inteligenței artificiale, energiile regenerabile și multe altele. După cum se observă toate aceste procese depind esențial de decizii în timp real, fiind destinate utilizării de persoane fără cunoștințe tehnice avansate. De aceea, în dezvoltarea și în utilizarea CPS-urilor trebuie acordată o mare atenție responsabilității sociale și etice. Acestea includ asigurarea unui design etic, minimalizarea impactului asupra mediului și a societății, asigurarea egalității de acces și evitarea discriminării în exploatarea lor.

3.2. Bazele sistemelor ciber-fizice și rolul relațiilor feedback pentru dezvoltarea lor

Putem observa că CPS-urile sunt rezultatul integrării perfecte și sigure a unui sistem distribuit într-un spațiu, format din rețele de senzori, actuatoare, procesoare, sisteme de control și sisteme de feedback care interacționează între ele printr-o rețea de comunicații, în timp real, într-un mediu deopotrivă fizic și cibernetic, în folosul utilizatorilor umani.

Conceptul de CPS a dezvoltat conceptul de „sisteme informaționale" încorporate prin generalizarea și adaptarea cercetărilor științifice și a dezvoltările cibernetice aplicate, precum și din observarea modalităților de adaptare a dezvoltărilor paralele în domenii conexe precum: rețele de senzori, sisteme încorporate și sisteme de control în rețelele securizate.

1. Rețele de senzori

Senzorii conectează lumea fizică cu lumea cibernetică prin conversia realității fenomenelor lumii reale în semnale care pot fi procesate, stocate, vizualizate și acționate în lumea cibernetică. Prin urmare, rețelele de senzori pot fi integrate în multe dispozitive și utilizate în numeroase aplicații. În ultimul deceniu, progresele rapide în proiectarea de low-power, pe fondul ieftinirii senzorilor, au contribuit la apariția rețelelor distribuite de senzori (DSN).

DSN-urile sunt compuse din grupări de senzori, cu dispunere densă și funcționare nesupravegheată, cunoscute sub denumirea de „noduri”. Acestea au rolul de observare, comunicare (deseori prin mijloace wireless) și coordonare pentru a realiza în mod colectiv sarcini de inferență la nivel înalt. DSN-urile reprezintă un concept pentru schimbarea modului în care oamenii și mașinile monitorizează și interacționează cu mediul fizic și au găsit o gamă largă de aplicații, inclusiv supraveghere, siguranța, monitorizarea stării și automatizarea proceselor. De exemplu, DSN-urile pot fi angajate pentru a monitoriza și proteja infrastructuri civile, precum poduri și tuneluri, pentru colectarea informațiilor de sănătate structurală folosind senzori de vibrații, distribuiți spațial.

Natura distribuită și colaborativă a DSN-urilor introduce mai multe provocări și beneficii. Provocările cu care se confruntă dezvoltarea și adoptarea DSN-urile includ siguranța, securitatea, performanța în timp real și consumul de energie, precum și disponibilitatea, fiabilitatea și robustețea în medii dure. Beneficiile majore asociate cu DSN includ rentabilitate, flexibilitate, eficiență, autonomie, redundanță și natură distribuită.

DSN-urile pot fi considerate drept primul bloc în organizarea CPS-urilor care oferă un cost-eficient, o platformă flexibilă și fiabilă pentru monitorizarea și interacțiunea cu lumea fizică, în timp real.

2. Sisteme încorporate

În general, sistemele încorporate pot fi definite ca dispozitive care conțin componente fizice (mecanice și/sau electrice) și cibernetice (procesoare și software) conectate pentru a îndeplini o anumită sarcină. Majoritatea sistemelor încorporate operează în medii restrânse și interacționează cu lumea fizică, în timp real, ceea ce impune limitări ale resurselor disponibile, precum dimensiunea memoriei, puterea de procesare și puterea consumată.

Sistemele încorporate sunt prezente în aproape toate dispozitivele din jurul nostru, cum ar fi cele de uz caznic: cuptorul cu microunde, cuptor electric, frigider, mașină de spălat vase, imprimante, ceasuri inteligente etc. În CPS-urile industriale, sistemele încorporate distribuite îndeplinesc mai multe sarcini într-un mod coordonat și colaborativ, în timp real. Deși sistemele încorporate cuprind formule de calcul care reprezintă fundamentul unui CPS, nevoia de distribuție, de coordonare și de colaborare în timp real creează provocări specifice, așa cum este cerința de modelare asincronă a proeselor de calcul.

3. Sistemele de control

Implementarea rapidă a senzorilor, actuatoarelor, a rețelelor de comunicații distribuite, au produs apariția rețelelor sistemelor de control cu procesoare dedicate. Sistemele de control în rețea sunt sisteme centrale sau distribuite de control care urmăresc transferul de date dintre senzorii și actuatorii distribuiți, prin comunicare pe bază de rețea. În comparație cu sistemele tradiționale de control, sistemele de control a rețelelor oferă mai multe beneficii, inclusiv costuri reduse, flexibilitate îmbunătățită, fiabilitate și interoperabilitate. Cu toate acestea, incertitudinea în integritatea datelor primite de la senzorii distribuiți, care răspund comenzilor transmise de către actuatoare, poate produce o potențială indisponibilitate a rețelelor de comunicații, situație care introduce noi provocări în proiectarea sistemelor de control în rețea. De exemplu, indisponibilitatea semnalelor din bucla de feedback, din cauza pierderii canalului de comunicație poate provoca instabilitate pentru sistemele de control, cu consecințe drastice.

Eforturile de a aborda aceste provocări au dus la apariția stării de siguranță a sistemelor de control în rețea. Domeniul sistemelor de control în rețeaua securizată reprezintă baza proiectării sistemelor de control care pot supraviețui condițiilor în care sunt compromise disponibilitatea și integritatea datelor. Designul sistemelor de control, distribuite, sigure, robuste și tolerante la erori, formează fundamentul sistemelor de control în rețea, a căror siguranță este necesară pentru dezvoltarea CPS-urilor. În scopul înțelegerii unor funcții specifice și în scop de învățare propunem în figura 3.2 un model general de CPS și relațiile care se stabilesc în mediul informațional.

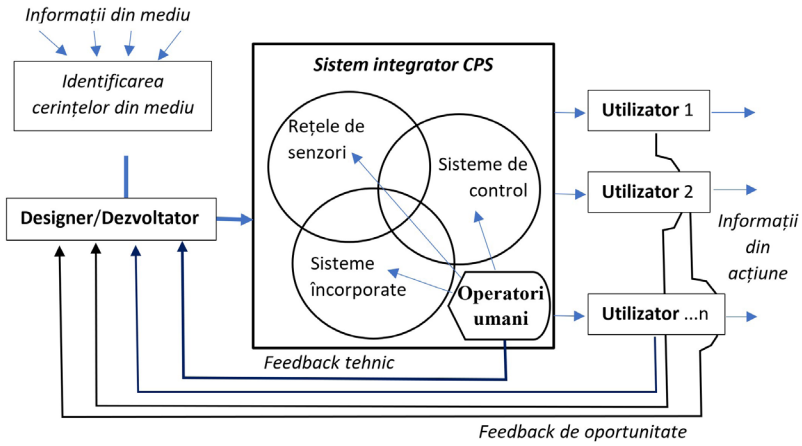

Figura 3.2. – Model general de CPS și relațiile sale de feedback

Provocările majore cu care se confruntă inovarea, dezvoltarea și adoptarea CPS-urilor pot să fie clasificate în provocări tehnologice, educaționale și juridice. De o importanță majoră pentru personalul uman care nu face parte din categoria specialiștilor și experților implicați în proiectarea și dezvoltarea unui CPS sunt înțelegerea rolului și a locului relațiilor de feedback.

Acestea pot fi:

1). Feedback tehnic

Provocările tehnologice provin parțial din caracteristicile distinctive ale CPS-urilor în comparație cu sistemele clasice. De exemplu, progresele tehnologice sunt necesare pentru dezvoltarea de sisteme distribuite, interoperabile, autonome și de securitate care pot proteja siguranța, confidențialitatea, fiabilitatea și securitatea cibernetică a CPS-urilor.

Dezvoltarea sistemelor interoperabile cu un anumit nivel de modularitate și compoziție, precum și a celor care pot combina și integra componente tradiționale, a fost inițiată în industrie, în urmă cu un deceniu. Din cauza timpului relativ scurt, se poate considera că stadiul de dezvoltare este încă de început, principalii factori care impun ample cercetări în domeniu fiind implementarea, testarea și validarea CPS-urilor. În prezent, funcțiile de siguranță și de fiabilitate sunt principalele bariere pentru sistemele autonome care pot fi implementate în diferite sectoare. Volumul imens de date care vor fi generate, stocate și prelucrate de CPS-uri, dezvoltarea diferitelor mecanisme de protejare a confidențialității datelor sunt provocări tehnologice, de origine economică și științifică, care ar trebui abordate în mod corespunzător. Nu în cele din urmă, securitatea cibernetică este cea mai importantă provocare tehnologică care trebuie abordată în timpul proiectării CPS-urilor, având în vedere rolul critic pe care îl joacă în siguranță societală. Este posibil ca o bună parte din beneficiile asociate utilizării CPS-urilor să nu să fie cuantificabile folosind modele clasice de afaceri, deoarece în multe cazuri ele doar contribuie la facilitarea proceselor sau la furnizarea de servicii și nu la obținerea unui produs. De aceea, concomitent cu dezvoltarea CPS-urilor trebuie dezvoltate și noi modele de afaceri și de instrumente de analiză cost/beneficiu pentru a justifica investiția în aceste sisteme. Mai mult decât atât, având în vedere transdisciplinaritatea naturii CPS-urilor, inovațiile în acest domeniu necesită contribuții științifice din zona

multor domenii. Prin urmare, ar trebui stabilită pentru modelarea, proiectarea și implementarea CPS-urilor o bază de cunoștințe, de mare amploare și cu profunzime adecvată, din destul de multe domenii.

În cele din urmă, aspectul socio-tehnic al CPS-urilor joacă un rol cheie pentru adoptarea lor în societate.

Un rol deosebit îl au operatorii și utilizatorii umani care prin relațiile de feedback specifice, pe care le numim relații de *feedback tehnic*, pot transmite către producători observații, sugestii, concluzii și propuneri tehnice rezultate pe timpul exploatării sistemelor încorporate și de control, precum și a rețelelor de senzori și a altor canale de legătură între componente. Acestea pot fi sub forma de informări și de rapoarte în care un individ să își exprime părerea despre mediul de lucru, despre utilitatea unor funcții reprezentate prin instrumentele de control, despre designul tehnologiei exploatate etc. Aceste opinii pot fi pozitive sau negative. Trebuie înțeles că această metodă trebuie aplicată în mod sistematic, fără a dezvolta frustrări și sentimente negative la locul de muncă, reprezentând un proces prin care atât operatorii individuali, echipele de lucru dar și utilizatorii participă activ la dezvoltarea CPS-ului și a relațiilor de muncă.

Pe baza rapoartelor lor se creează pachete de pach, up-date și upgrade, se modernizează și inovează componentele mecanice și electronice, se modifică unii parametrii de design etc. De regulă, operatorilor umani le sunt făcute precizările privind modurile de exploatare a dispozitivelor prin fișa postului și prin normele de exploatare a tehnologiei respective.

De o mare importanță este însușirea informațiilor din manualelor de utilizare, mulți utilizatori dar și angajați eludând această activitate din considerente absurde de tipul „învățăm lucrând”. Cunoașterea dobândită prin consultarea manualului de utilizare furnizat de producător conduce la evitarea multor deranjamente ușoare și evitarea uzurii premature a echipamentelor.

2). Feedback de oportunitate

Acceptăm sub denumirea de feedback de oportunitate acele relații de comunicare directe, care se stabilesc între utilizatorii și producătorii de CPS-uri. Acestea constau în comunicări despre modul de comportament a sistemului introdus

în exploatare, ca opinii evaluative, prescriptive și descriptive, despre diverse componente cu care utilizatorul intră în contact direct.

Feedbackul evaluativ este o formă subiectivă de evaluare a comportamentului unor componente sistemice, adesea putând deveni destul de personală. În situația în care evaluările sunt obiective și pozitive pot avea rezultate benefice în comparație cu cele negative, care pot crea presiune și pot sugera aspecte inexistente despre comportamentul sistemului.

Feedbackul prescriptiv este mai degrabă o opinie de cum ar trebui să se comporte sistemul sau o componentă a acestuia. Astfel de opinii sunt utile, de regulă, în fazele incipiente de proiectare, precum și în cele de modernizare/inovare, putând fi un mod de susținere a unor opinii constructive legate de activitatea subansamblurilor sistemice. Utilizatorii sunt mai degrabă interesați de efectele imediate ale acțiunilor și nu de așteptările bazate pe informații generale și ipoteze acționale.

Feedbackul descriptiv reprezintă informările care descriu efectele utilizării CPS-ului. Acesta rezultă din observările sistematice și pertinente ale comportamentului dispozitivelor pe timpul exploatării, în conformitate cu destinația lor. Acest tip de feedback este cel mai aproape de definiția exactă a termenului și poate oferi rezultate pozitive atunci când este folosit corect, putând reduce reacția defensivă a producătorului de sisteme CPS, dacă este destul de explicit.

În plus, feedbackul de oportunitate poate dezvolta și alte aspecte care nu țin de liniile tehnologice dar care sunt extrem de importante pentru adaptarea CPS-urilor la mediu. Aceste provocări sunt din mediile educațional și juridic.

Prezentăm unele aspecte pe care le considerăm relevante și specifice mediilor conexe de evoluție pentru un CPS:

- Provocări educaționale

În prezent, lesne poate fi constatată o insuficiență a forței de muncă calificată, a experților cunoscuți, a profesioniștilor și formatorilor/cadrelor didactice cu o înțelegere profundă a CPS-urilor. De aceea, se așteaptă ca această provocare să devină majoră în raport cu inovarea, dezvoltarea și implementarea CPS-urilor, cel puțin în următorul deceniu. Aceasta este posibilă, în principal, pentru că domeniul

CPS necesită integrarea cunoștințelor din mai multe domenii ale ingineriei, cum ar fi computing, inginerie informatică, inginerie socială, inginerie mecanică sau electronică, în sisteme echilibrate corect, între teorie și practică.

Cantitatea și profunzimea cunoștințelor necesare pentru inovarea și dezvoltarea CPS-urilor face ca educația în acest domeniu să fie o provocare. Prin urmare, ar trebui proiectate și implementate noi sisteme de educație/formare pe baza cerințelor CPS. Există unele programe de pregătire în domeniul CPS-urilor dar limitate la pregătirea universitară în ingineria științelor automatizării și calculatoarelor. În cadrul acestora, de regulă, se studiază discipline necesare formării specialiștilor implicați în conceperea, implementarea și operarea de astfel de sisteme, fără să țină cont de caracteristicile societale ale mediului în care acestea trebuie să acționeze. Pentru adaptarea și integrarea în mediu este nevoie de alți specialiști a căror denumire recunoscută în codul ocupațiilor încă nu există.

În plus, lipsa laboratoarelor ciber-fizice și a poligoanelor de testare în instituțiile de învățământ și de cercetare științifică constituie un alt obstacol care împiedică furnizarea educației/formării necesare în domeniul CPS. Persoanele din domeniul CPS au nevoie de acces la bancuri de testare cu diferite niveluri de complexitate și de integrare a componentelor fizice și cibernetice, astfel încât să poată dezvolta programare, scenarii de simulare și experimente relevante.

- Provocări juridice

Aplicarea CPS-urilor și reglementarea comportamentului societal, în diferite sectoare, necesită legislație diferită și norme specifice care să vizeze confidențialitatea datelor, siguranța și securitatea sistemelor și a utilizatorilor, asumarea răspunderii, precum și testarea/certificarea CPS-urilor pentru exploatare în masă. Mai mult decât atât, având în vedere că CPS-urile pot fi globalizate, cu componente în state diferite, în provincii, regiuni sau chiar continente, este necesară o nouă legislație internațională pe baza căreia să se creeze standarde și norme cu termeni care să privească răspunderea specifică cerințelor și exploatării uzuale a CPS-urilor.

Concluzii parțiale

Sistemele CPS se vor impune ca elemente critice ale proiectării sistemelor moderne de inginerie societală. Rădăcinile lor multidisciplinare stimulează

colaborările și cercetarea științifică interdisciplinară. Există numeroase inovații poziționate la intersecția domeniilor care, în mod tradițional, sunt caracterizate prin discipline izolate.

Ca atare, CPS-urile reprezintă o schimbare de paradigmă, un alt mod de gândire și de abordare a dezvoltării sistemelor. Pe măsură ce tehnologiile devin intrinsece funcționării societăților inteligente, va fi imperativă nu numai abordarea provocărilor tehnologice ci și pregătirea corespunzătoare a forței de muncă.

Principalele direcții pentru dezvoltarea CPS-urilor sunt securitatea, competitivitatea economică, nevoile societale și dependența de tehnologii. Costul tehnologiilor de detectare, de control, de procesare a datelor și de comunicații este în scădere în comparație cu ritmul de dezvoltare a lor. Totodată cresc posibilitățile de conectivitate între sisteme ceea ce determină creșterea vulnerabilității sistemelor. În plus, se estimează că numărul și tipul atacurilor și a intruziunilor va fi și acesta în creștere. Astfel, este de așteptat o creștere a cheltuielilor cu securitatea în toate domeniile. De aceea, se estimează că într-un mediu digitalizat securitatea va fi principala motivație pentru dezvoltarea și pentru adoptarea unor sisteme de încredere, rezistente sub aspect cibernetic, sigure și de încredere.

Nivelul tot mai ridicat a cererilor consumatorilor și nevoia de îmbunătățire a eficienței vor genera o forță economică competitivă pentru inovare, dezvoltare și adoptarea CPS-urilor în orice domeniu. Interoperabilitatea, modularitatea și funcționalitatea ridicată a CPS-urilor combinate cu progresele în zona de siguranță, securitate și fiabilitate și devin tot mai evidente. Spre exemplu, pentru reglementarea piețelor de energie electrică este necesară stabilirea unor niveluri ridicate de eficiență, competitivitatea devenind o puternică motivație pentru inovare și pentru dezvoltarea conceptului de rețea inteligentă. Creșterea competitivității întreprinderilor în combinație cu implementarea sporită a culegerii de informații și a procesării lor, eficientizarea costurilor utilizării tehnologiilor de comunicații, modelarea viitoarelor implementări și adoptarea sistemelor în toate sectoarele economice reprezintă, de asemenea, un stimulent major pentru promovarea inovației în CPS.

Efortul de îmbunătățire a calității vieții, crearea de standarde și proceduri adecvate se cumulează într-o forță motrice pentru inovarea și dezvoltarea CPS-

urilor. Acestea joacă un rol cheie în domeniile care implică interacțiunea umană, cu implicații atât societale, cât și tehnice. În plus, tehnologiile ciber-fizice sunt capabile să îndeplinească sarcini care sunt periculoase sau dificile pentru a fi executate de oameni.

Nevoia de fiabilitate îmbunătățită, costuri reduse de instalare, automatizarea, interacțiunea fără întreruperi de tip om-mașină și nivelurile ridicate de conectivitate și de acces de la distanță etc., pot reprezenta motivații puternice pentru inovarea și dezvoltarea CPS-urilor în industrie. Acestea vor oferi platforme avansate pentru sisteme flexibile, adaptive și autonome care sunt compatibile cu sisteme eterogene care conțin sisteme tradiționale, cu dispozitive vechi și utilizatorii umani fără pregătire tehnică.

Nu în ultimul rând, acestea reduc semnificativ accidentele cauzate de eroarea umană. Spre exemplu, se estimează că aplicarea CPS în sectoare precum transportul, sănătatea și mineritul va deveni tot mai facilă, pe măsură ce acestea devin tot mai accesibile. Astfel, transformarea sistemelor tradiționale, pur inginerești, electrice și/sau mecanice, care au implementate sisteme de senzori fizici pentru detectare, acționare, control și asistarea luării deciziilor etc., în sisteme fizice cu elemente cibernetice (sub formă de senzori, procesoare și software) a dus la apariția sistemelor încorporate care sunt concepute pentru a scop specific. Ulterior, necesitatea dezvoltării de rețele și multi-sisteme de monitorizare, de supraveghere și de control în diverse aplicații inclusiv pentru apărare, pentru sisteme energetice, pentru sisteme de transport, pentru asistență medicală etc., a condus la apariția rețelelor de senzori și de control securizat în a sistemelor din rețea.

CPS-urile îmbunătățesc proprietățile sistemelor de eficiență, flexibilitate, fiabilitate, autonomie și auto-reparare, oferind în același timp niveluri ridicate de cunoaștere a situației, de robustețe, de reziliență și de interoperabilitate. În plus, CPS-urile permit o mai bună coordonare, colaborarea și controlul sistemelor mari și complexe. CPS-urile oferă oportunități pentru niveluri mai înalte de conectivitate și de acces la distanță. În cele din urmă, CPS-urile oferă numeroase oportunități pentru o forță de muncă calificată pentru proiectarea, dezvoltarea și furnizarea de noi dispozitive, sisteme și servicii.

Bibliografie suplimentară

1. Walid M. Taha, Abd-Elhamid M. Taha, Johan Thunberg (2021), *Cyber-Physical Systems: A Model-Based Approach*, (eBook), Springer, Open Acces, https://link.springer.com/book/10.1007/978-3-030-36071-9 la data de 03.08.2023
2. Eleonor Bird, Jasmin Fox-Skelly, Nicola Jenner, Ruth Larbey, Emma Weitkamp, Alan Winfield (2020), *The ethics of artificial intelligene: Issues and initiatives*, European Parliment report, https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2020)634452 la data de 03.08.2023
3. Ioan Dumitrache (2013), *Cyber-Physical-Systems (CPS) – Factor determinant în economia bazată pe inovare și cunoaștere*, Revista Română de Informatică și Automatică, vol.23, nr.4, 2013, https://rria.ici.ro/wp-content/uploads/2013/12/art.5-dumitrache.pdf la data de 10.11.2023

TEMA 4: PRINCIPII DE PROIECTARE A UNUI SISTEM CPS

Deși nu este necesar ca un utilizator de CPS să cunoască principiile de proiectare a unui sistem, înțelegerea generală a acestora de către utilizatori poate fi utilă în următoarele situații:

1. *Alegerea CPS-ului potrivit*: În general, cunoașterea principiilor de proiectare poate ajuta utilizatorul să înțeleagă diferențele dintre sisteme similare și să facă o alegere informată, în funcție de nevoile și de așteptările sale. Un utilizator care are cunoștințe de bază despre modul de proiectare a unui CPS poate evalua caracteristicile acestuia și poate determina dacă acesta corespunde scopului pentru care dorește să-l achiziționeze sau/și să-l exploateze;

2. *Utilizarea eficientă a CPS-urilor*: Cunoașterea principiilor de proiectare poate ajuta un utilizator să folosească un CPS în mod eficient. Spre exemplu, cunoașterea performanțelor interfețelor terminalelor va determina utilizarea acestuia într-un mod mai intuitiv și eficient.

3. *Depanarea și mentenanță sistematică*: Înțelegerea principiilor de proiectarea poate fi utilă atunci când apar erori sau alte probleme minore pe timpul utilizării CPS-urilor. De regulă, defecțiunile minore sunt prezentate în manualele de utilizare, care pot sugera moduri adecvate de a le rezolva inidentele, până la efectuarea de solicitări de asistență specializată din parte serviciului tehnic.

4. *Comunicarea cu echipa de suport tehnic ori cu echipa de răspuns la incidente de securitate cibernetică (CSIRT)*: În situația apariției unor dificultăți sau a unor întrebări despre sistem, cunoașterea principiilor de proiectare poate facilita comunicarea cu echipa destinată pentru rezolvarea uui incident. Astfel, se pot exprima clar problemele întâmpinate și se pot iniția dialoguri colaborative eficiente pentru găsirea de soluții sau pentru pregătirea intervenției echipei specializate.

5. *Conștientizarea limitelor și a aspectelor de securitate*: Cunoașterea principiilor de proiectare poate ajuta un utilizator să înțeleagă care sunt

posibilitățile sau vulnerabilitățile unui CPS și, în funcție de acestea, să își protejeze datele și informațiile personale. Adoptarea unor măsuri de precauție adecvate va spori nivelul de securitate fizică și cibernetică astfel încât CPS-ul să fie utilizat în deplină siguranță.

Prin urmare, nu este necesară o pregătire profesională în domeniu însă, pentru un utilizator obișnuit, înțelegerea principiilor de proiectare a unui CPS este utilă pentru alegerea sa, pentru utilizarea eficientă și pentru comunicarea cu echipele specializate de intervenție tehnică pentru gestionarea problemelor apărute care țin, în special, de securitatea individuală.

4.1. Principiile generale ale proiectării sistemelor ciber-fizice

După cum am observat, un CPS cumulează o serie de elemente fizice, cibernetice și de control/luare a deciziilor.

- Elementele fizice dintr-un CPS se referă la componentele electrice și mecanice similare lumii fizice cu care CPS-urile interacționează în timp real. Elementele fizice urmează principiile științelor naturale care includ fizica, matematica (în special modelarea matematică), probabilitatea, statistica, logica, algebra și analiza liniară.

- Elementele cibernetice din CPS se referă la software, structuri de date, baze de date, rețele de comunicații, procesoare și alte dispozitive computerizate. Elementele cibernetice urmează principiile ingineriei informațiilor și ale informaticii, care includ programare software și hardware, setarea procesoarelor și a algoritmilor de calcul încorporați etc. Tot în cadrul elementelor cibernetice pot intra și comunicațiile având în vedere cibernetizarea rețelelor dintre componentele unui CPS.

- Elementele de control/luarea deciziilor se referă la elementele cibernetice și fizice care procesează și monitorizează datele primite de la senzori și de la sistemele de comandă/control aferente care efectuează diverse sarcini prin buclele de control și de feedback. Controlul și decizia se realizează prin elemente care urmăresc principiile teoriilor de management, de control adaptiv și robust, de control distribuit și de toleranță la erori, de stabilitate și optimizare, teoriile realizării sistemelor hibride, a sistemelor digitale și a sistemelor de alertă timpurie și de informare în timp real.

Prin urmare, CPS-urile funcționează printr-o justă comunicare între componentele cibernetice și fizice, prin elementele distribuite de detecție/senzori,

procesoare, dispozitive de control și de acționare, toate fiind relaționate în timp real, deopotrivă, cu mediul fizic și cu toți utilizatorii umani.

Proiectarea unui astfel de sistem trebuie să țină cont de o serie de principii care sunt justificate de următoarele caracteristici generale, distincte pentru CPS-uri, după cum urmează:

1. Modele și concepte de calcul avansat

CPS-urile se bazează pe rețele distribuite de senzori care oferă un număr variabil de intrări pentru informații. Aceste componente permit accesul, în timp real, a unui număr determinat de informații, stabilite prin cereri de date. În general, aceste informații sunt despre schimbarea stării mediului fizic și despre noile cerințe ale utilizatorilor umani, date despre controlul adaptiv și alte seturi de date standardizate, necesare pentru luarea deciziilor.

Un CPS are un număr variabil și de ieșiri, aferente numărului de utilizatori și de controlori.

Aceste caracteristici pot fi stabilite prin noi modele de procesare care pot fi diferențiate astfel:

- Pe baza modelelor de procesare cu număr adaptiv și variabil de intrări/ieșiri. De exemplu, atunci când se ia în considerare un număr de vehicule electrice a căror prezență la o stație de încărcare variază în timp, CPS-ul ar trebui să stabilească o negociere între mașini, dar și a acestora cu stația de încărcare. Aceasta din urmă va decide cum se încărcă/descărcă bateriile lor, în funcție de nevoile utilizatorilor și de disponibilitatea rețelei de surse de alimentare cu energie electrică. În acest scenariu, sistemul de încărcare a vehiculului electric primește semnale de intrare de la un număr diferit de sisteme de livrare și inclusiv din partea proprietarului (utilizator uman) al autovehiculului electric. În aceste condiții, CPS-ul trebuie să ia decizii corecte cu privire la încărcarea/descărcarea bateriei.

- Pe baza modelelor de procesare asincronă. Un scenariu specific acestui tip de modelare, poate fi cel prin care un set de autovehicule autonome ar trebui să-și schimbe viteza în funcție de starea traficului și de nevoile pasagerilor. Procesul de modelare pentru acest exemplu este în întregime în contrast cu modelele clasice de calcul, care sunt dezvoltate pe baza unui număr fix și cunoscut de intrări/ieșiri. În acest scenariu sunt necesare modele de calcul distribuit și colaborativ, coordonate în

mod sincron sau asincron. În modelele de calculul clasic, procesarea datelor se face secvențial. Pentru un astfel de CPS, numărul distribuit și variabil de variante de procesare stabilește calculul și comunică datele care pot determina coordonarea, în mod sincron sau asincron, a acțiunii, în funcție de aplicația respectivă. În modul sincron, procesarea este sincronizată prin comunicarea datelor în secvențe/pachete de date. CPS-ul procesează prin modelele asincrone, la viteze independente, schimbul de mesaje, în funcție de cerințe. În esență, așa ar putea fi rezolvată problema ambuteiajelor în intersecțiile marilor orașe.

În ambele exemple, pentru a se obține obiectivul dorit, sunt necesare modele autonome asincrone de calcul, aplicate fiecărui autovehicul, prin comunicare cu celelalte vehicule.

2. Matematică și modelare discretă și continuă

O diferență importantă între CPS-uri și sistemele cibernetice clasice este dată de faptul că pentru ambele tipuri se folosesc modele discrete, dar procesarea și modelarea continuă este necesară doar pentru CPS-uri. De regulă, astfel de sisteme sunt numite sisteme hibride. De exemplu, elementele cibernetice din CPS-uri sunt bazate pe modelarea matematică discretă a evenimentelor, în timp ce elementele fizice urmează modelarea continuă a evoluției în timp. Astfel, cunoașterea despre integrarea modelelor discrete și continue și a altor aspecte de modelare matematică reprezintă cerințe critice pentru proiectarea unui CPS. Aceste modele trebuie aplicate și sistemelor clasice.

Rețelele inteligente sunt principalele componente ale CPS-urilor prin care se stabilește comunicarea între componentele CPS și între două sau mai multe CPS-uri. Astfel, rețelele și sistemele de alimentare constituie elementele cibernetice și fizice care funcționează pe baza modelării discrete şi continue.

3. Calcul în timp real pentru lumea fizică

Acțiunea în timp real a CPS-urilor le diferențiază de clasa sistemelor convenționale. Într-un sistem care acționează în timp real, acuratețea și corectitudinea comportamentului acestuia depinde nu numai de corectitudinea și de acuratețea rezultatelor, ci și de momentul în care aceste rezultate sunt disponibile pentru a fi procesate. Ca atare, specific CPS-urilor sunt sistemele de operare, arhitecturile de calcul și limbajele de programare cu capacitatea de a răspunde solicitărilor pentru determinarea soluțiilor în timp real.

Este important de înțeles că toate aceste modele sofisticate trebuie dezvoltate pentru a performa capacitățile lor de predicție, în condițiile apariției întârzierile în timp, concomitent cu efectuarea controlului și cu elaborarea deciziilor în timp real. De exemplu, vehiculele autonome trebuie să recunoască limitele drumului, distanța față de diferite obiecte, să regleze viteza în funcție de acestea etc., în timp ce sunt estimate întârzierile de receptare și de procesare a datelor de la senzori, precum și timpul necesar pentru procesarea și comunicarea comenzilor către actuatori.

4. Interacțiunea cu lumea fizică

Interacțiunile CPS-urilor cu lumea fizică impune constrângeri complexe de proiectare pentru toate elementele lor. De exemplu, tipurile de senzori, de procesoare, de sisteme de control etc., vor determina tipul sistemelor, a rețelelor de comunicații și a actuatoarilor utilizate în conformitate cu caracteristicile lumii fizice, cu care interacționează CPS-ul. În plus, factori precum dimensiunea memoriei, puterea de procesare, consumul de energie, redundanța și toleranța la erori a elementelor, toate acestea pot deveni factori decisivi care conduc la apariția de eșecuri imprevizibile pe timpul funcționării sistemelor în mediul real. Această caracteristică evidențiază necesitatea realizării de verificări diverse în poligoane de testare, pentru a examina funcționarea unui CPS și respectarea cerințele de proiectare în raport cu particularitățile unui mediu sigur și controlat.

5. Aplicații critice pentru siguranță

Testarea, validarea și certificarea sistemelor și a dispozitivelor a căror defecțiuni nu produc consecințe grave sunt efectuate în mod normal în etapa finală, înainte de implementarea sistemului. Majoritatea CPS-urilor sunt sisteme critice pentru siguranță iar defectarea lor poate produce pierderi de vieți omenești, daune materiale semnificative sau daune asupra mediului. Astfel, siguranța, fiabilitatea și securitatea lor reprezintă un criteriu prioritar raportat la costul lor și la performanță.

Aplicațiile critice pentru siguranța funcționării CPS-urilor în sectoare precum asistența medicală, transportul și apărarea națională necesită noi genuri de testări, de validări și de proceduri de certificare pentru care sunt necesare poligoane de testare și bancuri de probe complexe, aflate încă din faza de proiectare. Este cunoscut faptul că verificarea CPS-urilor trebuie să fie permanentă, soluțiile propuse trebuind verificate până la etapa de implementare, inclusiv în etapele de proiectare, de asamblare și de livrare.

Prin urmare, CPS-urile sunt susținute de tehnologii transversale care demonstrează următoarele caracteristici ce pot fi considerate repere pentru estimarea prin comparare a performanțelor unui CPS. Acestea sunt stabilite în faza de proiectare și urmărite până la livrare formând setul de principii de proiectare.

- Abstractizare, modularitate și continuitate complexă;
- Standardizare și interoperabilitate;
- Adaptabilitate și previzibilitate;
- Asigurarea controlului ierarhic și securizat în rețea și în procesele de luare a deciziilor;
- Detecție distribuită, comunicații, control și acționare autonomă;
- Redundanță, rezistență și auto-reparare;
- Mecanisme noi de testare, validare și certificare;
- Autonomie și interacțiune umană;
- Securitate cibernetică;
- Resursă limitată.

Pentru membrii echipelor de testare și pentru operatori înțelegerea principiilor de proiectare a CPS-ului pe care îl exploatează este esențială din mai multe motive dintre care enumerăm:

- *Îmbunătățirea eficienței și performanței*. O bună înțelegere a principiilor de proiectare permite identificare și implementarea soluțiilor optime pentru sistemul respectiv. Astfel, se obțin performanțele așteptate, se pot evita probleme de performanță precum: timp de răspuns îndelungat și consum inutil de resurse;

- *Scalabilitate*. Proiectarea unui CPS scalabil este extrem de important pentru extinderea structurilor sau infrastructurii într-un mod eficient, care să poată gestiona un număr sporit de date și de cereri;

- *Flexibilitate și modularitate*. Astfel pot fi create sisteme care pot fi adaptate ușor la schimbări de cerințe sau tehnologii. O abordare

modulară permite dezvoltarea și întreținerea mai ușoară a sistemului, precum și reutilizarea componentelor în alte proiecte;

- *Fiabilitate și gestionare a erorilor*. Principiile de proiectare includ și modalități de a face sistemul mai fiabil și de a gestiona erorile în mod eficient. Înțelegerea acestor principii permit dezvoltatorilor să proiecteze sisteme rezistente la erori și să implementeze mecanisme de recuperare în cazul în care apar probleme;

- *Securitate*. Buna înțelegere a principiilor de proiectare permite implementarea unor măsuri de securitate adecvate în sistem. Acestea pot include autentificare, autorizare, criptare și alte practici de securitate pentru protejarea datelor și pentru prevenirea accesului neautorizat;

- *Îmbunătățirea colaborării și comunicării*. Înțelegerea principiilor de proiectare permite o comunicare eficientă și o mai bună colaborare între membrii echipei de dezvoltare. Folosirea unui set comun de principii și o terminologie adecvată facilitează înțelegerea și discuțiile cu privire la decizii de proiectare, de arhitectură, de realizare a pachetelor de pach și de up-date etc.

4.2. Aspecte generale privind conținutul feedback-ului de oportunitate

În mod similar inițierii unui dialog cu producătorii unui sistem în vederea actualizării și/sau modernizării acestuia, utilizatorii trebuie ca să țină cont de următoarele considerații:

1. *Să consulte site-ului oficial al producătorului*: Verificarea site-ului oficial al companiei producătoare a CPS-ului respectiv sau al produsului în care CPS-ul este implementat reprezintă o obligație în situația în care se dorește inițierea unui dialog cu aceasta. Acolo vor fi găsite informații despre performanțele produsului, despre actualizările disponibile și instrucțiuni despre cum să fie utilizat sau achiziționat produsul;

2. *Să urmărească notificările comunicate de furnizor*: În situația achiziționării sau exploatării unui CPS prin intermediul unui furnizor sau partener autorizat, trebuie urmărite notificările și alte comunicări primite de la aceștia. Astfel, utilizatorii pot fi informați cu privire la

actualizările disponibile. În plus, utilizatorii vor găsi informații despre modul de asigurare a asistenței tehnice;

3. *Să se înscrie în comunități și forumuri online*: Verificarea forumurilor online sau a comunităților de utilizatori este utilă prin faptul că mulți dintre participanți pot împărtăși informații despre performanțe, despre utilizarea, despre actualizări disponibile și despre modul de obținere a acestora. În aceste canale mai pot fi găsite și tutoriale sau ghiduri care pot ajuta la efectuarea unor verificări, update-uri și depanări minore.

4. *Să consulte documentația și manualele de utilizare*: Este necesară revizuirea documentației și a manualelor de utilizare furnizate împreună cu dispozitivul achiziționat. Acestea vor conține informații utile pentru utilizatori în vederea exploatării și întreținerii corecte, informații despre actualizări și despre procesele de actualizare etc.

5. *Să apeleze la serviciile autorizate de consultanță tehnică*: În cazul în care nu sunt găsite informațiile necesare sau sunt întâmpinate dificultăți în procesul de utilizare a CPS-ului, este recomandată contactarea unei asistențe autorizate. Echipele tehnice pot ghida utilizatorul respectiv în procesul de depanare sau pot asigura intervenția de urgență în situația în care securitatea utilizatorului este pusă în pericol. De asemenea, pentru evitarea pierderii unor date importante este recomandată efectuarea unor copii pentru backup-ul acestora în situația atacurilor cibernetice sau a altor defecțiuni.

Este important ca fiecare utilizator să urmeze instrucțiunile și recomandările producătorului sau furnizorului de CPS, pentru a asigura un proces corect și sigur de exploatare. De aceea, este necesar ca, anterior elaborării de notificări către producători, să fie revizuite modalitățile de îndeplinire a următoarelor activități cheie:

1. *Revederea setărilor produsului*. În majoritatea cazurilor, CPS-urile au opțiunea de actualizare automată sau o secțiune în setările sale care să permită verificare și instalare de noi produse software și hardware. Accesați meniul sau panoul de control al utilizatorului și căutați opțiuni legate de actualizări sau noile versiuni software.

2. *Înregistrarea produsului*. Dacă CPS-ul sau o componentă a acestuia necesită înregistrare prin crearea unui cont online sau prin altă formă, este necesară înregistrarea produsului. Astfel, se vor obține toate informațiile necesare pentru actualizări software și pentru modernizări/ upgrade hardware. De multe ori producătorii oferă actualizări exclusive pentru utilizatorii înregistrați.

3. *Păstrarea materialelor de instruire și alte resurse de informare* (în format fizic sau online). Unii producători oferă materiale de instruire, tutoriale și explicații care descriu procesul de actualizare a CPS-urilor. Pentru aceasta, poate fi consultat site-ul oficial, canalele social media sau platformele de streaming video ale producătorului pentru a găsi resursele necesare.

4. *Verificarea compatibilității versiunilor update cu componentele deținute*: Înainte de a descărca o variantă update este necesară verificarea compatibilității cu versiunea actuală software a componentei CPS deținute. Este necesar totodată ca actualizarea să fie destinată modelului și versiunii deținute și că îndeplinește toate cerințele de sistem.

5. *Urmărirea evoluțiilor tehnologice*: A fi în contact cu noutățile din domeniu CPS-urilor este extrem de important. Producătorii pot lansa actualizări periodice pentru a adăuga funcții noi, pentru a rezolva probleme sau pentru a îmbunătăți performanța. Prin urmărirea acestor evoluții, pot fi adăugate cele mai recente versiuni software.

În general, procesele de actualizare a CPS-urilor pot diferi în funcție de producătorul componentelor utilizate. De aceea, este important de consultat cu atenție instrucțiunile de funcționare și ghidurile specifice furnizate de producător pentru a beneficia de performanțele sistemului.

Din punct al mentenanței preventive, un utilizator ar trebui să urmărească următoarele recomandări:

- *Verificarea actualizărilor de securitate*. Este necesară verificarea actualizărilor de securitate disponibile pentru a proteja sistemul împotriva amenințărilor cibernetice și neutralizarea vulnerabilităților identificate;

- *Realizarea unui backup complet*: înainte de implementarea unei modernizări de sistem sau a unui update se recomandă un backup complet al datelor și configurațiilor importante. Astfel, în situația în care nu funcționează ceva după actualizare se poate reveni la o versiune anterioară și pot fi restaurate datele conținute;

- *Testarea actualizărilor într-un mediu de testare*: se recomandă, efectuarea testării noilor pachete software și hardware într-un mediu separat, înainte de implementarea în sistemul principal. Aceasta oferă oportunități de verificare compatibilităților, de identificare a problemelor, de identificare a conflictelor etc., înainte de a afecta operațiunile și funcționarea întregului sistem;

- *Evaluarea cerințelor hardware*. *Verificarea* cerințelor de sistem a noilor versiuni hardware poate evita obligația de achiziții suplimentare software și hardware pentru a putea utiliza componenta achiziționată inițial;

- *Verificarea conectivității la o rețea stabilă*. Atât pe timpul funcționării dar, mai ales, în momentele actualizărilor este foarte important ca să existe o conexiune normală. O conexiune slabă sau cu întreruperi poate duce la apariția de probleme în procesul de implementare și de actualizare a sistemului;

- *Verificarea compatibilității cu aplicații și servicii terțe*: Pentru că un CPS se bazează pe interacțiunea în rețea, o serie de aplicații și servicii deservesc mai multe componente. De aceea verificare compatibilității terților este extrem de importantă. Pentru aceasta se recomandă contactarea producătorilor sau furnizorilor de servicii pentru a obține informații despre compatibilitate lor cu versiunile actualizate ale componentelor CPS;

- *Monitorizarea performanței și a stabilității sistemului după actualizare*: Această activitate va evita apariția erorilor sau a problemelor neprevăzute. Informarea producătorilor sau furnizorului componentei respective va oferi asistență tehnică suplimentară;

- *Asigurarea unor resurse suplimentare*: existența unor resurse suplimentare, cum ar fi spațiul de stocare, baterii încărcate, timp suficient pentru finalizarea proceselor fără întreruperi etc., duce la evitarea apariției de probleme suplimentare;

- *Respectarea politicilor de securitate ale organizației*: dacă un CPS are componente care sunt utilizate de mai multe organizații trebuie să respecte politicile și procedurile de securitate ale organizației respective. Pentru aceasta trebuie luată legătura cu echipele specializate de deservire a acestora din cadrul organizațiilor și obținerea aprobărilor de intervenție sau de asistență în procesul de actualizare ori de mentenanță a CPS-urilor

În urma acceptării și respectărilor cerințelor și recomandărilor producătorilor pentru beneficiari, utilizatorii pot iniția discuții pentru informarea producătorilor stabilindu-se rețele de colaborare. O astfel de rețea, pentru a deveni puternică necesită timp și efort din ambele părți. Pentru aceasta comunicarea trebuie să se bazeze pe unele reguli dintre care enumerăm:

- Efectuarea de către utilizatori a unei cercetări prealabile. Informarea despre compania producătoare de CPS, identificarea persoanelor și a punctelor de contact, va ajuta la formularea de întrebări pertinente și la primirea unor răspunsuri care vor ajuta dialogul la înțelegerea corecte a problemelor semnalate;

- Explicarea în mod clar a obiectului dialogului Atunci când este contactat producătorul CPS, prezentarea persoanei care sesizează problema trebuie să fie clară și concisă. De regulă, în această fază a dialogului se menționează numele persoanei, compania sau instituția reprezentată (dacă este cazul), motivul pentru care se dorește dialogul, prezentarea succintă și clară a motivului dialogului sau a întrebărilor formulate în legătură cu CPS. Dacă este nevoie de informații suplimentare, suport tehnic sau aveți întrebări specifice se explică în mod clar aceste cerințe;

- Respectarea canalului de comunicare preferat de producător. Unele companii preferă să fie contactate numai prin e-mail ori prin telefon. Se recomandă respectarea metodei de comunicare preferată de companie unde trebuie manifestată politețe și răbdare în comunicare. Datorită multitudinii de solicitări, pot exista întârzieri până la primirea răspunsului. Totodată este necesar a identifica ce alte informații sau documente suplimentare sunt necesare pentru rezolvarea problemei;

- Menținerea contactului. În cazul în care răspunsul primit nu se încadrează într-un interval rezonabil de timp se poate trimite un mesaj pentru a verifica stadiul solicitării. Menținerea contactului cu producătorul se face și prin acordare de răspunsuri la solicitările suplimentare din parte lui.

- Personalizarea mesajului într-un mod clar clar și concis. Personalizarea mesajului prin includere a exemplelor specifice sau a situațiilor relevante o cunoaștere a specificului activității producătorului și a dispozitivului CPS. Stilul clar și concis al comunicării duce la evitarea ambiguităților sau a terminologiei tehnice excesive;

- Respectarea politicii de confidențialitate. Dacă se discută sau se solicită informații confidențiale sau documentație protejată, este necesară respectarea politicii de confidențialitate a companiei, fie chiar și prin semnarea unui acord de confidențialitate;

- Demonstrarea cunoștințelor tehnice: Dacă sunteți familiarizat cu terminologia și conceptele specifice CPS arătați acest lucru în comunicarea dumneavoastră. Demonstrarea experienței poate crea un sentiment de încredere și poate facilita dialogul cu producătorul CPS;

- Pregătirea întrebărilor. Înaintea inițierii dialogului este necesară pregătirea unei liste de întrebări pe care doriți să le adresați producătorului CPS. Aceasta ajută la obținerea informațiilor necesare și la asigurarea că nu se ratează niciun aspect important în timpul conversației;

- Urmărirea feedbackului și rezultatele dialogului. După inițierea unei discuții, urmăriți feedbackul și rezultatele obținute. După primirea informațiilor solicitate sau dacă ați avut o întâlnire ori o prezentare se recomandă evaluarea rezultatelor și pentru a decide continuarea sau nu a colaborării cu producătorul CPS.

Bibliografie suplimentară

1. Cha, H.J., Yang, H.K., Song, Y.J. (2022), *A Study on Vehicle Monitoring Service Using Attribute-Based Security Scheme in Cyber-Physical Systems*, Special Issue Security Research and Challenge in Cyber-Physical Systens, Appl.Sci. 2022, 12(9), 4300; https://doi.org/10.3390/app12094300, https://www.mdpi.com/2076-3417/12/9/4300 la data 06.07.2023
2. Enisa, *ENISA good practices for security of Smart Cars*, la adresa https://www.enisa.europa.eu/publications/smart-cars la data 06.07.2023
3. Mlot, S. (2016), *BMW Teases the Ultimate Smart Car*, la adresa https://www.pcmag.com/news/bmw-teases-the-ultimate-smart-car la data de 06.07.2023

TEMA 5: COMUNICAREA ȘI REȚELE DE COMUNICAȚII ÎN CPS

Obiectivul principal al acestei teme constă în înțelegerea diferențelor de abordare a conceptului de informație atât ca element al comunicării cât și ca mediu care asigură suportul funcționării fluxurilor de informații. În CPS-uri, așa cum am văzut până acum, informația este folosită permanent. Fără această funcția de transfer al informațiilor nu există conceptul de rețea.

Utilizatorii trebuie să se facă distincție între comunicarea umană unde este vorba de informații în sensul de bază a comunicării umane și mediu de comunicare, suport al organizării rețelelor de comunicații CPS, intra și inter sistemice.

5.1 Bazele teoretice ale sistemelor bazate pe informații

În general, informația reprezintă conținutul abstractizării unui fenomen. Aceasta însumează și generalizează percepțiile și interpretările observațiilor, indiferent de înțeles. Tot ce se întâmplă în jurul nostru, fenomenele, faptele și evenimentele observabile generează constant informații. O dată ce un senzor devine interesat de o informație, începe procesul de interpretare a lor.

Sub acest aspect, conceptul de informație raționalizează o funcție extrem de importantă a existenței umane. De altfel, nu numai oamenii comunică între ei. Știința a demonstrat că toate ființele comunică cu semenii lor. Însă doar oamenii au reușit, ca prin dezvoltarea limbajului, să stabilească o serie de reguli și de simboluri prin care să-și comunice ideile. O comunicare cuprinde cuvinte ordonate după anumite reguli. Cuvintele sunt simboluri unanim acceptate. Prin cuvinte oamenii asimilează observații despre mediul înconjurător, în principal, obținute prin propriul sistem senzorial, precum și furnizate de alți oameni.

Cuvintele pot fi depozitate în vederea analizelor ulterioare, în biblioteci fizice sau digitale, sau să pot fi comunicate semenilor lor, prin viu grai sau prin diverse sisteme care le permit transmiterea informațiilor la distanțe ce depășesc nivelul de percepție a urechii umane, în cazul vorbirii directe.

În sens larg, sensul originar al noțiunii de informație este de noutate sau de anunț și constituie un transfer de semnificații. În mod practic, informația reprezintă o stare atribuită unui moment pentru transmiterea unei structuri informale organizată după reguli acceptate, precum și pentru transmiterea unei funcții ori acțiuni care

caracterizează un eveniment, un obiect, un fenomen sau o altă persoană. Informația exprimă o relație între laturi, dimensiuni, evenimente și obiecte.

În funcție de conținut, noțiunea de informație urmează două direcții de abordare:

1. informație = simboluri, date, observații, instrucțiuni în oricare mediu sau formă;

2. informație = înțeles care se atribuie activităților dinamice, format din date prin care se realizează o cunoaștere convențională a unei situații.

Clasificat după conținut, conceptul de informație prezintă două aspecte distincte:

A) Formă de exprimare a judecăților

Așa cum este acceptat în majoritatea teoriilor, informațiile formează baza proceselor de judecată. În urma procesării lor, rezultatele exprimate sunt tot informații care sunt comunicate celor interesați. Cu cât informațiile sunt mai evaluate și alocate unor reprezentări ele devin cunoștințe. Cunoștințele reprezintă stadiul superior al înțelegerii și se realizează prin judecăți și algoritmi de procesare. O dată cu implementarea și dezvoltare tehnologiilor digitale putem vorbi de o procesare a informațiilor mult mai rapidă, fiind specifică tehnologiilor AI și ML. În esență, aceste procese automatizate nu diferă de mecanismele de procesare a creierului uman.

Însă, oricât de performată este procesarea digitalizată a informațiilor, sistemul deține cel puțin o limită determinată de capacitatea de procesare a lor. Aceste limitele ale algoritmilor de procesare și ale altor mecanisme de comunicare a lor care nu pot atinge performanțele creierului uman. Numai omul poate realiza o analiză algoritmică a cuvintelor polisemantice și să elaboreze judecăți de valoare bazate pe emoții. Un sistem automatizat formulează soluții optime, limitate de cerințele de proiectare a acestuia, oricât ar fi de diverse, multiple și complexe. Chiar și sistemele bazate pe AI și ML au limite. În schimb, omul poate, uneori fără nici o regulă logică, să găsească o soluție și să o aplice, aparent, fără nici un sens. Unele dintre soluțiile elaborate în acest fel pot fi extrem de utile. Altele pot genera situații catastrofale. Acțiunea determinată de soluțiile extreme vor surprinde sistemele cu care sunt stabilite relații informale, obligându-le să-și reconfigureze evoluția în funcție de noile informații. De altfel, oricare conflict, de orice fel și de orice natură,

se bazează pe această particularitate. Din această cauză liderul uman nu va putea fi niciodată înlocuit.

Pe de altă parte, având în vedere viteza uluitor de mare de procesare a informațiilor de către un sistem automatizat, acesta se poate substitui oricărei componente cu rol de execuție a unei activități. Roboții pot înlocui oricare activitate umană care presupune o acțiune sistematică și repetată până la realizarea scopului urmărit. Aceștia sunt dependenți de traducerea informațiilor din mediu în limbajul mașinii. De altfel, sistemele AI și ML asigură performanța sistemelor prin introducerea de informații dinspre oameni. Procesarea volumului imens de informații și punerea la dispoziție a soluțiilor obținute, prin compararea scenariilor cunoscute, le permit sistemelor bazate pe AI să identifice cea mai bună variantă de rezolvare a unei probleme, adică atingerea celui mai bun randament.

Deci, dacă sunt introduse informații există rezolvare. De aceea, aceste tehnologii au apărut și s-au dezvoltat numai în urma globalizării informațiilor și implementarea masivă a rețelelor globale, de tipul Internet.

Totodată, informațiile sunt necesare și pentru îmbunătățirea performanțelor fizice și cibernetice a roboților sau pentru avertizarea privind modificările de mediu care, anterior, erau caracteristice doar sistemelor senzoriale ale ființelor. Această abordare conceptuală demonstrează existența informațiilor și faptul că nu cantitatea este importantă ci calitatea lor. Efectul produs de ele reprezintă esența controlului utilității lor. În plus, calitatea informațiilor este determinată de performanța senzorilor și a procesoarelor, pentru neutralizare redundanței și a incertitudinii. Aceștia trebuie să fie fiabili, flexibili, mobili și cu mare capacitate de trafic al informațiilor. Un senzor poate fi influențat fie prin informații puține și de calitate fie prin informații multe dar confuze și contradictorii.

De reținut este că, în această abordare, nu putem vorbi de o unitate de măsură a informațiilor ci de tehnologii de determinare a efectelor produse de informații.

B) Mediu - suport pentru realizarea fluxurilor informaționale

Această direcție de abordare se bazează pe o abordare sistemică care asigură optimizarea fluxurilor informaționale. Un flux informațional este necesar transmiterii informațiilor și este dependent de capacitățile de stocare și de transfer care pot fi analizate numai în relații clar definite. Mediile de stocare pot fi cele tradiționale precum înscrisuri, cărți, biblioteci etc., sau digitalizate precum memorii

ale procesoarelor, interne și externe, fișiere în diverși algoritmi ale componentelor automatizate și a rețelelor de date etc.

Pentru a înțelege mai bine această teorie, analizăm structura unei biblioteci cu cărți. Aceasta este acceptată și recunoscută ca bibliotecă pentru că știm că deține un număr imens de informații, stocate în scrierile din filele cărților. Dacă sunt extrase toate cărțile din rafturi va rămâne un mobilier și o sală cu pereți, organizată în conformitate cu structura clădirii respective. În situația bibliotecilor de informații digitale, înscrisurile din cărțile tradiționale se transformă în informații stocate digital. Dacă informațiile din aceste medii sunt alterate, șterse sau înlocuite cu informații nefolositoare rezultatul este, similar modelului tradițional de soatre a cărților din bibliotecă, adică, blocarea dezvoltării cunoașterii.

Prin urmare, rolul sistemelor de comunicații, a normelor de comunicare și a securității mediilor de stocare a informațiilor sunt extrem de importante, valoarea lor crescând o dată cu posibilitatea păstrării nealterate a informațiilor. Pe baza acestei abordări, informațiile pot fi măsurate prin cantitatea volumului de stocare sau prin determinarea vitezei de transfer dintr-un canal, cu aceeași parametrii determinați pentru toată lungimea fluxului de transfer. Un canal de transfer poate fi un fir de cupru sau de fibră optică, un ghid de undă pentru orice sistem de antene prin care se poate stabili o legătură directivă de comunicații. În esență, condiția de bază este ca aceeași parametri ai canalului de transfer a informaților, să rămână constanți de la intrarea în flux până la ieșire. Imaginați-vă o țeavă prin care curge un volum de apă. Dimensiunile secțiunii țevii la intrarea apei și pe tot traseul sunt aceiași cu cei de la ieșirea apei din țeavă. Astfel pot fi determinați parametri precum viteza de transfer, volmul de apă transferată, ritmul etc.

În mod similar, și în cadrul fluxurilor informaționale se impun condiții pentru stabilirea parametrilor de transfer a informațiilor. În acest caz, unitate de măsură a informațiilor este bit-ul.

CPS-urile sunt realizate, în mare parte, pentru a procesa și transfera informații. O mare problemă este dată de cantitatea de informații necesare și de calitatea componentelor de transmisie a acesteia. Este foarte simplu ca un utilizator să înțeleagă că acestea lucrează cu sisteme și baze mari de date, și, probabil, este indicat să nu caute să înțeleagă mecanismele de prelucrare a lor. Însă trebuie să rețină că regulile stabilite de producător trebuie respectate întocmai cum au fost ele proiectate și că oricare altă îmbunătățire, pe care ar crede că o poate aduce sistemului, trebuie comunicată producătorului și, ulterior, aplicată. Altfel, vor spori pierderile

materiale și cibernetice care vor determina, în mod inevitabil, uzura prematură a sistemului. Contează chiar și atitudinea utilizatorului. Vedetismul, informarea insuficientă a utilizatorului sau suprasolicitarea emoțională (stresul) operatorilor, vor constitui factori perturbatori a calității proceselor decizionale, chiar și a celor bazate pe inteligență artificială, prin stricarea rapoartelor de disonanță sau de consonanță dintre fenomene și senzori.

Oricare CPS poate reacționa rapid atunci când funcționează autonom dar decizia finală este tot a utilizatorului. Acesta poate corecta evoluția unei componente CPS, iar în condiții extreme îi poate opri funcționarea. În aceste condiții, toate celelalte componente își vor regla funcționarea în raport cu evoluția dispozitivului controlat. Oricare situație de pericol de producere a unor evenimente majore a căror efecte sunt fie de pierderi materiale fie de afectare a vieții umane pot fi evitate prin controlul uman. De aceea, comunicarea și securitatea rețelelor de comunicații sunt și vor fi principalele repere care susțin calitatea și utilitatea CPS-urilor.

5.2. Mediul informațional specific pentru un CPS

Înțelegând rolul și locul comunicării în cadrul conceptului CPS și a securității sistemelor de transfer a informațiilor prezentăm unele aspecte generale ale proceselor de transfer al informațiilor într-un CPS, din punct de vedere al utilizatorului.

Așa cum am precizat anterior, comunicarea în CPS reprezintă modalitatea prin care se face cunoscută o anumită informație. O comunicare poate fi realizată în scop de dezvoltare a cercetării științifice, în folosul dezvoltării componentelor CPS, pentru vânzări și marketing, pentru publicitate etc. Componentele de comunicații reprezintă sistemele tehnologice prin care se realizează trimiterea, interpretarea și prelucrarea datelor și a informațiilor de către utilizatorii umani sau de căter dispozitivele cibernetice. În cadrul sistemelor de comunicații avem fluxuri informaționale iar transferul informațiilor este dependent de capacitățile canalelor de comunicații.

Comunicarea nu trebuie confundată cu comunicațiile. Comunicarea este un proces dinamic, aflat într-o continuă schimbare, care implică participarea tuturor membri a unei societăți umane organizată în jurul unui scop. Pot exista mai multe tipuri de societăți umane care se evidențiază și se separă prin adoptarea unui cod propriu al comunicării, adesea denumit jargon. Varietatea jargoanelor este imensă fiind utilizate în diferite domenii și subculturi, precum limbajul medical, juridic, tehnic etc. Chiar și structurile de crimă organizată au propriul jargon.

Jargonul este important de cunoscut de către cei care doresc să se familiarizeze cu domeniul și subcultura respectivă.

Pentru CPS, fiind un domeniu relativ nou, se va forma un jargon prin adoptarea unor semnificații apropiate terminologiei digitale.

Pentru CPS-uri, enumerăm câteva dintre cele mai apropiate tipuri de jargoane:

- *Jargonul tehnic*: se utilizează în informatică, inginerie, medicină, marină, aviație etc. Acestea includ termeni specializați și acronime specifice pe care le înțeleg doar experții în domeniu. De exemplu: buffer, firewall, hiperplazie, AFCS (sistem automat de control al zborului) etc.

- *Jargonul internetului și al tehnologiei informației*: este utilizat în mediul online, în legătură cu tehnologia digitală. Acesta include termeni și expresii specifice legate de rețele sociale, platforme online și despre tehnologia digitală. Spre exemplu: hastag, metaverse, viral, machine learning, e-learning etc.

- *Jargonul financiar*: se utilizează în lumea afacerilor, în piețele financiare sau în instituțiile bancare și include termeni legați de tranzacții, investiții și indicatori economici. Unele exemple sunt: divident, dobândă compusă, bursă de valori, PIB etc.

Strict pentru sistemele ciber-fizice (CPS) există mulți termeni specifici utilizați pentru a descrie aspectele tehnice și conceptele cheie, după cum am văzut deja. Suntem convinși că, acest domeniu, pe măsură ce va fi aprofundat, comunicarea specifică va însuși o mulțime de termeni care pot fi considerați elemente de jargon specific CPS. Dintre cei mai utilizați până acum sunt:

- Real-time computing (Procesare în timp real) – se referă la procesare și răspunsul la evenimente în timp real, într-un interval de timp specificat și limitat;

- Embedded systems (Sisteme încorporate) – se referă la sisteme hardware și software integrate în dispozitivele fizice sau în alte produse precum: automobile, electrocasnice, dispozitive medicale etc.;

- Sensor fusion (Fuziunea senzorilor) – se referă la combinarea datelor provenite de la mai mulți senzori diferiți pentru a obține o imagine de ansamblu, mult mai completă și precisă a mediului înconjurător;

- Cybersecurity (Securitate cibernetică) – se referă la protejarea componentelor împotriva amenințărilor și atacurilor cibernetice pentru menținerea confidențialității, integrității și disponibilității datelor;

- Control systems (Sisteme de control) – se referă la tehnicile și algoritmii utilizați pentru a controla și monitoriza comportamentul sistemelor CPS asigurându-se că acestea funcționează în parametrii specificați de producător;

- Internet of Things (Internetul lucrurilor) – se referă la rețeaua globală de dispozitive conectate care interacționează și comunică între ele prin intermediul internetului, inclusiv în cadrul rețelelor CPS;

- Model-based design (Proiectare bazată pe modele) – se referă la utilizarea modelelor matematice, simulate, pentru a proiecta și dezvolta CPS-uri, permițând testarea și optimizarea acestora înainte de implementare.

- Este evident că lista cu termeni specifici CPS este mult mai lungă. Pentru cei interesați, aceasta se va completa cu temeni rezultați din materiale consultate, din manuale cu instrucțiuni și din diverse prezentări de produse.

Odată cu ritmul sporit de implementare a CPS-urilor în cotidian și prin evoluția comunicării interumană în domeniul CPS, jargonul CPS va evalua luând forme de comunicare în masă, cu aportul comunicării mediatizate.

În figura 5.1. prezentăm un model ipotetic de comunicare bazat pe rețea și integrarea modelului CPS în mediul ambiant.

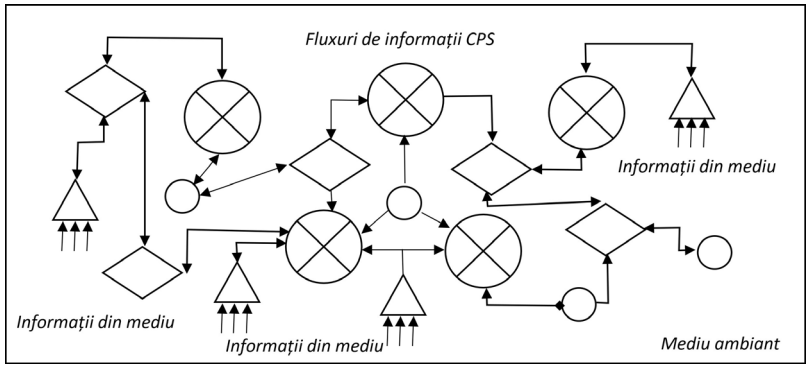

Figura 5.1 – Rețele ipotetice pentru CPS și integrarea acestuia în mediul ambiant

Fără ca această afirmație să fie considerată un postulat în CPS suntem convinși că o dată cu creșterea numărului de utilizatori de CPS-uri va îmbogăți comunicare specifică. De remarcat este faptul că, urmând principiile științei comunicării, cea specifică CPS poate avea o formă subiectivă (pentru manipularea opiniei publice) și o formă obiectivă (pentru informarea persoanelor interesate).

Existând interes, și sistemele de transfer a informațiilor vor cunoaște o evoluție rapidă. Ne referim, în mod deosebit, la rețelele sociale pe platforme digitale. De aceea, verificare permanentă a conținutului terminologiei utilizate și înțelegerea corectă a conținutului acesteia reprezintă cerințe ale comunicării a căror responsabilitate revine celui interesat. Acceptare unor termeni fără fond doar pentru că unii utilizatori îi folosesc pentru a descrie aspecte care pot fi asimilate altor sisteme, nu va ușura procesul comunicării de specialitate dintre utilizatori și producători.

Enumerăm o serie de tipuri de rețele și destinațiile lor, pe care le considerăm ca fiind cele mai reprezentative pentru un CPS:

1. Rețele locale fără fir (Wireless Local Area Networks – WLAN) – sunt rețele care stabilesc fluxuri de comunicații între dispozitivele dintr-o zonă restrânsă fară fir. De regulă sunt utilizate în spații înhise de lucru sau o clădire. În CPS-uri, WLAN-urile sunt utilizate pentru a conecta diverse dispozitive și senzori prin Wi-Fi. În cazul acestora putem include și rețelele de senzori fără fir (Wireless Sensor Networks – WSN) care sunt rețele formate într-un grup de senzori interconectați pentru colectarea și transmiterea datelor, pe fluxuri fără fir. Senzorii pot fi distribuiți în diverse medii fizice, în general, pentru monitorizarea și transmiterea informațiilor despre parametrii mediului precum: temperatura, umiditate, luminozitate, presiune etc.;

2. Rețele de comunicații celulare (Cellular Networks) - sunt rețele de comunicații mobile care permit transferul de date între dispozitivele CPS utilizând infrastructura de comunicații existentă de tipul 3G, 4G și 5G. Aceste rețele oferă o acoperire extinsă și o conectivitate bună, la mare distanță. De regulă, sunt utilizate pentru a permite controlul și comanda dispozitivelor mobile și a celor autonome. Rețelele dedicate CPS pot oferi caracteristici personalizate precum lățimea de bandă garantată, latența redusă și securitate avansată.

3. Rețele Ethernet – sunt rețele cu fir utilizate pentru a conecta dispozitive prin cabluri Ethernet. Acest tip de rețele oferă o conexiune rapidă și fiabilă fiind utilizate pentru realizarea conexiunilor cu echipamente fixe așa cum sunt serverele, sistemele de control și dispozitivele de monitorizare;

4. Rețele de comunicații prin satelit – sunt rețele care utilizează sateliții pentru a permite comunicarea în zone greu accesibile sau care nu dispun de alte infrastructuri de comunicații. De regulă sunt utilizate în medii izolate, la suprafața mării și în medii aero-nautice. În funcție de constelațiile de sateliți pot fi de mai multe tipuri precum:

    a. Rețele de comunicații satelitare în bandă îngustă (Narrowband Satellite Networks) – utilizează sateliți plasați în orbita joasă a Pământului (Low Earth Orbit – LEO) și oferă o acoperire globală. Pot asigura comunicare la nivel mondial în aplicații pentru monitorizarea mediului și de telemetrie satelitară. Sunt utile în aplicații de monitorizare și control în zone în care infrastructura terestră este limitată sau indisponibilă.

    a. Rețele de comunicații satelitare în bandă largă (Satellite Broadband Networks)– utilizează sateliți poziționați în orbite geostaționare (Geostationary Earth Orbit – GEO). Rețelele GEO sunt utilizate pentru transmiterea datelor și pentru asigurarea comunicării în timp real între diferite locații geografice.

5. Rețele de comunicații cu fibră optică – sunt rețele care oferă o lățime de bandă ridicată, o transmisie rapidă de date și o imunitate mare la interferențe electromagnetice. CPS-urile conectate pot utiliza aplicații care necesită transmisie rapidă și sigură a datelor precum în domeniul medical și în sistemele inteligente de transport.

6. Rețele de comunicații bazate pe radar (Radar Communication Networks) – utilizează tehnologii radar pentru a transmite și recepționa date dinspre alte dispozitive. Pot furniza informații despre poziția în spațiu, despre mișcare și despre prezența obiectelor în mediu.

7. Rețele de comunicații cu spectru vizibil (Visible Light Communication – VLC) – utilizează tehnologia LED sau alte surse de iluminat pentru a transmite semnale, permițând transfer de informații în interiorul clădirilor

sau în medii în care conectivitatea radio este limitată sau nedorită. Oferă o lățime de bandă mare, o rată de transfer mare și o securitate sporită fiind utilizate în aplicații care necesită transmisii rapide și sigure de date.

8. Rețele de comunicații bazate pe infraroșu (Infrared Comunication Networks) – utilizează fascicule de lumină în spectrul infraroșu pentru transmiterea de date între dispozitive. Sunt utilizate în aplicații de comunicații între dispozitive mobile, la distanță scurtă sau în încăperi cu dimensiuni restrânse.

9. Rețele de comunicații subacvatice (Underwater Comunication Networks) – utilizate în aplicații marine pentru asigurarea comunicațiilor între dispozitive subacvatice, autonome sau dirijate, cu stațiile de la suprafață.

10. Rețele de comunicații pe frecvențe radio în apropierea corpurilor umane (Body Area Networks – BAN) – sunt utilizate în aplicații de monitorizare și pentru dispozitive medicale purtabile. Aceste permit transmiterea datelor senzorilor, dinspre corpul uman altor dispozitive cibernetice, în aplicații care monitorizează sănătatea, colectează și transmit date medicale etc.

11. Rețele de comunicații industriale – sunt rețele specializate utilizate în industria de automatizare și control industrial. Exemple de astfel de rețele sunt Profibus, Modbus, EtherCAT și Foundation Fieldbus. Aceste rețele permit comunicarea între echipamente industriale precum: senzori, controlere, actuatori, sisteme de monitorizare etc.

12. Rețele de comunicații ad-hoc – sunt rețele formate din dispozitive care se conectează între ele direct, fără a fi nevoie de o infrastructură preexistentă. Dispozitivele din aceste rețele pot comunica între ele și pot forma rețele temporare și flexibile, pentru situațiile în care o infrastructură de comunicații tradițională este limitată sau inexistentă. Așa sunt rețele ad-hoc vehiculare (VANET) care sunt utilizate în aplicații de transport inteligent pentru conectarea autovehiculelor cu infrastructura rutieră. Astfel, se realizează coordonarea vehiculelor prin schimb de date despre trafic, despre avertizări de coliziune, despre gestionarea traficului etc.

După cum se observă această clasificare este realizată în funcție de suportul de transmitere a datelor și de tehnologia de proiectare a rețelelor. Obiectivul general al listei urmărește asigurarea unei comunicații fiabile și în timp real, într-un mediu complex. Pentru acestea, principalele repere în selectarea unei rețele sunt lățimea de bandă, latența, securitatea și fiabilitate comunicării în funcție de cerințele specifice aplicațiilor implementate în CPS.

În interiorul unui CPS, rețelele de comunicații sunt diverse și se adaptează la cerințele și la scenariile de utilizare. Alegerea rețelei potrivite depinde de aspecte precum distanța de comunicare, lățimea de bandă necesară, cerințe de latență, costuri, disponibilitatea infrastructurii, alte considerații specifice aplicațiilor CPS. Fiecare tip de rețea are propriile caracteristici, beneficii și limitări.

De reținut este că alegerea rețelei potrivite depinde de cerințele specifice aplicațiilor CPS și de condițiile de implementare. Prezentăm doar câteva exemple de rețele de comunicare utilizate în CPS-uri după cum urmează:

1. Rețele CAN (Controller Area Network) – sunt utilizate în industria auto și în aplicații industriale pentru a conecta diverse componente și dispozitive cibernetice și fizice precum: senzori, actuatori, module de control etc. Rețelele CAN sunt proiectate pentru asigurarea comunicării fiabile și în timp real.

2. Rețele LoRaWAN (Long Range WAN) – se organizează pe baza tehnologiei LoRa pentru a permite o legătură de comunicații la distanțe mari și cu consum redus de energie. De regulă, sunt utilizate în CPS și în aplicații IoT pentru monitorizarea și controlul dispozitivelor în medii extinse aș acum ar fi în agricultura inteligentă, în rețele de senzori urbani sau în alte scenarii pentru aplicații de tipul „smart city” (orașul inteligent).

3. Rețele 6LoWPAN – sunt rețele care se bazează pe tehnologia IPv6 (Internet Protocol V6) și permit comunicarea între dispozitivele CPS și IoT pe baza protocolului standard. Acestea sunt proiectate pentru a funcționa eficient cu dispozitive cu resurse limitate de energie și de putere de procesare.

4. Rețele SDN (Software Defined Network) – sunt rețele caracterizate prin separarea controlului rețelei de infrastructura fizică a CPS-ului. Prin utilizarea SDN este posibilă gestionarea și controlul centralizat al

fluxurilor de date și configurarea dinamică a rețelei, facilitând adaptarea și scalabilitatea sistemului.

5. Rețele Fog și rețele Edge – aceste rețele permit extinderea infrastructurii de comunicații la nivelul de apropiere a dispozitivelor și a senzorilor cibernetici și fizici. În aceste rețele, prelucrarea datelor și luarea deciziilor are loc la nivelul marginii rețelei (edge). Astfel se reduce latența și identificarea de cerințe suplimentare de lățime de bandă pentru transmiterea datelor către centrul de control.

6. Rețele P2P (Peer-to-Peer) – permit comunicarea directă între dispozitive fără intermedierea unui server central. În CPS, rețelele P2P pot fi utilizate pentru partajarea și pentru transferul de date între dispozitivele cibernetice și fizice fără a depinde de o infrastructură centralizată.

7. Rețelele Zigbee – acestea sunt utilizate pentru aplicații cu consum redus de energie. Pot fi utilizate și de IoT, pentru comunicații fără fir, cu un consum redus de energie și o lățime de bandă mică. Sunt potrivite pentru dispozitivele care necesită autonomie crescută și o interconectare extinsă.

8. Rețele de comunicații haptice (Haptic Communication Networks) – acestea permit transferul informației tactile și a senzațiilor între dispozitive cibernetice și fizice, precum și între utilizatori. Ele sunt utilizate în aplicații care oferă feedbak tactil și senzații realiste precum realitatea virtuală, medicină haptică sau interacțiunea om-mașină.

9. Rețele de comunicații avansate (Advance Communication Networks) – includ tehnologii emergente și inovatoare așa cum sunt rețele cuantice, rețele de comunicare cognitivă și rețele de comunicații bio-inspirate. Chiar dacă sunt încă în stadiul de dezvoltare, aceste rețele exploatează noi paradigme de comunicație și potențialul tehnologiilor avansate pentru a îmbunătăți performanța și funcțiile CPS-urilor.

5.3. Importanța comunicării și a comunicațiilor pentru CPS-uri

Importanța comunicării și a comunicațiilor în diferite domenii în care CPS-urile au un impact semnificativ derivă din necesitatea asigurării unei transmiteri corecte și de calitate a informațiilor, prin fluxuri sigure. Aceste condiții asigură

integrarea și funcționarea corectă a componentelor cibernetice și fizice, permit realizarea beneficiilor și utilizarea la potențialul maxim a CPS-ului.

Prin urmare, prezentăm unele direcții de evoluție și domeniile de aplicare din care rezultă importanța comunicării și a comunicațiilor în CPS-uri, cu mențiunea că pot constitui teme ale unor proiecte de cercetare și dezvoltare:

- Comunicarea și sisteme autonome: CPS facilitează dezvoltarea sistemelor autonome precum roboții autonomi sau vehicule autonome. Comunicarea în aceste sisteme este esențială pentru a permite schimbul de informații între componente și pentru a facilita deciziile autonome bazate pe date și pe informații, obținute în timp real. Spre exemplu, în cazul transportului inteligent, sistemul de comunicații facilitează comunicarea între autovehiculele autonome, infrastructura rutieră și cu alte entități cum ar fi pietonii și bicicliștii.

- Comunicarea și managementul resurselor: CPS poate fi utilizat pentru gestionarea și monitorizarea eficientă a resurselor, precum apa, energia sau a diverselor materiale. Comunicarea în aceste sisteme facilitează colectarea datelor de la senzori și de la dispozitive, analiza informațiilor și optimizarea utilizării resurselor pentru a obține eficiență și sustenabilitate.

- Comunicarea și interacțiunea cu utilizatorul: în CPS-uri, comunicarea eficientă și intuitivă între sistem și utilizatori este esențială pentru a permite controlul, monitorizarea și interacțiunea umană într-un mod facil și eficient. Interfețele intuitive, feedbak-urile în timp real și mecanismele de comunicare adaptabile sunt importante pentru a facilita interacțiunea om-mașină în mediul CPS. De exemplu, în domeniul sănătății digitale comunicare permite transmiterea datelor medicale, monitorizarea constantă a pacienților, comunicarea între pacienți și profesioniștii medicali, în vederea evaluării stării pacienților și a stabilirii tratamentului eficient al afecțiunilor.

- Comunicarea și sistemele de siguranță: CPS joacă un rol crucial în dezvoltarea sistemelor de siguranță așa cum sunt sistemele de detectare și de prevenire a incendiilor sau sistemele de securitatea a clădirilor. Comunicarea în aceste sisteme facilitează transferul rapid de informații și emiterea de alerte între componente, permițând intervenția rapidă, adecvată și coordonată în situații de criză și de urgență. Spre exemplu: în domeniul agriculturii inteligente, comunicarea permite monitorizarea factorilor agricoli critici (umiditatea solului, temperatura, nivelul de

nutriente, starea plantelor), intervenția oportună pentru restabilirea parametrilor agricoli optimi și evitarea altor eventuale pericole.

- Comunicarea în sistemele de gestionare a traficului aerian: CPS-urile implicate în gestionarea traficului aerian au ca funcție prioritară asigurarea comunicării pentru siguranța și eficiența zborurilor. Comunicarea între controlorii de trafic aerian, între piloți și între sistemele de navigație facilitează coordonarea zborurilor și transmiterea informațiilor relevante, în timp real.

- Comunicarea și sistemele mobile de asistență medicală: CPS-urile pot fi utilizate în sisteme mobile de asistență medicală care implică furnizarea de îngrijire medicală în locații extreme sau în mișcare. Comunicarea în aceste sisteme permite transmiterea datelor medicale, consultarea la distanță și coordonarea între profesioniștii medicali și pacienți. Astfel poate fi asigurată o asistență medicală adecvată, în orice moment și oriunde.

- Comunicarea și sistemele de automatizare industrială: CPS-urile facilitează comunicarea în sistemele de automatizare industrială, unde sunt esențiale integrarea și coordonarea dispozitivelor și a proceselor. Sistemul de comunicații permite transmiterea comenzilor și a informațiilor de la senzori și de la dispozitive CPS la sistemele de control, asigurând astfel o funcționarea eficientă și sigură a sistemului industrial.

- Comunicarea și realitatea augmentată/virtuală: CPS-urile pot beneficia de comunicare în realitate augmentată (AR) și virtuală (VR). În aceste cazuri, comunicarea este utilizată pentru a sincroniza informațiile și acțiunile într-un mediu virtual sau augmentat și mediul fizic permițând interacțiunea utilizatorilor cu elementele virtuale sau augmentate într-o manieră integrată și integratoare.

- Comunicarea în sistemele de securitate publică: CPS joacă un rol esențial în dezvoltarea sistemelor de securitate și de apărare a vieții umane. Cele mai cunoscute sunt sistemele de detectare a incendiilor, sistemele de alertă timpurie în caz de dezastre sau rețelele de comunicare pentru echipele de intervenție. Sistemele de comunicații asigură schimbul de informații în timp real, coordonarea operațiunilor și asigurarea securității și protecției publicului și a echipelor de intervenție.

În CPS-uri comunicarea și comunicațiile sunt deosebit de importante pentru că permit integrarea componentelor cibernetice și fizice într-un sistem coerent și

funcțional. Astfel, CPS-ul formează și susține o interacțiune între lumea fizică cu cea digitală, în care dispozitivele inteligente, senzorii și actorii implicați sunt conectați prin rețele de comunicații pentru a comunica și coopera în mod eficient. În principal, comunicarea trebuie să fie scalabilă și adaptabilă pentru a face față diversității dispozitivelor și configurației sistemului. Acestea pot fi utilizate individual sau în combinație, în funcție de cerințele sistemului.

În cadrul unui CPS, o comunicare eficientă este determinată prin standarde și protocoale de comunicare în care sunt incluse și norme de securitate a datelor și a sistemului de comunicații. Dat fiind că un CPS implică transfer de date sensibile și controlul dispozitivelor fizice este esențial să se asigure confidențialitatea, integritatea și disponibilitatea datelor. Numai așa pot fi descurajate atacurile cibernetice și securitatea componentelor software și hardware.

Pentru aceasta trebuie urmărite următoarele aspecte:

10. Arhitectura comunicațiilor CPS: comunicarea în CPS se bazează pe o arhitectura complexă care poate implica interconectarea dispozitivelor fizice și a componentelor software. Această arhitectură poate varia în funcție de specificațiile sistemului și poate include niveluri diferite de acces, precum nivelul senzorilor, nivelul rețelelor de comunicații și nivelul de control și management. Pot exista și rețele hibride care combină rețelele fără fir cu cele cu fir. Comutarea inteligentă între acestea poate asigura robustețe și eficiența comunicării.

11. Internetul lucrurilor (IoT): IoT deține un rol semnificativ în CPS. Acesta permite conectarea dispozitivelor fizice și a senzorilor la internet. Rețeaua globală existentă facilitează transferul de date în timp real și permite controlul și monitorizarea dispozitivelor de la distanță. Unele sisteme pot necesita un tip de comunicare edge-to-cloud pentru dispozitivele aflate la marginea rețelei (edge devices) și serviciile cloud. O comunicare eficientă între aceste două niveluri poate contribui la performanța sistemului.

12. Big data și analiza datelor: comunicarea în CPS generează o cantitate uriașă de date care trebuie stocate și transferate. Prin urmare ele trebuie colectate, înmagazinate, analizate și procesate pentru a genera informații valoroase. Analiza datelor ajută la îmbunătățirea performanței sistemului, la identificarea defecțiunilor și la optimizarea operațiunilor.

13. Comunicarea M2M (machine-to-machine): CPS implică comunicare directă între diferite dispozitive cu componentele sistemului, cu sau fără intervenție umană. Acest aspect facilitează schimbul rapid și eficient de informații între senzori, actuatori și alte dispozitive în scop de coordonare și de control al sistemului.

14. Securitatea comunicațiilor: așa cum am mai prezentat CPS-ul presupune interconectare în lumea digitală și cea fizică. Securitatea comunicațiilor este o cerință esențială a sistemului. CPS-urile trebuie să fie protejate atât în comunicațiile interne, care asigură funcționarea sistemului, cât și în cadrul comunicațiilor externe reprezentate, în mod deosebit, din zona interacțiunii cu operatorii umani. Dispozitivele CPS trebuie să fie protejate împotriva atacurilor cibernetice, iar operațiunile trebuie protejate împotriva intruziunilor și a manipulărilor malițioase.

15. Standardizare și interoperabilitate: pentru asigurarea compatibilității și interoperabilității între componentele CPS este necesară utilizarea standardelor și protocoalelor comune de comunicare și de comunicații. Acestea facilitează integrarea și schimbul de informații între entități. Selectarea unui protocol de comunicare adecvat este esențială pentru un CPS. Cele mai utilizate protocoale sunt MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol) și OPCUA (OPC Unified Architecture), care permit comunicarea eficientă și securitizată între dispozitive și servicii.

Se observă că cele două cerințe, comunicarea și comunicațiile, reprezintă o componentă esențială în CPS. Prin utilizarea tehnologiilor adecvate se poate facilita schimbul eficient și securizat de informații între dispozitive pentru funcționarea coordonată și optimă a sistemului. În acest sens tehnologia nu trebuie limitată doar la o linie tehnologică de producție sau la un serviciu. Acesta presupune și abordări know-how, manageriale și de feedbak ale execuției.

Privind discuția despre comunicare și comunicațiile în CPS prezentăm unele aspecte suplimentare:

Comunicarea în timp real: CPS implică necesitate comunicării în timp real între diferitele componente ale sistemului. De exemplu, un sistem de control al traficului rutier ar trebui să primească și să trimită actualizări rapide și sincronizate pentru a coordona semafoarele și pentru a optimiza fluxul de trafic.

Comunicare ad-hoc: uneori, în CPS pot apărea situații în care dispozitivele trebuie să comunice direct între ele într-o rețea ad-hoc, fără a fi conectate la o infrastructură de comunicații preexistentă. Acest tip de comunicare este determinant în situații de urgență sau în medii în care nu există infrastructuri de comunicații stabile.

Integrare în cloud: comunicarea în CPS poate include transfer de date între dispozitive fizice și servicii cloud. Cloud-ul cibernetic oferă capacitate de stocare și putere extinsă de procesare, permițând analiza și prelucrarea datelor colectate de sistemele CPS. Prin intermediul comunicațiilor, datele pot fi transferate rapid între dispozitive și servicii cloud alocate, pentru procesare lor în timp real și într-o manieră centralizată.

Unele CPS-uri sunt utilizate *în medii critice* așa cum sunt industriile petrochimice, centralele nucleare sau în medicină. De regulă, comunicare în aceste medii este asigurată prin sisteme de comunicații cu sau fără fir. Particular acestor CPS-uri este faptul că în aceste medii sunt interferențe, zone periculoase sau cerințe stricte de securitate ceea ce determină o atenție deosebită asigurării sistemelor de comunicații fără fir. Acestea trebuie adaptate la organizarea de sisteme ad-hoc securizate sau la impunerea unor protocoale speciale pentru a asigura comunicarea în condiții de securitate.

Comunicarea interdomeniu: uneori, CPS implică interacțiunea între diferite domenii sau medii. Dintre acestea enumerăm sistemele inteligente de transport, de sănătate digitală și de producție inteligentă. Acest tip de comunicare implică integritatea și interoperabilitate între domenii, prin schimb de informații în mod coordonat operațional.

Optimizarea comunicațiilor: într-un CPS este important ca sistemul de comunicații să fie optim pentru a reduce latența și pentru a sigura o utilizare eficientă a resurselor. Aceasta poate implica utilizarea de algoritmi adecvați de rutare, planificarea transmiterii datelor și tehnici de compresie a datelor pentru a reduce cantitatea de date transferate.

Interacțiunea om-mașină: Așa cum am observat, în CPS-uri, comunicarea nu se limitează doar la interacțiunea dintre dispozitivele și componentele acestuia. Interacțiunea de tip om-mașină este esențială deoarece utilizatorii umani trebuie să poată controla și monitoriza sistemul. Interfețele intuitive și eficiente de comunicare sunt important pentru a facilita interacțiunea om-mașină și pentru a permite utilizatorilor să intervină în funcționarea sistemului.

Telemetrie și monitorizare: comunicarea în CPS poate include telemetria și monitorizarea dispozitivelor și sistemelor. Acest lucru permite colectarea și transmiterea datelor de stare, a informațiilor de diagnostic și a altor măsurători relevante pentru a asigura funcționarea optimă a sistemului și pentru a detecta eventualele defecțiuni sau probleme.

Comunicarea cu rețele de energie inteligentă și de fabricație inteligentă: în CPS-uri, integrarea cu rețelele de energie inteligentă (smart grids) poate avea loc prin comunicarea între dispozitivele de gestiune a energiei, contoare inteligente și alte componente ale sistemului. Acestea permit monitorizarea consumului de energie, optimizarea eficienței energetice și gestionarea distribuției de energie într-un mod inteligent. În domeniul fabricației inteligente, comunicarea este esențială pentru gestionarea proceselor de producție. Astfel mașinile, roboții și sistemele de control interacționează și colaborează în timp real, pentru optimizarea producției, pentru reducerea timpilor de inactivitate și pentru îmbunătățirea eficienței generale a fabricii.

În concluzie comunicarea eficientă, interoperabilitate și securitatea sunt esențiale pentru asigurarea funcționării și coordonare CPS-urilor pentru toate domeniile.

Temă:

Studiați site NORSIT, *Securitatea cibernetică în contextul Industry 4.0*, la adresa https://norsit.ro/securitatea-cibernetica-in-contextul-industry-4-0 (la data de 03.08.2023) și identificați un domeniu unde sunt utilizate CPS-uri. Întocmiți și prezentați un eseu (8 pagini, TNR, 12 p., la un rând) în care să și descrieți principalele funcții pe care le considerați că trebuie să le îndeplinească CPS-ul ales, în raport cu cerințele de proiectare pe care le stabiliți dumneavoastră.

TEMA 6: PRINCIPII ALE OPTIMIZĂRII PROCESELOR ÎN CPS

În general, optimizarea se referă la procedeul de găsire a celei mai bune soluții sau a unui set optim de decizii în vederea maximalizării unui obiectiv sau a minimalizării unei funcții de cost. Știința optimizării, este adesea cunoscută sub denumirea de cercetarea operațională și reprezintă o disciplină a matematicii, în care informatica deține un rol principal prin dezvoltarea de algoritmi și tehnici pentru a oferi soluții eficiente diferitelor probleme.

Optimizarea pentru CPS se referă la identificarea și aplicarea tehnicilor și metodelor de optimizare, hardware și software, pentru a îmbunătăți performanța și eficiența componentelor sistemului. Un CPS reprezintă, el însuși, un sistem integrator de entități cibernetice și fizice care relaționează în sisteme inteligente, în rețele și autonome. Prin urmare am putea considera că un CPS este un sistem optim din momentul implementării sale și a dării în exploatare.

Însă, vom observa că odată cu dezvoltarea și cu implementarea de noi tehnologii cibernetice și fizice un CPS are o durată limitată de utilizare, adecvată la schimbările condițiilor mediului ambiant. În această temă ne propunem să înțelegem importanta și rolul deosebit pe care îl dețin informațiile din mediu și prognozele evoluției unui CPS pentru a fi modernizat până în momentul în care acesta își menține un cost minim în raport cu consumul de resurse, prin prisma principiilor optimizării.

6.1. Aspecte generale privind optimizarea pentru CPS

În general, procesele de optimizare implică definirea unui obiectiv clar și a unei funcții care se dorește să se maximalizeze sau să se minimalizeze. Spre exemplu, obiectivul poate fi maximalizarea profitului, minimalizarea costurilor, optimizarea eficienței, minimalizarea timpului de execuție, maximalizarea nivelului de satisfacție pentru un serviciu etc. Un proces de optimizare presupune identificarea unui set de variabile sau de parametri care pot fi ajustați pentru a influența rezultatul obținut până la o valoare așteptată. Acești parametri sunt utilizați pentru a construi o funcție matematică, numită obiectiv sau funcție de cost. Cu aceasta se măsoară performanța sistemului în funcție de valorile parametrilor.

Cu alte cuvinte, algoritmii de optimizare sunt utilizați pentru a explora domeniul soluțiilor și pentru a identifica valorile optime parametrilor care satisfac

obiectivele dorite. Acești algoritmi pot fi de natură matematică, precum metodele de programare liniară, metoda gradientului, algoritmi evolutivi, alți algoritmi derivați, precum și tehnici de învățare automată, așa cum sunt algoritmii genetici sau rețelele neurale.

Toate sistemele în care se preconizează eficientizarea a ceva pot fi optimizate. Prin urmare, optimizarea este aplicată într-o gamă largă de domenii cum ar fi: inginerie, economie, logistică, planificarea resurselor, analiza datelor, proiectare de produse și activități etc. Scopul său este de a găsii soluții pentru maximalizarea eficienței și minimalizarea costurilor pentru diferite scenarii dinamice. Optimizarea pentru CPS este un domeniu complex și multidisciplinar, care presupune aplicarea tehnicilor și metodologiilor de optimizare aflate la intersecția științelor matematică, inginerie și multe altele, pentru îmbunătățirea performanței, eficienței, fiabilității și funcționalității acestora.

Așa cum am văzut până acum, CPS-ul reprezintă integrarea componentelor cibernetice (software, rețele, sisteme informaționale etc.) cu cele fizice (senzori, actuatori, mașini, procese industriale etc.) pentru a crea sisteme inteligente și autonome. Poate fi considerat ca un rezultat al științei combinatorii și a tehnicilor de reglare a funcționării în mediile cibernetice și fizice cu un consum minim de resurse.

Mecanismele de reglare a funcționării se bazează pe prelucrarea automată de date culese prin propriile sisteme sau procesate pe baza cerințele utilizatorilor. Însă, sunt necesare informații încă din faza de proiectare a unui CPS pentru identificarea unor posibile soluții în vederea stabilirii limitelor funcționale ale sistemului, în conformitate cu destinația sa. Rezultatul final devine bun de exploatat numai în urma testelor aplicate în fazele următoare proiectării sistemului. Optimizare proceselor funcționale contribuie esențial la dezvoltarea tehnologică și la dezvoltarea soluțiilor inteligente și autonome într-o gamă largă de domenii ale CPS. Cerințele identificate și dialogul cu utilizatorii permit corectarea modelului inițial, generare de update și upgrade sistematic, iar atunci când se constată că sistemul depășește nivelurile de randament proiectate, să fie abandonat, iar pe baza lecțiilor învățate să fie creat un nou sistem.

Prin urmare, optimizarea pentru CPS-uri reprezintă, în general, urmărirea continuă a găsirii celor mai bune soluții posibile pentru eficiența energetică, pentru utilizarea resurselor, pentru sporirea performanței sistemului, pentru satisfacerea cerințelor de timp real și pentru optimizarea costurilor. Optimizarea poate implica

luarea deciziilor în timp real pentru a obține o stare și un comportament eficient al CPS-ului, prin algoritmi și tehnici matematice. De exemplu, într-un sistem de control inteligent al traficului urban, optimizarea ar putea implica identificarea celor mai bune rute pentru autovehicule. În funcție de parametri precum timpul de călătorie, itinerarul optim, consum de carburant, nivelul de poluare, alte cerințe stabilite de utilizatori, CPS-ul propune cea mai economică rută. Un alt exemplu ar fi optimizarea unui sistem de producție industrială pentru a minimaliza timpul de inactivitate și a maximaliza utilizarea resurselor. Suntem convinși că oricine poate identifica și alte exemple însă nu ne propunem să le enumerăm aici, soluțiile identificate putând fi optime (obiectivul ideal al optimizării unui CPS) sau sub-optime (pentru unele componente de execuție), determinate de cerințele specifice și de constrângerile sistemului.

În ansamblu, fără aplicații de optimizare, un CPS nu poate fi utilizat în mod eficient, inteligent și sustenabil.

Prezentăm câteva exemple de **domenii** unde optimizarea pentru CPS-urilor aduce beneficii cunoscute semnificative:

Optimizare resurselor: CPS-urile implică deseori gestionarea eficientă a resurselor limitate, așa acum ar fi energia, lățimea de bandă a traficului în rețele sau capacitatea de procesare. Prin optimizare se pot dezvolta algoritmi și strategii pentru a aloca și utiliza aceste resurse în mod eficient, asigurând un consum și o funcționare optimă a sistemului. Optimizarea consumului de energie, spre exemplu, se realizează pentru a se stabili eficiența energetică mai ales în aplicații mobile sau alimentate de surse limitate de energie. Aceste tehnici pot minimaliza consumul de energie al sistemului, prin adaptarea dinamică a consumului în funcție de necesități.

Optimizarea planificării și programării: CPS-urile pot implica planificarea și programarea activităților complexe și interconectate. În acest context, optimizarea poate fi utilizată pentru a găsi programe și planuri de acțiune care minimalizează timpul total necesar, minimalizează efectul conflictelor între componente și optimizarea utilizării resurselor. Învățarea automată poate fi optimizată. Prin aceste tehnici un CPS își poate îmbunătăți performanța și se poate adapta mai bine la mediu. În acest context, optimizarea poate include optimizarea algoritmilor de învățare automată, a parametrilor componentelor, a arhitecturii sistemului etc., toate fiind destinate să obțină rezultate mai precise și eficiente, în timp real. Mai mult decât atât, pot fi optimizate procesele de planificare a traseelor, programarea sarcinilor și luarea deciziilor în timp real.

Optimizarea securității și rezistenței: CPS-urile trebuie să fie robuste și rezistente la atacuri cibernetice și la defecțiuni. Prin optimizare se pot identifica și implementa măsuri de securitate și mecanisme de detecție a vulnerabilităților, tehnici de recuperare a datelor etc., toate fiind menite să maximalizeze protecția sistemului și să minimalizeze riscurile potențiale. Optimizarea securității în timp real implică dezvoltarea de algoritmi și de tehnici de detectare, de prevenire și de reacție la amenințările de securitate. În plus, o creștere a numărului de componente sau de schimbări în mediul de operare poate expune CPS-ul la riscuri suplimentare. Astfel, pot fi optimizate strategii și algoritmi care să permită scalabilitatea, extensibilitatea sistemului și reconfigurarea lui, asigurând o funcționare optimă în fața creșterii volumului de date și a numărului de componente.

Optimizarea comunicațiilor și rețelelor: comunicarea și conectivitatea între componentele CPS-urilor sunt servicii critice. Optimizarea poate fi înțeleasă ca o metodă de identificare a itinerariilor eficiente în rețele de comunicații, tehnici de minimalizare a latenței sistemului și a protocoalelor de rețea (jitter), metode de maximalizare a lățimii de bandă disponibile și pentru a asigurarea transferului de date între componentele acestuia cu maximă eficiență. Jiter-ul rezultă din congestionarea rețelelor, din variații de timp și din schimbări ale rutelor rețelelor cibernetice. Mai mult decât atât, în situația în care un CPS este compus din entități neeterogene și diverse, provenite de la diferiți producători sau dezvoltatori, optimizarea interoperabilității este extrem de necesară și se concentrează pe dezvoltarea de standarde și de protocoale comune, pentru adaptarea componentelor și interfețelor în vederea asigurării eficienței funcționării acestora.

Optimizarea performanței sistemului: CPS-urile pot avea cerințe stricte de performanță, precum timpul de răspuns, latența sau transportul de date (throughput). Din punct de vedere al sistemelor cibernetice debitul datelor reprezintă o măsură a câte unități de informații poate procesa un sistem într-o perioadă de timp. Debitul datelor se aplică pe scară largă sistemelor informatice, în special a celor industriale, variind de la diverse dispozitive fizice, la rețele de date și la întreg sistemul. Acesta este înrudit cu lățimea de bandă și cu latența sistemului. Adesea termenii sunt utilizați în mod eronat. Pentru a-l înțelege corect, menționăm că într-un CPS pot fi procesate unități precum trilioane de operațiuni în virgulă mobilă pe secundă (terafloops). Această informație oferă o măsurătoare pentru un producător pentru a compara costul calculului brut în timp. Optimizarea poate fi utilizată pentru a identifica și implementa strategii și algoritmi care maximalizează performanța sistemului, asigurând un timp

de răspuns cât mai rapid și o execuție eficientă a sarcinilor. Reziliența sistemului reprezintă un alt domeniu care necesită optimizări. Prin optimizarea rezilienței se asigură menținere funcționării serviciilor esențiale în fața defecțiunilor și recuperarea rapidă a funcțiilor în caz de perturbări de date.

Optimizarea deciziilor în timp real: CPS-urile trebuie să ia decizii în timp real pe baza informațiilor și datelor provenite din mediul fizic și cibernetic. Optimizarea poate fi folosită pentru a dezvolta algoritmi și modele care să ajute la luarea deciziilor rapide și precise, ținând cont de multiplele cerințe și de toate constrângerile sistemului.

Acestea sunt doar câteva exemple de domenii unde optimizarea este necesară la nivelul unui CPS, aplicațiile fiind ample și în continuă dezvoltare. Totuși, în cadrul proceselor de optimizare trebuie să se țină cont de unele **cerințe generale,** dintre care enumerăm:

Optimizarea trebuie să fie adaptivă: CPS-urile pot fi supuse unor condiții de mediu dinamic și variabil. Optimizare adaptivă se referă la capacitatea sistemului de a se ajusta și de a se adapta în timp real la schimbările din mediul fizic și cibernetic. Această cerință implică utilizarea algoritmilor și tehnicilor care pot monitoriza și înțelege mediul înconjurător, astfel încât să poată lua decizii și să acționeze optim, în funcție de context.

Optimizarea trebuie să permită interacțiunea între sisteme multi-agent: CPS-urile pot fi compuse din entități autonome care să coopereze și să interacționeze reciproc, pentru a atinge un obiectiv comun. Optimizarea funcționării acestor sisteme se referă la găsirea strategiilor și a regulilor de interacțiune care să maximalizeze performanța și eficiența sistemului, în ansamblul său. Aceasta implică echilibrarea între tehnicile de cooperare, asigurarea competiției între agenți și găsirea soluțiilor de optimizare atât pentru tot sistemul cât și la nivelul interacțiunii directe dintre agenți.

Optimizarea trebuie să permită luarea deciziilor în timp real: așa cum am menționat, CPS-urile necesită luarea deciziilor în timp real și identificarea de răspunsuri rapide la evenimentele și stimulii din mediul înconjurător. Optimizarea în timp real se concentrează pe dezvoltarea de algoritmi și de tehnici care permit luare de decizii rapide și eficiente, în timp real, în funcție de obiectivele și de constrângerile sistemului. Acest tip de optimizare poate implica tehnici online, care se adaptează și se eficientizează, în timp real, pe măsură ce se obțin informații noi.

Optimizare trebuie să fie aplicabilă sistemelor distribuite: CPS-urile pot fi compuse din entități distribuite și interconectate precum senzori, actuatori și dispozitive de procesare răspândite pe o largă suprafață geografică. Optimizarea sistemelor distribuite urmărește dezvoltarea de algoritmi și protocoale care să permită comunicarea și cooperarea eficientă între toate componentele distribuite, scopul fiind de a atinge un obiectiv comun și a optimiza performanța și eficiența întregului sistem.

Optimizarea trebuie să fie rezistentă al schimbări și la incertitudini: optimizarea performanței de rezistență fizică a CPS-urilor vizează asigurarea funcționării eficiente în condiții variabile și de incertitudine ale mediului înconjurător. Aceasta se referă la dezvoltarea de strategii și de algoritmi care să mențină funcționarea sistemului, indiferent de variațiile și de evenimentele perturbatoare din mediul fizic și cibernetic. Soluțiile trebuie să fie rezistente la erori, la zgomot, la defecțiuni sau la alte schimbări neprevăzute, în condiții de funcționare stabilă.

Principalele metode și tehnici de optimizare **pot fi aplicate** următoarelor componente, dispozitive și servicii:

În infrastructura IoT: CPS-urile sunt adesea parte integrantă a infrastructurii IoT în care obiectele fizice sunt conectate și interacționează cu mediul online. Optimizarea în acest context se concentrează pe gestionarea eficientă a datelor, pe securitatea comunicațiilor și pe optimizarea consumului de energie în mediu distribui al obiectelor interconectate. Rețelele CPS pot suferi schimbări în topologie, a disponibilității resurselor și modificarea condițiilor de mediu. Optimizarea adaptabilă a rețelelor se realizează prin algoritmi și prin protocoale care se pot adapta dinamic la aceste schimbări, pot reconfigura rețeaua, pot redistribui sarcini și pot adapta rețeaua în funcție de noile condiții.

În infrastructuri critice și de securitate: CPS-urile sunt utilizate în diverse domenii critice și sensibile, precum aviația, navigația la suprafața apei și în imersie, industria nucleară, asistența medicală etc. Optimizarea în mediile specifice acestor domenii socio-profesionale implică asigurarea funcționării sigure și fiabile a sistemelor, prin algoritmi și protocoale care să valideze și să verifice riguros soluțiile și standardele de aplicare strictă a reglementărilor. Acestea pot fi distribuite pe o arie geografică extrem de extinsă. În plus, CPS-uri pentru monitorizarea mediului sau a rețelelor inteligente de energie implică dezvoltarea de algoritmi și de tehnici care să asigure comunicarea eficientă și coordonată între componentele distribuite

geografic, pe suprafețe foarte mari, pentru a funcționa optim pentru infrastructurile critice și de securitate.

În componente care asigură interacțiunea om-mașină: CPS-urile implică interacțiunea între utilizatorii umani și sistemele automatizate. Optimizarea în acest context se referă la îmbunătățirea experienței utilizatorului, la optimizarea interfețelor de utilizator, la adaptarea la preferințele și la cerințele utilizatorilor, precum și la optimizarea eficienței și eficacității comunicării și a colaborării între om și mașină. Astfel, se optimizează performanța și precizia mișcărilor roboților, se adaptează funcționarea mașinilor la nevoile și la preferințele utilizatorilor, se asigură o interacțiune sigură și eficientă etc.

În echipamente durabile și sustenabile: CPS-urile au un rol important în dezvoltarea soluțiilor tehnologice durabile și ecologice. Optimizarea în acest context implică reducerea consumului de resurse, minimalizarea emisiilor de carbon, integrarea surselor de energie regenerabilă și dezvoltarea soluțiilor care susțin dezvoltarea durabilă și protecția mediului înconjurător. Tehnicile avansate de inteligență artificială precum învățarea automată, rețelele neuronale și algoritmii genetici implică algoritmi și parametri AI pentru obținerea performanței superioare și o înțelegere mai bună a datelor, pentru luarea deciziilor precise și eficiente, în timp real, asigurând o stabilitate durabilă și sustenabilă.

În infrastructuri de securitate și de protecție a datelor: CPS-urile gestionează și procesează o cantitate mare de date sensibile și de informații personale. Optimizarea în acest context implică implementarea măsurilor de securitate adecvate, criptarea datelor, gestionarea accesului și protecția confidențialității utilizatorilor și a informațiilor sensibile. Extragerea informațiilor relevante și a cunoștințelor din date, reducerea redundanței și a zgomotului și optimizarea întregului sistem sunt generate de o utilizare optimă, în condiții de securitate și de protecție a datelor provenite din mediile fizic și cibernetic.

Toate aspectele prezentate evidențiază nevoia de abordare a provocărilor specifice CPS-urilor și de dezvoltare a soluțiilor optimizate care să asigure performanța, fiabilitatea și securitatea lor. Prin aplicarea tehnicilor și metodelor de optimizare adecvate, se poate obține o îmbunătățire semnificativă a funcționalității și eficienței CPS-urilor, contribuind la dezvoltarea de sisteme inteligente și autonome într-o varietate largă de domenii și de aplicații.

6.2. Metodă de optimizare a obiectivelor pentru CPS

Pentru a înțelege de ce și cum se identifică valoarea unui obiectiv strategic pentru CPS-uri și numai, prezentăm cea mai simplă metodă de optimizare, prin ușurința învățării de către persoane care nu au o pregătire profesională tehnică. Este vorba de metoda numită CARVER (Criticaly, Accessibitity, Recuperability, Vulnerability, Effect, Recognizability). Unii o numesc tehnică managerială. Acesta a apărut în anii '80 și a fost dezvoltată de CIA (SUA) pentru evaluarea și prioritizarea amenințărilor potențiale într-un sistem sau organizație, la adresa infrastructurilor critice. Un utilizator CPS, poate apela la această metodă pentru a-și selecta un obiectiv decizional, pe baze științifice atât în relațiile CPS cât și în comunicarea cu alți utilizatori. Metoda, în sine, nu reprezintă o noutate deosebită. În practica curentă mulți o folosesc fără știe că se denumește așa, având practic o aplicabilitate nelimitată.

CARVER derivă din „metoda utilității globale", fiind o metodă de cercetare operațională. De regulă, este utilizată pentru rezolvarea rapidă a situațiilor complexe și pentru alegerea unei decizii optime, pe baze raționale și științifice. Diferența constă în faptul că matricea decizională poate conține un număr variat de criterii iar evaluarea poate fi făcută și cu note nu doar cu procente. Vom înțelege aceste aspecte din modelul de aplicabilitate a CARVER într-un scenariu propus.

CARVER poate fi definită ca direcție de acțiune selectată în mod conștient, din mai multe opțiuni, în urma unui proces complex de informare și analiză, în scopul orientării și selectării variante cu pierderile cele mai mici într-o situație creată[1]. Este o metodă foarte simplă dar destul de subiectivă, rezultatul putând fi foarte ușor influențat lipsa unei corectitudini în respectarea raportului de evaluare, precum și de consecvența utilizatorului în a-și respecta criteriile de selecție.

Scopul major al utilizării ei este de a obține o înțelegere aprofundată a nivelului de recunoaștere a fiecărui element analizat, pe baza informațiilor pentru dezvoltarea de strategii de protecție mult mai eficiente. Evaluarea se poate face pentru întregul CPS-ul sau doar pentru o componentă a acestuia.

CARVER poate fi aplicată unui CPS în sectoare precum protecția infrastructurilor, securitate cibernetică, managementul resurselor, protecția activelor critice etc. Această metodă constă în analiza prin comparație a indicatorilor

[1] Cam.(r)dr. Grad Vasile, col.dr. Stoian Ion, drd. Kovacs Emil-Carol, col.dr. Dumitru Vasile, *Cercetare operațională în domeniul militar*, Editura Sylvi, București , 2000, p. 32-35.

reprezentativi pentru cele șase elemente componente ale acronimului CARVER, pe care le-am tradus din limba engleză astfel: 1. *Examinare critică*; 2. *Accesibilitate*; 3: *Recuperabilitate*; 4. *Vulnerabilitate*; 5. *Consecințe*; și 6. *Recognoscibilitate*.

Pentru cei șase indicatori enumerați mai sus se stabilesc valori prin însumarea evenimentelor sau a unor elemente măsurabile. În funcție de criteriile stabilite de utilizator pentru fiecare criteriu, sunt introduse într-o matrice de decizie. În urma analizei valorilor determinate, scorul obținut prin însumarea lor se împarte la valoarea inițială a fiecărui criteriu pentru a se obține o valoare procentuală care este adimensionată și permite compararea în matrice.

Astfel, coeficientul obținut permite identificarea variantei dorite, cu valoarea maximă sau minimă, în funcție de ce își propune utilizatorul să analizeze.

Pentru acordarea unor note sau valori măsurabile fiecărui criteriu al CARVER, pentru un CPS prezentăm următoarea metodologie:

1. Examinare critică: se referă la importanța sau la semnificația obiectivului. Stabilește valoarea unui element sau a unei activități critice, adică a acelor activități sau obiective a căror impact este semnificativ pentru funcționarea sistemului sau pentru succesul activității desfășurate. Evaluează potențiale consecințe sau impactul în cazul în care scopul ar fi compromis sau componenta ar fi distrusă. Obiectivele care au o valoare critică ridicată sunt considerate mai valoroase sau mai strategice.

2. Accesibilitate: evaluează cât de ușor poate fi obținut sau afectat un element sau un obiectiv. Acestea ia în considerare factori precum apropierea de potențiale amenințări, măsuri de securitate aplicate și dificultatea de a obține acces la un dispozitiv CPS. Componentele CPS mai accesibile sunt vulnerabile la atacuri cibernetice sau la alte perturbații funcționale. Cele care sunt ușor accesibile sunt considerate mai vulnerabile.

3. Recuperabilitate: măsoară cât de repede poate fi restabilită funcționarea normală a unei componente sau dispozitiv după ce a fost afectat sau atacat. Nu este vorba despre uzura sistematică ci de efectul unui eveniment neașteptat și nedorit. Poate fi considerată și valoarea de reziliență. Elementele cu recuperabilitate redusă pot avea un impact mai mare asupra CPS, necesitând timp îndelungat sau resurse semnificative pentru a se recupera, mărind astfel impactul unui atac.

4. Vulnerabilitate: reprezintă valoarea nivelului de slăbiciune sau valoarea estimată a punctelor slabe ale unui obiectiv sau a unei componente. Acesta ia în considerare factori precum măsurile de securitate, protecția fizică și potențialele vulnerabilități din infrastructura sau sistemele CPS. Elementele cu vulnerabilități ridicate sunt susceptibile la atacuri sau la daune.

5. Consecințe: se estimează consecințele sau efectele impactului potențial pe care l-ar avea un atac asupra CPS. Se atribuie valori a cât de mare ar fi acest incident perturbator asupra elementului sau a activității evaluate. Pot fi analizați factori precum amploarea distrugerii, victime, impact economic, întreruperi de servicii critice etc. Elementele cu cel mai semnificativ efect pot fi ținte preferate pentru amenințări potențiale.

6. Recognoscibilitate: se evaluează capacitatea de identificare corectă sau de detecție a unui element sau a unei activități desfășurată în cadrul sistemului. Cu cât recunoașterea unei componente este mai dificilă, cu atât este mai puțin probabil a fi vizată de amenințări potențiale. În stabilirea unei note (valori) trebuie să se țină cont de: vizibilitatea obiectului evaluat (componentele care sunt ascunse sau greu de identificat au o recunoaștere scăzută), proeminență (elementele care se remarcă mai greu în mediul înconjurător sau într-un anumit context sunt mai puțin evidente și prezintă o recunoaștere mai mică), comportament previzibil (dacă sunt tipare predictibile atunci acțiunea sau comportamentul este ușor de anticipat), măsuri de protecție existente (un element protejat de măsuri de securitate îngreunează recunoașterea lui de către amenințări potențiale), precum și caracteristici distinctive (elementele unice sau cu semnături specifice pot fi mai ușor de recunoscut în comparație cu cele care se aseamănă cu alte elemente din mediul lor).

Exemplu de aplicare a CARVER pentru un CPS:

Ne propunem să analizăm critic vulnerabilitatea și riscul unei rețele IoT pentru CPS, model aplicat sistemului rutier într-un „smart city”. În urma analizei critice a elementelor cheie ale rețelei și nivelurilor de risc asociate CPS-ului, clasificăm elementele identificate pe cele șase criterii de evaluare și obținem:

Examinare critică - elementele critice identificate sunt sistemul de control, centrele de securitate, routere, stâlpi ai rețelei de comunicații, receptoarele senzorilor cu impact semnificativ asupra funcționării globale a CSP-ului. Toate acestea au determinat o valoare de 52010 elemente.

Accesibilitate - analizăm cât de ușor pot fi atinse sau afectate elementele critice. De exemplu stâlpii de comunicații pot fi afectați mai ușor fizic. Funcționarea receptoarele senzorilor poate fi perturbată prin interferențe electromagnetice, de origine naturală sau prin neasigurarea compatibilității electromagnetice. Valoarea cumulată este de 682 de tipuri de evenimente fizice și cibernetice, cu mare impact asupra funcționării CPS-ului.

Recuperabilitate - evaluăm cât de repede se pot recupera elementele critice în urma unui atac sau a unui incident perturbator. De exemplu într-o rețea de comunicații rerutarea permite continuarea funcționării rețelei fără a introduce timpi semnificativi în continuarea funcționării. Se determină un timp total estimat de recuperare de 45 de minute.

Vulnerabilitate - identificăm vulnerabilități specifice fiecărui eveniment pentru interferențe naturale, atacuri fizice și cibernetice. De exemplu valoarea pierderilor pentru un sistem de control este mai mare pentru atacurile cibernetice, putând produce mari pierderi materiale și de vieți umane față de un atac prin tehnici de inginerie socială sau atac fizic. Determinăm o valoare de 620 de vulnerabilități cu mare impact.

Consecințe - analizăm impactul unui atac sau a unui incident asupra fiecărui element critic. De exemplu atacul asupra unui autovehicul în mișcare poate produce pierderi de vieți umane și distrugerea acestuia, cumulate cu alte distrugeri materiale. Valoarea totală a pierderilor materiale o estimăm la 500000 de euro.

Recognoscibilitate - evaluăm elementele de identificare și de recunoaștere a componentelor CPS-ului analizat. Spre exemplu o serie de materiale de publicitate precum stickere cu seria dispozitivelor, flyere, panouri publicitare etc., care conțin date tehnice despre elementele componente oferă suficiente informații pentru recunoașterea componentelor. Determinăm o valoare estimată de 80500 de puncte.

După evaluarea fiecărui element cheie al rețelei IoT a CPS-ului analizat, în funcție de cele șase criterii CARVER, vom avea o imagine clară asupra vulnerabilităților și riscurilor asociate securității CPS-ului. Valoarea cumulată este de: 52010 + 682 + 45 + 620 + 500000 + 80500 = 633857.

Determinăm valorile procentuale (*rotunjite*) pentru fiecare criteriu:

1. 52010 : 633857 x 100 = 8,201 %
2. 682 : 633857 x 100 = 0,101 %
3. 45 : 633857 x 100 = 0,007 %
4. 620 : 633857 x 100 = 0,097 %
5. 500000 : 633857 x 100 = 78,882 %
6. 80500 : 633857 x 100 = 12,701 %

Pe acestea le comparăm cu valorile altor rețele.

Atenție: Trebuie respectat același sistem de evaluare, chiar dacă este o modalitate extrem de subiectivă.

Spre exemplu, pentru rețeaua Internet a aceluiași CPS vom identifica următoarele valori:

1. 8, 302 %; 2. 0,081%; 3. 0,008%; 4. 0,082%; 5. 92,008 %; 6. 9,504%.

Aceste valori le introducem în matricea de decizie astfel:

	C	**A**	**R**	**V**	**E**	**R**	**Suma**
IoT	**8,201**	0,101	**0,007**	0,97	**78,882**	12,701	**100,862**
Internet	8,302	**0,081**	0,008	**0,082**	92,008	**9,504**	109,985

Concluzii:

Observăm că varianta Internet a cumulat un număr estimat mai mare de riscuri și vulnerabilități pentru securitatea rețelei. Însă, la criteriul A (accesibilitate), V (vulnerabilitate) și R (Recognoscibilitate) sunt valori mai mici în comparație cu cele pentru IoT.

Pe baza acestui model se pot face o serie de analize și simulări pentru modificarea valorilor care interesează. În plus, se pot introduce în analiză și alte tipuri de rețele.

După cum observăm evaluarea CARVER a ajutat la prioritizarea obiectivelor și la concertarea resurselor în mod corespunzător pentru îmbunătățirea securității

rețelelor CPS-ului. Pe baza acesteia se pot stabili și dezvolta strategii de securitate și măsurilor urgente pentru protejarea unor componente CPS.

Prin urmare, optimizarea prin metoda CARVER pentru CPS este utilă în următoarele zone de activitate:

Pentru fundamentare în luarea deciziilor: CARVER oferă deciziei utilizatorului o abordare structurată pentru a-și organiza, pe criterii prioritare, obiectivele sale. Evaluând critic vulnerabilitățile identificate în raport cu alți factori, decizia va fi bazată pe alegeri informate în ceea ce privește alocarea resurselor, investițiile în securitate și chiar modalități operaționale. Planificarea răspunsului la incidente, prin identificarea vulnerabilităților potențiale și impactul lor corespunzător asupra componentelor CPS, permite dezvoltarea de planuri de răspuns proactive, inclusiv strategii de izolare, protocoale adecvate de comunicare, proceduri de recuperare, toate fiind adoptate pentru minimalizarea impactului unui incident.

Pentru planificarea scenariului de acțiune: Evaluarea CARVER poate fi utilizată pentru a analiza diferite scenarii de acțiune și impactul potențial al acestora asupra obiectivelor. Luând în considerare diferiți vectori de acțiune și efectele lor corespunzătoare, sistemul poate dezvolta planuri de urgență și strategii de răspuns, adaptate activității cu eficiența maximă.

Pentru stabilirea raportului cost-eficiență: Tehnica CARVER ajută la identificarea obiectivelor cu cel mai mare impact potențial, precum și a vulnerabilităților, permițând sistemului să-și aloce resursele în mod eficient. Prin concentrarea eforturilor pe obiective de mare valoare, cu vulnerabilități semnificative, sistemul își poate optimiza investițiile în mărimi de securitate. Astfel, pot fi identificate și strategiile de diminuare a riscurilor.

Pentru dezvoltarea relațiilor de comunicare și de cooperare: CARVER oferă o variantă de comunicare și un cadru comun pentru realizarea comunicării între diferite părți interesate, implicate în managementul riscurilor. Aceasta facilitează cooperarea între personalul de securitate, factorii de decizie și experții în domeniu, permițând o abordare coordonată și cuprinzătoare a protecției obiectivelor.

Pentru continuarea îmbunătățirii sistemului: Metoda CARVER încurajează monitorizarea ciclului de îmbunătățire continuă prin evaluarea eficienței măsurilor de atenuare și de adaptare a strategiilor. Urmărind schimbările de comportament ale CPS-ului în diverse situații, a progreselor tehnologice sau a vulnerabilităților sistemice,

pot fi făcute ajustări pentru îmbunătățirea protecției la interferențe, precum și pentru reducerea riscurilor. Astfel sunt continuate și celelalte activități antreprenoriale putând fi evaluat potențialul timpului de nefuncționare sau întreruperea proceselor critice în cazul unui incident. Planurile de îmbunătățire și de dezvoltare a afacerii se vor baza pe informații adecvate care vor asigura operațiunile esențiale pentru restabilirea funcționării CPS-ului, în timp util.

În plus, utilizând CARVER se pot încuraja părțile interesate (utilizatori, echipele tehnice, proiectanți etc.) să colaboreze și să se implice în procesul de evaluare a riscurilor. Entități externe, precum agențiile guvernamentale, colegii industriale, entitățile academice și de cercetare etc., pot completa experiența utilizatorilor și perspectivele operatorilor CPS. Acestea pot încorpora observații ale altor profesioniști în securitate, ale experților în domeniu și a altor factori cheie de decizie pentru identificarea celor mai bune soluții în vederea îmbunătățirii sistemelor. Este evident că, pentru a reduce factorii de subiectivism a aceastei metode, pot fi integrate și instrumente de analiză a riscurilor precum tehnicile de analiză SWOT (puncte tari, puncte slabe, oportunități și amenințări), tehnici de analiză cost-beneficiu sau alte metode decizionale cu criterii multiple (MCDA). Simulând ponderi diferite se poate evalua și compara cantitativ importanța relativă a obiectivelor, a vulnerabilităților și a impacturilor potențiale. Toate acestea vor asigura o înțelegere holistică a riscurilor și a potențialelor vulnerabilități, fiind adaptabilă multor sectoare și domenii.

Înțelegând consecințele potențiale și vulnerabilitățile asociate CPS-urilor, toate structurile implicate pot lua decizii bazate pe risc care se aliniază cu toleranța generală la risc și cu priorități antreprenoriale. În acest sens, putem afirma, cu real temei, că optimizarea pentru CPS determină, pe fondul analizei și a atenuării riscurilor de securitate și stabilirea unui cadru normativ adecvat. Acesta, poate fi utilizat pentru dezvoltarea de programe de formare și pentru creșterea gradului de conștientizare a personalului cu privire la riscurile și vulnerabilitățile potențiale. Totodată, permite indivizilor, indiferent de nivelul lor de pregătire profesională, să contribuie la eforturile de gestionare a riscurilor și să rămână vigilenți în identificarea și raportarea unor potențiale amenințări.

Fără a fi exhaustivi, înțelegând ca discuțiile despre CPS sunt încă în forme incipiente privind evoluția lor, prezentăm unele domenii de aplicare a optimizării prin CARVER asupra CPS-urilor:

Securitate cibernetică: Prin CARVER poate fi extinsă evaluarea riscurilor și vulnerabilităților de securitate cibernetică. Principiile metodei ajută la prioritizarea

eforturilor de securitatea cibernetică și la stabilirea unor proceduri de alocare a resurselor pentru protejarea optimă a sistemelor și a datelor critice ale CPS.

Managementul riscurilor în lanțurile de aprovizionare: CARVER poate fi utilizat pentru a evalua și gestiona riscurile din cadrul lanțului de aprovizionare. Evaluând critic, vulnerabilitățile și efectele unor evenimente sau compromisurile în diferite puncte de aprovizionare cu resurse, se pot identifica zonele de risc și pot fi implementate strategii de atenuare pentru a asigura continuitatea și minimalizarea impacturilor potențiale.

Planificarea rezilienței: Evaluarea CARVER oferă informații valoroase asupra rezilienței componentelor CPS. Aceasta ajută la identificarea punctelor slabe, a dependențelor și a potențialelor puncte de eșec, permit dezvoltarea planurilor de reziliență care să se concentreze pe reducerea vulnerabilităților și pe creșterea rapidă a capacității de a se recupera după întreruperi.

Instrument pentru protecția infrastructurilor critice: Tehnica CARVER este utilă în evaluarea riscurilor și a vulnerabilităților în sectoare de infrastructură critică, așa cum sunt cele din domeniile energiei, transporturilor, telecomunicațiilor etc. Astfel pot fi stabilite priorități pentru investiții și pot fi implementate măsuri de protecție pentru serviciile esențiale CPS.

Considerații de securitate regională și globală: Metoda CARVER poate fi adaptată pentru abordarea unor considerente de securitate regională și internațională prin evaluarea riscurilor CPS-urilor de utilitate globală. Înțelegerea contextelor internaționale și a riscurilor specifice facilitează colaborarea și coordonarea acțiunilor internaționale pentru atenuarea riscurilor și pentru asigurarea securității regionale.

Transferul riscurilor și generare de asigurări: CARVER poate sprijini infrastructura CPS pe timpul luării deciziilor în cunoștință de cauză cu privire la transferul riscurilor și a opțiunilor de asigurare. Cuantificând impactul potențial și vulnerabilitățile asociate, utilizatorii pot evalua necesarul de acoperire de asigurare și pot negocia termeni corespunzători pentru atenuarea riscurilor.

Cercetare și dezvoltare: CARVER poate ghida eforturile de cercetare și de dezvoltare a CPS prin identificarea domeniilor în care sunt necesare soluții inovatoare pentru a aborda vulnerabilitățile. Poate informa dezvoltarea de noi tehnologii, procese sau măsuri de securitate pentru a spori protecția și rezistența CPS.

Audituri de conformitate: Metoda poate fi folosită ca instrument pentru efectuarea auditurilor de conformitate pentru asigurarea respectării standardelor de securitate, a reglementărilor și bunelor practici. Aceasta permite utilizatorilor să-și evalueze sistematic practicile de management a riscurilor și să identifice zonele de neconformitate sau zonele de îmbunătățire.

Siguranța publică și planificarea pentru situații de urgență: CARVER poate fi aplicată în scenarii de siguranță publică și de planificare pentru situații de urgență pentru CPS. Astfel se pot dezvolta măsuri de securitate robuste, planuri de evacuare și strategii de răspuns în situații de urgență pentru a proteja siguranța publică.

Evaluarea amenințărilor interne: Metoda poate fi utilizată pentru evaluarea riscului prezentat de amenințările interne, din perspectiva unei persoane malițioase (sabotor, hacker sau oricare altă persoană rău intenționată), din interior. Astfel, la nivelul CPS se pot identifica potențiale vulnerabilități și pot fi implementate măsuri pentru a detecta, descuraja și atenua amenințările interne.

Integrare în comunicarea riscurilor: CARVER poate fi integrată cu strategiile de comunicare a riscurilor pentru a transmite în mod eficient riscurile către părțile interesate. Prin traducerea constatărilor evaluării CARVER în mesaje clare, concise și acționabile, componentele pot facilita înțelegerea, implicarea și sprijinul pentru eforturile de atenuare a riscurilor.

Aplicare în managementul proiectelor: Metoda poate fi aplicată în managementul proiectelor pentru CPS, în scopul evaluării riscurilor asociate, în etape de referință și în produsele livrabile. În contextul unui proiect, utilizatorii pot identifica și aborda în mod proactiv riscurile potențiale, de-a lungul ciclului de viață al proiectului.

Așa cum am observat, versatilitatea și adaptabilitatea CARVER o transformă într-un instrument valoros, în diverse sectoare și domenii în contextul managementul riscului, pentru luarea deciziilor și a strategiilor de atenuare, pentru protejarea activelor, a reputației și a operațiunilor esențiale, împotriva majorității amenințărilor și vulnerabilităților.

Bibliografie suplimentară

1. Edward A. Lee (2015), *The Past, Present and Future of Cyber-Physical Systems: A Focus on Models*, Sensors 2015, 15, 4837-4869; doi:10.3390/s150304837, https://www.mdpi.com/1424-8220/15/3/4837 la data de 03.08.2023
2. Edward Ashford Lee & Sanjit Arunkumar Seshia (2017), *Introduction to Embedded Systems, A Cyber-Physical Systems Approch*, Second Edition, Berkeley University, MIT Press, https://ptolemy.berkeley.edu/books/leeseshia/ la data 03.08.2023

TEMA 7: INTRODUCERE ÎN SECURITATE CIBERNETICĂ - STANDARDE ȘI BUNE PRACTICI. RISCURI ȘI VULNERABILITĂȚI COMUNE

Securitatea cibernetică reprezintă un domeniu al securității informaționale care se concentrează pe protejarea sistemelor informatice, a rețelelor și a datelor împotriva atacurilor cibernetice și a accesului neautorizat. Scopul principal al asigurării securității cibernetice este de a asigura confidențialitate, integritatea și disponibilitatea datelor (a informațiilor digitale) și de a preveni eventualele daune care pot fi generate de atacurile cibernetice.

Securitatea cibernetică pentru CPS reprezintă un domeniu esențial aflat în continuă dezvoltare, deoarece tehnologia evoluează rapid și apar noi tipuri de amenințări. O abordare preventivă și implementarea celor mai bune practici de securitate sunt esențiale pentru a proteja infrastructura critică și pentru a asigura funcționarea sigură și eficientă a sistemelor CPS. Aceasta cuprinde un set de practici, tehnologii și măsuri destinate protejării componentelor cibernetice și fizice, interconectate, care sunt implicate în controlul și monitorizarea proceselor fizice și industriale. Așa cum am văzut până acum, comunicarea și relaționarea între componentele CPS se realizează prin sisteme informaționale și prin rețele de comunicații, toate fiind expuse atacurilor cibernetice. De aceea, managementul riscurilor specifice și atenuarea vulnerabilităților sistemului constituie obiectivul principal al securității cibernetice a CPS-urilor. Accesul neautorizat la sistemele fizice, manipularea datelor sau a comenzilor cibernetice, sabotajul, furtul de date și alte asemenea atacuri pot genera evenimente cu consecințe grave asupra mediului fizic, a personalului care deservește sistemului, a utilizatorilor sau, chiar, a întregului sistem.

Tema prezentă își propune ca să stabilească un cadru conceptual pentru securitate cibernetică aplicată CPS-urilor. Apreciem că, analiza riscurilor și a vulnerabilităților comune va permite unui cititor să înțeleagă necesitatea impunerii unor norme de prevenire a atacurilor cibernetice pentru CPS-uri și pentru protecția personalului, într-o manieră adecvată mediului și componentelor specifice CPS.

7.1. Aspecte generale privind securitatea cibernetică la CPS-uri. Riscuri și vulnerabilități comune

Modalitățile de aplicare a normelor care fundamentează conceptul de securitate cibernetică au ca scop realizarea unei stări confortabile bazate pe percepții de protecție sigură împotriva unor amenințări variate, precum haking-ul, malware-ul, phishing-ul, atacurile DoS (Denial-of-Service), ransonmware, alte tipuri de atacuri cibernetice care pot include și tehnici ale ingineriei sociale. Aceste amenințări pot viza atât elemente de infrastructură cât și indivizi sau componente care asigură guvernarea CPS-ului.

Principalele obiective ale securității cibernetice pentru CPS-uri urmăresc menținerea stărilor de:

1. Confidențialitate: Protejarea datelor împotriva accesului neautorizat și a interceptării datelor de către persoane neautorizate. Criptarea datelor este unul dintre mecanismele folosite pentru a asigura confidențialitatea.

2. Integritate: Reprezintă o stare de asigurare că datele și informațiile nu sunt modificate sau corupte în mod neautorizat. Prin verificarea integrității, se confirmă realitatea că datele nu au fost alterate pe parcursul transmiterii sau stocării lor.

3. Disponibilitate: Este o asigurare că sistemele și serviciile sunt disponibile și funcționează corespunzător, fără întreruperi sau degradări datorate atacurilor cibernetice sau a altor evenimente nefavorabile.

4. Autenticitate: Constă în verificarea identităților utilizatorilor, a dispozitivelor sau a serviciilor pentru a evita accesul neautorizat și pentru a preveni falsificaera identității.

5. Non-repudiere: Reprezintă o asigurare că acțiunea sau tranzacția efectuată nu poate fi negată ulterior de către o entitate implicată, furnizând astfel un nivel de încredere în tranzacții și în comunicări.

6. Reziliența la atacuri: Constă în capacitatea sistemelor și a infrastructurii de a rezista și de a se recupera rapid după un atac cibernetic, pentru a minimaliza impactul și a reveni la o stare normală de funcționare.

Sistemele CPS prezintă o serie de riscuri și vulnerabilități, unele dintra acestea fiind comune cu cele mai întâlnite în alte sisteme informatice și industriale. Însă sunt și unele specifice determinate de specificul interconectării cu lumea fizică și cea digitală.

Dintre acestea enumerăm următoarele riscuri și vulnerabilități comune și frecvente pentru CPS-uri:

1. Atacuri cibernetice: Sistemele CPS pot fi expuse la diverse tipuri de atacuri cibernetice precum atacuri DoS, malware, ransomware, phishing etc. Acestea pot produce oprirea sau degradrea funcționării sistemului, facilitarea accesului neautorizat la date, facilitarea obținerii controlului unor dispozitive fizice etc.

2. Interconectivitate: Interconectarea dintre componentele și dispozitivele CPS poate crea puncte de intrare pentru atacatori. Dacă o singură componentă este compromisă, întregul sistem poate fi afectat.

3. Securitatea dispozitivelor IoT: Frecvent, dispozitivele IoT sunt utilizate în CPS-uri pentru colectarea datelor și pentru controlul proceselor fizice. Aceste dispozitive pot avea adesea vulnerabilități de securitate sau pot fi ușor de compromis.

4. Păstrarea datelor în echipamente vechi sau scoase din uz: Odată cu scoaterea din uz a unor echipamente ciberentice trebuie ca toate datele stocate să fie șterse complet și în mod sigur. Astfel se previne accesul neautorizat la informații sensibile.

5. Lipsa actualizărilor și a patch-urilor de securitate: Unele sisteme CPS (în special cele mai vechi) pot avea dificultăți în a primi actualizări de securitate sau patch-uri. Această situație le face vulnerabile la atacurile bazate pe vulnerabilitățile cunoscute. Actualizarea sistemelor de operare și configurarea lor corectă asigură protecția împotriva vulnerabilităților cunoscute. Sistemele de operare nesecurizate pot fi ușor de exploatat de către atacatori.

6. Gestionarea identității și a accesului: O gestionare defectuaoasă a identității și a accesului poate permite accesul neautorizat la

componentele critice ale CPS-ului sau poate duce la escaladarea privilegiilor neadecvate.

7. Suprasolicitarea și încărcarea rețelelor: Sisteme CPS pot fi supuse la solicitări de uzură în urma unor atacuri de tip DDoS. Acestea pot determina opriri ale sistemului sau deteriorarea funcționării corespunzătoare a componentelor sistemice.

8. Manipularea datelor și a comenzilor: Datele sau comenzile trimise către componentele CPS pot fi interceptate, modificate sau manipulate, ducând la efecte neintenționate sau periculoase în mediul fizic. Astfel, utilizarea programelor și aplicațiilor nesecurizate, a codurilor sursă deschise (open-source), a altor produse cibernetice netestate și neverificate pot determina noi vulnerabilități care să fie utilizate de către atacatori pentru obținerea accesului neautorizat, pentru manipularea datelor și comenzilor către un CPS, în vederea influențării deciziilor și acțiunilor sale. Prin urmare, numai adoptarea unor proceduri critice stabilește un nivel optim de asigurare că datele și comenzile sunt autentice și sigure.

9. Securitate fizică insuficientă: Într-un CPS este esențială protejarea infrastructurii fizice. Dacă nu este restricționat accesul fizic la echipamentele critice, atacatorii pot obține un avantaj nesperat asupra sistemului. Măsurile de securitate fizică reprezintă domeniul altui tip de audit. Însă o securitate fizică ineficientă poate avea efecte la nivelul multor componente, pătrunderea ilegitimă nelimitându-se la deschiderea unei uși sau spargerea unui geam a încăperii cu servere, spre exemplu, ci și la utilizarea multor tehnici care pot generea un atac cibernetic. Pot exista și vulnerabilități hardware determinate de securitatea insuficientă a componentelor cibernetice. Acestea pot fi evitate prin monitorizare sistematică și prin adordări adecvate ale actualizărilor și schimbărilor de componente.

10. Lipsa conștientizării despre nevoia de securitate: Utilizatorii și angajații implicați în operarea CPS-urilor trebuie să fie conștinenți de riscurile de securitate și să respecte politicile de securitate adoptate pentru a evita

atacuri cauzate de neglijență și de erori umane. Oamenii pot reprezenta unul dintre cele mai slabe puncte de securitate în CPS-uri. Atacatorii pot utiliza tehnici de inginerie socială pentru a manipula utilizatorii să dezvăluie informații sensibile sau să compromită securitatea sistemului. Exemplele sunt diverse și extrem de ingenioase. Nu insistăm asupra lor.

11. Amenințările interne: În cadrul unui CPS, riscul apariției unor amenințări cibernetice, neintenționate, din parte personalului intern este o realitate. Implementarea politicilor și a mecanismelor de securitate care să protejeze sistemul împotriva unor astfel de amenințări va minimaliza numărul și tipul riscurilor și a vulnerabilităților specifice.

12. Schimbările de mediu: Sistemele CPS pot fi vulnerabile la schimbările de mediu (fizic sau cibernetic) care nu au fost luate în considerare în proiectarea sau în implementarea inițială a sistemului. În situația în care sunt implicați furnizori sau terți în gestionarea CPS-ului, prin limitarea și controlul accesului acestora, se va preveni accesul neautorizat și protecția față de potențiale amenințări.

Este evident că lista riscurilor și a vulnerabilităților variază în funcție de capabilitățile tehnologice și de destinația CPS-urilor. De reținut este faptul că managementul riscurilor și a vulnerabilităților este un factor crucial pentre menținerea securității sistemului. Pentru aceasta, este necesară o abordare holisitică a securității cibernetice care implică toate aspectele de la proiectare și de dezvoltare, până la operare și mentenanță. Actualizările periodice, monitorizarea activă, evaluările de securitate și educarea personalului sunt doar câteva dintre măsurile care pot fi luate pentu a asigura un nivel adecvat de securitate în cadrul CPS.

7.2. Aspecte esențiale pentru asigurarea securității cibernetice a unui CPS

Securitatea cibernetică pentru un CPS implică o serie de măsuri robuste, tehnice, operaționale și organizaționale pentru a asigura o protecție optimă a acestor sisteme complexe. Implementarea lor este esențială pentru protejarea componentelor și serviciilor critice, pentru evitarea efectelor devastatoare a unor atacuri potențiale. În plus, evaluarea periodică și îmbunătățirea lor continuă va particulariza securitatea

cibernetică a CPS-urilor față de noile amenințări, în funcție de evoluția tehnologiilor implementate în acestea.

Vom enumera câteva măsuri esențiale pentru CPS-uri, după cum urmează:

- Protecție împotriva malware și ransomware: Presupune implementare unor soluții eficiente de securitatea pentru prevenirea, detectarea și eliminarea malware, precum viruși informatici, troieni și alte amenințări software. Ransomware este o amenințare cibernetică gravă în care atacatorii criptează datele și cer o răscumpărarea pentru a le elibera. Pentru a preveni acest tip de atac, trebuie implementate politici de backup corespunzătoare și măsuri de protecție antivirus și antimalware actualizate.

- Separarea rețelelor și a zonelor de securitate: Implementarea zonării spațiilor de securitate și separarea rețelelor de comunicații asigură accesul pentru fiecare segment de rețea la resursele și serviciile necesare. Acest lucru va reduce riscul propagării atacurilor și va izola componentele critice de posibile amenințări. Protejarea canalelor de comunicații între componentele CPS previne interceptarea sau manipularea datelor transmise. În plus, implementarea firewall-urilor contribuie semnificativ la limitarea accesului neautorizat la componente critice și la izolarea eventualelor atacuri.

- Securizarea dispozitivelor IoT: Dispozitivele IoT sunt o componentă esențială a CPS-urilor și, totodată, un punct vulnerabil major, deoarece sunt expuse la internet și pot fi ținte ușoare pentru atacatori. Securitatea acestor dispozitive constă în configurarea corespunzătoare, folosirea parolelor unice, actualizări cu cele mai recente patch-uri de securitate. Monitorizarea traficului generat de aceste dispozitive reprezintă o condiție de detectare a activităților și a comportamentelor suspecte.

- Criptarea datelor, a cheilor și autentificarea prin mai mulți factori: Criptarea cheilor de autentificare și implementarea autentificării prin mai mulți factori (MFA) sunt măsuri care sporesc nivelul de securitate, destinate împiedicării accesului neautorizat. Asigurarea confidențialității datelor transmise între componente astfel încât să poată fi interceptate și utilizate în mod neautorizat reprezintă o măsură critică pentru funcționarea CPS.

- Izolare și monitorizarea dispozitivelor compromise: Detectarea și izolarea rapidă a oricărui dispozitiv compromis sau cu un comportament suspect permite blocarea răspândirii atacurilor și minimalizarea daunelor.

- Reziliență la atacuri, eșecuri și redundanță: Planificarea redundanței pentru componentele critice în situațiile unui atac potențial sau a unui eșec funcțional este o cerință esențială. Astfel se poate trece rapid sau automat pe funcționarea cu sisteme de rezervă, în scopul menținerii continuității operațiunilor. Sistemele CPS trebuie să fie concepute cu un nivel sporit de rezistență la atacuri, precum și de a se recupera rapid și eficient în urma unui incident de securitate. Efectuarea de copii de siguranță a datelor și a configurărilor sistemului ajută la revenirea stării funcționale în cazul unui atac cibernetic sau a unui eveniment neașteptat.

- Protecția împotriva atacurilor fizice: Întrucât CPS implică atât componente fizice cât și cibernetice, securitatea fizică a echipamentelor și a infrastructurii reprezintă un aspect esențial pentru prevenirea accesului neautorizat și pentru deteriorarea fizică a acestora. Pentru aceasta trebuie permis accesul doar persoanelor autorizate. Pentru aceasta, trebuie implementate o serie de măsuri de securitatea fizică, dintre cele mai elementare fiind instalarea de camere de supraveghere și de dispozitive diverse de control al accesului.

- Autentificarea și autorizarea pentru comunicarea între componente, în timp real: Asigurarea că toate componentele comunică între ele, prin rețele protejate, se realizează prin autentificarea adecvată și prin autorizare strictă. Astfel, se împiedică manipularea datelor și a comenzilor automatizate. Se realizează prin implementarea unor mecanisme solide de autentificare pentru verificarea identității utilizatorilor și a dispozitivelor, precum și prin acordarea de privilegii adecvate pentru fiecare entitate. În plus, actualizările de securitate, în timp real, va permite ca CPS-ul să fie, permanent, în măsură să facă față noilor amenințări.

- Managementul incidentelor și recuperarea după atacuri: Managementul incidentelor începe prin identificarea și evaluarea riscurilor asociate CPS-ului evaluat. Acesta implică o analiză detaliată a amenințărilor potențiale, a vulnerabilităților sistemului și a impactului asupra operațiunilor și siguranței. Va fundamenta dezvoltarea unor planuri

detaliate de gestionare a incidentelor pentru a reacționa la atacuri, în timp real, precum și pentru a înțelege natura acestora, precum și pentru a implementa măsuri adecvate corective. Aceste planuri determină întocmirea unor proceduri specifice pentru fiecare componentă CSP. În plus, elaborarea unor planuri de recuperare va ajuta la minimalizarea impactului atacurilor.

- Monitorizarea constantă a amenințărilor și actualizarea politicilor de securitate: Securitatea cibernetică nu este o abordare de tip „set and forget". Informarea curentă despre cele mai recente amenințări cibernetice și actualizarea continuă a politicilor de securitate reprezintă condiții critice pentru adaptarea sistemului la noile tactici de atac din mediile fizic și cibernetic. Implementarea soluțiilor de detecție a intruziunilor și de gestionare a evenimentelor de securitatea va permite detectarea rapidă a comportamentelor anormale și va detecta, în timp real, indicii de recunoaștere a unui atac. Asigurarea că toate componentele CPS sunt actualizate cu cele mai recente patch-uri de securitate contribuie esențial la remedierea vulnerabilităților identificate. Totodată, se impune și menținerea personalului la curent cu cele mai noi tehnologii și practici de securitate.

- Testarea robustă a securității: Se realizează prin efectuarea testelor ample de securitate precum teste de penetrare (pentru identificarea vulnerabilităților sistemului) și teste de rezistență la atacuri (pentru evaluarea capacității sistemului de a face față unor atacuri avansate). Efectuarea periodică a testelor de penetrare, în scopul evaluării rezistenței la atacuri cibernetice, implică angajarea de experți în securitate cibernetică pentru evaluarea sistemelor. În plus, monitorizarea și detectarea amenințărilor prin utilizarea de sisteme de monitorizare a comportamentelor anormale sau a posibilelor atacuri și notificarea rapidă a administratorilor, pentru a interveni rapid, reprezintă o măsură eficientă pentru descurajarea atacurilor și pentru creșterea securității CPS.

- Educație, formare și conștientizarea utilizatorilor: Atât personalul care deservește sistemul cât și utilizatorii trebuie să fie conștienți de riscurile de securitate specifice. Aceștia trebuie să fie instruiți în privința practicilor sigure de utilizare a CPS-ului. Astfel, se va forma o cultură solidă de securitate cibernetică unde toți utilizatorii și angajații sunt

conștienți de riscurile și de practicile sigure pentru prevenirea atacurilor și pentru reziliența sistemului.

- Conformitate cu standardele și cu reglementările în vigoare: Asigurarea că sistemul CPS respectă toate standardele de securitate relevante și reglementările privind protecția datelor și de securitate cibernetică îi va proteja personalul și utilizatorii CPS-ului atât împotriva distrugerilor și pagubelor potențiale, în urma unui atac, cât și în fața răspunderii managerilor pentru neaplicarea lor de către utilizatori. Pentru aceasta este necesară realizarea unui audit periodic pentru evaluarea nivelului de securitate și de conformitatea cu standardele și cu alte reglementările relevante.

- Colaborarea între industrie și cercetare: Pentru a răspunde la amenințările cibernetice, în continuă evoluție, este important ca industria și mediile de cercetare, academic și de producție, să colaboreze și să împărtășească informații cu privire la noile tipuri de atacuri și de tehnologii de securitate. Această colaborare va permite managerilor să identifice și o serie de criterii care le va permite dezvoltarea planurilor de continuare a afacerii, pentru a asigura recuperarea și eficiența CPS-urilor în cazul unor atacuri sau a unor evenimente nedorite. Proiectarea securizată a unui CPS reprezintă o cerință primordială încă din fazele proiectării sistemului. Aceasta presupune, printre altele, separarea logică a funcțiilor critice, implementarea protecției datelor și a canalelor de comunicații securizate, precum și folosirea unor protocoale standardizate de securitate.

Conchidem prin observația că abordările de securitatea cibernetică pentru CPS trebuie să fie continuă, iar planurile și politicile de securitate să fie actualizate în mod regulat pentru a face față noilor amenințări și evoluții tehnologice. Prin combinarea unor măsuri tehnice și operaționale eficiente, se pot minimaliza riscurile și se va putea asigura că sistemul CPS funcționează în mod sigur și eficient.

Securitatea cibernetică pentru CPS este o responsabilitate complexă și un efort continuu și de durată de evaluare, adaptare și îmbunătățire a măsurilor de securitate, pentru a face față amenințărilor în schimbare. Aceasta, se realizează prin abordări proactive și actualizări permanente a măsurilor adecvate CSP-urilor. În plus, formarea și promovarea unei culturi de securitate cibernetică va contribui esențial acestui deziderat, care se va concretiza în măsuri adecvate pentru minimalizarea riscurilor și protecția CPS-urilor împotriva amenințărilor cibernetice.

7.3. Standarde și bune practici pentru securitate cibernetică cu impact asupra domeniilor de utilizare a CPS-urilor

În ce privește securitatea cibernetică pentru CPS-uri există mai multe standarde și cadre normative de lucru, dezvoltate de organizații internaționale și naționale, pentru a asigura protecția și integrarea sistemelor CPS în activitățile vieții cotidiene. În plus, la nivelul organizațiilor pot fi adoptate ghiduri și seturi de bune practici personalizate la nevoile sistemelor sau componentelor specifice sistemelor lor. Acesta, pentru că, așa cum am precizat anterior, securitatea cibernetică trebuie să fie considerată o preocupare prioritară pentru toți implicați în domeniul CPS, de la proiectanți și dezvoltatori la administratori și utilizatorii finali.

Enumerăm câteva dintre cele mai relevante **standarde internaționale** pentru securitatea CPS, prezentate în ordine alfabetică:

ANSI/ISA-95: este un standard al Institutului Național American pentru Standardizare (ANSI) și al Societății Internaționale de Automatizare (ISA). Acesta oferă o abordare integrată pentru interoperabilitatea CPS și acoperă aspecte de securitate cibernetică;

CSA CCS 9001: este un stndard al Asociației pentru Securitate Cibernetică (CSA) care propune cerințe de management al securității cibernetice pentru CPS;

ENISA SPSO: este un ghid al Agenției Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) privind scuritatea cibernetică pentru CPS;

IEC 61508: este un standard internațional pentru sistemele de securitate funcțională, cre poate fi adaptat și aplicat pentru a evalua și asigura securitatea CPS;

IEC 62407: este un standard care specifică cerințele pentru securitatea rețelelor de comunicații industriale, inclusiv în domeniul CPS;

IEC 62443: cuprinde o serie de standarde dezvoltate de Comitetul Electrotehnic Internațional (IEC) pentru securitatea rețelelor de comunicații industiale și a sistemelor de control. Acest set de standarde includ ghiduri și recomandări pentru identificarea și cotracararea amenințărilor cibernetice în mediul CPS;

IIC (Industrial Internet Consortium Security Framwork): IIC dezvoltă un cadru de securitate pentru CPS și sisteme industriale. Cuprinde ghiduri și bune

practici recomandate pentru identificarea, evaluarea și atenuarea riscurilor de securitate cibernetică. IIC SMM (Security Maturity Model) este un model matur de cadru de evaluare și de îmbunătățire a securității sistemelor CPS;

ISA/IEC 62443-4: este un standard care cuprinde cerințe pentru securitatea tehnică a sistemelor CPS. Oferă recomandări pentru inginerii de sistem, dezvoltatori și administrtori.

ISO/IEC 15408: este cunoscut și sub denumirea de Evaluare și Certificare Comună a Securității. Acest standard oferă un cadru pentru evaluarea și certificarea securității produselor și sistemelor IT, inclusiv CPS;

ISO/IEC 21878: este un standard care definește termenii și conceptele de bază pentru CPS, inclusiv a celor care privesc securitatea cibernetică;

ISO/IEC 27001: este o normă internațională care stabilește cerințele pentru implementara unui Sistem de Management al Securității Informației (SMSI). Deși nu specifică domeniul CPS, multe dintre principiile și practicile sale pot fi aplicate și în domeniul securității CPS;

ISO/IEC 27005: este un standard internațional care oferă cadru pentru gestionarea riscurilor de securitate a informațiilor, inclusiv pentru CPS;

ISO/IEC 30111: este un standard care cuprinde cerințe pentru diseminarea informațiilor privind vulnerabilitățile se securitate și furnizează direcții pentru raportarea responsabilă a acestora. Totodată, oferă linii directoare pentru furnizarea asistenței post-exploatare și atenuarea vulnerabilităților pentru produsele software și hardware;

NIST SP 800-160: este un ghid special al Institutul Național de Standarde și Tehnologie (NIST) din SUA. Oferă principii de proiectare a securității cibernetice pentru CPS;

NIST SP 800-53: este un ghid al NIST care oferă o colecție de măsuri de control și de securitate pentru sistemele informatice. Pot fi aplicate și în contextul CPS;

NIST SP 800-82: este un ghid dezvoltat de NIST care propune măsuri pentru protejarea sistemelor industriale și de automatizare, inclusiv CPS, împotriva amenințărilor cibernetice;

NISTIR 8183: este o pubicație specială a NIST care oferă un cadru specific pentru securitatea CPS. Nist Framework for Cyber-Physical Systems abordează probleme precum securitatea datelor, protecția integrității sistemului și reacția la incidente cibernetice;

NISTIR 8228: este o publicație specială a NIST care oferă orientări pentru selecția caracteristicilor și a controalelor de securitate pentru protecția CSP;

UL 2900: este un standard dezvoltat de Laboratoarele Underwriters (UL) și stabilește cerințe de securitate cibernetică pentru echipamente și rețele conectate, inclusiv CPS;

P8 TA(2017) 0051 – Normele de drept civil privind robotica – Rezoluția Parlamentului European din 16.02.2017. Acesta conține recomandări adresate Comisiei, referitoare la normele de drept civil privind robotica (2015/2103, INL), în urma evaluării aspectele etice ale sistemelor ciber-fizice (Ethical Aspects of Cyber-Physical Systems). Studiul este efectuat în numele Comitetului pentru Evaluarea opțiunilor științifice și tehnologice (STOA) din cadrul Parlamentului și gestionat de Unitatea de Prospecivă Științifică (STOA) și Direcția Generală Servicii de cercetare parlamentară.

Este important să reamintim că, în funcție de regiune sau de țară, pot exista și alte standarde locale sau sectoriale, relevante pentru securitatea CPS. De asemenea, având în vedere rapiditatea evoluției tehnologice și a amenințătilor cibernetice, este vital să se păstreze actualizate informațiile despre reglementările în domeniu și să se adopte cele mai bune practici pentru asigurarea unei securități eficiente a CPS-urilor.

În Uniunea Europeană, Agenția Uniunii Europene pentru Securitatea Cibernetică (ENISA), încă de la înființare (2004) a elaborat și propus o serie de norme și de bune practici pentru consolidarea politicii cibernetice a UE și pentru îmbunătățirea fiabilității produselor, a serviciilor și a proceselor TIC. Prin schimbul de cunoștințe și prin ample campanii de sensibilizare, ENISA a sporit încrederea în economia conectată, în scopul sporirii rezistenței infrastructurii Uniunii și pentru a asigura securitatea digitală a societății europene și a cetățenilor săi.

În anul 2023, ENISA a realizat și publicat un set de rapoarte care vizează sporirea securității cibernetice la nivelul UE. Dintre acestea, enumerăm pe cele publicte în acest an:

- Papaphilippou, M., Moulinos, K. & Theocharidou, M., *Good Practices for Supply Chain Cybersecurity* (Bune practici pentru fluxurile esențiale de securitate cibernetică), iunie 2023, în care sunt abordate relațiile esențiale și entitățile importante cu impact direct asupra aprovizionării directe și asupra serviciilor furnizorilor operate pentru infrastructuri critice.

- Ntalampiras, S., Misuraca, G. & Rossel, P., *Artificial Intelligence and Cybersecurity Research, ENISA Research and Innovation Brief* (Studii de inteligență artificială și securitate cibernetică), iunie 2023, în care sunt abordate aspecte ale unor concepte cheie ale inteligenței artificiale și perspectivele apelării la aceasta pentru dezvoltarea industriilor europene. Raportul cuprinde un exemplu (studiu de caz) privind implicațiile utilizării CPS și securitatea cibernetică.

- Mattiolii, R., Malatras, A., Hunter, E.N., Penso, M.G.B., Betram, D., Neubert, I., *Identifying Emerging Cyber Security Threats and Challenges for 2030* (Identificarea amenințărilor emergente de securitatea cibernetică și provocări pentru 2030), martie 2023, în care sunt propuse o serie de modele și de scenarii pentru securitatea cibernetică aplicată diverselor domenii a infrastructurilor emergente.

- Theocharidou, M., Stanic, Z., Drougkas, A., Figueiredo R.D-S., Tsekmezoglou, E., Naydenov, R., Lella, I., Malatras, A., *ENISA Threat Landscape: Transport Sector* (ENISA, Sectorul amenințărilor pentru transporturi), martie 2023, care dezvoltă o analiză a amenințărilor cibernetice și a incidentelor specifice sectorului transporturilor, pentru perioada ianuarie 2021 – octombrie 2022.

- Polemi, N., Praca, I., *A multilayer framework for good cybersecutity practices for AI* (Cadru multistrat de bune practici a securității cibernetice pentru AI), iunie 2023, în care sunt prezentate rezultatele unei analize pe trei straturi (1. Fundamentul securității cibernetice, 2. Fundamentele AI și ale securității cibernetice, 3. Bune practici pentru sectorul specific de securitate cibernetică) și o serie de concluzii și propuneri de urmat, pentru creare de standarde și alte proiecte în acest domeniu.

Pentru CPS-uri, **nu trebuie omis,** efortul Parlamentului UE de a consolida legislația privind securitatea cibernetică în vigoare, ca urmare a adoptării a Directivei

privind securitatea rețelelor și informațiilor 2 (NIS2), în ianuarie 2023. Aceasta se bazează pe directiva existentă a UE NIS și solicită statelor membre să adopte o reglementare mai strictă în materie de securitatea cibernetică, susținută de o aplicare mai dură și îi vizează, în special, pe operatorii de infrastructuri industriale critice. Aceasta, oferă oportunitatea de a evalua capabilitățile și operațiunile în raport cu cerințele consolidate de securitate cibernetică, reprezentând și un semnal de alarmă pentru îmbunătățirea capacităților cibernetice a operatorilor care nu și le-au îmbunătățit până la acest moment.

În România, se fac pași mici către alinierea cu legislația europeană cu standardele și bunele practici internaționale. Astfel, denumirea de Cyber-Physical Systems apare în *Anexa la Hotărârea Guvernului nr. 492/2019 pentru aprobarea Strategiei 5G pentru România*, din 20.06.2019 (Mof I nr. 551/04.07.2019), unde se precizează că, împreună cu IoT contribuie la dezvoltarea productivității prin digitalizarea industriei manufacturiere.

În Anexa la Hotărârea Guvernului nr.1/086/2022 pentru aprobarea Strategiei naționale privind sistemele de transport inteligent pentru perioada 2022-2030, din 31.08.2022 (Mof.I. nr. 867/02.09.2022), nu se face referire directă la CPS dar din prezentare se pot înțelege unele reglementări privind abordarea întrunită a problematicii legate de securitatea fizică și cibernetică pentru echipamentele și sistemele tehnice. Aceasta stabilește cadrul tehnic și organizațional pentru implemetarea schemelor de certificare și pentru acreditarea privind securitatea cibernetică în cazul C-ITS.

Mai pot fi identificate o serie de articole și trimiteri care reglementează aspecte de comportament a componentelor CSP, fără a le denumi așa. Astfel de norme putem găsi în:

Pentru domeniul securității cibernetice:

Anexele nr. 1 și 2 l Hotărârea nr. 1.321/2021 privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, din 30.12.2021 (Mof.I. nr. 2/03.01.2022), care publică Strategia în domeniul securității cibernetice pentru România.

Legea 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative (Mof I nr. 214/15.03.2023),

unde sunt precizate modul de organizare a sistemului național de securitate cibernetică, organizarea managementului incidentelor de securitate cibernetică, precum și modul de cooperare în domeniul securității și apărării cibernetice.

Legea 11/2022 pentru aprobarea Ordonanței de urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică (Mof.I. nr. 25/07.01.2022), prin care DNSC primește responsabilități privind securitatea cibernetică a spațiului cibernetic național civil, componentă a securității naționale.

Legea 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate (Mof.I. 752/27.07.2022), în care se stabilește obligativitatea autorităților și instituțiilor publice, a persoanelor juridice, precum și a persoanelor care exercită profesii liberale să închei un contract de schimb de date cu asigurarea protecției datelor cu caracter personal și a securității cibernetice.

Legea 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice (Mof.I. nr. 21/09.01.2019), cu regementări privind cooperare DNSC cu ENISA privind intervenția la incidente de securitate cibernetică.

Legea energiei electrice și a gazelor naturale nr. 123/2012 (Mof.I. nr. 485/16.07.2021) în care sunt reglemetări privind siguranța fizică sau securitatea persoanelor, a aparatelor sau a instalațiilor ori integritatea sistemului, operatorului de transport și de sistem în fața unor meninţări generate de o criză neașteptată pe piața de gaze naturale.

OUG nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică (Mof I nr. 918/24.09.2021), unde sunt stabilite responsabilități privind evaluarea securității cibernetice a noilor tehnologii, precum și pentru educarea și pregătirea în domeniul securității cibernetice.

OUG nr. 49/2019 privind activitățile de transport alternativ cu autoturism și conducător auto (Mof.I. nr. 537/01.07.2019) care prevede proceduri de a obține avizul tehnic, în funcție de metodele și procedurile de asigurare a securității cibernetice și protecția datelor.

OUG nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și

instituțiile publice (Mof.I. nr. 638/28.06.2022), în care sunt reglementați termenii de risc de securitate cibernetică și vulnerabilități în spațiul cibernetic, stabilind că STS asigură securitatea cibernetică a serviciilor și a sistemelor informatice proprii din Cloudul privat guvernamental.

Metodologia de identificare a infrastructurilor critice naționale din sectorul tehnologia informației și comunicații din 23.03.2012, parte a Ordinului 213/2012 (Mof.I. 352/24.05.2012), în care Ministerul Comunicațiilor și Societății Informaționale stabilește ca servicii esențiale pe cele destinate managementului incidentelor de securitate cibernetică.

Metodologia de stabilire a efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale, din 21.06.2019 (Mof.I. nr. 590/18.07.2019), în care MCSI stabilește responsabilități pentru asigurarea disponibilității serviciilor furnizate prin mijloace alternative, chiar și în cazul unor incidente de securitate cibernetică.

Norme privind procedura de acordare/retragere a avizului tehnic pentru platformele digitale de transport alternativ cu autoturism și conducător auto, din 27.10.2020 (Mof.I. nr. 1018/02.11.2020), în care Autoritatea pentru Digitalizarea României (ADR) stabilește că avizul tehnic necesită implementarea de metode și proceduri adecvate de asigurare a securității cibernetice și de protecție a datelor.

Norme tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicate operatorilor de servicii esențiale, din 09.11.2020 (Mof.I. nr. 1142/26.11.2020), în care SGG stabilește un set de măsuri de gestionare a crizelor în caz de incidente de securitate cibernetică pentru asigurarea continuității activității organizațiilor.

Normele privind autorizarea și verificarea furnizorilor de servicii de formare pentru securitate cibernetică, din 14.10.2022, elaborare de DNSC, parte integrantă a Ordinului 106/2022, în care sunt reglementări privind autorizarea furnizorilor de servicii de formare, despre formarea și furnizarea serviciilor de formare pentru securitate cibernetică, despre verificarea activităților specifice, precum și despre organizarea și desfășurarea examenului/evaluării în domeniul auditului de securitate cibernetică.

Norme privind interferențele dintre securitatea nucleară, securitatea radiologică, protecția fizică, protecția împotriva amenințărilor cibernetice și controlul de garanții nucleare, din 03.12.2019 (Mof.I. nr. 989/09.12.2019), în care Comisia Națională pentru Controlul Activităților Nucleare (CNCAN) stabilește cerințele privind interferențele între aceste domenii, specificând modul în care acestea vor fi gestionate.

Principalele instituții și autorități din România cu atribuții specifice în ce privește reglementarea domeniului CPS sunt:

1. Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM). Are rolul de a reglementa și supraveghea domeniul comunicațiilor electronice, inclusiv aspecte legate de securitatea cibernetică și de protecția infrastructurilor critice, care sunt de interes în domeniul CPS;

2. Autoritatea Națională pentru Protecția Consumatorilor (ANPC): Are atribuții în domeniul securității produselor și echipamentelor comercializate în România. Acest aspect poate fi important în contextul CPS deoarece implică integrarea tehnologiilor electronice și fizice;

3. Autoritatea de Supraveghere Financiară (ASF): Are rolul de a reglementa și supraveghea domeniul asigurărilor și al pieței financiare care poate include aspecte legate de tehnologiile utilizate în industria asigurărilor și a serviciilor financiare, ce pot fi conectate la CPS;

4. Autoritatea Națională pentru Protecția Datelor cu Caracter Personal (ANSPDCP): Este autoritatea cu misiunea de a proteja drepturile și libertățile fundamanteale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal. În contextul CPS, protecția datelor personale poate fi o preocupare importantă având în vedere volumul mare de date colectate și procesate;

5. Ministerul Transporturilor, Infrastructurii și Comunicațiilor: Acest minister are competențe în reglementarea și dezvoltarea infrastructurii critice precum transporturile și telecomunicațiile. Parte din tehnologiile aferente sunt implementate în CPS-uri.

Este important de menționat că, datorită complexității și interdisciplinarității domeniului CPS, nu există în prezent o instituție direct responsabilă cu acesta. De aceea, cooperarea între diferitele organisme, autorități și agenții este crucială pentru identificarea abordărilor corespunzătoare a provocărilor specifice în vederea dezvoltării continue a industriei și a economiilor conexe. De asemenea, în perioada imediată și viitoare, vor apărea noi dezvoltări și reglementări în domniul CPS, în România și în UE, așa că este important să se țină cont de actualizările ulterioare, din surse oficiale.

Suntem convinși că întregul sistem legislativ, național, european și internațional va evolua și se va adapta continuu pentru a indentifica și aplica cele mai bune soluții în vederea reducerii decalajului decizional, pentru asigurarea condițiilor celor mai bune pentru securitatea fizică și cibernetică a cetățenilor, precum și pentru menținerea condițiilor echitabile pentru întreprinderi, în vederea dezvoltării economice a tuturor țărilor.

Recomandăm, ca bibliografie suplimentară, consultarea tuturor reperelor normative prezentate în capitolul 7.3., urmând ca, o dată cu actualizarea acestora și apariția altor publicații, cunoștințele dobândite să fie actualizate și să se identifice eventualele schimbări ale strategiilor și politicilor care abordează sistemele CPS

TEMA 8: EVALUAREA ȘI MANAGEMENTUL RISCURILOR - SOLUȚII DE SECURITATE CIBERNETICĂ SPECIFICE

Evaluarea și managementul riscurilor în sistemele ciber-fizice sunt servicii esențiale pentru asigurarea funcționării sigure și eficiente a acestora. Așa cum am văzut, CPS-urile sunt sisteme în care componentele de procesare a datelor sunt integrate în rețele de comunicații și asigură interacțiunea cu sistemele fizice pentru a îndeplini o anumită funcționalitate.

În general, evaluarea și managementul riscurilor pentru CPS-uri sunt procese complexe și continue care implică evaluarea și reducerea riscurilor, implementarea măsurilor de protecție și monitorizarea constantă a sistemelor pentru a asigura funcționarea lor sigură și fiabilă.

8.1. Metodologie de evaluare și gestionare a riscurilor de securitate pentru CPS-uri

Gestionarea riscurilor pentru CPS-uri reprezintă o funcție importantă a acestora care necesită o abordare multidisciplinară, precum și colaborare și conștientizare din partea utilizatorilor. Prin implementarea măsurilor adecvate, prevenție și răspuns la incidente, CPS-ul poate fi certificat că funcționează în mod sigur, fiabil și eficient, minimalizând impactul riscurilor asupra utilizatorilor și a mediului înconjurător.

În prezentarea noastră vom propune o serie de pași importanți pentru evaluarea și managementul riscurilor CPS-urilor urmând ca, ulterior, să dezvoltăm acele aspete esențiale pentru înțelegerea valorii lor critice în funcționarea CPS-urilor în condiții de securitate cibernetică într-un mediu caracterizat de provocări multiple și complexe.

Pentru aceasta ar trebui respectată următoarea metodologie de evaluare:

1. Identificarea riscurilor: În primul rând, trebuie să se identifice toate riscurile potențiale pentru CPS, în cadrul sistemului. Aceasta poate fi realizată printr-o analiză atentă a tuturor componentelor și a interacțiunilor dintre ele. Riscurile pot include atacuri cibernetice, erori de programare, defecțiuni ale componentelor, condiții de mediu nefavorabile etc.

2. Evaluarea probabilității de producere a evenimentelor și evaluarea impactului estimat: După identificarea riscurilor, următorul pas este să se evalueze probabilitte ca acestea să apară și impactul pe care îl vor avea asupra sistemului și a mediului înconjurător. Această evaluare poate fi efectuată folosid metode analitice, simulări sau, chiar, prin observații bazate pe experiența în domeniu.

3. Definirea măsurilor de reduce a riscurilor: După ce riscurile sunt cunoscute, trebuie luate măsuri pentru a le reduce, până la un nivel acceptabil. Acest lucru poate include îmbunătățirea securității cibernetice, testarea riguroasă a sistemului, reducerea redundanțelor, utilizarea tehnicilor de criptare și de autentificare etc. În plus, pot fi necesare actualizări periodice software și modernizarea componentelor hardware pentru a rezista la noile amenințări cibernetice și fizice.

4. Implementarea și monitorizarea măsurilor de securitate: Odată ce măsurile de reducere a riscurilor au fost definite, ele trebuie implementate și monitorizate constant pentru a se asigura că sunt eficiente și că sistemul este protejat în mod corespunzător.

5. Reevaluarea periodică a riscurilor: Mediul în care operează CPS-urile poate suferi schimbări, ceea ce poate duce la apariția de noi riscuri sau la modificarea importanței celor existente. Prin urmare, este important ca evaluarea riscurilor să fie un proces continuu, cu reevaluări periodice pentru a menține securitatea și integritatea CPS-ului.

6. Reziliența și planificarea de urgență: În ciuda tuturor măsurilor de gestionare a riscurilor, nu pot fi eliminate complet posibilitățile de apariție a unui incident din necunoscut. Prin urmare, este important să se planifice strategii de reziliență și planuri de urgență astfel încât să se poată reacționa rapid și eficient la un eveniment neprevăzut.

Cele prezentate sunt etape generale care, în funcție de complexitatea și de aploarea CPS-ului pot fi completate cu secvențe suplimentare precum:

- Ierarhizarea și prioritizarea riscurilor: Nu toate riscurile sunt egale sub aspectul efectelor pe care le pot genera așa că, este important să

se ierarhizeze și să prioritizeze, în funcție de probabilitatea apariției și de impactul lor asupra sistemului. Astfel, pot fi alocate corespunzător resursele pentru a aborda cele mai critice riscuri, în regim prioritar.

- Rezolvarea rapidă a vulnerabilităților: Atunci când sunt identificate vulnerabilități sau probleme de securitate, acestea ar trebui abordate rapid și eficient pentru a reduce expunerea la riscuri. În cazul în care se descoperă vulnerabilități critice, ar trebui luate măsuri imediate de remediere, chiar și prin întreruperea temporară a funcționării sistemului pentru a preveni atacuri potențiale.

- Audit de securitate și revizii periodice: În paralel cu monitorizarea permanentă, auditul de securitate și reviziile periodice pot aduce o perspectivă obiectivă asupra sistemului și pot identifica posibile probleme sau erori ce pot fi ignorate, în mod normal. Aceste revizii ar trebui să fie efectuate de specialiști în securitate cibernetică și de experți în CPS.

- Protecție împoriva amenințărilor emergente: Tehnologia și mediul cibernetic evoluează rapid, iar noi genuri de amenințări pot apărea în mod constant. De aceea, este esențial ca evaluarea și managementul riscurilor să fie flexibile și să se adapteze la noile provocări. O abordare reactivă și proactivă este necesară pentru a proteja în mod corespunzător sistemele CPS față de aceste amenințări emergente.

- Adoptarea cerințelor și intereselor relevante din partea utilizatorilor: CPS-urile pot avea o varietate de utilizatori cu interese multiple. Implicarea utilizatorilor în procesul de evaluare și în managementul riscurilor poate aduce noi perspective de identificare a riscurilor, aspecte pe care proiectanții și dezvoltatorii sistemelor nu le-ar fi luat în considerare.

Obiectivele esențiale acestor funcțiilor de gestionare a riscurilor sistemice sunt:

1. *Asigurarea integrității și autenticității datelor*: În CPS-uri, datele colectate și procesate sunt esențiale pentru luarea deciziilor corecte și pentru funcționarea corespunzătoare a sistemului. Este crucial să

se asigure integritatea și autenticitatea acestor date pentru a preveni manipularea sau modificarea lor de către actorii rău intenționați;

2. *Securitata comunicațiilor*: Componenta cibernetică a CPS-ului implică comunicarea între dispozitive, senzori și sisteme de control. Securitatea comunicațiilor este o funcție critică pentru a proteja CPS-ul împotriva interceptării neautorizate a datelor, împotriva atacurilor de tip „man-in-the middle" sau a altor tipuri de atacuri cibernetice care pot afecta integritatea și confidențialitatea informațiilor transmise;

3. *Gestionarea vulnerabilităților terțelor părți*: În multe scenarii, CPS-urile implică integrarea componentelor software și hardware în relații cu terțe părți. Este important să se evalueze și să se gestioneze riscurile asociate cu aceste componente externe prin verificarea regulată a actualizărilor de securitate și a respectării standardelor de securitate de la furnizori;

4. *Resursele fizice și umane*: În evaluarea riscurilor nu trebuie neglijate și aspectele legate de resursele fizice și umane. Riscurile fizice pot apărea din cauza neutilizării necorespunzătoare sau a uzurii premature a echipamentelor fizice, iar riscurile umane din erorile de operare a sistemului. Astfel, instruirea corespunzătoare a personalului și întreținerea regulată a echipamentelor pot contribui la reducerea acestor riscuri;

5. *Planificarea continuității activității*: Chiar dacă denumirea de afacere ne sugerează obținerea unui rezultat bun, planificarea continuității funcționării CPS evită un dezastru în situația apariției unui incident de securitate. Aceasta poate implica, spre exemplu, utilizarea redundanțelor sau a unor evenimente alternative de backup, mai ales pentru situațiile critice;

6. *Crearea unei culturi a securității pentru CPS*: Pentru a aborda în mod corespunzător riscurile în CPS trebuie să existe o cultură a securității încorporată în organizația responsabilă cu exploatarea sistemului. Toți cei implicați trebuie să înțeleagă importanța securității și să fie responsabili pentru respectarea măsurilor și a politicilor de securitate adoptate, specifice CPS-ului în cauză.

Prin aplicarea unei abordări comprehensive și actualizate care presupun un cadru normativ specific și proceduri de protecție a componentelor CPS se poate asigura funcționarea sigură și eficientă a sistemului, într-un mediu în continuă schimbare. Pentru aceasta trebuie să se urmărească următoarele aspecte:

1. *Stimularea colaborării și menținerea comunicării*: Pentru a aborda riscurile într-un mod holistic și eficient este esențială o colaborare strânsă între toți cei implicați în proiectarea, implementarea, operarea și exploatarea sistemului. Comunicarea deschisă între echipele de ingineri, specialiștii în securitate cibernetică și fizică și utilizatori poate contribui semnificativ la identificarea și soluționarea potențialelor vulnerabilități.

2. *Testarea componentelor și simularea incidentelor*: Testarea și simularea riguroasă în CPS pot ajuta la identificarea potențialelor probleme și a riscurilor într-un mediu controlat. Aceste teste pot include teste de securitate, teste cu scenarii de risc, stimularea situațiilor de urgență etc., toate fiind metode de evaluare a reacției sistemului în situații critice;

3. *Gestionarea datelor și asigurarea confidențialității*: CPS-ul implică culegerea, prelucrarea și manipularea datelor sensibile. Prin urmare, este importnt să se implementeze măsuri de securitate pentru protejarea datelor și a confidențialității utilizatorilor. Utilizarea tehnologiilor de criptare, protejarea accesului la date și aplicarea politicilor de gestionare a datelor pot ajuta la minimalizarea riscurilor asociate cu trasferul defectuos a datelor;

4. *Conformitatea cu regelmentările și standardele de securitate*: CPS trebuie să respecte reglementările și standardele relevante în materie de securitate, sănătate umană și protecția datelor. Respectarea acestor reglementări este esențială pentru evitarea consecințelor juridice și pentru asigurarea unui nivel adecvat de securitate;

5. *Monitorizarea permanentă și actualizări*: Sistemele CPS trebuie să fie monitorizate în mod constant pentru a idntifica evantualele incidente sau încercări de atac. În plus, actualizările regulate, software și hardware, sunt cruciale pentru a aborda noile amenințări și vulnerabilități care pot apărea în timp;

6. *Educație și conștientizare*: Conștientizarea privind riscurile de securitate și educarea utilizatorilor și a personalului implicat în exploatarea CPS-urilor sunt elemente cheie pentru prevenirea incidentelor și a erorilor umane care pot conduce la riscuri suplimentare. Utilizatorii trebuie să fie informați cu privire la practicile de securitate și să fie instruiți cu privire la modul corect de utilizare a sistemelor;

7. *Existența planurilor de recuperare în caz de incidente*: Chiar și prin aplicarea celor mai bune măsuri de prevenire pot apărea incidente de securitate sau situații de urgență. De aceea, este important să se dezvolte și să se testeze planuri de recuperare în caz de dezastre, astfel încât să se poată răspunde rapid și eficient la astfel de evenimente.

8.2. Înțelegerea conceptelor de confidențialitate, integritate și disponibilitate a datelor. Tehnici de aplicare

Ușor se poate observa că la baza unei culturi de securitate pentru CPS-uri, care cuprinde aspecte de securitate fizică și cibernetică, se situează înțelegerea de către utilizatori și de către tot personalul implicat în domeniul CPS-urilor a modalităților de aplicare a conceptelor de confidențialitate, integritate și disponibilitate. Acestea sunt strâns legate între ele și formează un model de securitate care ajută un sistem CPS să-și păstreze evoluția într-un cadru bine delimitat bazat pe aspectele importante ale menținerii unui mediu sigur.

Descrise pe scurt, cele trei concepte au următorul conținut:

1. *Confidențialitate*. Datele sensibile, precum informații de identificare personală (PII), coduri de identificare, numere de cont bancar etc., trebuie păstrate în condiții de deplină confidențiale. Este important de înțeles că acest concept este diferit de conceptul de secret. Secretul cuprinde tema filozofică că „dacă nu se știe că există ceva, înseamnă că nu există" (spre exemplu: un set de date sau un serviciu web). Dar păstrarea a ceva secret, în sine, nu asigură confidențialitatea. Sunt cunoscute poveștile despre hackeri (sau chiar navigatori obișnuiți pe internet) care au identificat, uneori accidental, informații secrete pe diverse site-uri web. Pentru a asigura confidențialitatea datelor, un utilizator trebuie să se asigure că

nimeni nu poate ajunge la ele, chiar dacă altcineva ar putea fi conștient de valoarea lor. Un exemplu relevant este cel al datelor procesate într-un magazin, despre cardurile de credit ale clienților sau a partajărilor de fișiere cu date sensibile. Pentru păstrarea confidențialității se utilizează alte metode precum controlul accesului, acordarea de permisiuni pentru acces la fișiere, autentificare cu doi pași etc. În interiorul sistemului, fișierele pot fi criptate mai ales pentru protecția datelor stocate, folosirea hashing-ului pentru protejarea datelor în mișcare etc. Pentru securitatea fizică a datele în uz (spre exemplu: ecrane cu tehnologii de confidențialitate, separare fizică între fluxurile de date de uz curent față de cele personalizate prin controlul accesului etc.). se apelează la alte metode. Pot fi utilizate servicii de tip „implicit deny" pentru interzicerea accesului, cu excepția situației autorizării în mod expres a unui utilizator.

2. *Integritate*. Reprezintă funcția de certificare că datele nu sunt modificate decât prin procedurile corecte de procesare și de actualizare a lor. Criptarea ajută la asigurarea integrității datelor aflate în repaus. Însă, nu este o soluție recomandată pentru datele în mișcare. Hashing-ul atribuie datelor o valoare numerică care este procesată de sursă înainte de transferul lor. Acestea, vor fi aduse la forma reală de către destinatar. Această formă de transfer demonstrează integritatea datelor.

3. *Disponibilitate*. Pentru a asigura disponibilitatea ridicată a serviciilor și a datelor, se utilizează tehnici precum servicii și aplicații în cluster, site-uri reziliente, corectarea automată a erorilor, echilibrarea sarcinilor, redundanța componentelor hardware și software, toleranță la erori etc. Tehnicile enumerate pot neutraliza, spre exemplu, un atac de tip denial of service (DoS) care supraîncarcă un sistem CPS cu cereri nevalide sau cu solicitări care durează mult timp de procesare.

În vederea evaluării și aplicării acestor concepte trebuie stabilite unele principii de guvernare a securității pentru CPS-uri. Astfel, ar trebui adoptat un cadru care să includă următoarele aspecte:

1. Alinierea funcțiilor de securitate la strategie, scopuri, misiune și obiective. Oricare CPS are o misiune şi foloseşte o strategie, planuri și obiective

pentru a îndeplini misiunea determinată prin destinația CPS-ului. Strategia trebuie urmată, de regulă 2-5 ani, cu posibilități de autosusținere pentru o perioadă mai mare. Pe termen mai scurt, de obicei 1 - 2 ani, sunt realizate planuri tactice care sunt aliniate cu planul strategic. Planurile tactice generează planuri operaționale, adică o detaliere a planurilor tactice care mențin operativitatea CPS-ului în funcțiune, zi de zi. Obiectivele sunt cele mai apropiate de activitățile curente și reprezintă micile activități pentru îndeplinirea unei misiuni. De exemplu, misiunea unui producător de CPS-uri pentru transportul rutier ar putea fi să asigure un transport în siguranță și să utilizeze cât mai multe mașini de înaltă calitate. Obiectivele ar putea include extinderea automatizării pentru a reduce timpul total de rulare a unei mașini și extinderea de la două la trei puncte de încărcare/descărcare. Un cadru de securitate trebuie să fie strâns legat de misiunea și de obiectivele CPS-ului, permițând o îndeplinire a obiectivelor și o deplasare rapidă protejând, în același timp, mediul, pe baza toleranței la risc. Continuând cu exemplul CPS-ului rutier, cadrul de securitate trebuie să permită extinderea automatizării. Dacă cadrul de securitate nu permite extinderea automatizării, atunci acesta nu este suficient aliniat cu misiunea și cu obiectivele strategice.

Alte procese organizatorice care pot determina noi tipuri de riscuri pot fi legate de achiziții, cesionări, alte procese de guvernanță. Pentru aceasta, trebuie conștientizate riscurile unor noi achiziții (starea mediului IT care urmează să fie integrat este necunoscut, apariția de pagube sau de vătămări critice a utilizatorilor umani etc.) și a unor noi cesionări (partajarea infrastructurii cibernetice, utilizarea de noi identități și de acreditări etc.). În plus, trebuie înțeleasă corect valoarea proceselor de guvernanță (guvernarea furnizorilor, guvernarea proiectelor, guvernarea arhitecturii etc.). De regulă, personalul cu atribuții de securitate sunt în infrastructurile cu rol de revizuire a arhitecturilor fizice și cibernetice, a proiectelor și a incidentelor (de securitate sau de altă natură). Aceștia permit adoptarea de noi strategii sau direcții și urmăresc, în mod exclusiv, securitatea informațiilor.

2. Roluri și responsabilități organizaționale. Într-un CPS, există mai multe funcții cu rol în asigurarea securității fizice și cibernetice. Managementul are responsabilitatea de menținere a operativității sistemului și de a

maximaliza profiturile și valoarea lor pentru utilizatori. Responsabilul cu securitate arhitecturii are responsabilitatea de a înțelege cerințele sistemului, particularitățile mediului fizic și cibernetic existent, starea actuală de securitate și vulnerabilitățile CPS-ului. Acesta trebuie să propună strategii (îmbunătățiri, configurații și contramăsuri) care ar putea maximaliza securitatea și minimaliza riscul. Nu în ultimul rând, în cadrul pesonalului trebuie să fie specialiști și experți care să faciliteze comunicarea între utilizatori cu componentele tehnice. Costurile trebuie să fie justificate și rezonabile, bazate pe cerințe, raportate la riscurile specifice.

3. Cadrul optim de control al securității. Controlul securității să se realizeze într-un cadrul normativ care să optimizeze procesele funcționale și nu să le blocheze sau să le îngreuneze. Pentru aceasta există standarde din seria ISO precum și alte legi, norme de aplicare și regulamente. De regulă acest cadru vizează patru direcții și anume:

   - Control preventiv – are rolul de prevenire a problemelor de securitate și a încălcării politicilor și normelor de securitate. Acesta întărește conștientizarea rolului și funcților în CPS;

   - Control de descurajare – are rol de descurajare a activităților rău intenționate folosind controlul de acces sau tehnologii cibernetice precum: firewall, sisteme de detecție a intruziunilor, camere video activate de mișcare etc.

   - Controlul accesului - acesta permite descoperirea activității neautorizate în mediile aferente CPS-ului;

   - Controlul corectiv – are rolul de reducere a activității în mediile în care au fost identificate incidente de securitate;

4. Întreținere sistematică (due care) / verificarea antecendentelor (due diligence). Chiar dacă se aseamănă, cele două concepe sunt diferite și extrem de importante. Întreținerea sistematică reprezintă responsabilitatea reglementată de a executa controale pentru a se observa că se aplică politicile de securitate, că toate componentele și rețelele de comunicații funcționează normal și că alegerile direcțiilor de dezvoltare sunt rezonabile. Verificarea antecedentelor cuprinde conștientizarea și înțelegerea de către utilizatori

și personalul CPS-ului a principiilor de guvernare a securității (politici și proceduri) și a riscurilor specifice. Adesea, aceasta implică culegerea de informații, prin descoperire, despre evaluările de risc și despre revizuirea documentației existente; crearea documentației pentru actualizarea politicilor; precum și diseminarea informațiilor către toți cei implicați. Uneori, se confundă metodele de întreținere sistematică cu cele de verificare a antecedentelor, fiind acceptat tacit că întreținerea este metoda prin care se poate exercita verificarea.

După ce se stabilește cadrul de guvernare, este nevoie de formarea unei conștiințe de securitate. Tot personalul nou angajat ar trebui să finalizeze pregătirea conștientă în domeniul postului ocupat iar cei cu vechime ar trebui să se recertifice în mod regulat (de obicei anual). Astfel, se poate verifica că tot personalul uman, care deservește și utilizează un CPS, înțelege complexitatea securității mediului CPS și cunoaște reglemetările în domeniu.

Principale aspecte pe care ar trebui să le urmărească o verificare a nivelului de înțelegere a securității pentru CPS urmăresc următoare aspecte:

Infracțiunile cibernetice și protecția datelor. În situația unui CPS, cu o infrastructură extinsă la nivel regional sau internațional, este important de înțeles sistemul juridic al spațiului aferent și ce modificări ar fi necesare privind gestionarea și securitatea datelor. Spre exemplu, în Statele Unite, Healt Information Technology for Economic and Clinical Health (HITECH) Act impune notificarea unei încălcări a protecției datelor în situația expunerii informațiilor despre sănătatea persoanelor, informații care ar trebui protejate în conformitate cu Legea privind portabilitatea și responsabilitatea asigurărilor de sănătate (HIPAA). Mai mult decât atât, Gramm-Leach-Bliley (GLBA) Act se aplică organizațiilor financiare și de asigurări și presupune notificarea autorităților federale de reglementare, a agenților de aplicare a legii și a clienților atunci când are loc o încălcare a datelor. La nivelul UE și în alte țări sunt propriile reglementări privind protecția datelor și informațiilor. În UE, Convenția Consiliului Europei privind criminalitatea cibernetică, tratat semnat de multe țări, stabilește o serie de standarde pentru politica de criminalitate cibernetică. Astfel, GDPR are cerințe foarte stricte de notificare a încălcării datelor și stabilește sancțiuni în cazul nerespectării acestora. Tot la nivelul UE este în procedură de adoptare Digital Operational Resilience Act (DORA) care va reglementa activitatea sistemelor complexe TIC, utilizate zilnic, în sectorul finaciar. Însă, sunt și țări în care nu sunt stabilite responsabilități de raportare în acest sens.

Cerințe de licențiere și proprietate intelectuală. Acestea sunt reglementări în jurul mărcilor comerciale (siglă, simbol, mascotă utilizată pentru comercializarea unei mărci), brevetelor (monopol temporar pentru producerea unui anumit produs, nou și unic), drepturilor de autor (utilizarea exclusivă a operelor artistice, muzicale, literare etc., care împiedică duplicarea neautorizată), licențelor (contract între producătorul de software și consumator care limitează utilizarea și/sau distribuția sau modificare produsului).

Prodecuri de control și alte norme juridice. Fiecare țară are legi privind securitatea cibernetică. În zona transfrontalieră ar mai trebui cunoscute și legile care reglementează importul și exportul de hardware și software. De exemplu, Statele Unite au restricții în ceea ce privește exportul de tehnologie criptografică, iar Rusia solicită licență pentru a importa tehnologii de criptare fabricate în afara țării.

Fluxul de date transfrontalier. Dacă CPS-ul respectă legile și reglementările specifice de securitate, atunci acestă cerință trebuie aplicată, indiferent unde sunt poziționate geografic componente CSP. De exemplu, dacă datele transferate sunt stocate în copii de rezervă în altă țară, trebuie aplicate legile acelei țări. În unele cazuri, este posibil ca mediile de stocare a datelor curente și a celor de actualizare să nu poată fi scoase din țara care adminstrează teritorial punctul unde s-a efectuat intervenția. În alte situații, echipele tehnice de intervenție ar putea să nu fie atente cu protecția datelor personale, în țara respectivă neexistând legislație în domeniu. Exemplele pot continua.

Confidențialitate. Multe legi includ protecția vieții private și a datelor cu caracter personal. Noul GDPR are reguli puternice de confidențialitate care se aplică oricărei structuri și oriunde se stochează sau prelucrează datele cu caracter personal, pentru cetățenii UE. În particular, persoanele trebuie să accepte modul de culegere și de utilizare a datelor lor. Regulamentul Organizației pentru Cooperare și Dezvoltare Economică (OCDE) privind asigurarea confidențialității impune instituțiilor evitarea blocajelor nejustificate a fluxurilor de date transfrontaliere, limitarea culegerii datelor cu caracter personal, protejarea datelor cu caracter personal prin măsuri rezonabile de securitate și multe altele.

Nu în ultimul rând, în cadrul CPS-urilor, înțelegerea, respectarea și promovarea eticii profesionale reprezintă o cerință de bază în vederea asigurării securității cibernetice specifice. Acestea sunt prevăzute în codul de etică profesională și ar trebui completate și în codul de etică, propriu organizației care utilizează CPS-

ul respectiv. Astfel, pe fondul protejării infrastructurii și a securtității personale, vor fi cunoscute și înțelese regulele eticii profesionale, scopul final fiind menținerea securității mediului în care operează CSP-ul.

De altfel, legile prin care se guvernează un sistem politic, administrativ sau economic trebuie respectate și aplicate de toată lumea. Nerespectarea lor produc amenzi, închisoare pentru manageri, oprirea unei afaceri și alte măsuri coercitive. Pentru evitarea acestor aspecte, controalele de conformitate sunt extrem de importante. Prin acestea, pot fi verificate modalitățile de respectare și de aplicare a standardelor și a legislației în vigoare. În principal, trebuie verificate contractele, standardele industriale și cerințele de reglementare legislativă. În unele țări, spre exemplu, normele de drep civil sunt înlocuite cu legea religioasă. În țările islamice, legea este Sharia întemeiată pe Coran și Hadith. Dreptul cutumiar adoptat în practici comune, locale și acceptate de populație, se transformă în legi. Cunoașterea acestor aspecte și înțelegerea lor va facilita comunicarea cu utilizatorii și va consolida starea de securitate a CPS-ului.

Nu în ultimul rând, educația și instruirea continuă a utilizatorilor și a personalului CPS-ului reprezintă cheia formării unei bune culturi de securitate pentru CPS. Aceasta secvență managerială acoperă toate aspectele privind confirmarea că personalul uman este conștient de nevoia de păstrare a securității și este familializat cu politicile și cu procedurile specifice.

În general, cea mai eficientă metodă este campania de conștientizare și instruirea detaliată. De exemplu, fiecare angajat trebuie să învețe că programele malware sau campaniile de phishing determină riscuri de executare de atacuri, cu efecte grave asupra stării de securitate a poziției sale în structura organizației. Înțelegerea doar a imaginii de ansamblu a riscului nu este o soluție foarte eficientă pentru un sistem.

Privind educația și instruirea personalizată la locul de muncă, propunem următoarele direcții de urmărit:

- Aplicarea de metode și de tehnici adecvate de prezentare a conștientizării riscurilor. De obicei, echipele de securitate a informațiilor sunt foarte bine instruite în domeniile securității. Însă, majoritatea personalului nu deține un nivel bun de instruire în acest sens. În cadrul organizației trebuie să existe programe educaționale, oferite de angajatori, pentru întregul personalul. Angajații trebuie să înțeleagă de ce să fie conștienți

(tipuri de amenințări, cum ar fi phishingul sau utilizarea de stick-uri USB gratuite), să înțeleagă cum să-și desfășoare activitatea la locurile lor de muncă în siguranță (criptare de date sensibile, protecție fizică a bunurilor valoroase etc.) și a modului în care securitatea deține un rol important în imaginea de ansamblu a CPS-ului (reputația companiei, profituri, pierderi etc). Programele de formarea continuă ar trebui să fie oferite sistematic angajaților. În plus, ar trebui efectuate teste de rutină de securitate operațională așa cum sunt verificările inopinate la sosirea la muncă, teste de penetrare și de inginerie socială (precum campaniile controlate de ethical hacking) etc.

- Revizuiri periodice. Complexitatea și diversitatea amenințărilor trebuie să se regăsească în relevanța și în intensitatea antrenamentelor și exercițiilor de instruire. Aceasta înseamnă actualizarea materialelor de instruire și conștientizarea schimbării testării aplicării modalităților de securitate. Dacă se utilizează întotdeauna aceeași campanie de testare sau se trimite din același cont în aceeași zi a anului un email de phishing controlat (ethical hacking), testarea nu este eficientă. Același lucru este valabil alocarea de timp de consultare a documentației și altor materiale de instruire. Într-o lume digitală, instruirea ar trebui să ia în seamă utilizarea de instrumente interne de social media, precum videoclipuri și campanii interactive.

- Evaluarea eficacității programului de instruire. O bună instruire pentru securitate necesită timp și fonduri alocate de managementul CPS-ului. Structura de securitate ar trebui să urmărească unele valori cheie stabilite pentru securitatea CPS, precum procentul de angajați care accesează un link dintr-un e-mail de test de phishing. Conștientizarea personalului și buna instruire ar trebui să reducă numărul total de clicuri. Dacă nu se constată aceasta, programul trebuie reevaluat.

Bibliografie suplimentară

1. ***, *Metodologie de management al riscurilor*, elabortă în cadrul proiectului „Consolidarea implementării standardelor de control intern managerial la nivel central și local – cod SIPOCA 34” , la adresa https://sgg.gov.ro/1/wp-content/uploads/2018/07/Metodologia-de-management-al-riscurilor-2018.pdf la data de 03.08.2023

CONCLUZII FINALE

Fără îndoială, cunoștințele în domeniile științei, tehnologiei și științelor sociale au jucat un rol cheie în modelarea lumii moderne. De o importanță deosebită sunt cunoștințe în domeniile de TIC și ale comunicării. Mai ales în ultimul timp, aceste științe au cunoscut o dezvoltare excepțional de rapidă, dovada fiind progresele inedite în informatica digitală și în comunicații. Raportate la evoluția cunoașterii umane, putem observa că în istoria relativ recentă a științelor nu au fost identificate modalități de comune de fundamentare, toate disciplinele aferente lor fiind abordate în mod separat. Mai mult decât atât, atât în cercetarea științifică și în învățământul academic, încă sunt teme legate de informatica digitală, de comunicare și de comunicații fără o abordare comprehensivă, fiind considerate ca aparținând celor trei domenii distincte de specializare. Această carențe ale sistemului educațional contribuie esențial la menținerea disfuncțiilor de adaptare pentru utilizarea optimă a tehnologiilor secolului 21, păstrând încă, în rândul pieței forței de muncă, a unui număr destul de mare de analfabeți funcționali.

Din alt punct de vedere, luată ca un întreg, piața forței de muncă deține o experiență specializată, formată în timp îndelungat. Însă, actualele specializări din economia cunoașterii creează provocări în care inovarea conduce la descoperiri bazate pe abordări critice, pe interdisciplinaritate și pe colaborare. Numeroase produse digitale necesită o prezență fizică umană, indiferent de tipul și genul tehnologiilor informaționale. Astfel, un sistem tehnologic presupune expertiză diversificată în mai multe domenii (mecanică, informatică, electronică, arhitectură, marketing etc.). Pentru realizarea colaborării între domeniile implicate este nevoie de un limbaj comun. În multe cazuri, este dificilă găsirea de puncte comune pentru fundamentarea acestor aspecte, în conformitate cu teoriile disciplinelor aferente. Specialiștii și experții trebuie să urmeze alte programe de pregătire și de formare, în domenii conexe, cu un conținut limitat pentru una sau mai multe ocupații și nu la o cultură comunitară bazată pe bunăstare.

Oricine poate constata realitatea acestor particularități ale vieții cotidiene. O serie de specialiști, din nevoia de personal calificat, susțin renunțarea la unele ocupații tradiționale și instruirea în noi ocupații, bazate pe tehnologii digitale. Astfel, se dorește ca, odată cu pătrunderea rapidă a tehnologilor în viața modernă, să se reformeze și educarea populației pentru adaptarea rapidă la particularitățile noului mediu social, permițând dezvoltarea și a altor produse inovative. Spre exemplu,

numai pentru uzul casnic, pentru sănătate, pentru divertisment etc., există dispozitive a căror inovare a presupus bune colaborări între persoane cu pregătire academică (master sau doctorat) și cu speciaiști din entități de cercetare și industriale. Dar, programele de studii universitare propuse de facultățiile actuale, par să împiedice interdisciplinaritatea comunicării, fundamentul realizării unei astfel de colaborări. În plus, cadrul legislativ în domeniul învățământului universitar impune unele norme care, chiar dacă pretind încurajarea colaborării academice, mențin organizarea programelor de studii pe discipline tradiționale, care, adeseori, nu-și mai găsesc reprezentare, prin conținutul lor, în viața reală. Toate acestea, chiar dacă par probleme ale unui sistem social distinct, au implicații concrete pentru educarea forței de muncă, a căror nerezolvare vor continua erodarea capacității colective de înțelegere corectă a evoluției mediului în care trăim.

Fără să le numim așa, multe aplicații tehnologice contemporane sunt CPS-uri care ne umplu activitățile cotidiene. În numeroase gospodării pot fi găsiți roboți pentru curățenie sau de bucătărie, sisteme inteligente de iluminat și de încălzire, sisteme inteligente de ventilație și de aer condiționat (sau sisteme HVAC) etc. Mai mult decât atât, transportul este optimizat cu autovehicule inteligente, avioane, scutere motorizate, biciclete electrice, segway-uri etc. Autovehiculele există de aproape 350 de ani, însă, cele care sunt produse acum au funcții noi, disponibile în majoritatea liniilor de producție a autovehiculelor rutiere. Amintim sistemele de avertizare la impact (LDWS). În plus, soluțiile medicale contemporane includ stimulatoare cardiace, pompe de insulină, roboți de asistență personală, proteze inteligente etc., multe dintre aceste tehnologii neexistând până în prezent. Acestea au potențialul atât de a salva vieți cât și de a îmbunătăți semnificativ sănătatea și bunăstarea cetățenilor. Sistemele purtabile de fitness și cele de monitorizare a sănătății promit să aibă un nivel uriaș de impact pozitiv asupra utilizatorilor, indiferent dacă aceștia sunt sau nu sănătoși sau dacă au o stare fizică bună ori o dizabilitate cognitivă. Putem accepta că sistemele de monitorizare a sănătății sunt doar un exemplu al întregului sector al rețelelor de senzori, care include rețele formate din senzori miniaturizați, utilizați pentru observarea și monitorizarea spațiilor mari, terestre, marine sau aeriene. Nu în ultimul rând, trebuie să enumerăm sistemele din sectorul energetic care includ morile de vânt, rețelele inteligente de transport și diverse tehnologii de captare a energiei. Apreciem că sistemele inteligente existente sunt reprezentative și încurajează inovarea pentru dezvoltări semnificative în viitor. De fapt, nu este o exagerare să ne gândim la întreaga planetă poate deveni un CPS masiv.

Prin urmare, atunci când observăm astfel de exemple în aplicații aparent futuriste sau mai puțin spectaculoase trebuie să înțelegem că pot conține cel puțin un sistem integrat sau sunt componentele unui CPS. De exemplu, dacă într-un autovehicul rutier contemporan, componentă cibernetică poate fi considerată un gadget pentru că rularea se poate executa și fără aceasta, un segway având doar două roți, chiar dacă nu este evident, va încorpora componente cibernetice, cel puțin, pentru a-l menține în poziția verticală. Din punct de vedere mecanic, segway-ul este un sistem instabil a cărei funcționare poate fi demonstrată matematic că nu ar putea fi posibilă fără un procesor care să îl mențină în poziție verticală, atunci când este oprit. Segway-ul folosește un sistem de control în timp real care rulează pe un sistem dedicat, încorporat într-un sistem de calcul. În timp ce, în mod tradițional, multe sisteme au fost proiectate pentru a fi stabile în absența controlului activ, segway-ul și multe alte platforme mobile (generațiile noi de autovehicule și de avioane) includ, deja, aplicații fără de care stabilitatea operării lor este critică fără control activ. Aceste observații ne determină să concluzionăm că tot mai multe proiecte pentru tehnologiile viitoare nu vor fi eficiente fără control activ, ceea ce presupune implementare de CPS-uri. Din mai multe motive tehnice, acest tip de control nu este posibil fără cel puțin o componentă cibernetică.

Prin urmare, scopul principal al acestui curs este de a-i familiariza pe utilizatori și pe alți indivizi dornici de a-și actualiza cunoștințele, cu perspectiva că oricare tip de dispozitiv tehnic va fi tot mai greu de realizat fără componente cibernetice, chiar dacă aceste teme de discuție par a fi de domeniul viitorului futurist. Se observă că tehnologiile implementate în proiectele viitorelor aeronave pot genera capacități impresionante de transport, dar direcțiile de utilizare a lor sunt relativ limitate, iar impactul asupra vieții umane poate fie minim. În schimb, tehnologiile specifice conceptelor de „casă inteligentă" și de „oraș inteligent" pot fi percepute prin impactul direct, net superior, pentru siguranța confortului cetățenilor. Spre exemplu, în prezent oricine poate fi afectat de costurile generate de consumul de energie electrică folosită pentru încălzirea și răcirea încăperilor, pentru spălarea și uscarea hainelor, pentru transportul de persoane și de mărfuri către și dinspre spațiile de locuit etc. În aceste condiții, optimizarea sistemelor HVAC poate avea un impact semnificativ asupra consumului global de energie și se va reflecta în scăderi ale consumului, adică în fonduri reduse pentru aceleași funcții. În mod similar, tehnologiile informaționale pot asigura un grădinărit hidroponic sofisticat, chiar în casă, care să asigure o

aprovizionare locală optimă cu nutrienți proaspeți. Combinarea celor două domenii poate permite, de asemenea, un management avansat pentru diferiți parametri de confort în locuință, precum: un nivel optim de umiditate a aerului, un nivel scăzut de dioxid de carbon, îmbunătățirea sănătății și a condițiilor de viață.

Chiar și în relațiile specifice asigurării stărilor de securitate națională, regională și internațională pot exista CPS-uri. Astfel, tendința generală a statelor este de a stoca tot mai multe date și informații, în biblioteci digitale, pe teritoriul lor administrativ. Acestea pot fi din diverse domenii, în special date critice din domeniile de sănătate socială și din identitățile digitale ale cetățenilor. Prin urmare, multe state vor trebui să-și echilibreze suveranitatea datelor și a informațiilor în sistemele economice globale. Cu cât păstrează mai multe date și informații în limitele granițelor naționale, cu atât pot beneficia mai puțin de pe urma facilităților economiei digitale internaționale. Fluxul liber al datelor va fi esențial, mai ales pentru economiile mici și orientate spre export. În plus, partajarea datelor va fi esențială pentru abordarea oricărei probleme globale, așa cum sunt cele generate de pandemii și de schimbările climatice. În același timp, datele care sunt colectate și procesate la nivel local pot genera noi servicii de inteligență artificială și de date deschise, la scală națională sau regională. O tehnologie reformată pe aceste principii ar putea sprijini creșterea economiilor locale și ar putea reduce profiturile unor mari companii tehnologice care practică tehnici de menținere a monopoului pe un domeniu.

Dacă exceste concluzii pot fi atractive pentru specialiști, nu în ultimul rând, trebuie stimulată și dezvoltarea experienței utilizatorilor de CPS-uri. Aceștia, pot acorda un suport esențial pentru conturarea concluziilor privind modul de proiectare a sistemelor în vedera utilizării eficiente și pentru îmbunătățirea anumitor caracteristici/parametri ai acestora. Aceste informații de feedback pot produce îmbunătățiri de tipul:

- Modelarea complexității sistemului CPS prin:
    - Creșterea gradului de libertate (în modelele de sisteme fizice).
    - Creșterea dimensiunii spațiului de stare (în modelele sistemelor cibernetice).
    - Reducerea a ceea ce poate fi detectat sau acționat (în sistemele de control).
    - Reducerea fiabilității componentelor (pentru toate aspectele).

- Aplicarea unor ecuații simplificate în raport cu cele dependente de timp precum:
    - Ecuații diferențiale ordinare (ODE), de la cele liniare până la cele neliniare.
    - De la ODE la ecuații diferențiale parțiale (PDE).
    - De la ODE la ecuații integrale/diferențiale (IDE).
- Îmbunătățirea modelelor de optimizare așa, cum ar fi:
    - Trecerea de la circuite booleene la sisteme Turing și AI.
    - Aplicare sistemeleor discrete și/sau continue numai asupra componentelor care implică comportamente hibride.
- Modelarea parametrii de structură, de dimensiune și de determinism în condiții de incertitudine etc.

Trebuie reținut că sistemele complexe, printre care se numără și CPS-urile, reprezintă o provocare pentru proiectanții care dezvoltă instrumente de ultimă generație, precum şi pentru cercetătorii care efectuează cercetare fundamentală. Dezvoltarea sensibilității instrumentelor actuale, analitice și de procesare a datelor, va permite o inovare eficientă, concentrată pe proiecte fezabile. Pentru aceasta este nevoie o pregătire susținută din punct de vedere academic. De asemenea, utilizarea CPS-urilor va permite o înțelegere corectă a limitelor aflate la frontierele cunoașterii, condiție prealabilă pentru progresul cercetării fundamentale și a evoluției sociale. Chiar dacă sunt voci care susțin, pe diverse tonalități, că implementarea CSP-urilor reprezintă o ameninare a locurilor de muncă în majoritatea sectoarelor economice, oameni trebuie să fie convinşi că viitorul implică folosirea CPS-urilor în toate domeniile. Pentru a-i „liniști" pe simpatizanții teoriilor conspiraționiste să ne amintim ce impact a avut introducerea motorului în economie. Chiar dacă istoricii nu sunt de acord cu cine și când a fost inventat tractorul, o mulțime de ramuri economice beneficiază de utilizarea lui. Agricultura nu este concepută fără tractoare și alte tipuri de motoare. Transporturile de tot felul sunt direct dependente de vehicule cu motoare, cu ardere internă și electrice. Turismul este mai facil prin utilizarea autovehiculelor, a navelor și aeronavelor. Exemplele pot continua.

Revenind la aplicațiile cibernetice, chiar dacă sunt puțin cei care cunosc cum a apărut internetul toată lumea îl folosește în diverse aplicații. Rețele sociale facilitează comunicarea oriunde și oricând. Industria de divertisment utilizează internetul. Însăși productivitatea întreprinderilor contemporane a crescut prin prisma dezvoltării legăturilor de comunicații pe baza internetului.

Prin urmare, ritmul de adoptare a tehnologiilor informaționale creează firmelor noi oportunități de dezvoltare. Prin urmare, toți care se pregătesc pentru a înțelege aceste tehnologii ale viitorului, în care includem și CPS-urile vor identifica oportunități reale de evoluție, cu beneficii uriașe atât pe plan individual cât și organizațional.

Felicitări pentru finalizarea acestui curs!

Sugerăm cititorilor ca această publicație să fie acceptată ca o provocare pentru dezvoltarea lor personală, în ritm continuu, și un început al stabilirii de noi relații de comunicare cu specialiștii și experții în astfel de sisteme, pentru realizarea unui sport real al dezvoltării aplicațiilor cibernetice și fizice, în proiecte de securitate a vieții cotidiene.

Bulevardul Mareșal Averescu 8-10,
sector 1, 011455, București, România

editura@ici.ro

www.ici.ro