ASIGURAREA CONFORMITĂŢII CU STANDARDELE DE SECURITATE CIBEMETICĂ PRIN INTEGRAREA MAI MULTOR STANDARDE ÎN CONTEXTUL PROIECTELOR DE DEZVOLTARE SOFTWARE ÎN INDUSTRIA AUTO

Teză de doctorat – Rezumat

pentru obținerea titlului științific de doctor la

Universitatea Politehnica Timișoara

în domeniul de doctorat ____Inginerie si Management____

autor ing. __Darius Barmayoun__

conducător științific ___ Prof.ing.dr.ec Marian Mocan __

luna_02_ anul_2025_

INTRODUCERE

Industria auto trece printr-o transformare semnificativă, determinată de progresele tehnologice rapide și de creșterea conectivității. Această schimbare nu se referă doar la introducerea unor noi tehnologii, ci la o redefinire fundamentală a designului, dezvoltării și operării vehiculelor. Creșterea numărului de vehicule conectate amplifică riscurile cibernetice, expunând societatea la potențiale atacuri cibernetice (1). Vehiculele moderne nu mai sunt doar mijloace de transport, ci sisteme sofisticate, interconectate, care integrează capabilități de conducere autonomă, dispozitive IoT și arhitecturi electronice complexe. Această evoluție introduce provocări critice de securitate cibernetică, pe măsură ce probabilitatea și severitatea amenințărilor cibernetice continuă să crească (2).

Asigurarea securității cibernetice în industria auto a devenit acum o prioritate esențială. Pe măsură ce sistemele electrice și electronice (E/E) avansează, protocoalele tradiționale de comunicație, precum Controller Area Network (CAN) bus, sunt completate sau înlocuite de tehnologii mai avansate, cum ar fi automotive Ethernet (3). Aceste progrese extind suprafața de atac, făcând vehiculele și ecosistemele acestora vulnerabile la amenințări cibernetice care pot compromite confidențialitatea utilizatorilor, siguranța și integritatea operațională. Acest risc se extinde și asupra producătorilor de echipamente originale (OEM) și a furnizorilor lor, ceea ce face necesară implementarea unor măsuri solide de securitate cibernetică (4).

Securitatea cibernetică în sectorul auto necesită o abordare specifică industriei, având în vedere caracteristicile unice ale domeniului, cum ar fi ciclurile lungi de viață ale produselor, lanțurile de aprovizionare complexe și cerințele stricte de siguranță. Acest lucru implică securizarea comunicațiilor Vehicle-to-Everything (V2X), protecția serviciilor bazate pe cloud și asigurarea integrității unităților de control electronic (ECU). Deși atacurile cibernetice asupra V2X sunt încă în fază incipientă, se estimează că acestea vor deveni tot mai frecvente în următorii ani (4).

Ca răspuns la aceste riscuri, autoritățile de reglementare și organismele industriale au introdus standarde și cadre cuprinzătoare pentru securitatea cibernetică. Printre cele mai importante se numără ISO/SAE 21434 și ASPICE for Cybersecurity, care stabilesc metodologii structurate pentru gestionarea riscurilor cibernetice în sistemele auto. În plus, reglementările UNECE WP.29 R155 și R156, introduse în 2021, impun conformitatea cu cerințele de securitate cibernetică pentru toate vehiculele noi începând cu iulie 2024 (5). Aceste reglementări și standarde asigură o abordare structurată a managementului riscurilor cibernetice, oferind cele mai bune practici și un limbaj comun pentru toți actorii din industrie.

Standarde și reglementări esențiale:

1. ISO/SAE 21434 – Un cadru fundamental pentru securitatea cibernetică, care abordează gestionarea riscurilor pe tot parcursul ciclului de viață al vehiculelor, incluzând evaluarea riscurilor, răspunsul la incidente și recuperarea (6).
2. ASPICE for Cybersecurity – O adaptare a Automotive SPICE, care oferă ghiduri pentru dezvoltarea și evaluarea proiectelor auto legate de securitatea cibernetică (7).
3. UNECE WP.29 R155 & R156 – Reglementări globale care impun măsuri de securitate cibernetică în producția auto și obligativitatea auditurilor de conformitate, cu implementare completă începând din iulie 2024 (8,9).

Deși aceste standarde oferă abordări structurate pentru securitatea cibernetică, implementarea lor rămâne o provocare, în special pentru furnizorii de nivel 1 și 2. Aceștia trebuie să integreze cerințele de securitate cibernetică în produsele și procesele lor de dezvoltare, un proces complex și care necesită resurse semnificative. Creșterea numărului de reglementări impune dezvoltarea unor mecanisme eficiente de conformitate, pentru a reduce eforturile necesare pentru audituri și evaluări.

Prin urmare, această introducere stabilește fundamentul pentru înțelegerea securității cibernetice în sectorul auto, analizând UNECE R155 & R156, ISO/SAE 21434 și ASPICE for Cybersecurity. Se subliniază necesitatea armonizării acestor cadre de reglementare, pentru a simplifica conformitatea și a îmbunătăți rezistența la amenințările cibernetice. Abordarea acestor provocări va permite industriei auto să dezvolte un ecosistem mai sigur și mai robust, asigurând conformitatea și atenuând amenințările cibernetice emergente. Această discuție contribuie atât la cercetarea academică, cât și la implementarea practică în industrie, subliniind rolul critic al securității cibernetice în sistemele auto moderne.

SECURITATEA CIBERNETICĂ ÎN INDUSTRIA AUTO

Securitatea cibernetică în industria auto a evoluat semnificativ, devenind o preocupare critică doar în ultimii ani. Istoric, industria auto s-a concentrat pe siguranța funcțională, prioritizând integritatea fizică și fiabilitatea vehiculelor pentru a preveni defecțiunile mecanice și accidentele. Spre deosebire de sectoare precum finanțele sau sănătatea, care au integrat securitatea cibernetică încă de la început datorită naturii lor digitale, industria auto a întârziat adoptarea măsurilor de securitate cibernetică (10).

Odată cu introducerea tehnologiilor CASE (Connected, Automated/Autonomous, Shared/Service, Electrification) și ascensiunea Industriei 4.0, industria auto se confruntă acum cu provocări tot mai mari legate de securitatea cibernetică. Tranziția către vehicule conectate și autonome a extins suprafața de atac, introducând amenințări care nu compromit doar siguranța fizică, ci și securitatea datelor și confidențialitatea utilizatorilor (11,12).

Creșterea utilizării IoT, telematicii și conducerii autonome a sporit semnificativ expunerea vehiculelor la riscuri cibernetice. Vehiculele autonome, care se bazează pe senzori și procesarea datelor, sunt vulnerabile la falsificarea senzorilor, manipularea software-ului și breșe de securitate în rețea (13). În plus, vehiculele electrice (EVs) prezintă noi provocări de securitate cibernetică, legate de rețelele de încărcare, sistemele de management al bateriei și protecția datelor (14). De exemplu, atacul asupra unui Jeep Cherokee din 2015 a demonstrat riscurile reale ale vulnerabilităților cibernetice, cercetătorii reușind să preia controlul de la distanță asupra unui vehicul prin sistemul său de divertisment (15). În mod similar, integrarea crescută a senzorilor în vehiculele electrice a generat preocupări legate de confidențialitate, deoarece acestea colectează și stochează date sensibile ale șoferilor, care pot fi exploatate în scopuri rău intenționate (16,17).

Principalele Amenințări Cibernetice în Industria Auto:

- Hackeri susținuți de state, care vizează infrastructura și sistemele publice (8).
- Hackeri Black-Hat, care exploatează vulnerabilitățile vehiculelor pentru câștiguri financiare, cum ar fi furtul de vehicule fără cheie (8).
- Hackeri pentru câștig personal, care modifică software-ul sau hardware-ul vehiculelor pentru modificări neautorizate (8).

A Conform raportului Upstream Cybersecurity din 2022, 84.5% dintre atacurile cibernetice din 2021 au fost atacuri la distanță, demonstrând tranziția de la atacuri fizice la metode de hacking de lungă distanță, utilizând rețele celulare, API-uri și vulnerabilități bazate pe internet (8). Până în 2022, 97% dintre atacuri erau de la distanță, reflectând sofisticarea tot mai mare a infractorilor cibernetici și extinderea suprafeței de atac a vehiculelor conectate (5).

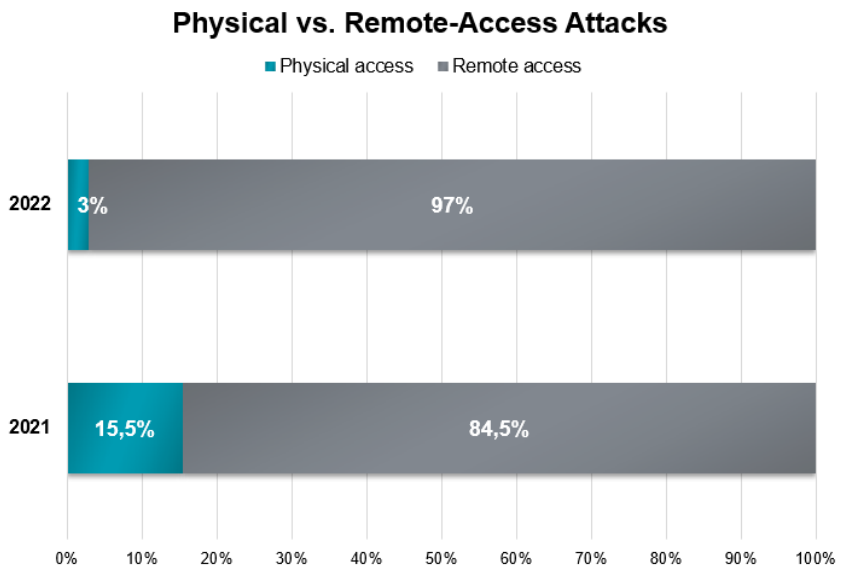

Fig. 1. Atacuri fizice vs. Remote 2021 vs.2022
[8][5]

Conștientizarea riscurilor de securitate cibernetică a condus la introducerea unor standarde de reglementare menite să securizeze sistemele auto. Reglementările UNECE WP.29, dezvoltate de Comisia Economică a Națiunilor Unite pentru Europa, au reprezentat un punct de cotitură în securitatea cibernetică a industriei auto (5). Aceste reglementări impun gestionarea continuă a riscurilor cibernetice, actualizări software și audituri de conformitate pe tot parcursul ciclului de viață al unui vehicul. WP.29 stabilește securitatea cibernetică ca un element fundamental al siguranței auto, schimbând abordarea industriei de la una reactivă la o strategie de securitate proactivă și holistică.

Pe lângă WP.29, ISO/SAE 21434 oferă o abordare structurată pentru gestionarea riscurilor cibernetice, acoperind evaluarea riscurilor, măsurile de atenuare și răspunsul la incidente (5). Împreună, aceste standarde integrează securitatea cibernetică în procesul de dezvoltare și operare a vehiculelor. Implementarea reglementărilor și standardelor de securitate cibernetică transformă designul vehiculelor, procesul de fabricație și serviciile post-vânzare. Companiile auto trebuie să investească în evaluarea riscurilor cibernetice, dezvoltarea securizată a software-ului și procese de conformitate, ceea ce aduce provocări financiare și operaționale (5). Totuși, conformitatea cu cerințele de securitate cibernetică nu mai este doar o obligație de reglementare, ci a devenit un avantaj competitiv, influențând încrederea consumatorilor, răspunderea legală și diferențierea pe piață.

Privind spre viitor, tehnologiile emergente precum Inteligența Artificială (AI) și Blockchain sunt așteptate să joace un rol crucial în consolidarea securității cibernetice în sectorul auto. Soluțiile de securitate bazate pe AI pot detecta și răspunde la amenințări în timp real, în timp ce tehnologia blockchain poate îmbunătăți integritatea datelor și transparența rețelelor vehiculelor (5).

Securitatea cibernetică a devenit un element indispensabil al sistemelor auto moderne, evoluând de la o preocupare neglijată la un pilon esențial al siguranței și conformității cu reglementările. Tranziția către vehicule conectate și autonome a extins peisajul amenințărilor, impunând măsuri avansate de securitate, aliniere reglementară și cooperare la nivelul întregii industrii. Reglementările UNECE WP.29 și standardul ISO/SAE 21434 au stabilit un nou fundament pentru securitatea cibernetică în industria auto, asigurând că aceasta nu este doar o necesitate tehnică, ci și un imperativ strategic pentru mobilitatea viitorului.

DEZVOLTAREA STANDARDELOR PENTRU SECURITATEA CIBERNETICĂ

Creșterea complexității și frecvenței amenințărilor cibernetice în sectorul auto a impus dezvoltarea unor cadruri de reglementare și standarde cuprinzătoare, menite să protejeze vehiculele conectate și autonome. În trecut, industria auto s-a concentrat în principal pe siguranța funcțională, asigurând integritatea fizică și fiabilitatea vehiculelor. Însă, odată cu transformarea digitală accelerată a vehiculelor, securitatea cibernetică a devenit un pilon esențial al siguranței auto moderne. Dependența tot mai mare de funcționalități bazate pe software, servicii conectate și actualizări over-the-air (OTA) a sporit riscurile cibernetice, necesitând o abordare sistematică și proactivă a conformității cu cerințele de securitate cibernetică (18). Ca răspuns la aceste provocări, reglementările și standardele-cheie, precum UNECE WP.29 R155 și R156, ISO/SAE 21434 și ASPICE for Cybersecurity, au fost introduse pentru a stabili măsuri uniforme de securitate de-a lungul ciclului de viață al vehiculelor. Aceste cadre nu sunt doar recomandări, ci mandate obligatorii, care impun producătorilor auto integrarea securității cibernetice în proiectarea, dezvoltarea, producția și post-producția vehiculelor (18).

Reglementările UNECE WP.29, introduse în iunie 2020, au marcat un punct de cotitură în securitatea cibernetică globală a industriei auto. Regulamentul R155 impune constructorilor auto să implementeze un Sistem de Management al Securității Cibernetice (CSMS), pentru a asigura gestionarea și reducerea continuă a riscurilor cibernetice pe tot parcursul ciclului de viață al vehiculelor. Această reglementare obligă producătorii să identifice și să atenueze amenințările cibernetice în timpul dezvoltării, să implementeze măsuri de securitate cibernetică în producție și să mențină protecția continuă a vehiculelor după comercializare (19). În plus, R156 se concentrează pe securitatea actualizărilor software, cerând producătorilor să securizeze mecanismele de actualizare OTA și să reaplice pentru aprobare în cazul modificărilor software care afectează performanța tehnică (20). Aceste reglementări asigură că securitatea cibernetică nu este limitată doar la dezvoltarea pre-lansare, ci rămâne o obligație continuă pe întreaga durată de utilizare a unui vehicul.

Alături de reglementările UNECE, ISO/SAE 21434 a devenit un standard fundamental pentru securitatea cibernetică în industria auto. Dezvoltat în colaborare de ISO și SAE International, acest standard stabilește o abordare structurată pentru evaluarea și gestionarea riscurilor cibernetice în întregul proces de inginerie auto. Spre deosebire de UNECE WP.29, care se axează pe conformitatea reglementară, ISO/SAE 21434 oferă un cadru detaliat pentru evaluarea riscurilor, răspunsul la incidente și guvernanța securității cibernetice în cadrul organizațiilor auto. Acest standard definește metodologii pentru calcularea scorurilor de risc, prioritizarea gestionării vulnerabilităților și integrarea practicilor de securitate cibernetică de la conceptualizare până la scoaterea vehiculului din uz (4). Prin furnizarea de ghiduri tehnice despre modul în care trebuie îndeplinite cerințele de securitate cibernetică, ISO/SAE 21434 sprijină reglementările UNECE WP.29, asigurând astfel că securitatea devine o parte integrantă a procesului de inginerie auto, și nu o măsură implementată tardiv.

Rapoartele Upstream Security Global Automotive Cybersecurity (2021 și 2022) subliniază dificultățile întâmpinate de autoritățile de reglementare în menținerea ritmului cu progresele tehnologice rapide. Raportul din 2021 evidențiază faptul că viteza inovației în tehnologiile vehiculelor conectate a depășit frecvent dezvoltarea reglementărilor, un fenomen observat anterior și în domeniul protecției datelor, cum ar fi Regulamentul General privind Protecția Datelor (GDPR), care a fost adoptat după extinderea utilizării tehnologiilor digitale (18). În mod similar, industria auto a înregistrat un decalaj între implementarea tehnologiilor conectate și introducerea reglementărilor de securitate cibernetică, ceea ce a dus la exploatarea vulnerabilităților de către infractorii cibernetici. Pentru a răspunde urgent acestei probleme, introducerea reglementărilor UNECE WP.29 și a standardului ISO/SAE 21434 în 2020 a reprezentat un pas crucial în închiderea acestor lacune de securitate. Aceste cadre nu doar că asigură conformitatea, dar permit și constructorilor auto să implementeze soluții inovatoare de securitate cibernetică, menținând controlul reglementar necesar (8).

Pe lângă UNECE WP.29 și ISO/SAE 21434, ASPICE for Cybersecurity joacă un rol esențial în integrarea practicilor de securitate cibernetică în dezvoltarea software auto. Automotive SPICE (ASPICE) este un cadru de referință recunoscut la nivel global pentru îmbunătățirea proceselor de inginerie software, iar extensia sa pentru securitate cibernetică se asigură că măsurile de securitate sunt implementate încă din fazele timpurii ale proiectării. ASPICE for Cybersecurity ajută producătorii auto și furnizorii să simplifice conformitatea cu cerințele de securitate cibernetică, să îmbunătățească securitatea software-ului și să dezvolte procese sistematice pentru identificarea și reducerea riscurilor cibernetice. Prin integrarea securității cibernetice în întregul ciclu de viață al software-ului auto, ASPICE asigură că scrierea de cod securizat, testarea vulnerabilităților și modelarea amenințărilor devin practici standard în dezvoltarea auto, reducând riscul vulnerabilităților cibernetice în vehiculele de serie.

Relația dintre aceste cadre de reglementare și standarde evidențiază o schimbare de paradigmă în industria auto, de la măsuri reactive de securitate cibernetică la strategii proactive și integrate. UNECE WP.29 oferă baza reglementară, ISO/SAE 21434 definește metodologii tehnice pentru gestionarea riscurilor, iar ASPICE for Cybersecurity aliniază securitatea software-ului cu cele mai bune practici din industrie. Această abordare multi-strat asigură că riscurile de securitate cibernetică sunt gestionate în fiecare etapă a producției și operării vehiculelor, oferind un cadru cuprinzător pentru protejarea vehiculelor conectate și autonome împotriva amenințărilor cibernetice în continuă evoluție (4).

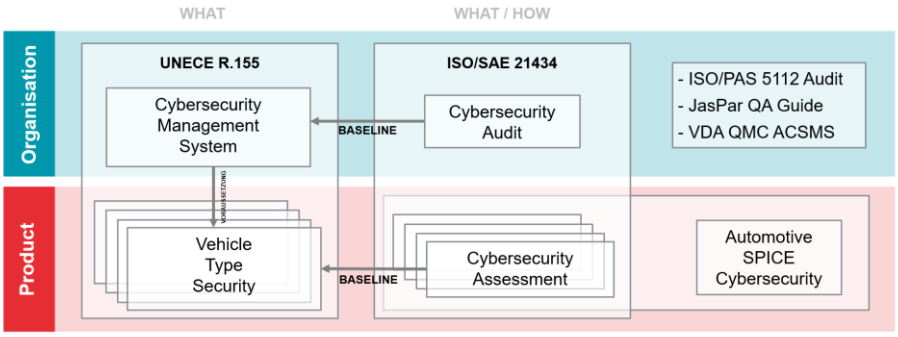

Fig. 2. Relația dintre reglementări, standarde și cadre de referință

Prin urmare, evoluția reglementărilor privind securitatea cibernetică în industria auto reflectă o transformare mai amplă în modul în care securitatea cibernetică este percepută și implementată. Ceea ce odinioară era considerat o preocupare secundară a devenit acum o necesitate reglementară și un imperativ strategic pentru producătorii auto. Implementarea UNECE WP.29, ISO/SAE 21434 și ASPICE for Cybersecurity reprezintă un efort global de creare a unei abordări standardizate pentru conformitatea cu cerințele de securitate cibernetică, asigurând că industria ține pasul cu progresele tehnologice și amenințările cibernetice emergente. Pe măsură ce sectorul auto continuă să evolueze, integrarea securității

cibernetice în proiectarea vehiculelor, procesul de fabricație și serviciile post-producție va fi esențială pentru menținerea încrederii consumatorilor, conformitatea cu reglementările și reziliența pe termen lung a industriei.

ISO/SAE 21434 ȘI INTEGRAREA SA

ISO/SAE 21434, intitulat „Vehicule rutiere – Inginerie de securitate cibernetică”, este un standard esențial în industria auto, marcând o evoluție semnificativă în abordarea securității cibernetice în dezvoltarea software-ului auto. Adoptarea sa subliniază recunoașterea tot mai mare a securității cibernetice ca un element fundamental al siguranței și fiabilității vehiculelor. Pe măsură ce sistemele auto au avansat în ceea ce privește funcționalitatea și conectivitatea, acestea au devenit tot mai interconectate și vulnerabile la amenințări cibernetice (12). Standardul stabilește un cadru cuprinzător pentru gestionarea riscurilor de securitate cibernetică pe întregul ciclu de viață al vehiculului, de la faza de concept până la proiectare, producție, operare, mentenanță și dezafectare. Având în vedere complexitatea vehiculelor moderne, care nu mai sunt sisteme mecanice izolate, ci fac parte dintr-un ecosistem digital mai larg, securitatea cibernetică trebuie să fie un principiu integrat în inginerie, și nu doar o preocupare la nivel de proiect (21).

ISO/SAE 21434 se diferențiază de standardele anterioare, cum ar fi SAE J3061, prin faptul că nu urmează un proces secvențial strict, ci conturează o abordare flexibilă, bazată pe activități, pentru gestionarea riscurilor de securitate cibernetică. Standardul oferă obiective clare, metodologii practice și exemple ilustrative pentru a ajuta producătorii auto și furnizorii să integreze eficient principiile de securitate cibernetică (22). Având în vedere că organismele de reglementare acordă o prioritate tot mai mare securității cibernetice în industria auto, conformitatea cu ISO/SAE 21434 devine esențială pentru accesul pe piață și pentru avantajul competitiv. Standardul furnizează un limbaj comun și practici structurate pentru ingineria securității cibernetice, încurajând colaborarea și schimbul de cunoștințe în întregul sector auto. Astfel, acesta consolidează semnificativ postura generală a industriei în ceea ce privește securitatea cibernetică. Cu toate acestea, în ciuda importanței sale, există în continuare o lipsă de cadre de referință și instrumente pentru instruirea și testarea în domeniul securității cibernetice în sectorul auto, ceea ce generează provocări pentru implementarea sa pe scară largă (23).

Obiectivul principal al ISO/SAE 21434 este integrarea considerentelor de securitate cibernetică în procesele de inginerie ale sistemelor electrice și electronice (E/E) din vehiculele rutiere (6). Pe măsură ce vehiculele moderne depind din ce în ce mai mult de unități electronice de control (ECU), software încorporat și funcționalități de rețea, standardul asigură că principiile de securitate evoluează odată cu progresele tehnologice. Extinzând domeniul de aplicare al ISO 26262 (Standardul pentru Siguranță Funcțională), ISO/SAE 21434 impune integrarea securității cibernetice pe întreg ciclul de viață al vehiculului, asigurând o abordare bazată pe risc în ceea ce privește ingineria securității cibernetice (4).

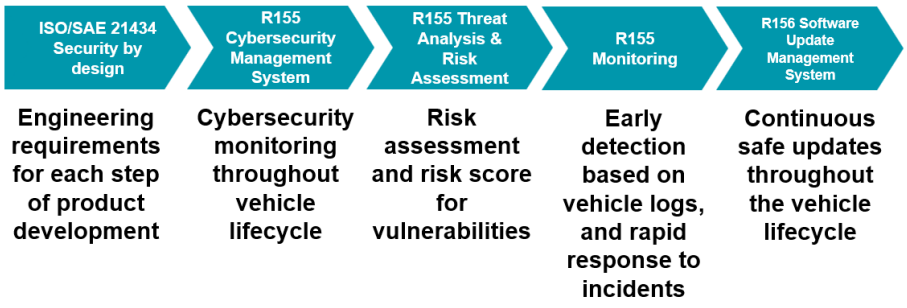

Fig.3. ISO/SAE 21434 și WP.29 colaborează pentru a proteja vehiculele [5]

ISO/SAE 21434 oferă organizațiilor un cadru structurat pentru:

- Dezvoltarea și implementarea politicilor și proceselor de securitate cibernetică care sunt aliniate cu cerințele reglementare și cele mai bune practici din industrie.
- Gestionarea eficientă a riscurilor de securitate cibernetică prin prioritizarea evaluării amenințărilor, atenuarea vulnerabilităților și implementarea unor controale de securitate proactive.
- Cultivarea unei culturi puternice a securității cibernetice în cadrul organizațiilor prin promovarea conștientizării, instruirii și implicării active în inițiativele de securitate cibernetică.

Prin integrarea acestor principii, ISO/SAE 21434 permite organizațiilor să stabilească un Sistem de Management al Securității Cibernetice (CSMS). Acest sistem asigură o abordare sistematică și consecventă a securității cibernetice, acoperind monitorizarea continuă, planificarea răspunsului la incidente și implementarea controalelor de securitate cibernetică pe tot parcursul ciclului de viață al sistemelor electrice și electronice (E/E). Adoptarea CSMS, conform ghidului oferit de ISO/SAE 21434, permite companiilor din industria auto să răspundă eficient la amenințările cibernetice emergente, menținând în același timp conformitatea cu reglementările internaționale privind securitatea cibernetică.

ASPICE FOR CYBERSECURITY ȘI INTEGRAREA SA

Integrarea ASPICE pentru Securitate Cibernetică în cadrul dezvoltării auto reprezintă un progres semnificativ în abordarea securității cibernetice a industriei. Inițial introdus la începutul anului 2021 de către Asociația Germană a Industriei Auto (VDA), acest modul suplimentar extinde modelul de evaluare a proceselor ASPICE (PAM) versiunea 3.1, prin integrarea unor cerințe specifice de securitate cibernetică. Această dezvoltare constituie un răspuns strategic la complexitatea tot mai mare a amenințărilor cibernetice pe care producătorii de echipamente originale (OEM) și furnizorii trebuie să le gestioneze, asigurând în același timp conformitatea cu cerințele stricte de reglementare (24). Modulul garantează că practicile de securitate cibernetică sunt integrate eficient pe întregul ciclu de inginerie, acoperind fazele de dezvoltare, producție, mentenanță și scoatere din uz. În plus, acesta aliniază procesele de securitate cibernetică cu politicile organizaționale și cadrele de management al proiectelor, consolidând o abordare sistematică pentru reducerea riscurilor cibernetice (25).

Un aspect notabil al acestei inițiative este introducerea Automotive SPICE pentru Securitate Cibernetică, care stabilește ghiduri pentru implementarea securității cibernetice în proiectele auto. Acesta servește drept referință pentru implementatorii de modele de proces și evaluatori, permițând evaluarea componentelor de securitate cibernetică (atât la nivel de sistem, cât și software) pe baza cerințelor ISO/SAE 21434 (26). Deși a fost lansată versiunea ASPICE 4.0 (27), ASPICE pentru Securitate Cibernetică rămâne un modul suplimentar independent, mai degrabă decât o parte integrată în procesul de cartografiere al grupurilor PAM 4.0. Această decizie subliniază caracterul specializat al securității cibernetice în dezvoltarea auto, recunoscând că aceasta implică provocări distincte care necesită o atenție dedicată.

ASPICE pentru Securitate Cibernetică extinde Automotive SPICE prin introducerea unui nou grup de procese și modificarea grupurilor de procese Acquisition (ACQ) și Management (MAN) (26). Acest lucru asigură că fiecare proces din ASPICE PAM este susținut de rezultate specifice, produse de ieșire desemnate și practici fundamentale de bază, făcându-l mai aplicabil pentru evaluările de securitate cibernetică. Deși ASPICE pentru Securitate Cibernetică urmează o abordare formalizată de evaluare, evaluarea calității produsului necesită analize tehnice detaliate și liste de verificare pentru revizuirea produselor de lucru (28).

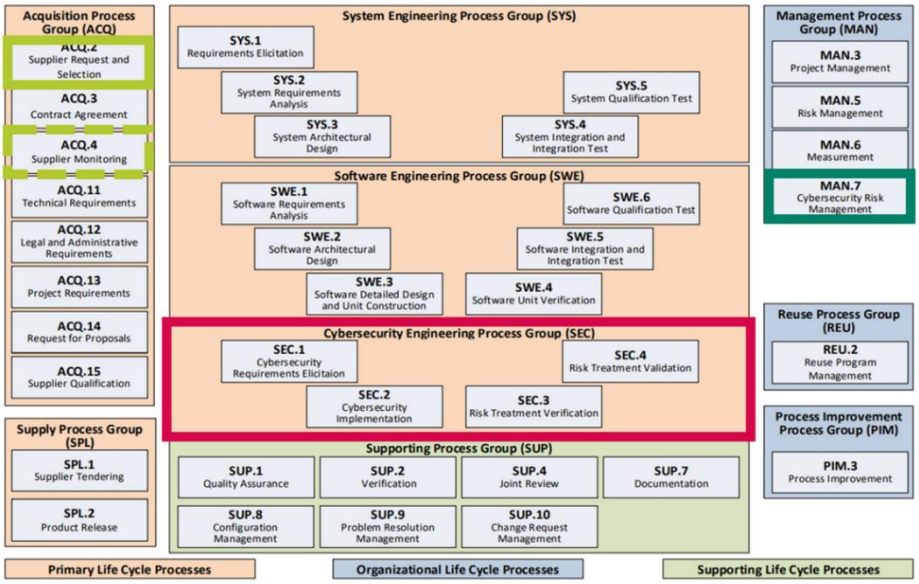

Fig. 1. Prezentare generală a ASPICE– Model de Referință al Proceselor (PRM) [24]

O schimbare structurală majoră este introducerea Grupului de Procese de Inginerie a Securității Cibernetice (SEC), care include patru procese esențiale pentru securitatea cibernetică: Elicitarea Cerințelor de Securitate Cibernetică (SEC.1), Implementarea Securității Cibernetice (SEC.2), Verificarea Tratamentului Riscurilor (SEC.3) și Validarea Tratamentului Riscurilor (SEC.4). Fiecare dintre aceste procese este aliniat cu obiectivele generale de securitate cibernetică, asigurând o abordare sistematică pentru identificarea și reducerea riscurilor de securitate cibernetică în industria auto (29). În plus, procesul Managementul Riscului de Securitate Cibernetică (MAN.7) este acum integrat în Grupul de Procese de Management (MAN), punând accent pe analiza continuă a amenințărilor și evaluarea riscurilor (TARA) (30). Această integrare este esențială, deoarece facilitează identificarea, prioritizarea, monitorizarea și reducerea riscurilor, asigurând în același timp conformitatea cu reglementările globale privind securitatea cibernetică.

Prin alinierea ASPICE pentru Securitate Cibernetică la Regulamentul UNECE R155, acest cadru nu doar că îndeplinește cerințele reglementare, ci stabilește și un standard mai ridicat pentru cele mai bune practici în domeniul securității cibernetice din industria auto. Abordarea sa structurată asigură că producătorii auto (OEM) și furnizorii pot naviga complexitatea securității cibernetice auto, protejând vehiculele conectate împotriva amenințărilor digitale emergente, menținând totodată încrederea consumatorilor și conformitatea cu reglementările.

ASPICE pentru Securitate Cibernetică este strâns legat de ISO/SAE 21434, în special în ceea ce privește identificarea lacunelor în gestionarea ciclului de viață, procesele de securitate și evaluările riscurilor (31). În timp ce Automotive SPICE PAM 3.1 și ASPICE pentru Securitate Cibernetică acoperă în principal ingineria sistemelor și software-ului, ele nu includ indicatori pentru disciplinele ingineriei mecanice și hardware-ului. Totuși, odată cu lansarea ASPICE PAM 4.0, a fost introdus Grupul de Procese pentru Ingineria Hardware-ului, extinzând cadrul pentru a aborda preocupările mai largi legate de securitatea auto (27).

Deși ASPICE pentru Securitate Cibernetică este integrat cu ISO/SAE 21434, acesta nu acoperă toate elementele din cadrul acestuia. Anumite aspecte, cum ar fi managementul securității cibernetice, măsurile de securitate continue și acțiunile post-dezvoltare, sunt gestionate în cadrul Sistemului de Management al Securității Cibernetice Auto (ACSMS) și sunt evaluate separat în timpul unui audit ACSMS (7).

ASPICE pentru Securitate Cibernetică joacă un rol esențial în avansarea măsurilor de securitate cibernetică din industria auto, oferind un cadru structurat pentru gestionarea riscurilor și conformitate. Prin integrarea cu UNECE WP.29 R155 și alinierea la ISO/SAE 21434, acest model asigură că securitatea cibernetică este inclusă sistematic în procesele de dezvoltare auto. Introducerea de noi procese specifice securității cibernetice, modele de evaluare și produse de lucru consolidează capacitatea OEM-urilor și furnizorilor de a atenua amenințările cibernetice într-un mediu auto din ce în ce mai conectat. Pe măsură ce amenințările cibernetice continuă să evolueze, ASPICE pentru Securitate Cibernetică devine esențial pentru asigurarea conformității reglementare, protejarea sistemelor vehiculului și menținerea încrederii consumatorilor. Abordarea sa structurată ajută companiile auto să implementeze măsuri robuste de securitate cibernetică, sprijinind reziliența pe termen lung împotriva amenințărilor digitale din industria auto.

DEZVOLTAREA MATRICEI DE CONFORMITATE

Asigurarea conformității cu multiple standarde din industria securității cibernetice auto reprezintă un proces complex, dar esențial. Două dintre cele mai importante standarde, ISO/SAE 21434 (6) și ASPICE pentru Securitate Cibernetică (7), oferă cadre structurate pentru ingineria securității cibernetice și evaluarea proceselor. Având în vedere necesitatea organizațiilor din domeniul auto de a respecta ambele standarde, a fost dezvoltată o matrice de conformitate pentru a alinia sistematic cerințele acestora. Această matrice servește drept instrument structurat pentru facilitarea înțelegerii, implementării și conformității simultane cu ISO/SAE 21434 și ASPICE pentru Securitate Cibernetică.

Scopul principal al matricei de conformitate este de a oferi o cartografiere clară între cerințele ISO/SAE 21434 și practicile de bază ASPICE. Această abordare îmbunătățește eforturile de conformitate prin identificarea suprapunerilor și corespondențelor dintre cele două standarde, reducând astfel duplicarea muncii și crescând eficiența auditurilor și evaluărilor. Matricea oferă, de asemenea, raționalizări detaliate pentru a ajuta practicienii să înțeleagă cum implementarea unui standard sprijină conformitatea cu celălalt, asigurând o abordare integrată a securității cibernetice. Mai mult, aceasta servește ca instrument de îmbunătățire continuă, permițând organizațiilor să își rafineze și să își îmbunătățească procesele de securitate cibernetică în funcție de evoluția amenințărilor și a cerințelor de reglementare.

Dezvoltarea matricei de conformitate a început prin crearea unui instrument bazat pe Excel, ales pentru capacitatea sa de a gestiona seturi mari de date cu relații complexe. Procesul a implicat listarea tuturor cerințelor relevante din ISO/SAE 21434 pe un ax și cartografierea acestora în raport cu practicile de bază ale ASPICE pentru Securitate Cibernetică pe celălalt ax. Relațiile de cartografiere au variat de la unu-la-unu, unu-la-multe, multe-la-unu și multe-la-multe, necesitând o analiză detaliată pentru a asigura precizia și completitudinea. Pentru consolidarea relațiilor din matrice, fiecare corelare a fost justificată prin analizarea intenției, domeniului de aplicare și utilizării cerințelor din ambele standarde, identificarea temelor comune, cum ar fi evaluarea riscurilor, analiza amenințărilor și verificarea securității, și explicarea modului în care conformitatea cu un standard contribuie la conformitatea cu celălalt. În timpul dezvoltării matricei de conformitate, au apărut mai multe provocări. Diferențele de terminologie dintre ISO/SAE 21434 și ASPICE pentru Securitate Cibernetică au condus uneori la interpretări greșite, necesitând o analiză atentă pentru a stabili echivalențele. Variabilitatea structurală a reprezentat o dificultate suplimentară, deoarece ISO/SAE 21434 urmează un model bazat pe cerințe, în timp ce ASPICE este centrat pe procese, ceea ce a impus o abordare flexibilă a corelării. Unele cerințe ISO/SAE 21434 se suprapuneau cu multiple practici ASPICE, în timp ce altele nu aveau un corespondent direct, ceea ce a necesitat o analiză aprofundată pentru a gestiona aceste goluri de conformitate. Pentru a asigura precizia și aplicabilitatea practică, matricea de conformitate a trecut prin mai multe iterații de rafinare. Experții în securitate cibernetică auto au revizuit relațiile de cartografiere și raționalizările, identificând inconsecvențele și propunând îmbunătățiri. Ulterior, matricea a fost testată în proiecte reale, evaluându-se eficiența sa în optimizarea eforturilor de conformitate. Pe baza feedback-ului primit și a rezultatelor

testelor, au fost efectuate ajustări pentru îmbunătățirea utilizabilității și preciziei acesteia. Având în vedere limitările unui instrument bazat pe Excel, în special în ceea ce privește scalabilitatea și experiența utilizatorului, matricea de conformitate a fost transformată într-o aplicație web. Această tranziție a adus numeroase avantaje. O matrice de conformitate bazată pe web permite accesul în timp real de pe orice dispozitiv, facilitând colaborarea între echipe distribuite geografic. Aplicația dispune de o interfață intuitivă și interactivă, cu funcționalități de căutare, filtrare și hyperlinkuri, îmbunătățind utilizabilitatea. Actualizările centralizate asigură că toți utilizatorii au acces la cele mai recente informații, evitând ineficiențele actualizării manuale a mai multor versiuni de fișiere Excel. În plus, aplicația web poate fi integrată cu instrumente de management al proiectelor și documentației, sporind eficiența conformității.

Dezvoltarea matricei de conformitate și tranziția sa către o platformă web au implicații majore asupra eforturilor de conformitate în industria auto. Organizațiile pot economisi timp și resurse prin utilizarea matricei pentru abordarea simultană a mai multor standarde, în timp ce formatul web simplifică navigarea, implementarea și accesul la documentație. Un instrument centralizat de conformitate asigură aplicarea consecventă a standardelor de securitate cibernetică în cadrul diferitelor proiecte și echipe, reducând riscul de inconsecvențe sau lacune. Raționalizările detaliate incluse în matrice îmbunătățesc înțelegerea practicienilor asupra modului în care diferite standarde interacționează, sporind eficacitatea proceselor de securitate cibernetică. În timpul auditurilor sau evaluărilor de reglementare, matricea de conformitate servește ca dovadă concretă a conformității, iar platforma web facilitează prezentarea și revizuirea eficientă a documentației necesare. În ansamblu, matricea de conformitate este un instrument revoluționar în domeniul securității cibernetice auto, asigurând alinierea fără probleme între ISO/SAE 21434 și ASPICE pentru Securitate Cibernetică. Abordarea sa structurată, corelările revizuite de experți și implementarea web permit organizațiilor să navigheze mai eficient prin cerințele complexe ale securității cibernetice, consolidând conformitatea reglementară, gestionarea riscurilor de securitate cibernetică și reziliența globală a industriei auto.

MAPAREA ÎNTRE ISO/SAE 21434 ȘI ASPICE

Maparea dintre ISO/SAE 21434 (6) și ASPICE pentru Securitate Cibernetică (7) urmărește alinierea cerințelor și proceselor acestor două standarde esențiale pentru securitatea cibernetică auto, asigurând conformitatea integrată și implementarea eficientă în dezvoltarea vehiculelor. Acest capitol prezintă corelările detaliate între anumite clauze din ISO/SAE 21434 (7, 9, 10, 11 și 15) și practicile de bază corespunzătoare din ASPICE pentru Securitate Cibernetică.

Pentru fiecare clauză din ISO/SAE 21434, maparea include explicații despre modul în care cerințele specifice corespund practicilor de bază ale ASPICE. În plus, sunt furnizate raționalizări care clarifică relațiile dintre cele două standarde, asigurând că practicienii înțeleg modul în care conformitatea cu un standard sprijină respectarea celuilalt.

Această mapare detaliată reprezintă un instrument practic pentru organizațiile care doresc să își eficientizeze eforturile de conformitate. Prin identificarea alinierilor și corespondențelor, practicienii pot reduce redundanța, îmbunătăți eficiența implementării și stabili o abordare unificată a securității cibernetice. În cele din urmă, acest cadru de mapare facilitează conformitatea simultană cu ambele standarde, promovând o abordare mai coerentă și eficientă a securității cibernetice în industria auto.

Deoarece acesta este un rezumat al tezei de doctorat, va fi prezentată doar o selecție de mapări între ISO/SAE 21434 și ASPICE pentru Securitate Cibernetică. Următorul exemplu ilustrează alinierea între cerința ISO 21434 RQ-10-01 și practicile de bază ASPICE pentru Securitate Cibernetică SEC.2.BP1, SEC.2.BP4 și SEC.2.BP6.

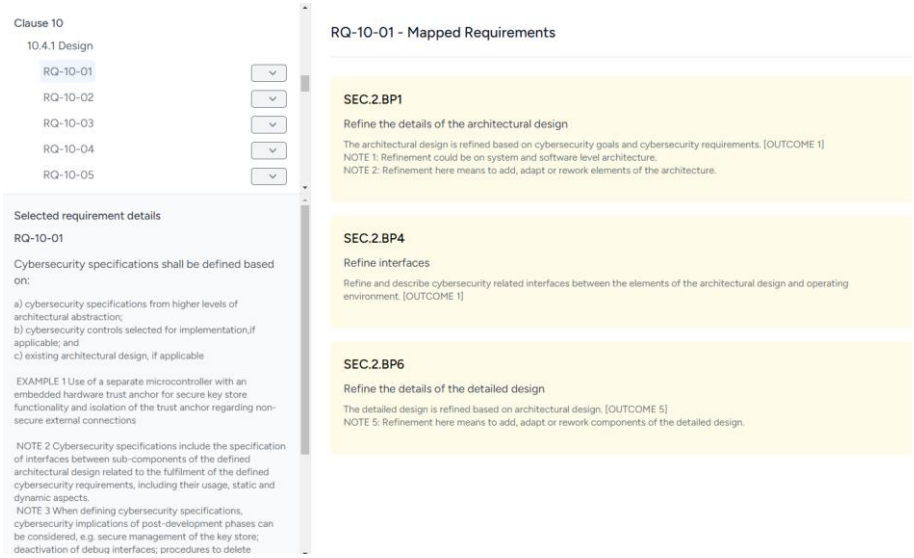

Fig.5. Maparea ISO 21434 Requirement RQ-10-01

Cerința ISO 21434 RQ-10-01 impune ca specificațiile de securitate cibernetică să fie definite pe baza unor elemente esențiale, inclusiv specificațiile de securitate cibernetică de nivel superior, controalele de securitate selectate și proiectele arhitecturale existente. Această cerință subliniază integrarea timpurie a măsurilor de securitate cibernetică în arhitectura sistemului, în locul implementării lor tardive în procesul de dezvoltare. De asemenea, solicită o descriere detaliată a interfețelor dintre subcomponente, acoperind atât aspectele statice, cât și cele dinamice, pentru a asigura interacțiuni sigure. În plus, include măsuri de securitate post-dezvoltare, cum ar fi stocarea sigură a cheilor criptografice, dezactivarea interfețelor de depanare și protecția informațiilor de identificare personală. Cerința sugerează, de asemenea, identificarea parametrilor de configurare și calibrare, precum setarea corectă a modulelor de securitate hardware (HSM), și evaluarea capacităților componentelor, inclusiv performanța procesorului și resursele de memorie, pentru a asigura implementarea eficientă a controalelor de securitate cibernetică.

În ASPICE pentru Securitate Cibernetică, practicile de bază SEC.2.BP1, SEC.2.BP4 și SEC.2.BP6 sunt aliniate îndeaproape cu RQ-10-01, oferind o abordare structurată pentru integrarea securității cibernetice în proiectarea arhitecturală și detaliată.

SEC.2.BP1 se concentrează pe rafinarea proiectării arhitecturale pentru a încorpora obiectivele și cerințele de securitate cibernetică la nivel de sistem și software. Acest lucru asigură că securitatea cibernetică este o parte integrantă a procesului de proiectare, aliniindu-se cu accentul pus de ISO 21434 pe utilizarea specificațiilor de securitate cibernetică de nivel superior și a arhitecturilor existente.

SEC.2.BP4 abordează securitatea interfețelor dintre elementele sistemului și mediul lor operațional, asigurând că toate interfețele sunt analizate și definite în ceea ce privește implicațiile lor de securitate cibernetică. Acest aspect susține direct cerința RQ-10-01, care solicită specificații detaliate ale interfețelor dintre subcomponente, permițând interacțiuni sigure și reducând vulnerabilitățile potențiale.

SEC.2.BP6 se asigură că rafinamentele proiectării detaliate încorporează măsuri de securitate cibernetică, abordând aspecte specifice ale implementării, precum selecția hardware-ului (de exemplu, performanța procesorului și resursele de memorie) și configurațiile software-ului. Această practică este în conformitate cu cerința RQ-10-01, care pune accent pe capacitățile componentelor și pe parametrii de configurare necesari pentru a sprijini controalele eficiente de securitate cibernetică.

Împreună, aceste practici ASPICE asigură integrarea sistematică a considerațiilor de securitate cibernetică la toate nivelurile proiectării, de la arhitectura de nivel înalt până la detaliile fiecărei componente. Această abordare holistică garantează că riscurile de securitate cibernetică identificate în fazele de analiză a amenințărilor și evaluare a riscurilor (TARA) sunt atenuate eficient prin strategii arhitecturale și de proiectare cuprinzătoare.

Cerința ISO/SAE 21434 RQ-10-02 impune ca cerințele de securitate cibernetică să fie alocate unor componente specifice ale arhitecturii sistemului. Această cerință evidențiază importanța integrării considerațiilor de securitate direct în arhitectura sistemului, asigurând că fiecare componentă contribuie la un cadru cuprinzător de securitate cibernetică. Prin atribuirea cerințelor de securitate cibernetică fiecărei componente, organizațiile garantează integrarea securității la toate nivelurile sistemului, creând o apărare stratificată împotriva potențialelor amenințări cibernetice. Acest proces de alocare este esențial pentru construirea unor mecanisme robuste de apărare cibernetică, deoarece asigură că toate elementele arhitecturale contribuie colectiv la atingerea obiectivelor globale de securitate cibernetică..

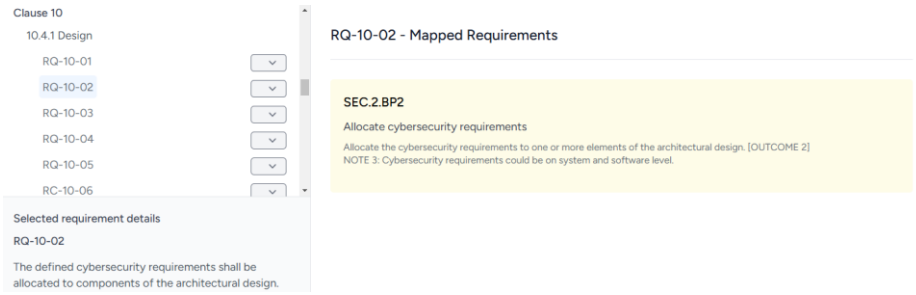

Fig. 62. Maparea ISO 21434 Requirement RQ-10-02

Această cerință ISO este strâns aliniată cu practica de bază SEC.2.BP2 din ASPICE pentru Securitate Cibernetică, care se concentrează pe atribuirea cerințelor de securitate cibernetică unor elemente specifice ale arhitecturii sistemului. SEC.2.BP2 solicită o alocare deliberată și sistematică a cerințelor de securitate atât pentru componentele hardware, cât și pentru cele software, asigurând că riscurile identificate sunt atenuate la toate nivelurile sistemului. Nota care însoțește SEC.2.BP2 subliniază faptul că cerințele de securitate cibernetică pot fi alocate la nivel de sistem, abordând securitatea hardware-ului și a infrastructurii, sau la nivel software, protejând aplicațiile și codul acestora.

Atât cerința ISO RQ-10-02, cât și practica ASPICE SEC.2.BP2 subliniază că simpla definire a cerințelor de securitate cibernetică nu este suficientă; aceste cerințe trebuie distribuite în mod atent și strategic în cadrul componentelor sistemului pentru a asigura eficiența lor. Această abordare permite ca măsurile de securitate să fie adaptate funcționalităților și vulnerabilităților specifice fiecărei componente, consolidând astfel postura generală de securitate a sistemului.

În plus, atât cerința ISO, cât și practica ASPICE subliniază necesitatea de a lua în considerare toate nivelurile sistemului în procesul de alocare a cerințelor de securitate cibernetică. Amenințările cibernetice pot viza orice strat al arhitecturii sistemului, iar alocarea cerințelor de securitate la mai multe niveluri asigură o protecție completă. Această strategie de apărare în profunzime, promovată pe scară largă în cele mai bune practici de securitate cibernetică, implementează mai multe straturi de securitate pentru a atenua o varietate de amenințări.

STUDII DE CAZ

În Studiul de Caz A, utilizarea strategică a Matricei de Conformitate a dus la o reducere a costurilor cu 52% în timpul evaluării ASPICE. Prin abordarea proactivă a neconformităților identificate în auditul

ISO/SAE 21434 și maparea acestora cu practicile de bază din ASPICE pentru Securitate Cibernetică, echipa de proiect a minimizat eforturile duplicate și a închis eficient lacunele înainte de evaluarea ASPICE. Acest proces a optimizat evaluarea, reducând timpul și resursele necesare pentru conformitate. Impactul acestei abordări a fost vizibil în mai multe faze ale auditului. Auditul de Proiect a fost redus de la patru la trei zile, Faza de Pregătire de la trei la o zi, iar Faza de Închidere a Lacunelor de la cinci la două zile. Aceste reduceri au fost realizate prin utilizarea matricei de conformitate pentru a alinia sistematic neconformitățile ISO cu practicile ASPICE, asigurând că multe probleme au fost rezolvate în avans. Aceasta a dus la un număr mai mic de neconformități noi în timpul evaluării ASPICE, permițând evaluatorilor să se concentreze pe practicile specifice ASPICE care necesitau atenție.

Tabel 1. Reducerea eforturilor în cazul în care un audit ISO/SAE a fost deja efectuat (Valorile sunt exprimate ca Număr de Angajați x Număr de Zile)

	ISO 21434	ASPICE	Îmbunătățire ASPICE
Audit Organizațional	5x5		
Audit/ Evaluare Proiect	5x5	5x4 ->	5x3
Pregătire	6x5	6x3 ->	6x1
Închidere lacune	10x5	6x5 ->	6x2

Dincolo de economiile de timp și resurse, matricea de conformitate a îmbunătățit pregătirea echipei, facilitând o documentație mai bună, o comunicare mai eficientă cu evaluatorii și o înțelegere mai clară a cerințelor de conformitate. Deși nu toate practicile de bază ASPICE corespund direct cu ISO/SAE 21434, această abordare proactivă a redus surprizele în timpul evaluării, ajutând echipa să abordeze cerințele ASPICE într-un mod mai eficient. Economiile de costuri s-au extins dincolo de evaluarea imediată, având un impact pozitiv asupra eficienței pe termen lung a conformității. Reputația furnizorului în gestionarea securității cibernetice a fost consolidată, sporind încrederea OEM-urilor și creând noi oportunități de afaceri. Prin instituționalizarea matricei de conformitate, furnizorul Tier 1 poate replica aceste beneficii în proiectele viitoare, făcând conformitatea mai eficientă, scalabilă și rentabilă.

În Studiul de Caz B, utilizarea strategică a Instrumentului Web Matricea de Conformitate de către un furnizor Tier 1 a dus la o reducere a costurilor cu 37% în timpul auditului ISO 21434. Prin valorificarea mapării neconformităților din evaluarea ASPICE, furnizorul a optimizat procesul de conformitate ISO, reducând alocarea resurselor și costurile aferente auditului. Munca preexistentă din evaluarea ASPICE a oferit o bază solidă pentru conformitatea cu ISO 21434, minimizând eforturile duplicate și optimizând fluxul de lucru al auditului (6,7).

Deși faza auditului organizațional a rămas neschimbată, necesitând cinci angajați timp de cinci zile, s-au înregistrat reduceri semnificative în celelalte faze ale auditului. Auditul de proiect s-a redus de la cinci zile la trei, faza de pregătire de la cinci zile la două, iar faza de închidere a lacunelor de la cinci zile la trei. Aceste reduceri au fost obținute prin identificarea preventivă a lacunelor de securitate cibernetică cu ajutorul matricei de conformitate, permițând o alocare mai eficientă a resurselor și reducerea evaluărilor redundante..

Tabel 2. Reducerea eforturilor în cazul în care o evaluare ASPICE a fost deja efectuată (Valorile sunt exprimate ca Număr de Angajați x Număr de Zile)

	ASPICE	ISO 21434	Îmbunătățire ISO 21434
Audit Organizațional		5x5 ->	5x5
Audit/ Evaluare Proiect	5x4	5x5 ->	5x3
Pregătire	6x3	6x5 ->	6x2
Închidere lacune	6x5	10x5 ->	10x3

Această eficiență a întărit angajamentul furnizorului față de securitatea cibernetică, consolidând încrederea OEM-ului și conducând potențial la noi oportunități de afaceri. Instituționalizarea metodologiei matricei de conformitate asigură că beneficiile economice pot fi replicate în mai multe proiecte, făcând conformitatea mai eficientă și mai scalabilă. Acest studiu de caz evidențiază modul în care planificarea proactivă, utilizarea strategică a resurselor și alinierea standardelor pot aduce avantaje financiare și operaționale semnificative în peisajul tot mai reglementat al securității cibernetice în industria auto.

ANALIZĂ FINANCIARĂ

Analiza cost-beneficiu a instrumentului de conformitate pentru evaluările ASPICE pentru Securitate Cibernetică demonstrează îmbunătățiri semnificative în eficiență și performanță financiară. Comparând costurile planificate versus costurile reale, studiul confirmă că instrumentul oferă un randament ridicat al investiției (ROI), cu economii considerabile de costuri generate prin reducerea efortului necesar, optimizarea documentației și accelerarea procesului de închidere a lacunelor.

Implementarea instrumentului de conformitate a dus la reduceri semnificative ale costurilor pentru efectuarea evaluării ASPICE pentru Securitate Cibernetică, în principal prin scăderea timpului de pregătire, eficientizarea revizuirii documentației și accelerarea procesului de remediere a neconformităților. Costul inițial al evaluării, care era de 62.368,94 EUR, a fost redus la 29.440,91 EUR după utilizarea instrumentului. Luând în considerare taxa anuală de abonament de 2.250 EUR, costul total după implementare a fost de 31.690,91 EUR, ceea ce a dus la economii totale de 32.928,03 EUR.

Impactul financiar al instrumentului de conformitate a fost evaluat prin indicatori financiari esențiali:

- Valoarea Actualizată Netă (NPV): 30.678,03 EUR, indicând un câștig economic net semnificativ după deducerea costului instrumentului.
- Raport Beneficiu-Cost (BCR): 14,65, ceea ce înseamnă că pentru fiecare 1 EUR investit, organizația a obținut 14,65 EUR în beneficii financiare, demonstrând profitabilitatea ridicată a instrumentului.

- Randamentul Investiției (ROI): 1367,9%, indicând că pentru fiecare 1 EUR investit, organizația a economisit 13,68 EUR, confirmând astfel că instrumentul este o investiție extrem de valoroasă.

Deși costurile regionale ale forței de muncă, în special în Bavaria, Germania, pot influența estimările de costuri, instrumentul a demonstrat constant reducerea timpului și costurilor asociate evaluărilor. Cu toate acestea, factori precum nivelul de expertiză al echipei, complexitățile neprevăzute și schimbările de reglementare pot influența proiecțiile financiare, necesitând o abordare flexibilă în gestionarea resurselor financiare.

În ciuda acestor provocări, instrumentul de conformitate optimizează alocarea resurselor financiare, îmbunătățește eficiența conformității și accelerează procesele de evaluare, demonstrându-și valoarea în industrii puternic reglementate, precum securitatea cibernetică în domeniul auto. Instrumentul asigură sustenabilitate pe termen lung în eforturile de conformitate, permițând organizațiilor să îndeplinească cerințele de reglementare, menținând în același timp eficiența operațională și optimizarea costurilor.

Acești indicatori financiari confirmă faptul că instrumentul de conformitate îmbunătățește semnificativ eficiența costurilor în evaluările de securitate cibernetică, oferind randamente ridicate, recuperare rapidă a costurilor și beneficii financiare pe termen lung. Implementarea sa nu doar reduce costurile asociate evaluărilor, ci și crește eficiența conformității, făcând din acesta un instrument strategic pentru organizațiile care gestionează cerințele de reglementare în securitatea cibernetică auto.

CONTRIBUȚIA ȘTIINȚIFICĂ

Această cercetare aduce mai multe contribuții semnificative în domeniul conformității cu cerințele de securitate cibernetică în industria auto, concentrându-se pe îmbunătățirea eficienței, integrării și automatizării proceselor de conformitate. Contribuțiile cheie ale acestei lucrări pot fi rezumate astfel:

1. Dezvoltarea unei Matrice de Conformitate pentru ASPICE pentru Securitate Cibernetică și ISO/SAE 21434

Această matrice acoperă decalajul dintre ASPICE pentru Securitate Cibernetică și ISO/SAE 21434, oferind o mapare structurată a cerințelor comune. Reduce munca redundantă, identificând activitățile de conformitate comune și diminuând astfel efortul inutil. Îmbunătățește alinierea dintre procesele de dezvoltare software și managementul riscurilor de securitate cibernetică. Crește pregătirea pentru audituri, oferind o abordare clară și structurată pentru verificarea conformității. Facilitează conformitatea continuă, permițând actualizări și întreținerea documentației de securitate cibernetică.

2. Dezvoltarea unui Instrument Web pentru Conformitate

Înlocuiește urmărirea conformității bazată pe Excel cu o platformă dinamică și interactivă. Automatizează verificarea conformității, reducând efortul manual în evaluarea alinierii cu standardele. Permite urmărirea în timp real a conformității cu cerințele de securitate cibernetică, îmbunătățind vizibilitatea proiectelor. Sprijină colaborarea echipelor, permițând implicarea mai multor părți interesate într-un sistem centralizat de conformitate. Facilitează actualizări și scalabilitate, adaptându-se la schimbările cerințelor de reglementare fără a necesita reproiectări majore.

3. Integrarea Standardelor de Securitate Cibernetică într-un Cadru Unificat

Prezintă o metodologie pentru integrarea mai multor standarde de securitate cibernetică într-un singur cadru de conformitate. Reduce complexitatea respectării cerințelor de reglementare, făcând conformitatea mai eficientă. Asigură o abordare sistematică pentru gestionarea conformității între cadre multiple, facilitând organizațiilor administrarea mai multor standarde simultan. Permite organizațiilor tranziția către un model de conformitate continuă, reducând eforturile de certificare de ultim moment.

4. Contribuții Practice pentru Industrie

Simplifică procesele de conformitate pentru OEM-uri și furnizori, reducând costurile și efortul necesar pentru evaluările de securitate cibernetică. Optimizează fluxurile de lucru pentru conformitate, asigurându-se că standardele de securitate sunt respectate fără a perturba procesele de dezvoltare. Îmbunătățește formarea și transferul de cunoștințe, făcând conformitatea mai ușor de înțeles și de implementat în cadrul echipelor de inginerie. Abordează nevoia unei metodologii structurate pentru conformitate, umplând un gol existent în industrie privind alinierea ASPICE pentru Securitate Cibernetică cu ISO/SAE 21434.

5. Contribuții Academice

Extinde cercetările privind integrarea standardelor de securitate cibernetică, oferind un model pentru viitoarele studii de conformitate în industria auto. Introduce o metodologie de mapare a cerințelor între cadre multiple, aplicabilă și în alte domenii, cum ar fi siguranța funcțională (ISO 26262). Fundamentează cercetări ulterioare privind instrumentele automate de conformitate, digitalizare și utilizarea inteligenței artificiale (AI) pentru conformitatea în securitate cibernetică. Contribuie la subiectul emergent al "conformității continue", o direcție de cercetare în evoluție în domeniul standardizării securității cibernetice.

În concluzie, această cercetare introduce progrese teoretice și practice în domeniul conformității cu cerințele de securitate cibernetică în industria auto, oferind metodologii structurate, instrumente practice și soluții orientate spre industrie. Prin alinierea ASPICE pentru Securitate Cibernetică cu ISO/SAE 21434, dezvoltarea unei platforme digitale de conformitate și crearea unui cadru pentru conformitatea integrată, această lucrare îmbunătățește eficiența, reduce redundanța și stabilește un nou standard pentru evaluările de securitate cibernetică în sectorul auto.

REFERINȚE

[1] A. Torok, Z. Szalay, and B. Saghi, "New Aspects of Integrity Levels in Automotive Industry-Cybersecurity of Automated Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 1, pp. 383–391, Jan. 2022, doi: 10.1109/TITS.2020.3011523.

[2] H. Martin *et al.*, "Combined automotive safety and security pattern engineering approach," *Reliab Eng Syst Saf*, vol. 198, 2020, doi: 10.1016/j.ress.2019.106773.

[3] D. Zelle, C. Plappert, R. Rieke, D. Scheuermann, and C. Krauß, "ThreatSurf: A method for automated Threat Surface assessment in automotive cybersecurity engineering," *Microprocess Microsyst*, vol. 90, 2022, doi: 10.1016/j.micpro.2022.104461.

[4] Upstream Security Ltd., *2024 Global Automotive Cybersecurity Report - The automotive cybersecurity inflection point: From experimental hacking to large-scale automotive attacks— the focus shifts to im-pact*. 2024.

[5] Upstream Security Ltd., *2023 Global Automotive Cybersecurity Report - The Automotive industry is rapidly expanding into a vast smart mobility ecosystem, introducing new levels of cyber sophistication and attack vectors*. 2023.

[6] ISO/SAE 21434, *ISO/SAE 21434:2021 Road vehicles Cybersecurity engineering*. 2021.

[7] VDA QMC, *Automotive SPICE® Process Reference and Assessment Model for Cybersecurity Engineering*, 1st Edition. VDA QMC, 2021.

[8] Upstream Security Ltd., *2022 Global Automotive Cybersecurity Report - Automotive Cyber Threat Landscape In Light Of New Regulations*. 2022.

[9] L. Rehberg and A. Brem, "Industrial prototyping in the German automotive industry: bridging the gap between physical and virtual prototypes," *Journal of Engineering and Technology Management - JET-M*, vol. 71, 2024, doi: 10.1016/j.jengtecman.2024.101798.

[10] R. Barrios, D. Schippers, C. Heiden, and G. Pappas, "A cybersecurity strategy for Industry 4.0," in *Autonomous Systems: Sensors, Processing, and Security for Vehicles and Infrastructure 2019*, M. C. Dudzik and J. C. Ricklin, Eds., SPIE, May 2019, p. 23. doi: 10.1117/12.2524667.

[11] F. Siddiqui *et al.*, "Cybersecurity Engineering: Bridging the Security Gaps in Advanced Automotive Systems and ISO/SAE 21434," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, IEEE, Jun. 2023, pp. 1–6. doi: 10.1109/VTC2023-Spring57618.2023.10200490.

[12] T. Kaneko, S. Yamashita, A. Takada, and M. Imai, "Triad concurrent approach among functional safety, cybersecurity and SOTIF," *Journal of Space Safety Engineering*, vol. 10, no. 4, 2023, doi: 10.1016/j.jsse.2023.09.001.

[13] G. Baldini, "Detection of cybersecurity spoofing attacks in vehicular networks with recurrence quantification analysis," *Comput Commun*, vol. 191, 2022, doi: 10.1016/j.comcom.2022.05.021.

[14] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and M. Warren, "Cybersecurity Readiness for Automated Vehicles," in *2022 International Conference on Frontiers of Artificial Intelligence and Machine Learning (FAIML)*, IEEE, Jun. 2022, pp. 7–12. doi: 10.1109/FAIML57028.2022.00012.

[15] M. Schellekens, "Car hacking: Navigating the regulatory landscape," *Computer Law and Security Review*, vol. 32, no. 2, 2016, doi: 10.1016/j.clsr.2015.12.019.

[16] Z. Muhammad, Z. Anwar, B. Saleem, and J. Shahid, "Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on Human and Environmental Sustainability," *Energies (Basel)*, vol. 16, no. 3, 2023, doi: 10.3390/en16031113.

[17] R. Aghapour, M. Zeraati, F. Jabari, M. Sheibani, and H. Arasteh, "Cybersecurity and Data Privacy Issues of Electric Vehicles Smart Charging in Smart Microgrids," in *Green Energy and Technology*, 2022. doi: 10.1007/978-3-031-05909-4_4.

[18] Upstream Security Ltd., *2021 Global Automotive Cybersecurity Report - Research Into Cyber Attack Trends In Light Of Cybersecurity Standards And Regulations*. 2021.

[19] UNECE R155, *Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system*. 2021.

[20] UNECE R156, *Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system*. 2021.

[21] S. Japs, F. Kargl, H. Anacker, and R. Dumitrescu, "Why make it hard?-Usage of aggregated statistical data for risk assessment of damage scenarios in the context of ISO/SAE 21434," in *Procedia CIRP*, 2022. doi: 10.1016/j.procir.2022.05.252.

[22] C. Schmittner, B. Schrammel, and S. König, "Asset Driven ISO/SAE 21434 Compliant Automotive Cybersecurity Analysis with ThreatGet," in *Communications in Computer and Information Science*, 2021. doi: 10.1007/978-3-030-85521-5_36.

[23] T. Faschang and G. Macher, "An Open Software-Based Framework for Automotive Cybersecurity Testing," in *Communications in Computer and Information Science*, 2023. doi: 10.1007/978-3-031-42307-9_22.
[24] D. Barmayoun, M. Marian, and R. Bogdan, "Automotive Internal Development Process Improvement for Assuring Compliance with the ASPICE for Cybersecurity Extension," in *Communications in Computer and Information Science*, 2022. doi: 10.1007/978-3-031-15559-8_25.
[25] E. Magdy, "A-SPICE for Cybersecurity: Analysis and Enriched Practices," in *Communications in Computer and Information Science*, 2021. doi: 10.1007/978-3-030-85521-5_37.
[26] N. Moselhy, A. Adel, and A. Seddik, "Automotive SPICE Draft PAM V4.0 in Action: BETA Assessment," in *Communications in Computer and Information Science*, 2023. doi: 10.1007/978-3-031-42310-9_7.
[27] VDA QMC, *ASPICE PAM 4.0*. 2023.
[28] C. Schlager *et al.*, "Consistency of Cybersecurity Process and Product Assessments in the Automotive Domain," in *Communications in Computer and Information Science*, 2023. doi: 10.1007/978-3-031-42307-9_24.
[29] VDA QMC, *Automotive SPICE® for Cybersecurity Guidelines*. 2021.
[30] R. Messnarz, D. Ekert, G. Macher, S. Stolfa, J. Stolfa, and A. Much, "Automotive SPICE for Cybersecurity – MAN.7 Cybersecurity Risk Management and TARA," in *Communications in Computer and Information Science*, 2022. doi: 10.1007/978-3-031-15559-8_23.
[31] VDA QMC, *Automotive SPICE® Guidelines*, 2nd Edition. 2023.