CYBERSECURİTY AND SOFTWARE UPDATE REGULATİONS İN THE AUTOMOTİVE SECTOR: A FULL CİTATİON MAPPİNG ANALYSİS OF UNECE R155 AND R156



Mehmet SEN,

Chief Superintendent (R),
Crime Scene Investigation
and Cyber Security Expert

ABSTRACT

The increasing digitalization of modern vehicles has expanded the cybersecurity attack surface, necessitating regulatory intervention. The United Nations Economic Commission for Europe introduced UNECE Regulation No. 155 and Regulation No. 156 to address cybersecurity risks and software update management in road vehicles. This study provides a structured analysis of these regulations using full citation mapping, linking each requirement to its corresponding regulatory article. The findings demonstrate that R155 establishes a lifecycle-based cybersecurity management framework, while R156 ensures secure and traceable software updates. Together, these regulations form a comprehensive compliance model for software-defined vehicles.

1. INTRODUCTİON

The automotive industry has evolved into a software-driven ecosystem where vehicles are increasingly connected and exposed to cyber threats. This transformation has introduced new risks associated with remote access, software vulnerabilities, and system integration challenges. To mitigate these risks, regulatory frameworks such as UNECE R155 and UNECE R156 have been introduced.

UNECE R155 requires manufacturers to establish a Cybersecurity Management System (CSMS) to manage risks throughout the lifecycle of the vehicle (R155, Art. 5.1.1; Art. 7.2). In parallel, UNECE R156 mandates the implementation of a Software Update Management System (SUMS) to ensure secure and controlled software updates (R156, Art. 5.1; Art. 7.1).

2. CYBERSECURİTY FRAMEWORK UNDER UNECE R155

2.1 CSMS Implementation

Manufacturers are required to establish, implement, and maintain a CSMS to systematically manage cybersecurity risks (R155, Art. 5.1.1). This system must be demonstrated during the type approval process (R155, Art. 7.2).

2.2 Risk Identification and Assessment

R155 mandates that manufacturers identify and assess cybersecurity risks associated with vehicle systems (R155, Art. 5.1.2–5.1.3). This includes evaluating potential vulnerabilities and defining mitigation strategies.

2.3 Threat Analysis (TARA)

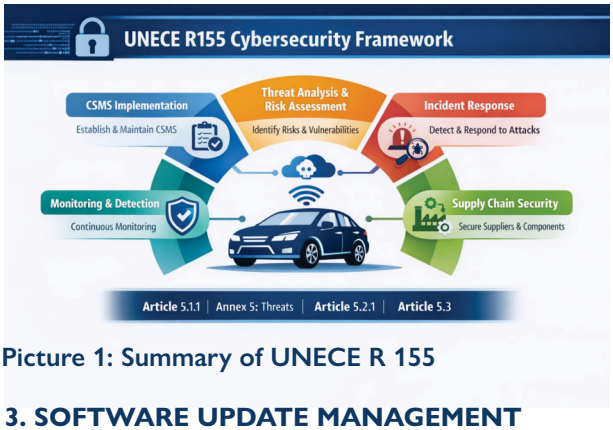
A structured threat analysis approach is required to identify attack vectors and system weaknesses (R155, Art. 5.1.4; Annex 5). Annex 5 provides detailed threat scenarios, including unauthorized access and communication manipulation.

2.4 Incident Detection and Response

Cybersecurity incidents must be detected, monitored, and responded to effectively (R155, Art. 5.2.1–5.2.2). This includes establishing mechanisms for real-time monitoring and incident reporting.

2.5 Supply Chain Security

R155 extends cybersecurity requirements to suppliers and third-party components (R155, Art. 5.3). Manufacturers must ensure that all components meet cybersecurity requirements.



Picture 1: Summary of UNECE R 155

3. SOFTWARE UPDATE MANAGEMENT UNDER UNECE R156

3.1 SUMS Implementation

Manufacturers must establish a Software Update Management System (SUMS) to manage software updates securely (R156, Art. 5.1). Compliance must be demonstrated during type approval (R156, Art. 7.1).

3.2 Integrity and Authenticity

Software updates must maintain integrity and authenticity at all times (R156, Art. 5.2.1–5.2.2). This ensures that updates are not tampered with or unauthorized.

3.3 Version Control and Traceability

Manufacturers must maintain detailed records of software versions and updates (R156, Art. 5.3–5.4). This enables full traceability throughout the vehicle lifecycle.

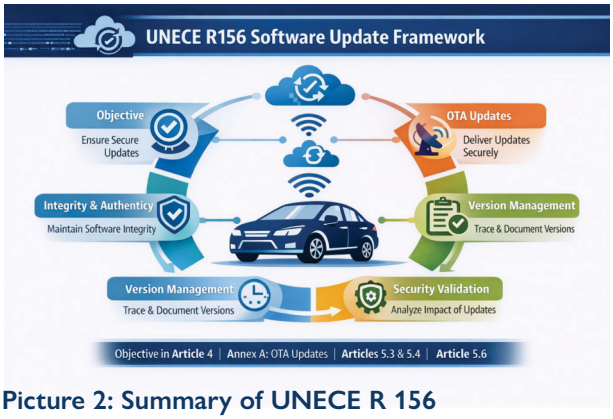
3.4 Secure OTA Updates

Over-the-Air (OTA) updates must be securely deployed and verified (R156, Art. 5.5; Annex 1). This includes :

authentication and validation processes before installation.

3.5 Safety Validation

Software updates must not negatively affect vehicle safety or regulatory compliance (R156, Art. 5.6). Safety validation is required prior to deployment.



Picture 2: Summary of UNECE R 156

4. INTEGRATİON OF R155 AND R156

R155 and R156 operate as complementary frameworks. While R155 focuses on identifying and mitigating cybersecurity risks, R156 ensures that software updates are securely managed. Together, they provide an end-to-end lifecycle security approach.

The integration of these regulations ensures:

Continuous risk management (R155, Art. 5.1)

Secure update processes (R156, Art. 5.5)

Lifecycle traceability (R156, Art. 5.3)

5. IMPLEMENTATİON CHALLENGES

5.1 Technical Challenges

Complexity of ECU-based architectures

Integration of cybersecurity controls

Secure OTA implementation

5.2 Organizational Challenges

Supplier coordination (R155, Art. 5.3)

Documentation and compliance

5.3 Regulatory Challenges

Type approval requirements (R155, Art. 7.2; R156, Art. 7.1)

Continuous compliance monitoring

6. CONCLUSİON

UNECE R155 and R156 establish a comprehensive regulatory framework for automotive cybersecurity and software update management. R155 ensures that cybersecurity risks are managed throughout the vehicle lifecycle, while R156 guarantees that software updates are secure, traceable, and compliant. The integration of these regulations is essential for the safe deployment of software-defined vehicles.

REFERENCE LİST

1. United Nations Economic Commission for Europe (UNECE).UN Regulation No. 155 – Uniform provisions concerning the approval of vehicles with regard to cybersecurity and cybersecurity management system. Geneva: UNECE, 2021.

2. UNECE. UN Regulation No. 155 (Cyber security and Cyber Security Management System).

Автомобиль секторындағы киберқауіпсіздік және бағдарламалық қамтамасыз етуді жаңарту ережелері: UNECE R155 және R156 бойынша сілтемелерді толық картаға түсіру талдауы

Мехмет Шен, бас суперинтендант (R), қылмыс орнын тергеу және киберқауіпсіздік сарапшысы

Аңдатпа

Заманауи көліктердің цифрлануының артуы киберқауіпсіздікке қатысты шабуылдардың ауқымын кеңейтті, бұл реттеуші шаралардың енгізілуін қажет етеді. Біріккен Ұлттар Ұйымының Еуропалық экономикалық комиссиясы жол көліктеріндегі киберқауіпсіздік тәуекелдерін және бағдарламалық қамтамасыз етуді жаңарту басқаруын реттеу үшін UNECE №155 және №156 ережелерін енгізді.

Бұл зерттеу аталған ережелерді толық дәйексөздік сәйкестік әдісі арқылы құрылымдық түрде талдайды, әрбір талапты тиісті нормативтік баптармен байланыстырады. Зерттеу нәтижелері R155 ережесінің өмірлік циклге негізделген киберқауіпсіздік басқару жүйесін қалыптастыратынын, ал R156 ережесінің қауіпсіз әрі бақыланатын бағдарламалық жаңартуларды қамтамасыз ететінін көрсетеді.

Осылайша, аталған екі регламент бірге бағдарламалық қамтамасыз етуге негізделген көлік құралдары үшін кешенді сәйкестік моделін қалыптастырады.

Аннотация

Возрастающая цифровизация современных транспортных средств расширила поверхность кибератак, что обусловило необходимость нормативного вмешательства. Европейская экономическая комиссия Организации Объединённых Наций (UNECE) ввела Регламент № 155 и Регламент № 156 для управления рисками кибербезопасности и обновлениями программного обеспечения в дорожных транспортных средствах. В данном исследовании представлен структурированный анализ этих регламентов с использованием метода полной картографии ссылок, при котором каждое требование соотносится с соответствующей статьёй нормативного акта. Результаты показывают, что R155 формирует систему управления кибербезопасностью на протяжении всего жизненного цикла, тогда как R156 обеспечивает безопасность и прослеживаемость обновлений программного обеспечения. В совокупности эти регламенты образуют комплексную модель соответствия для программно-определяемых транспортных средств.