BlackBerry | QNX

WP.29 CYBERSECURITY VEHICLE REGULATION COMPLIANCE

WHAT IS WP.29?

Learn about the UNECE WP.29 regulations, the countries where they apply and how they aim to mitigate the cybersecurity risks posed to passenger vehicles.

GET THIS GUIDE AS A PDF CONTACT US →

In June 2020, WP.29 adopted a new international automotive cybersecurity regulation to pave the way for connected vehicles and mitigate the cybersecurity risks posed to passenger vehicles. The regulation establishes performance and audit requirements for cybersecurity and software update management for new passenger vehicles sold in the European Union and dozens of other countries. Specifically, WP.29 is the name of the World Forum for Harmonization of Vehicle Regulations, a United Nations Economic Commission for Europe's (UNECE's) Sustainable Transport Division working party. WP.29 incorporates into its regulatory framework technological innovations to make vehicles safer and more environmentally sound.

The cybersecurity and software update proposals adopted by WP.29 require automakers to implement measures to:

- Manage vehicle cybersecurity risks.
- Secure vehicles by design to mitigate risks along the supply chain.
- Detect and respond to security incidents across the vehicle fleet.
- Provide safe, secure software updates that do not compromise vehicle safety.

Three lifecycle phases are specifically called out in the cybersecurity regulation: development, production and post-production, which includes monitoring, detecting and responding to cyberattacks.

Passenger cars, vans, trucks and buses and other light vehicles are subject to the regulation as of January 2021.

COUNTRIES WHERE WP.29 APPLIES

WP.29 applies to the 54 countries that participate in the 1958 UNECE Transportation Agreements and Conventions, including the nations of the EU, the UK, Japan and South Korea, which combined produced one-third of the world's vehicles in 2018. Many more countries that do not formally participate in the 1958 agreement accept United Nations (UN)-compliant vehicles. All manufacturers (including US and Canadian automakers) selling into these markets need to consider the implications of WP.29 regulation for their products and processes.

Countries that do not participate in WP.29 include the US, Canada and China, which are not signatories to the 1958 agreement and do not recognize UN vehicle regulation. UN-compliant vehicles are not authorized for import to these countries without additional compliance testing specific to the countries' own transportation safety laws. The US, Canada and China are part of a separate 1998 UN Agreement on UN Global Technical Regulations (UN GTRs). It is possible that signatories to the 1998 agreement might ultimately adopt the same or similar requirements as a GTR.

ENFORCEMENT OF WP.29 REGULATIONS

UN regulations are legally enforceable. If a country or region adopts and enforces WP.29 regulations, proof of compliance is needed for an automotive manufacturer to achieve type approval to sell into a market. In Europe, type approval provides mutual recognition of compliance at the whole vehicle level, so a manufacturer can obtain certification for a vehicle type in one EU country and market it across the EU without further tests. Approval requires the manufacturer to convince a technical services auditor that it has met the WP.29 requirements.

In addition to preventing the sale of non-compliant vehicles in their market, countries and regions can force the withdrawal of such vehicles or force a recall.

DETAILS OF THE TWO ADOPTED PROPOSALS

Learn about the two parts of WP.29 regulations—cybersecurity and software updates—and requirements for each.

WP.29 CYBERSECURITY REGULATION

The adopted "proposal for a new UN regulation on uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system" specifies a list of processes vehicle manufacturers must put in place to:

- Identify and manage cybersecurity risks in vehicle design.
- Verify that the risks are managed, including testing.
- Ensure risk assessments are kept current.
- Monitor cyberattacks and respond effectively.
- Analyze successful and attempted cyberattacks.
- Assess if the cybersecurity measures are effective against new threats and vulnerabilities.

Manufacturers must demonstrate that they fulfill the following requirements:

- Have in place a cybersecurity management system and its application to vehicles on the road is available.
- Provide a risk assessment analysis that identifies critical risks.
- Have measures to detect and mitigate cyberattacks and provide evidence that the mitigations work.
- Possess data forensics capability.
- Monitor activities specific to the vehicle type.
- Transmit monitoring reports to the authority responsible for approving vehicles for sale (homologation authority).

A detailed list of the threats and mitigations in an appendix (Annex 5) requires OEMs to address:

- Back-end servers
- Communications channels (includes external connectivity)
- Software update procedures
- Unintended human actions
- Vehicle data and code
- Components that could be exploited without sufficient hardening

Specifically, some of the wider cybersecurity requirements include:

*7.2.2.2. The vehicle manufacturer shall **demonstrate** that the processes used within their Cybersecurity Management System ensure security is adequately considered, including risks and mitigations listed in Annex 5.*

*(a) The processes used within the manufacturer's organization to **manage cybersecurity***

*(c) The processes used for the **assessment, categorization and treatment of the risks identified***

*(d) The processes in place to verify that **the risks identified are appropriately managed***

*(g) The processes used to **monitor for, detect and respond to cyberattacks***

*(h) The processes used to **provide relevant data to support analysis** of attempted or successful cyberattacks.*

*7.3.1. The manufacturer shall have a **valid Certificate of Compliance for the Cybersecurity Management System** relevant to the vehicle type being approved.*

*7.3.2 The vehicle manufacturer shall **identify and manage**, for the vehicle type being approved, **supplier-related risks**.*

*7.3.7 Provide **data forensic capability** to enable analysis of attempted or successful cyberattacks.*

*8.1 **Every modification of the vehicle type which affects its technical performance** with respect to cybersecurity and/or documentation required in this Regulation shall be notified to the approval authority*

Read the full text of the WP.29 cybersecurity and cybersecurity management system regulation.

WP.29 SOFTWARE UPDATE REGULATION

The adopted "proposal for a new UN regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system" applies to vehicles that permit software updates. The regulation applies to trailers and agricultural vehicles, in addition to passenger cars, vans, trucks and buses.

The WP.29 software update regulation requires a vehicle manufacturer to put in place processes to:

- Record the hardware and software versions relevant to a vehicle type.
- Identify software relevant for type approval.
- Verify that the software on a component is what it should be.
- Identify interdependencies, especially with regards to software updates.
- Identify vehicle targets and verify their compatibility with an update.
- Assess if a software update affects the type approval or legally defined parameters.
- Assess if an update affects safety or safe driving.
- Inform vehicle owners of updates.
- Document all the above.

Manufacturers must demonstrate that they fulfill the following requirements:

- Have in place a software update management system and its application to vehicles on the road is available.
- Protect the software update delivery mechanism and ensure integrity and authenticity.
- Protect software identification numbers.
- Ensure the software identification number is readable from the vehicle.
- Over-the-air software updates must:

1. Restore function if the update fails.
2. Execute the update only if there is sufficient power.
3. Ensure safe execution.
4. Inform users about each update and its completion.
5. Ensure the vehicle is capable of conducting an update.
6. Inform the user when a mechanic is needed.

Read the full text of the WP.29 software update and software update management regulation.

INTERRELATIONSHIP OF WP.29 WITH OTHER CYBERSECURITY STANDARDS

Learn about how WP.29 is related to other cybersecurity standards, such as ISO 21434, ISO 24089 and the upcoming frameworks for software bill of materials (BOM).

ISO/SAE 21434 AND ISO/AWI 24089

Although WP.29 does not mention ISO/SAE 21434 (cybersecurity engineering) and ISO/AWI 24089 (software update engineering), it is understood that if an OEM and its supply chain can demonstrate compliance against these standard frameworks, then that compliance can be used to demonstrate compliance with the WP.29 regulation. Similarly, demonstrating compliance against these two standards should afford OEMs protection from liability.

As an international automotive cybersecurity framework with explicit controls, ISO 21434 will likely be the framework most OEMs and Tier 1 suppliers align or certify to. A timing issue exists, however. The WP.29 regulation will likely come into force before these industry standards are finalized.

FRAMEWORKS FOR SOFTWARE BILL OF MATERIALS (SBOM)

A software bill of materials (SBOM) can uncover security vulnerabilities and build a foundation for better cybersecurity. There are currently a number of organizations working on a framework for a more transparent software supply chain to itemize components in a SBOM. The expectation is that consumer demand for transparency will cause suppliers to deliver high-quality, more secure code.

The WP.29 regulation requires OEMs to demonstrate supplier-related cybersecurity risks, so compliance with the future frameworks for SBOM should help organizations demonstrate compliance with the WP.29 regulation.

BLACKBERRY QNX WP.29 READINESS ASSESSMENT

To help you navigate the regulations and prepare your development teams for these new requirements, the BlackBerry® QNX® Professional Services team has created a WP.29 readiness assessment to provide the risk

management techniques and insight needed to improve conformity to the WP.29 regulation.

Our WP.29 readiness assessment uses a data-driven methodology to help you understand your organization's conformity to the regulation and your overall cybersecurity posture, identify cybersecurity risks, and create a roadmap to WP.29 compliance. A robust methodology combines our industry-leading security expertise and cutting-edge cybersecurity technology through a systematic, step-by-step professional services engagement.

Our WP.29 readiness assessment is aligned to WP.29, ISO 21434, ISO 27001, NIST, GDPR and other leading frameworks and regulations across four domains—cybersecurity management, monitoring and response, risk management, and the development lifecycle.

The package includes:

- Workshops with an embedded systems security expert
- Automated analysis of binary images and support files to understand the SBOM, leakage of personal data and supply chain insights
- Detailed report with observations, risks, conformity levels and a pragmatic set of recommendations

LEARN MORE

RESOURCES

BROCHURE

Security Services Brochure

DOWNLOAD →

WEBINAR

Embedded System Security Across the Supply Chain

WATCH →

CONTACT US

Our team of experts are here to answer your questions.

CONTACT US →