Cyber Resilience Act

Brussels, 20th January 2023 – Tyre manufacturers on the top of manufacturing tyres have been heavily working on a variety of technologies to connect tyres to the internet and digital services accompanying the lifetime of the tyre, known as Tyre-as-a-Service (TaaS)[1]. The cybersecurity of these new products is a real concern for ETRMA in the broader context of the cybersecurity in transport. In this respect, the industry welcomes the European Commission's proposal for a Regulation on cybersecurity requirements for products with digital elements.

Tyre industry appreciates the comprehensive EU product-related legislative framework covering both software and hardware and defining essential cybersecurity requirements across a life cycle of at least 5 years, including a mandatory incident reporting to ENISA. Furthermore, the approval process, which is based on a cybersecurity risk analysis. Furthermore, the approval process, which is based on a cybersecurity risk analysis, is well flexible to offer the possibility of self-certification when the digital product is non critical and the possibility of submission to a third-party evaluation or a standard cybersecurity certification scheme when it is classified as critical.

Road vehicles, submitted to Type Approval, are excluded from the Cyber Resilience Act (CRA) since they are submitted to the UNECE R155 and R156 approval. This is what raises the question on the interplay between the CRA and the UNECE R155 regarding the cybersecurity requirements for systems, parts and applications sold in the aftermarket, not subjected to Type Approval and connected to the vehicle.

ETRMA asks for clarification and recommends that the Regulator takes the necessary steps to ensure that these systems, parts and applications are well covered by CRA. This is even more important due to the rapid pace of digitalization of road mobility, the advent of connected and automated driving, as well as, increased need for accessing in vehicle data and sharing under fair rules for all players in the ecosystem.

To ensure that CRA-approved automotive digital products are trustable and can be safely connected to the vehicle, the different levels of criticality of their impact on the functional safety of the vehicle must be addressed in their approval process. Criteria to define what are the CRA "critical" products in the automotive sector must be set up. By doing this, the CRA-approved digital products will be indisputably trustable by any stakeholder in the EU market, including Vehicle Manufacturers, who will be, then, in the position to give the authorization of connection in a reliable manner.

Overall, ETRMA calls for a harmonized implementation of CRA and UNR155, as well as, CRA's appropriate extension through Delegated and/or Implementing Acts to define the cybersecurity "critical products" for the automotive aftermarket.

About ETRMA

The European Tyre & Rubber Manufacturers Association (ETRMA) represent nearly 4.400 companies in the EU, directly employing more than 350.000 people. The global sales of ETRMA's 14 corporate members represent 70% of total global sales and 7 out of 10 world leaders in the sector are ETRMA Members[2]. We have a strong manufacturing and research presence within the EU and candidate countries, with 93 tyre-producing plants and 17 R&D centres.

[1] https://www.etrma.org/wp-content/uploads/2019/09/20190716-etrma-report-web-final.pdf
https://www.etrma.org/news/tyre-as-a-service-how-the-tyre-industry-drives-sustainable-change/

[2] *ETRMA's membership: APOLLO TYRES, BRIDGESTONE EUROPE, BRISA, CONTINENTAL, GOODYEAR, HANKOOK, MARANGONI, MICHELIN, NEXEN TIRE EUROPE, NOKIAN TYRES, PIRELLI, PROMETEON, SUMITOMO RUBBER INDUSTRIES AND TRELLEBORG WHEEL SYSTEMS. Furthermore, members include Associations in the following countries: Czech Republic, Finland, France, Germany, Hungary, Italy, the Netherlands, Poland, Slovak Republic, Spain and the UK.*