

To whom it may concern

18.04.2024

## **Declaration of conformity for body manufacturers with regard to UN-R155 & 156 on the subject of vehicle cybersecurity**

Following a review of UN Regulation No. 155 & 156 – Cyber Security and Cyber Security Management System, by the European Tail lift Manufacturers Association (ETMA), the member parties have determined that there is no cyber security relevance if the product to be delivered (service, product, etc.) has no influence on the vehicle's E/E architecture or is not part of it.

Based upon this assessment, the ETMA and its members determine that a tail lift does not impact Cyber Security or Cyber Security Management System, and therefore no further action is required by tail lift manufacturers in respect to additional compliance.

### **Definition: cyber security relevance**

Cyber security relevance exists if one of the following measures is planned or carried out:

- Changes or modifications to the E/E architecture that could have an impact on the system type approval (STA) or the overall vehicle type approval (WVTA).
- Changes or modifications to the interface between the provided vehicle and the body.
- Use of additional HW/SW components that provide third parties with access to the E/E architecture.
- Any other changes affecting cybersecurity in the vehicle.

In this case, the obligations in accordance with UN-R 155 and ISO/SAE 21434, which are part of the assembly guidelines, apply and the body builder must contact the vehicle OEM directly to cooperate with the respective Cyber Security manager and discuss further action.

**ETMA**

Ross Townshend  
Chairman