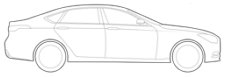
AUTOCRYPT



UNECE WP.29 CHECKLIST

In June 2020, the United Nations officially adopted two new regulations regarding automotive cybersecurity. When these regulations go into effect, becoming mandatory for the 54 contracting countries signed, the automotive industry won't be the same. While countries are already in the midst of implementing policies to be in compliance, here are some things that your organization can do if you are in the automotive industry (OEMs, Tier-1 Suppliers, software providers, etc.).

CYBER SECURITY MANAGEMENT SYSTEMS (CSMS)

For General Industry / Sector

- ☐ Identify and manage cyber security risks in vehicle design
- ☐ Verify that the risks are managed, including testing
- ☐ Ensure that risk assessments are kept current
- ☐ Monitor cyber-attacks and effectively respond to them
- ☐ Support analysis of successful or attempted attacks
- ☐ Assess if cyber security measures remain effective for new threats and vulnerabilities

For Manufacturers

- ☐ CSMS is in place and its application to vehicles on the road is available
- ☐ Provide risk assessment analysis, identify what is critical
- ☐ Mitigation measures to reduce risks are identified
- ☐ Evidence that mitigation measures work as intended
- ☐ Ensure measures are in place to detect and prevent cyber-attacks, and support data forensics
- ☐ Monitor activities specific for the vehicle type
- ☐ Transmit reports of monitoring activities to relevant approval authority

SOFTWARE UPDATE MANAGEMENT SYSTEMS (SUMS)

For General Industry / Sector

- ☐ Record hardware/software versions for vehicle type
- ☐ Identifying software relevant for type approval
- ☐ Verifying the software on a component
- ☐ Identify interdependencies, especially with regards to software updates
- ☐ Identify vehicle targets and verify compatibility with update
- ☐ Assess if software update affects type approval or legally defined parameters (including adding/removing functions)
- ☐ Assess if an update affects safety or safe driving
- ☐ Inform vehicle owners of updates

For Manufacturers

- ☐ SUMS is in place and its application to vehicles on the road is available
- ☐ Protect SU delivery mechanism and ensure integrity and authenticity
- ☐ Protect software identification numbers
- ☐ Ensure that software identification number is readable from the vehicle

OVER-THE-AIR (OTA) SOFTWARE UPDATES

- ☐ Restore function if update fails
- ☐ Execute update only if sufficient power
- ☐ Ensure safe execution
- ☐ Inform users about each update and their completion
- ☐ Ensure vehicle can conduct updates
- ☐ Inform user when a mechanic is needed

Source: United Nations Economic Commission for Europe Information Unit