TÜVRheinland®
Precisely Right.

Statement of

Product Cybersecurity Assessment

Customer/ Manufacturer	Hesai Technology Co., Ltd. Building L2-B, Hongqiao World Center, 201702 Shanghai, P.R. China
Order No.	245760956
Related Project	Certificate No. 962/CSP 1000.00/23
Product	Mechanical LiDAR Pandar128 (P128)

Type designation

Regarding the Product Cybersecurity Assessment on the Mechanical LiDAR Pandar128 (P128) from Hesai Technology Co., Ltd., hereby we TÜV Rheinland declare that:

- The review of documents (including CSM relevant documents, concept phase cybersecurity design, system phase cybersecurity design, detail design, V&V cybersecurity relevant documents and user manuals, etc.) by TÜV Rheinland side, the Mechanical LiDAR Pandar128 does not have the capability to store point cloud data or send any point cloud data out of vehicle.

See the appendix for details.

2023-10-19
Date

TÜV Rheinland
Industrial Services & Cybersecurity

Fancy Guo

TÜVRheinland®
Precisely Right.

Appendix

The product cybersecurity inspection summary of Mechanical LiDAR Pandar128 (P128) version V5.5

The Mechanical LiDAR Pandar128 Version V5.5 product development process meets

Hesai's cybersecurity management process (CSM) which was established according to ISO/SAE 21434:2021. It can be used in automotive cybersecurity application. The user is responsible for applying and configuring appropriate protection mechanisms in order to guarantee product cybersecurity while operating. The integrator is obliged to validate the assumptions and constraints defined by the manufacturer, under consideration of the instructions of the Security Manual.

The Identification of the inspection object

The functionalities of Mechanical LiDAR Pandar128 (P128) are described as following:

- Obstacle detection for emitting and receiving laser signal, calculating the distance of the obstacle and transmitting the obstacle information to System on Chip (SoC) via light pulses communication channel inside LiDAR.
- On board communication function for communicating obstruction information and instruction with other ECU's of the vehicle.
- Secure boot initialization for initializing hardware resources, configuration data, and supporting the cybersecurity of the bootloader and application software.
- Software update function for update of the calibration data and control algorithm(s).
- Communication between FPGA Chip and SoC via light pulses communication channel inside LiDAR.
- Diagnostic and logging function for recording fault code and cybersecurity incident information.

The inspection procedure about the cybersecurity risk of point cloud data related aspects

For item definition, TÜV Rheinland side has reviewed the definition of item, all lifecycle operation environment and related features have been defined, there has not defined the function of store point cloud data or sent any point cloud data out of vehicle.

For risk assessment and cybersecurity goals design, TÜV Rheinland side has reviewed the work products of risk assessment and cybersecurity goals in concept phase, there has not any contents about point cloud data nor threat scenarios through vehicle wireless links on Mechanical LiDAR Pandar128 (P128).

And the identified cybersecurity goals of Mechanical LiDAR Pandar128 (P128) as below:

Cybersecurity Goals	Applicable phase of the lifecycle
Prevent the software and firmware implemented in LiDAR Pandar128 from being manipulated, deceived, and repudiated.	In the operation phase
Prevent the debugging interface in LiDAR Pandar128 from being accessed without authorization.	whole product lifecycle except production phase
Prevent the on-vehicle Ethernet channel in LiDAR Pandar128 from being manipulated, deceived, repudiated and attack.	The operation phase
Prevent the information of update in LiDAR Pandar128 from being manipulated, deceived, and repudiated.	The operation phase
Prevent the configuration parameters and calibration parameters in LiDAR Pandar128 from being manipulated, deceived, and repudiated.	The maintenance phase and The production phase
Prevent the SW/FW image, calibration/configuration parameters and temporary variables stored in LiDAR Pandar128 from being manipulated, deceived, and stolen.	All product lifecycle
Prevent the communication data between FPGA and SoC in LiDAR Pandar128 from being manipulated, deceived.	The operation phase
Prevent the PIN information in LiDAR Pandar128 from being exposed.	All product lifecycle

Table 1: Cybersecurity goal of LiDAR Pandar128

For product development lifecycles process, TÜV Rheinland side has reviewed the relevant work products of system design and detail design.

- All the cybersecurity mitigation measures against which defined in cybersecurity concept phase have been refined and implemented via system architecture design, hardware design and software design.
- The cybersecurity mitigation measures have been verified by software unit verification, static coding scanning test and system integration tests. And the test results have been passed successfully and reviewed for completeness
- Cybersecurity test, cybersecurity test to find potential threats or vulnerabilities were carried out by penetration testing and fuzzing testing. No threat has been found that point cloud data can be leaked out of the vehicle through wireless links, and no point cloud data has been found stored in Mechanical LiDAR Pandar128 (P128).
- The product cybersecurity requirement traceability was performed in each development and verification work product and provided by the manufacturer.

Summary

The Mechanical LiDAR Pandar128 (P128) for cybersecurity, version V5.5 complies with the requirements according to ISO/SAE 21434:2021.

Hence, the Mechanical LiDAR Pandar128 (P128) is suitable for the use in cybersecurity related applications in line with ISO/SAE 21434:2021. The user is responsible for applying and configuring appropriate protection mechanisms in order to guarantee product cybersecurity while operating.

The integrator is obliged to validate the assumptions and constraints defined by the manufacturer, under consideration of the instructions of the Security Manual.

The above statement is only valid to the version of the product which has been certified and attached in the certificate.