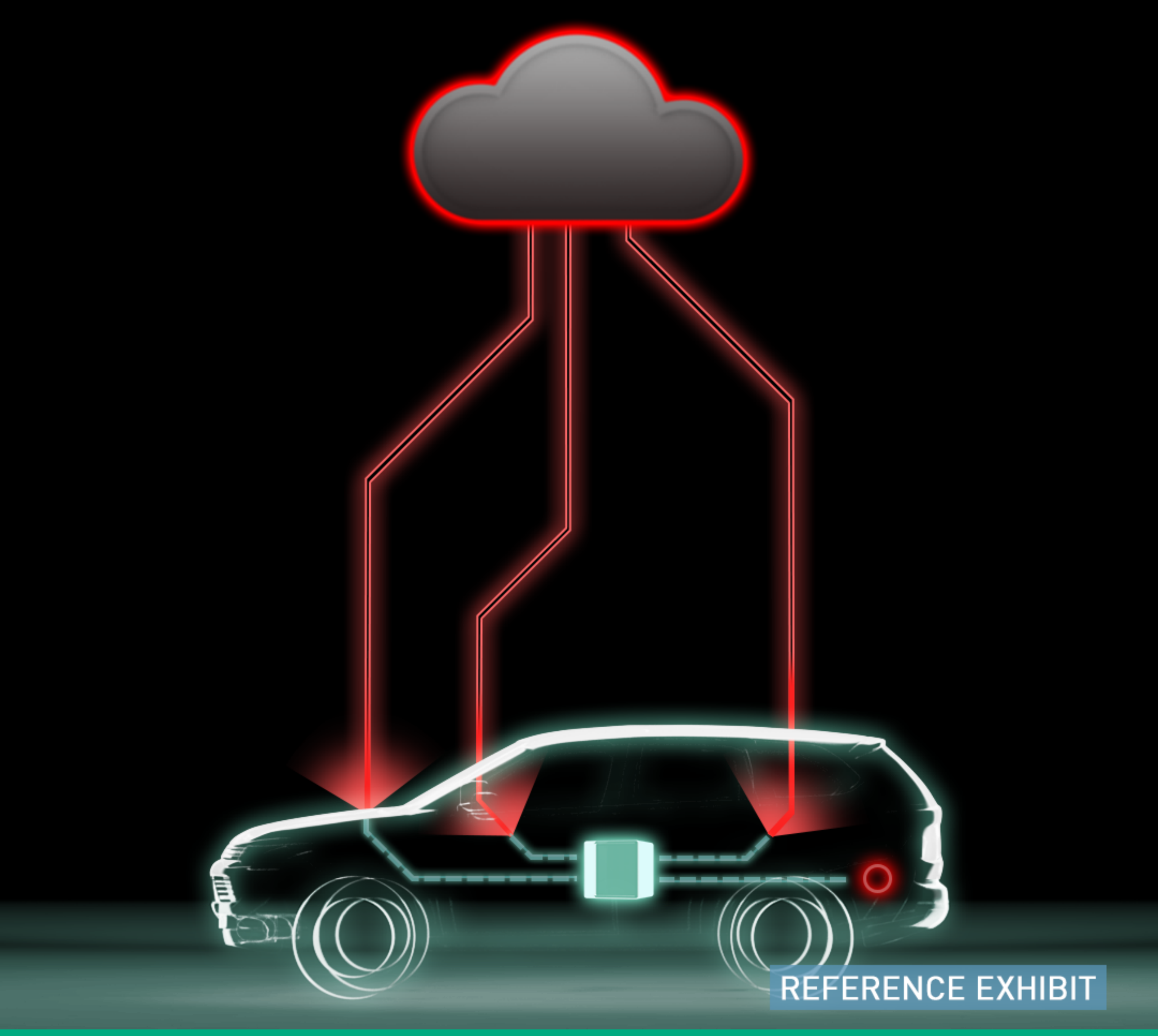


Security ECU

- Prompt detection of malicious CAN messages through full - time monitoring of CAN buses which the Security ECU is being attached to.

- Anti - intervention of harmful vehicle operation such as unexpected steering, acceleration and braking by disabling of the detected malicious CAN messages using the predefined rules.

- Machine-learning based anomaly detection of unknown attacks or signs of attack and update of the predefined rules to keep vehicles secure during their life cycle.

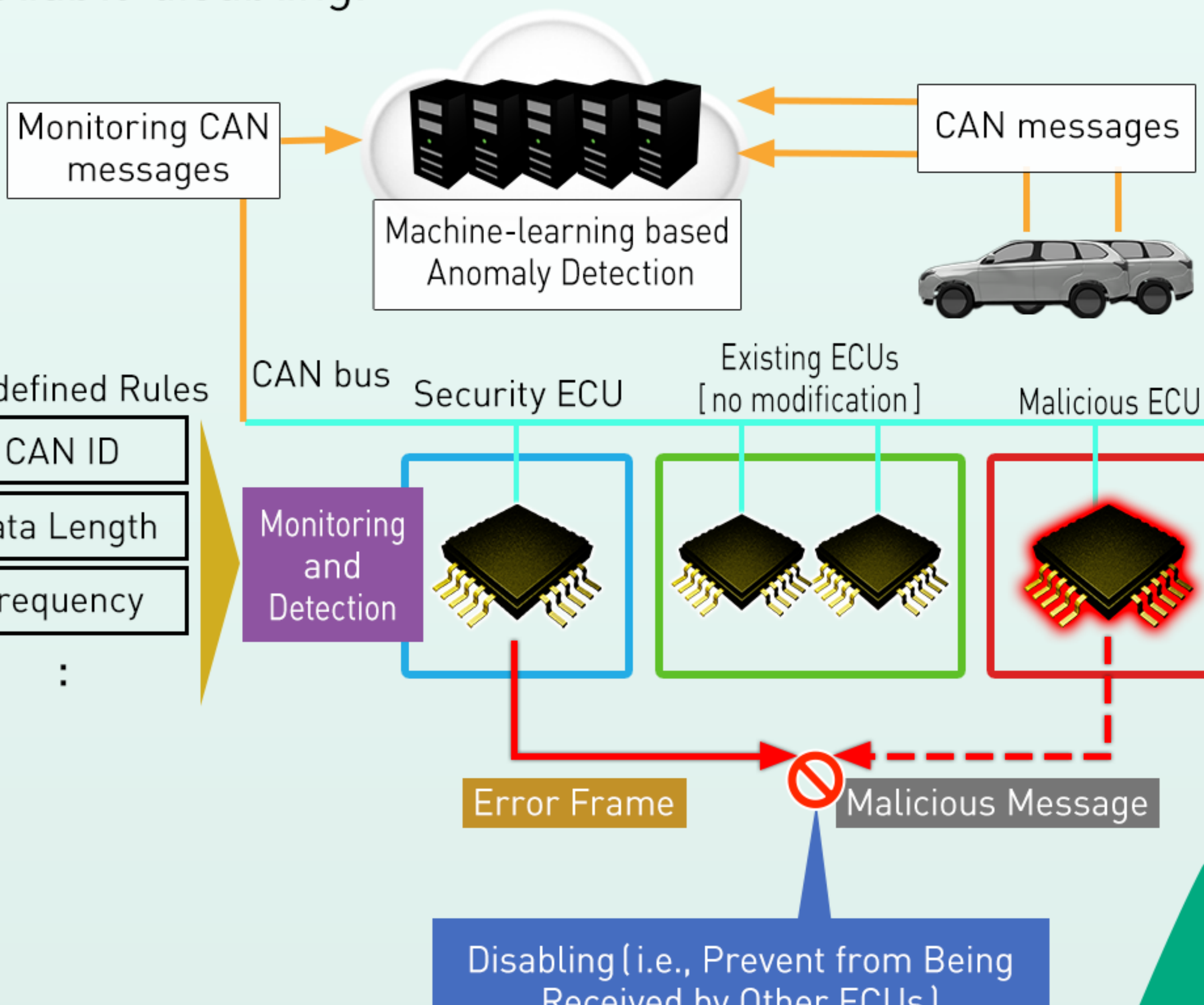
Panasonic
AUTOMOTIVE

Security ECU

REFERENCE EXHIBIT

Technical Advantage

- Multiple detection rules applied — accurate detection of malicious CAN messages by monitoring from various aspects.
- **Machine-learning based anomaly detection —** the Cloud system generates normal model from behaviors of CAN messages in real vehicles, and detects unknown attacks or signs of attack based on the difference between monitoring CAN messages and the normal model.
- **Hybrid architecture of software and hardware —** software-based detection rules for updatability, and hardware-based processing for prompt and reliable disabling.



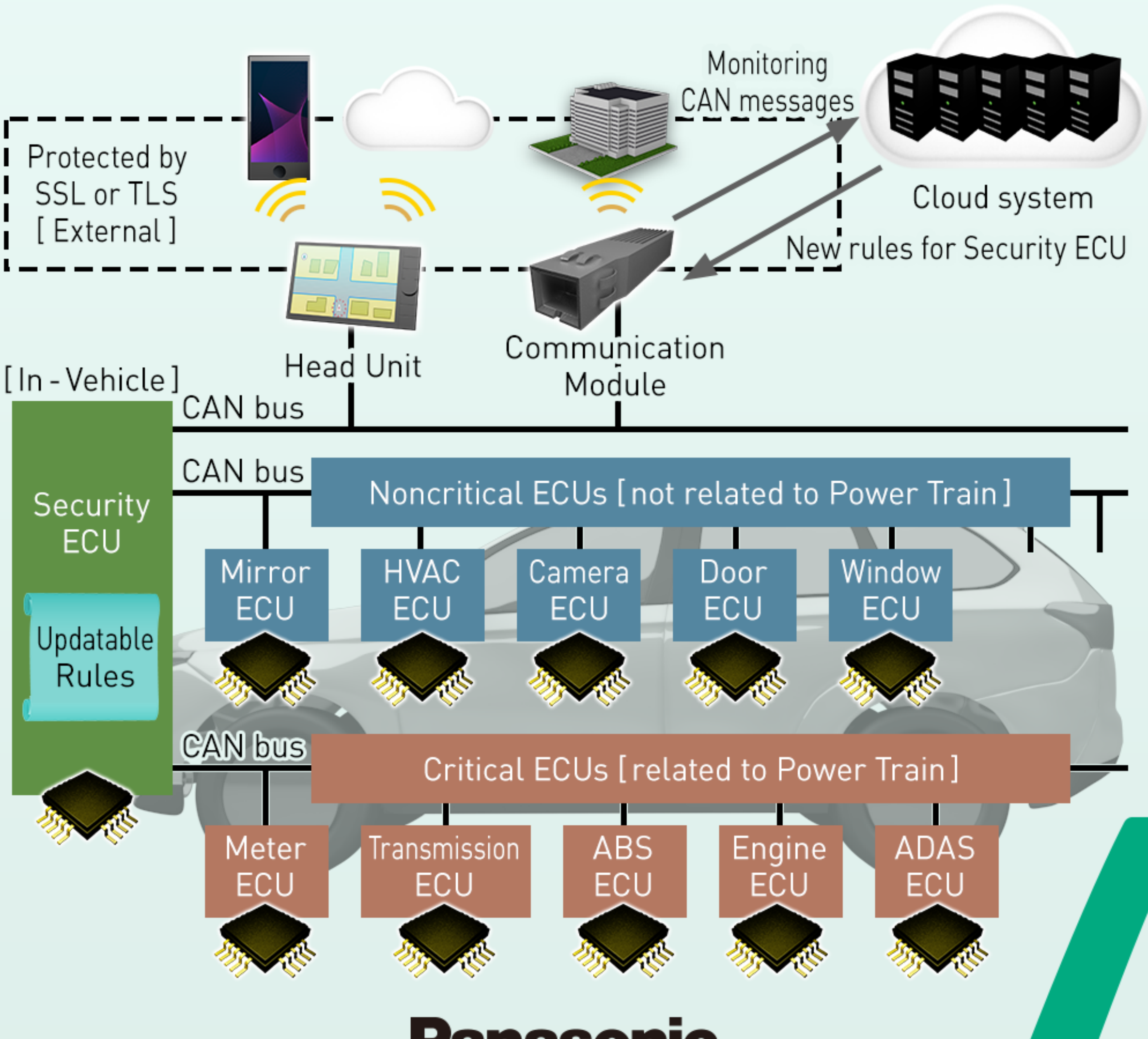
Panasonic AUTOMOTIVE

Security ECU

REFERENCE EXHIBIT

Application

- Security ECU is attached to the in-vehicle CAN network as a gateway of multiple CAN buses allowing itself to monitor all CAN messages transmitted over such buses.
- If it detects malicious CAN massages from ECUs that e.g., reprogrammed maliciously, then disabled and prevents them.
- The Cloud system detects anomaly from the monitoring CAN messages. If it's judged as an attack, then new rules to prevent such attack are created and the Cloud system updates the rules in the Security ECU.



Panasonic
AUTOMOTIVE