Security-risk-mitigation Measures for Automotive Remote Diagnostic Systems

Authors: M.Miyashita, H.Takakura

Presenter: Masaaki Miyashita
e-mail: m-miyashita@nii.ac.jp

The Graduate University for Advanced Studies, SOKENDAI (Japan)

Masaaki Miyashita

- Product Cybersecurity Expert Leader in Connected Car Off-board Development & Operation Department of Nissan Motor Co., Ltd.
- A member of the Society of Automotive Engineers of Japan.
- In April 2021, transferred to the third year of the doctoral program in Information Science at the Graduate University for Advanced Studies, SOKENDAI.

What is “Automotive Remote Diagnosis”?

- One of typical use case of Connected Car Services.
- Help for trouble shooting of vehicle electric components by skilled mechanics remotely through the wireless communication.
- Similar idea with Telemedicine doctor.

Why “Remote” ?

Electric systems using in-vehicle network communication have become indispensable for modern vehicles, but it makes failure analysis more complex and difficult.

→Lack of skilled mechanics is becoming serious problem.

Demands for Remote Operations

If no security risk, ”Authorized” remote operators generally require the following privileged Remote Diagnostic commands.

Examples of privileged commands

Input/Output Control

- ✓ Primary function to identify the failure point by controlling Input or Output of Electronic Control Unit(ECU) .

Write Data

- ✓ Change any parameters of ECU for parts calibration
- ✓ Overwrite ECU firmware for software update.

Read Data

- ✓ Data check stored in any memory address of ECU for the network communication error analysis or software defect investigation.

Security concerns for the Remote Diagnostic Systems

Wireless entry point of the remote diagnostic systems “Telematics Control Unit (TCU)” is one of the most exposed attack surfaces among devices in a vehicle.

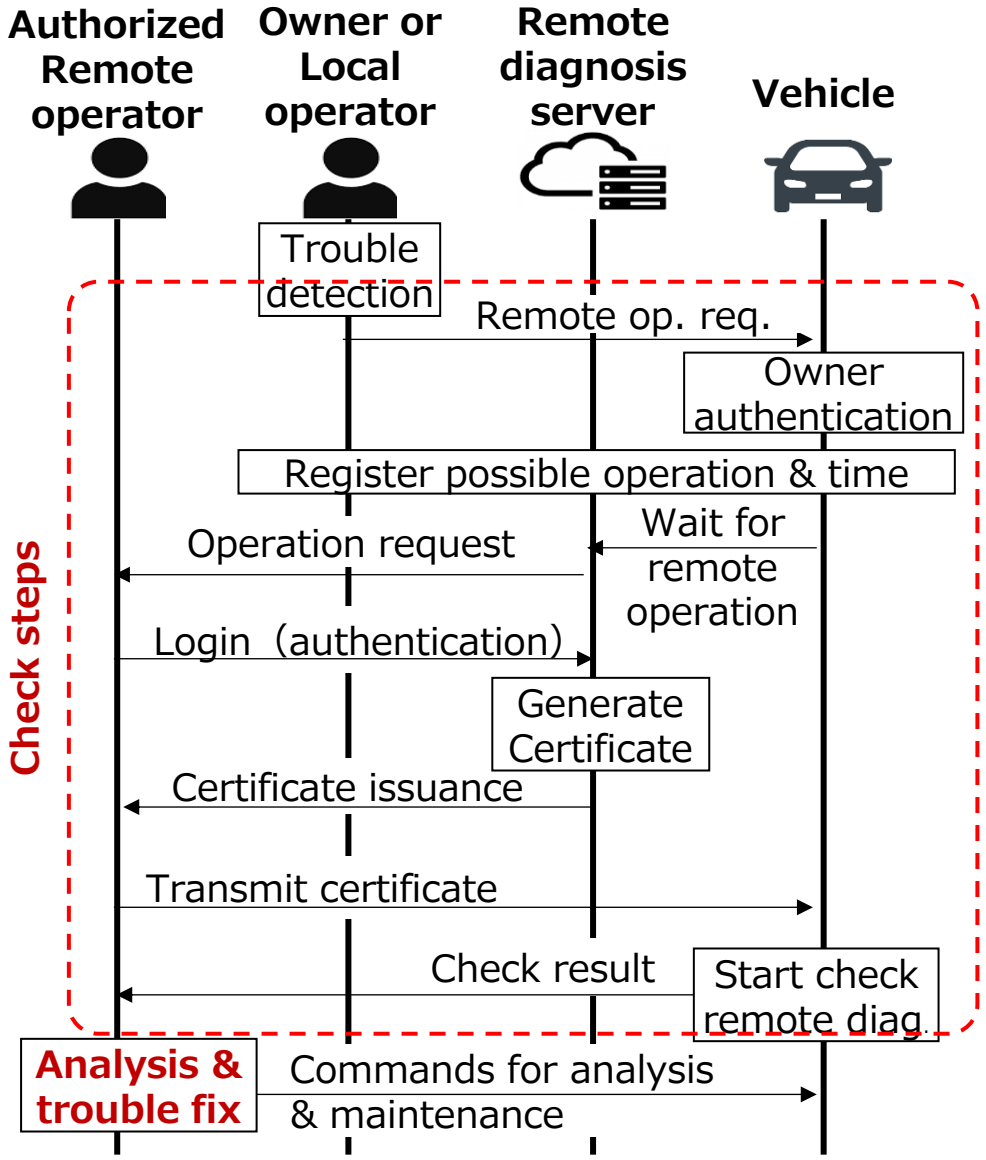
- ✓Frequent security patches for Operating System software.
- ✓Well-known hardware chips for the attackers are used.

If the privileged diagnostic commands are hijacked, the following cyberattacks will be possible.

- ✓Confidentiality: Interception of personal data stored in vehicle components.
- ✓Integrity: Unauthorized control of safety critical actuators.
- ✓Availability: Disabling ECU operation.

→Our goal : mitigating Security risks of the Remote diagnostic systems

Overview of security-risk mitigation

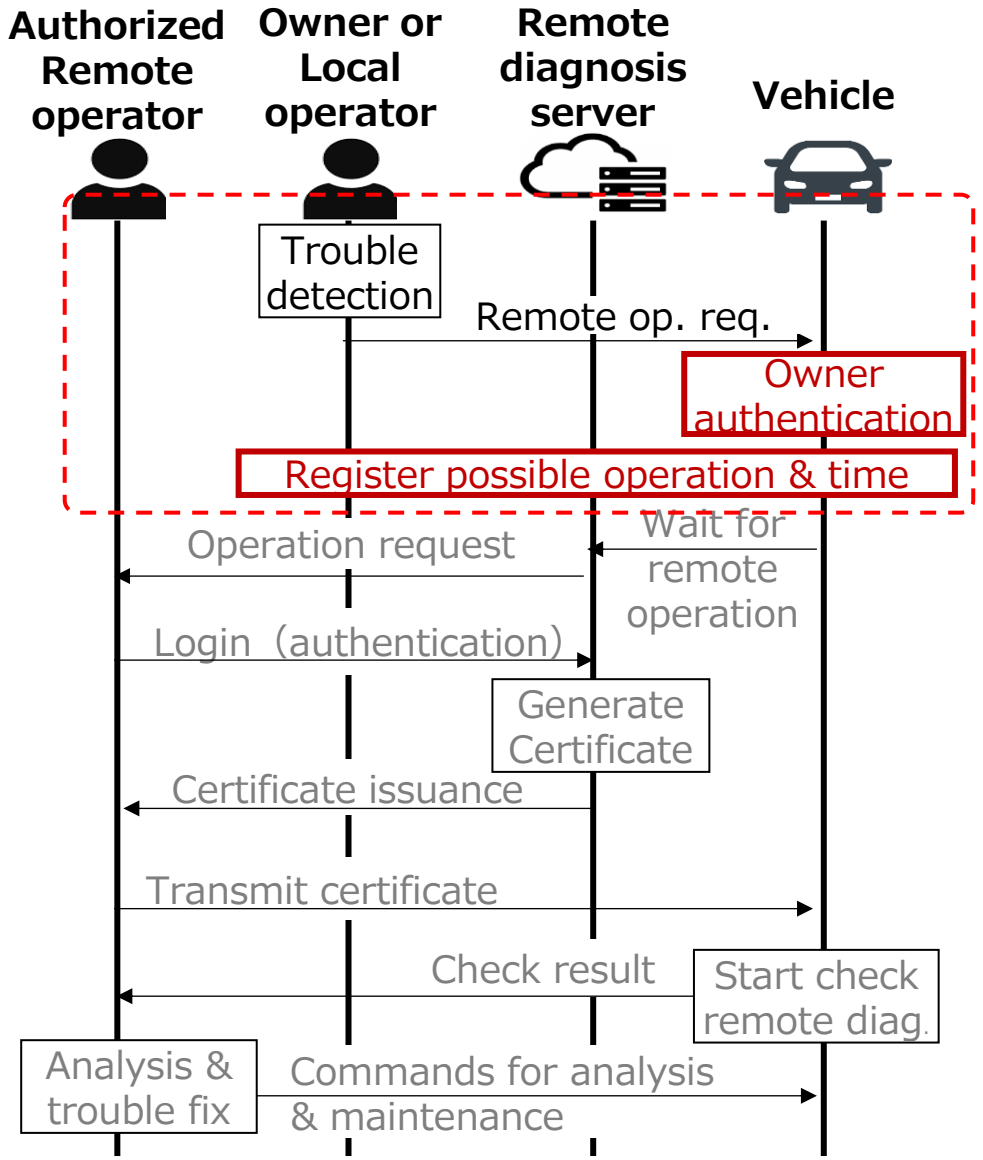


Our basic idea for risk mitigation is having several steps to check the following 3 points before starting remote analysis & trouble fix:

1. Owner really wants remote operation?
2. Remote operator is trustable?
3. Vehicle is in safe conditions for remote operation?

Next slides shows detail of each steps.

Step 1: Getting valid owner's permission



✓1st Key point : “Owner authentication” by physical access to vehicle.

(Proposed options as examples)

A) In vehicle switches or screen touch operation giving permission by entering remote operation password.

B) 2 or more owner’s intelligent wireless keys in the vehicle cabin during permission operation.

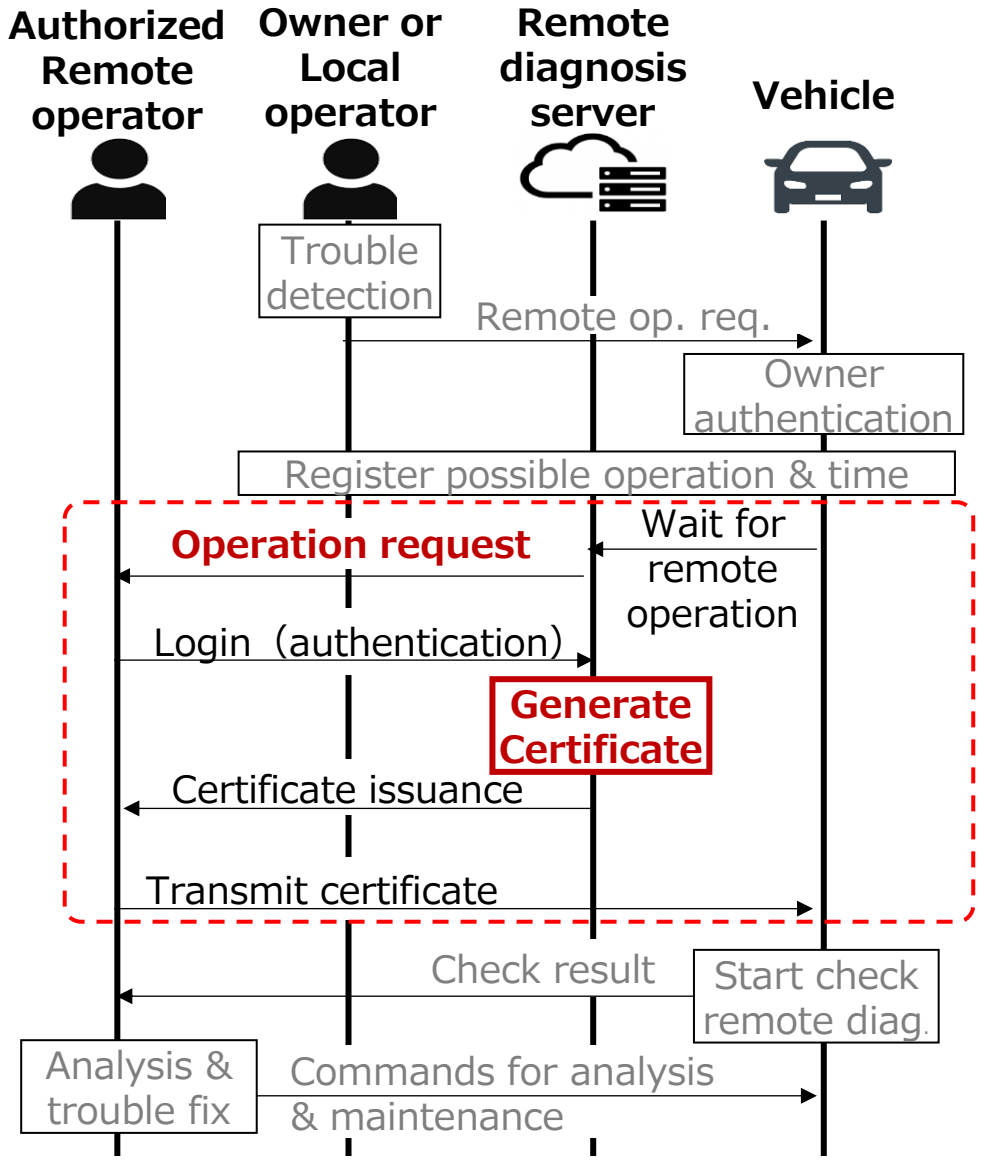
C) In-vehicle Near Field Communication (NFC) reader to detect a paired owner’s smartphone with unlocked permission by its APP.

✓2nd Key point : Registering possible operation & time to prevent any unexpected remote operation if the vehicle is in “Safe condition”

(e.g. the vehicle is stopped, engine food latch is open to proof “in maintenance mode”, GPS location)

SOKENDAI
国立大学法人 総合研究大学院大学
The Graduate University for Advanced Studies

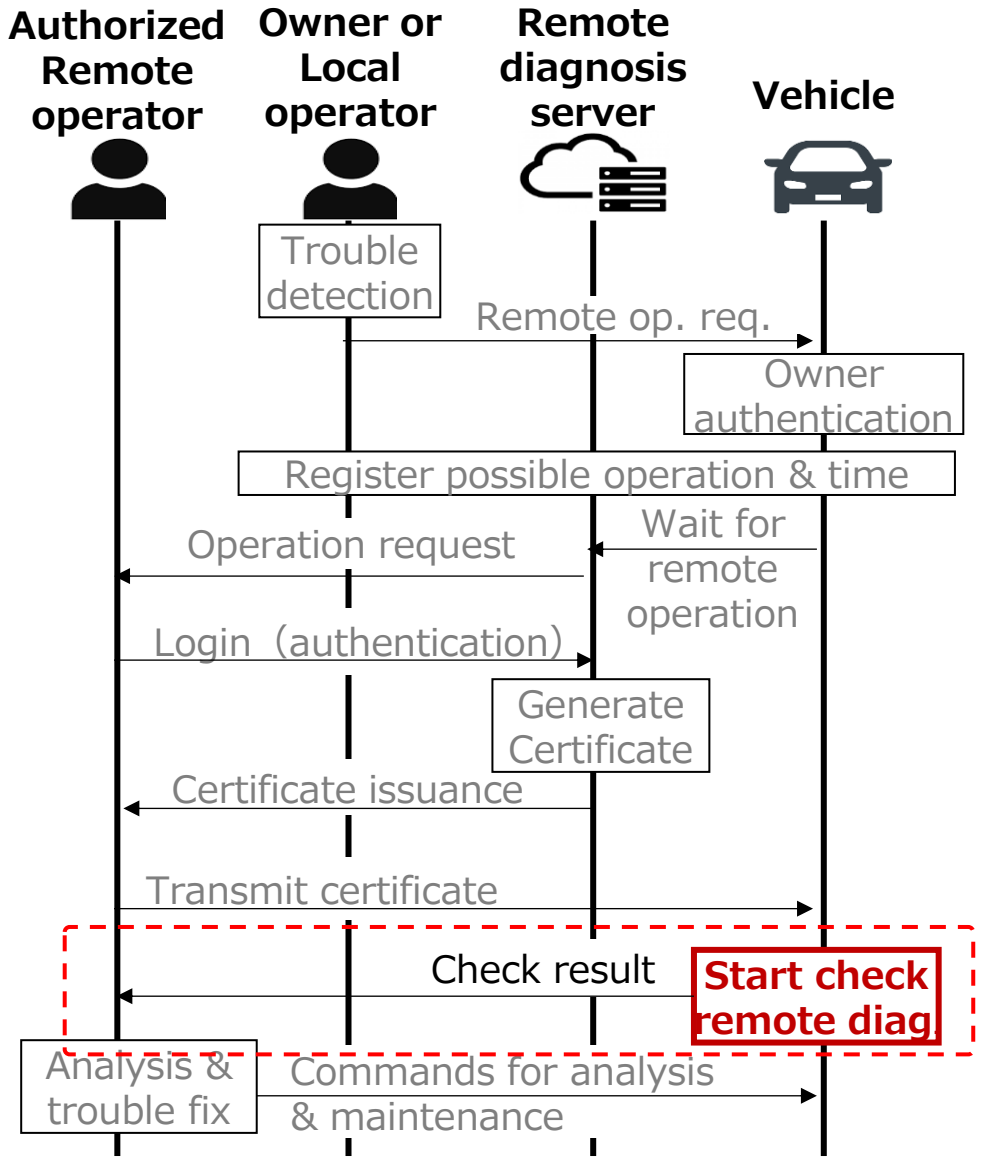
Step 2: Authentication of Remote operator



- ✓1st Key point : Only push request (including 1 time password) to Authorized operator is valid.

- ✓2nd Key point : Certificate signed by Remote diagnosis server for proofing authorized permission with time-out.
  (Remote diagnosis server can have an option to send a notice “Remote operator [name] got your permission!” to owner’s smartphone or/and in-vehicle display for preventing unexpected remote operation.)

Step 3: Safe condition check by Vehicle



- ✓1st Key point : Vehicle validates the signature of the certificate by the server's public key (Whether its contents are same as owner's requests or not?).

- ✓2nd Key point : Checking the Safe conditions are satisfied again, in order to avoid cyber-attack attempt to start remote operation when the vehicle is running.

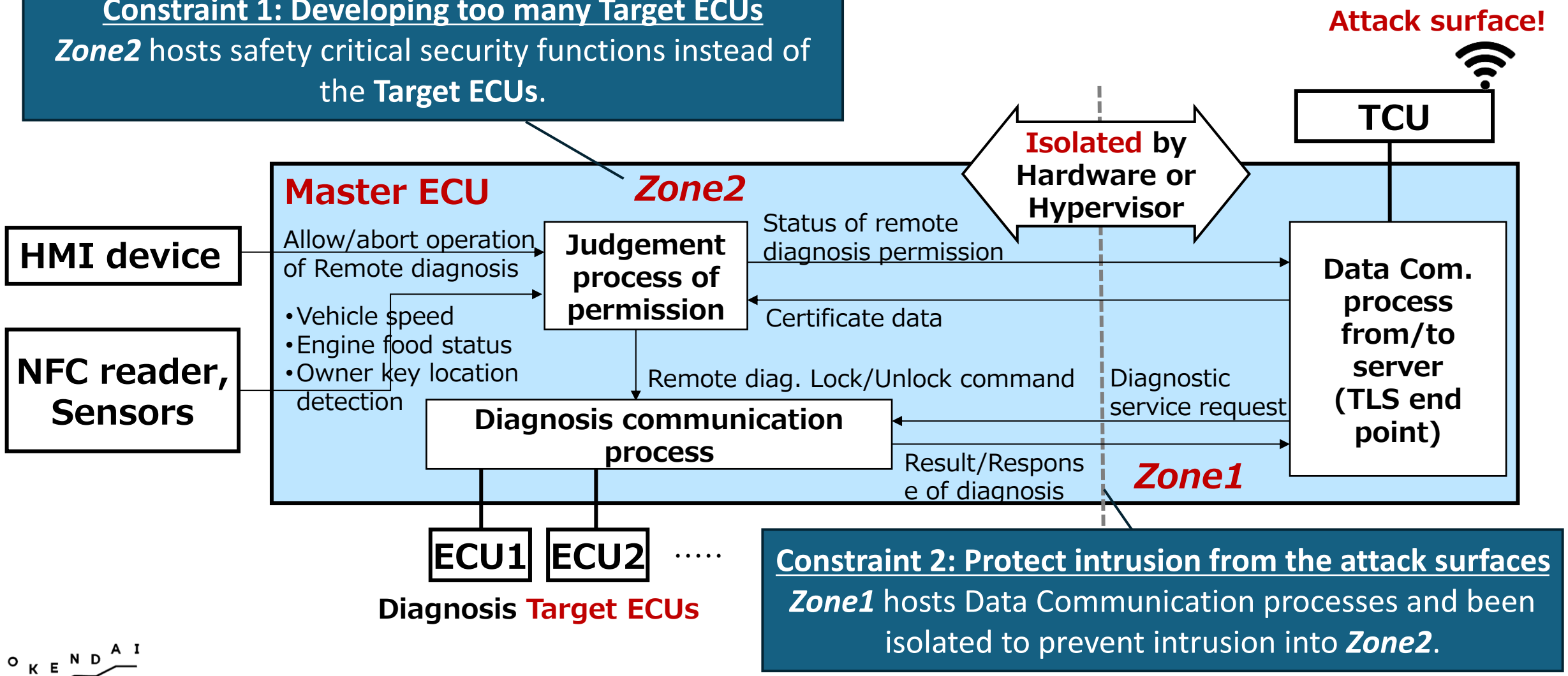
Just implementing 3 steps, easy?

→ No. Need to solve vehicle architecture constraints

Solution for constraints when implementing measures

Implement 3 steps security functions into "**Master ECU**" having isolated 2 Zones.

Constraint 1: Developing too many Target ECUs
Zone2 hosts safety critical security functions instead of the **Target ECUs**.

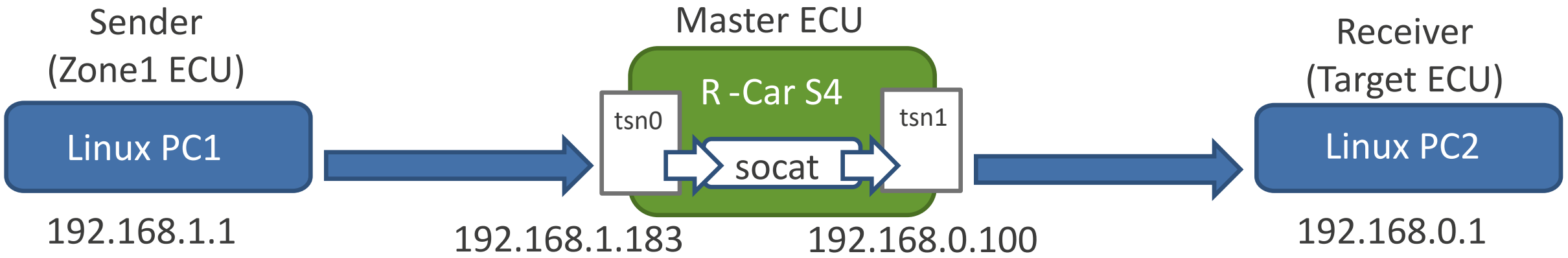


Constraint 2: Protect intrusion from the attack surfaces
Zone1 hosts Data Communication processes and been isolated to prevent intrusion into ***Zone2***.

Inspection environment of Communication Speed

- Not only isolating processors/memories for 2 zones, but also network separation by proxy is necessary to protect network between Zone2 & the Target ECUs.
  →***Throughput performance down can be acceptable level?***

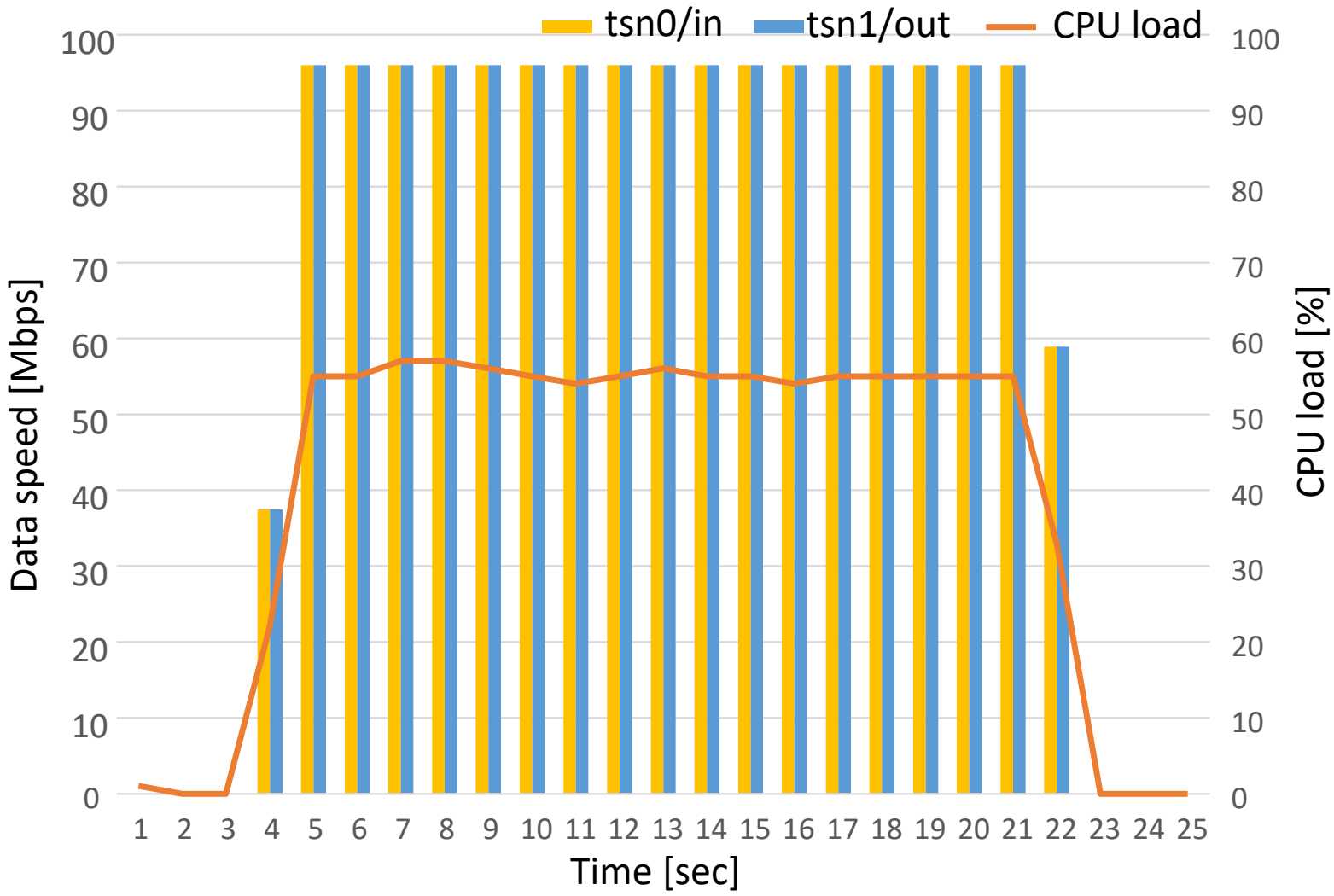
Inspection environment for most strict use case (Video transfer from Zone1 to Zone2)



- ✓ Proxy: “socat” hosted into one of A55 1,200MHz cores in Renesas R-car S4N-8A (Candidate processor for Master ECU)
- ✓ Protocol used: Real-time Transport Protocol (RTP)
- ✓ The operating system used for both R-Car & Linux PC1/PC2 : Ubuntu 20.04.
- ✓ **Target throughput 66 Mbps or more, latency 3 ms or less**

Inspection result

- ✓The proxy processing using “socat” could output 96-Mbps data without any data loss, and the CPU load at this time was only about 55%, leaving a margin.
- ✓The measured latency was 1.675ms, achieving the target of less than 3ms.



Conclusion & future work

- **Conclusion**
  Even if a man-in-the-middle attack is carried out by TCU, our security-risk mitigation measures can be effective in the following points.
  - ✓TLS communication between the Remote diagnosis server & Zone1.
  - ✓Even if an attacker can forge a certificate to conduct remote diagnostics, it is protected by multiple remote-diagnosis-permission conditions.
  - ✓To execute malicious code on the Master ECU to bypass the security functions, it is necessary to break into Zone2, but to do so from Zone 1, it is necessary to break through the separation between Zones1 & 2.
- **Future work**
  Since the Master ECU has sufficient processing power, we will investigate the possibility of enhancing security by, for example, adding an anomaly check for header information of communication packets.

Than you!