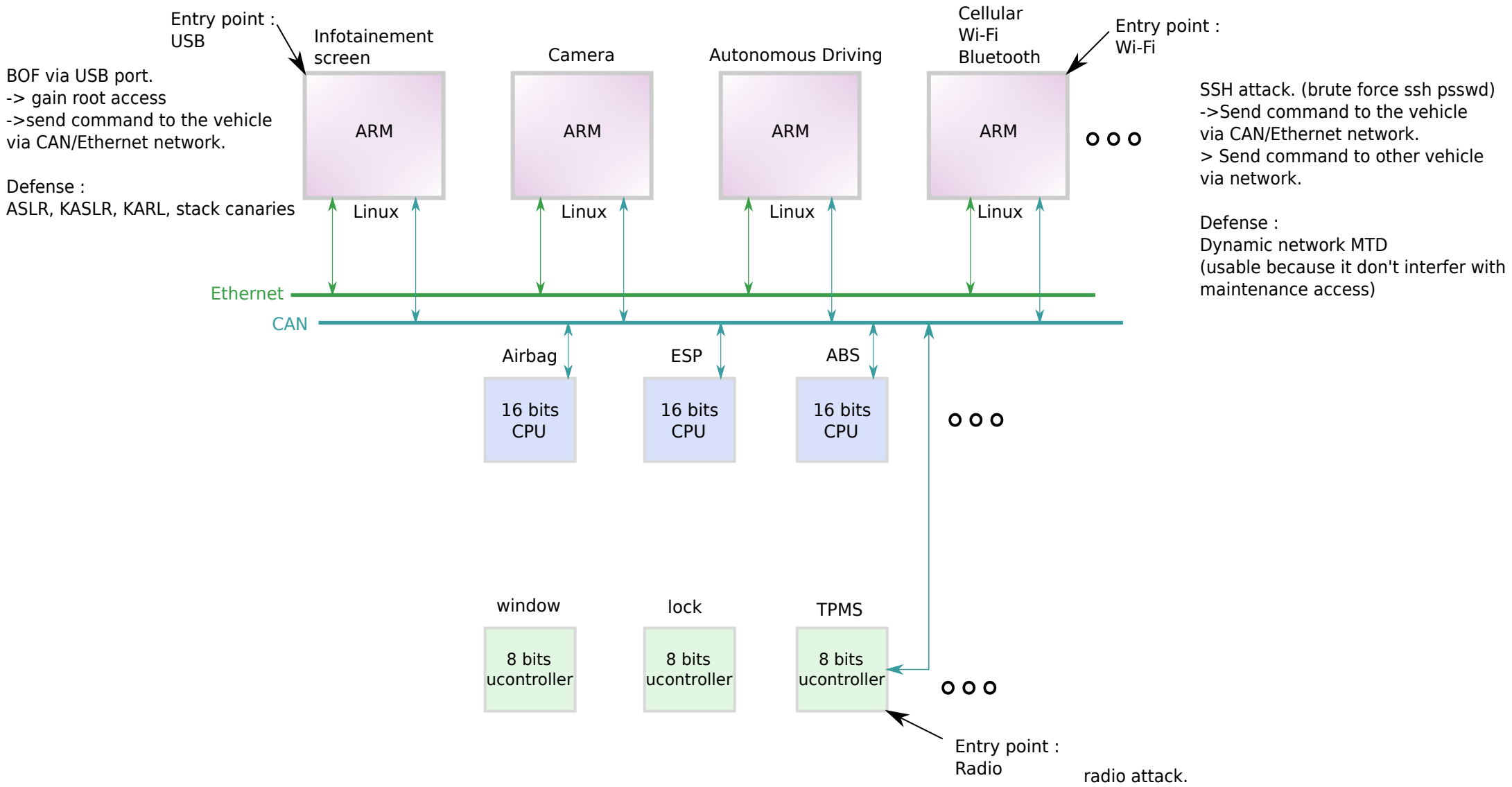

Scenario 1 : ***Attack via USB port***

- get a car into highway
- plug the usb
- perform a BOF on usb vulnerable driver
- get root
- send command to the network controller via ethernet or can bus.
  the command is a message to send to other car around (same constructor,
  any car in range...) to tell them to perform a dangerous action.
- send command to the network controller to send ransomware to other car around.

defense against Scenario 1 : ***Attack via USB port***

-> enable some stack canaries to harden BOF
-> enable ASLR to make BOF harder
-> Enable KASLR and KARL to re organize the kernel layout and disperce it into the memory

Scenario 2 : ***Attack via USB port***

- break into a car.
- start it and plug the usb stick.
- perform BOF on usb vulnerable driver.
- get root
- install ransomware, tracker, worm, backdoor...
- get out of the car

defense against Scenario 2 : ***Attack via USB port***

-> same as scenario 1

Scenario 3 : ***Attack via Network***

- get a car into highway
- scan network to find target in range
- try to get acces to it
- installransomware, send false messages to other car, send commad to the car to
  make it act dangerously.

defense against Scenario 3 : ***Attack via Network***

-> enable dynamic network mtd in order to make the vehicle not discoverble so it will not be possible to launch the attack.
  --> don't make problem with maintenance because it is just on the outside of car, the physical internal open ports will remains the same.
-> enable dynamic platform MTD, so the application will not be always on the same place. harden to find what we want.

Scenario 4 : ***Attack via TPMS***

- stand near a turn on car
- send an activation signal to the TPMS at 125kHz
- listen radio frequencies 315 MHz or 433 MHz to find the answers of the TPMS.

1 - get the information from the vehicule TPMSs to create a profil of the vehicule and track it, explode bomb when it pass nearby somewhere or else.
2 - send false informations to the vehicule to make it stop or something.
3 - perform DOS on multiple ECU by continously spoof TPMS package.
4 - get all of that but near a turned off car, send contuniously activation signal for the TPMS and drained the car battey.
5- send continiously packet and try to crash the TPMS ECU, the driver will be forced to visit a garage.

Scenario 4 : ***Attack via TPMS***

Don't know how to stop it with MTD..

-> enable authentification on packet sent.